N° Ordre :...../FMI/UB2/2023

RÉPUBLIQUE ALGÉRIENNE DÉMOCRATIQUE ET POPULAIRE
MINISTÈRE DE L'ENSEIGNEMENT SUPERIEUR ET DE LA RECHERCHE SCIENTIFIQUE
UNIVERSITÉ DE BATNA-2

FACULTÉ DES MATHÉMATIQUES ET D'INFORMATIQUE
DÉPARTEMENT DES MATHÉMATIQUES

THÈSE

Présentée par

ADOUI Salah

Pour obtenir le titre de

Docteur en Sciences

de l'université de Mustafa Ben boulaid-Batna 2

Spécialité : **MATHÉMATIQUES**

CONTRIBUTION À LA CRYPTOGRAPHIE ET SÉCURITÉ QUANTIQUE

Soutenue le : **... / ... /2023**, devant le jury composé de :

(Mme)	MENKAD Safa	**MCA**	Université de Batna 2	**Présidente**
(Mr)	NOUI Lemnouar	**Professeur**	Université de Batna 2	**Rapporteur**
(Mr)	GUEDJIBA Said	**Professeur**	Université de Batna 2	**Examinateur**
(Mr)	ZEDAM Lemnaouar	**Professeur**	Université de M'sila	**Examinateur**
(Mr)	BARKAT Omar	**MCA**	CU de Barika	**Examinateur**
(Mme)	CHATOUH Karima	**MCA**	Université de Batna 1	**Examinatrice**

Année universitaire 2022 /2023.

CONTRIBUTION À LA CRYPTOGRAPHIE ET SÉCURITÉ QUANTIQUE

≡

CONTRIBUTION TO CRYPTOGRAPHY AND QUANTUM SECURITY

ADOUI Salah

November 16, 2023

ACKNOWLEDGMENTS:

The realization of a thesis is not the result of the work of a single man, but of his interaction with all those gravitating around him to help him theoretically, technically and humanly. So I want to thank all those who have me of loan or of distance to give their support: We thank first and foremost the Almighty ALLAH which led me to complete this work. I would like to thank *Mr NOUI Lemnouar* professor at the University of Batna 2 who accepted with good heart and benevolence, to lead my work, and to follow me patiently through all stages of this study. I am grateful to him for his many remarks, his kindness and patience. My thanks also go to *Mme MENKAD Safa* professor at the University of Batna 2 to have agreed to preside over the jury. Likewise, I thank Mr *GUEDJIBA Said* professor at the University Batna-2, Mr *ZEDAM Lemnaouar* professor at the University of M'sila, *Mr BARKAT Omar* professor at University Centre of Barika, and *Mme CHATOUH Karima* Assistant professor at the University of Batna-1; to have agreed to review and judge this work. Thanks to the head of department and all the entire team of department of Mathematics at the University of Batna 2. I also thank my colleges and brothers in the office 16 of the department of mathematics *BENZEGHLI Brahim*, *SERRAR Mohamed eddine* and *BENHADID Ayache*. Finally, thank you to everyone I forgot to thank. And I dedicate this modest work to the spirit of my father *KHELIFA*, to my dear mother *FATMA*, to my beautiful little family: my wife and my children: *karim*, *mohcen*; *Mohamed*, *Razane* and *Ishak*, without forgetting *Amani*, *Meriem* and *Mahmoud Khalil*, and my sisters, brothers and all my loved ones.

Contents

Abstract

Cryptography pushes the development of cryptosystems in different fields. However, safety remains an unresolved issue. In this thesis, we have worked to improve the security of one of the well-known *Diffie-Hellman's key exchange protocol*. We know that encryption systems are divided into: symmetrical and antisymmetrical types. For the first one, it uses the same keys for encryption and decryption our data, but the problem is how to transport and exchange this common key in a secure way and to prevent any hacking. As a result, we have exploited some of the most important property of *circulant matrices*, namely that the multiplication of this type of matrices is commutative, and it is easy to store this kind of matrices. And, using a quantum channel, we can exchange parameters that help us to create a logistic sequence, whith a high sensitivity to the initial conditions, this allows us to create a highly secure shared key, finally an application in image encryption is given.

Key words: Cryptography, security, quantum cryptography, chaos, circulant matrices, Diffie-Hellman protocols, digital images.

Résumé

La cryptographie a permis le développement des cryptosystémes dans des différents domaines. Toutefois, la sécurité demeure un enjeu non résolu. Dans cette thése, nous avons travailler a amélioré la sécurité de l'un des systèmes bien connus qui est *le protocole d'échange de clés de Diffie et Hellman.* Nous savons que les systèmes de cryptage sont divisés en deux types: symétrique et antisymétrique. Le premier utilise la même clé pour crypter et décrypter les donnés, mais le probléme posé est toujours sur la façon de transporter et échanger la clé commune de manière sécurisée et d'empêcher tout piratage de cette clé et ainsi assurer la confidentialité des informations échangées. En conséquence, nous avons exploité certaines des caractéristiques les plus importantes des matrices circulantes, à savoir que la multiplication de ce type de matrices est commutative, d'autre part il est facile de stocker ce type de matrices. Ensuite, grâce à un canal quantique, nous pouvons échanger des paramètres qui nous aident à créer une suite logistique, dont les caractéristiques les plus importantes ont une sensibilité élevée pour les conditions initiales, ce qui nous permet de créer une clé secrète et commune très sécurisée que nous allons l'utilisée pour chiffrer les images numériques.

Mots-clés: Cryptographie, sécurité, cryptographie quantique, chaos, matrices circulantes, protocole Diffie-Hellman, images numériques.

ملخص

مكّن علم التشفير من تطوير أنظمة التشفير في العديد من المجالات المختلفة، ومع ذلك، لا يزال الأمن مشكلة مفتوحة. في هذه الرسالة قمنا بتحسين و رفع مستوى الأمن لأحد أنظمة تبادل المفاتيح المعروفة، فكما نعلم أن أنظمة التشفير تنقسم إلى قسمين رئيسيين الأول تناظري و الآخر ضد تناظري. بالنسبة للأول فهو يستعمل نفس المفتاح لتشفير و إعادة إسترجاع المعلومة و الاشكال المطروح دائما هو كيفية تبادل هذا المفتاح بطريقة مضمومة و منع أي اختراق لقرصنة هذا المفتاح و بالتالي ضمان سرية المعلومات المتبادلة. فعملا على هذا قمنا باستغلال بعض أهم خصائص المصفوقات الدورية والمتمثلة في كون أن عملية ضرب هذا النوع من المصفوفات هو تبديلي، ثم عبر قناة كوانتية يمكننا تبادل وسائط تساعدنا في انشاء متتالية لوجيستيكية و التي من اهم خصائصها الحساسية العالية اتجاه الشروط الابتدائية كل هذا مكننا لإنشاء مفتاح مشترك آمن جدا و الذي اتسعملناه في تشفير الصور الرقمية.

الكلمات المفتاحية: التشفير ، الأمن ، التشفير الكمومي ، الفوضى ،المصفوفات المتداولة ، بروتوكولات تبادل المفاتيح و الصور الرقمية.

List of Figures

List of Tables

Terminology and Vocabulary

- ☞ $\mathbb{K}$: Field(= $\mathbb{R}$ or $\mathbb{C}$).
- ☞ $\mathbb{F}_q$: finite field of q elements.
- ☞ $\mathcal{L}(E,F)$: All E Linear applications in F(E,F are vector spaces).
- ☞ $\mathcal{M}_n(\mathbb{K})$: all square matrices of order n.
- ☞ $\mathbb{H}$: The complex Hilbert space.
- ☞ $\langle|\rangle$: is a hermitic scalar product.
- ☞ **Encryption** : Transform a clear message into an encrypted message.
- ☞ **Decryption** : A reverse transformation of encryption that allows find from an encrypted message, the corresponding clear message.
- ☞ **Protocol :** Description of all the data necessary for Setting up the cryptography mechanism: all messages clear, encrypted messages, possible keys, transformations...
- ☞ **Encrypt:** Using an algorithm, transcribe a clear message into one incomprehensible sequence of symbols.
- ☞ **Plain text**: the message to encrypt.
- ☞ **Ciphertext:** the result of encryption.
- ☞ **Decipher:** find plaintext from ciphertext using a Parameterized algorithm.
- ☞ **Key:** the setting of the encryption and decryption algorithms.
- ☞ **Decrypt:** Find plaintext from ciphertext without the key.
- ☞ **Cryptography:** Science of Encryption.
- ☞ **Cryptanalysis:** Science of decryption without the key.
- ☞ **Cryptology:** cryptography and Cryptanalysis .
- ☞ **Cryptosystem:** all encryption and decryption methods that can be used securely.

General introduction

Nowadays, more and more people put personal information on the Internet, especially on social networks, on sales sites, ... To prevent this information from being used at our expense and being disclosed to dishonest individuals, cryptologists encrypt this information to keep it secret, that is, they ensure that messages and passwords clearly written on websites become coded information for users other than the author and recipients of the message. To get there, they use different methods.

The Cryptology science is responsible for protecting sensitive information as well as personal information relating to the privacy of each individual, thus making it possible to combat digital fraud and cyber-terrorism.

Cryptography is one of the disciplines of cryptology that seeks to protect ower informations (confidentiality, authenticity and integrity) by often using secret keys. It is different from steganography, which makes a message go unnoticed in another message, whereas cryptography makes a message supposedly unintelligible to someone else-of-right.

It has been used since antiquity, but some of its most modern methods, such as asymmetric cryptography, date from the late 20^{th} century. [24]

First, it will develop sophisticated algorithms to encrypt messages, authenticate authors as well as recipients and ensure the integrity of information sent or written on a site. Then, in a second step, it will perform the work of a cryptanalyst, that is to say, it will try to decipher encrypted messages by its own algorithms or by algorithms of colleagues to test the effectiveness of its programs in order to keep a margin of advance against hackers.

Cryptography will develop increasingly complex algorithms to fight the automated attacks of hackers they carry out with increasingly high-performance machines. For example, with all the advances in cryptology, the experts in this field have discovered public key cryptology which allows to solve the problems of exchange of keys which had to be carried out by a secure means because it was thanks to this key that the recipient and the author could make the coded message readable. The cryptology in which this key exchange is found is called private key cryptology. In this case, it is necessary that the author and the recipient have the same encrypting/decrypting key, hence the need to share it through a secure way. For public key cryptology one key is used for encryption, and a different key in decryption. Only the receive key can decipher the message.

PLAN OF THE THESIS

This thesis is composed of five chapters:

- The first chapter will be a reminder about the fundamental concepts in algebra, from the notion of groups, fields, linear application, presentation of matrices, and in particular the toeplitz matrices, as well as Circulant matrices and some of their properties that help us in the practical part (chapter 5), elliptic curves, ... These concepts are important for building algorithms and techniques in different systems.

- In second chapter, we present the fundamental concepts and terminology of cryptography, their objectives and these different types (classic and modern) as well as presents in detail some ciphers (Cézar, Hill, Diffie-Hellman, ...), and there crypanalysis.

- The third chapter is devoted to quantum cryptography and chaos theory: quantum cryptography is not an encryption algorithm, it simply makes it possible to implement a classic, even ancient, cryptographic algorithm, which is the only one that has been proven flawless **the "disposable mask"**. This algorithm, although perfectly safe, is rarely used because it requires a key exchange of as great length as the message to transmit. This key exchange poses security problems as important as the transmission of the message itself, which limits the field of applicability of this algorithm.

  However, quantum cryptography allows two interlocutors to exchange a key securely; indeed, this method not only allows to unmask any attempt to spy thanks to the properties of quantum mechanics, but also to reduce the amount of information held by a possible spy to an arbitrarily low level, thanks to traditional algorithms ("privacy amplification"). Quantum cryptography is therefore a valuable tool for symmetric cryptography systems where both interlocutors must have the same key and this in complete confidentiality.

  And we use quantum systems to share a key, not the message it self for two reasons:

  1. Bits of information exchanged by quantum cryptography cannot be chosen at random. It doesn't fit the message, but perfectly suitable for keys , in the case of the "disposable mask" can be random.
  2. Even if the quantum mechanism detects that there is spying, so we will lose the key instead of risking the message, and can renew a new key.

  Foundations of quantum cryptography were established, among others, by the work of Charles H. Bennett and Gilles Brassard in 1984. The first ideas were put forward by Stephen Wiesner in the 1960*'s*, but surprisingly, their publication had been rejected.

  Then there are several systems with this behaviour, they are called chaotic, they are governed by deterministic laws, they depend on one or more parameters and their evolution over time is unpredictable. The study of such systems is linked to the theory of chaos which experienced a great boom from 1960 through the results of many researchers such as Lorenz and the discovery of new computer tools. [10, 12].

Chaotic transmission is a mode of communication with a secret key. Knowledge of this key is necessary on the sender side of the message as well as a receiver to encrypt and decrypt the message. At the receiver level, a chaotic signal identical to the carrier must be available to recover the masked message.

- In cahpter 4 , we knew that in a symetric encryption system, both intelctors share the same key for encryption and decryption, however, the asymmetric system uses a public key to encrypt and another different private key to decrypt the message.

  Symmetrical systems are simple and faster, but their main drawback is that both sides must remain secure. The public key systems solve this problem, as the public key is distributed in unsecured channels, and the secret decryption key will never shared.

  So, we work in this chapter for sharing keys with deferent famous protocols as Deffie-Helman exchange protocol using deferent groups, $BB84$ quantum exchange protocol, ... [8].

- The fifth and final chapter describes our idea, we have proposed a new system to share a common key, which is used to encrypt and decrypt ower data.

  Two methods for creating common keys are proposed [8] :

  - The first one is a square matrix of ordre n generate by two methods:
    - generate by a chaotic logistic map [12] after we share two parameters through a quantum channal that uses a quantium exchange protocol its $BB84$.
      The logistics map of one dimensional has interest proprieties, such as: periodicity and sensitivy of the initial values, but it has a weak securty. And to achieve the level of security we can use several logistic maps to generate the key in the first step.
    - generate by the points components of an eliptic curve after having shared five parameters through a quantum channal that uses a quantium exchange protocol its $BB84$.
  - The second key is also a matrix obtained by using the first key and with the good property concerning the commutativity of the multiplication of circulant matrices and by using the protocol of key exchange called of Diffie-Hellman. This last key will be used for encryption znd decryption of data with defferent formila.

- Finally, we we finish our thesis with a general conclusion.

Chapter 1

Fundamental concept of Algebra

This chapter determine the fundamental concepts used in algebra,[32, 5, 6] from the notion of groups, fields, matrices, Circulant matrices [35], linear application, Elliptic curves,...

1.1 Algebraic structures

1.1.1 Group structure

Definition 1.1

Lets's $*$ be a law of internal composition defined on a set G, it is said that couple $(G,*)$ is a group if and only if:

1. *The law $*$ is associative: $\forall a,b,c \in E; (a*b)*c = a*(b*c)$*
2. *There is identity element e in $(G,*)$: $\forall a \in E,\ \ e*a = a*e = a$.*
3. *Every element a of G admits an inverse a^{-1}: $a^{-1}*a = a*a^{-1} = e$.*

▲ *And it is said that the group is commutative if the law $*$ is commutative.*

Examples 1.1

1. *$(\mathbb{Z}; +)$,$(\mathbb{R}; +)$ are commutative groups.*
2. *$(\mathbb{Q}_+^*;.)$, and $(\mathbb{R}_+^*;.)$ are commutative groups.*

Definition 1.2

Let $(G;*)$ be a group. A none-empty part H of G is a sub group of G if:

$$(x;y) \in H \times H \Rightarrow x*y \in H.....(1)$$

$$x \in H \Rightarrow x' \in H.....(2)$$

1.1.2 Homomorphism

Definition 1.3

Let (G_1;$*$) and (G_2;$\perp$) be two groups. An homomorphism of (G_1;$*$) in (G_2;$\perp$) is an application $f : G_1 \to G_2$ such that:

$$\forall (x, y) \in G_1^2, f(x * y) = f(x) \perp f(y)$$

Example 1.1

The application:

$$\begin{aligned} f : \mathbb{R} &\to \mathbb{R} \\ x &\mapsto f(x) = 2^x \end{aligned}$$

is a homomorphism of ($\mathbb{R}$; +) in ($\mathbb{R}$; .) since:

$$\forall (x, y) \in \mathbb{R}^2 : f(x + y) = 2^{(x+y)} = 2^x \times 2^y = f(x) \times f(y).$$

1.1.3 Ring and Field structures

Ring structure [36]

Definition 1.4

Let A be a set equiped with two operations: $+, \cdot : G \times G \to G$. A is a ring if:

1. *The set $(A, +)$ is a commutative group.*
2. *The Law $\cdot$ is associative.*
3. *The Law $\cdot$ is distributive over to the law $+$.*

Remarks

- If the Law $\cdot$ is commutative then the ring$(A, +, \cdot)$ said to be commutative.
- If A admits an identity element for the law $\cdot$ it is said unitary ring.

Example 1.2

$(\mathbb{Z}, +, \cdot)$ *commute, and it is an unitary ring.*

Field structure

Definition 1.5

Let $(\mathbb{K}, +, \cdot)$ is an unitary ring. A is a field if any none-zero element of $\mathbb{K}$ admits an inverse for the second law $\cdot$.

In other words ($\mathbb{K} \setminus \{0\}, T$) is a group.

▲ *Moreover, if the second law is commutative, $\mathbb{K}$ is a commutative field.*

1.1.4 Vector spaces and linear Applications

Vector spaces

Definition 1.6

Let E be a non empty set and $\mathbb{K}$ is a field. We assume that E is equiped with two operations: $+ : E \times E \to E$, $\cdot : \mathbb{K} \times E \to E$, E is $\mathbb{K}$–vectoriel space if:

- $(E, +)$ *is an abelian group.*
- $\forall \lambda, \mu \in \mathbb{K}$, $\forall x \in E$: $\lambda \times (\mu \times x) = (\lambda \times \mu) \times x$.
- $\forall \lambda, \mu \in \mathbb{R}$, $\forall x \in E$: $(\lambda + \mu) \times x = \lambda \times x + \mu \times x$.
- $\forall \lambda \in \mathbb{R}$, $\forall x, y \in E$: $\lambda \times (x + y) = \lambda \times x + \lambda \times y$.
- $\forall x \in E$: $1 \times x = x$.

Examples 1.2

$\mathbb{R}^2$ *and* $\mathbb{R}^3$ *are vector-spaces over the field* $\mathbb{R}$.

Vector subspaces

Definition 1.7

Let E be a $\mathbb{K}$–vector-space, and let F be a none-empty subset of E.

F is a vector-subspace of E if F is itself a $\mathbb{K}$––space for the addition and product laws defined on E.

Proposition 1.1

Let E be a vector-space, and let F be a subset of E. F is said a vector-subspace of E if:

1. *F is not empty: $F \neq \emptyset$.*
2. $\forall (x, y) \in F \times F$, $x + y \in F$.
3. $\forall x \in F, \forall \lambda \in \mathbb{K}$, $\lambda x \in F$.

Corollary 1.1

Let E be a $\mathbb{K}$-vector-space, and F a subset of E. If F checks the following properties (i) and (ii) then F is a vector subspace of E:

(i) F is not empty
(ii) $\forall (x, y) \in F \times F, \forall (\lambda, \mu) \in \mathbb{K}^2$, $\lambda x + \mu y \in F$.

Example 1.3

Let $E = \mathbb{R}^3$ be a $\mathbb{K}$-vector-space.

The set $F = \{(x, y, z) \in \mathbb{R}^3 / z = 0\}$ is a vector-subspace of $\mathbb{R}^3$.

Linear Applications

Definition 1.8

Let E,F be two vector-spaces on a field $\mathbb{K}$.

then, let let f *be an application of the set E in F* ($f : E \longrightarrow F$).
f *is said to be linear if it checks:*

- $\forall x, y \in E, f(x+y) = f(x) + f(y)$
- $\forall x \in E, \forall \lambda \in \mathbb{K} : f(\lambda x) = \lambda f(x)$

Notation.

We note to the set of all linear applications from the $\mathbb{K}$-vectorial space E to the $\mathbb{K}$-vectorial space F with: $\mathcal{L}(E,F)$.

1.2 Matrices

Definition 1.9 *[37]*

Let $f \in \mathcal{L}(E,F)$ *be a linear application. E, F of finite dimension n,p (respectively), and let's the two bases respectively of E, F:* $B_E = \{u_1, u_2, \ldots, u_n\}$ *and,* $B_F = \{v_1, v_2, \ldots, v_p\}$.

We call Matrix of f *in the bases* B_E *and* B_F *the table of "n" columns and "p" rows, given as follows:*

$$\mathcal{A} = \begin{bmatrix} a_{11} & a_{12} & \cdots & \cdots & a_{1n} \\ a_{21} & a_{22} & \cdots & \cdots & a_{2n} \\ \vdots & & & & \\ a_{p1} & a_{p2} & \cdots & \cdots & a_{pn} \end{bmatrix}, with \begin{cases} f(u_1) = v_1 a_{11} + v_2 a_{21} + \ldots + v_p a_{p1} \\ f(u_2) = v_1 a_{12} + v_2 a_{22} + \ldots + v_p a_{p2} \\ \vdots \\ \vdots \\ f(u_n) = v_1 a_{1n} + v_2 a_{2n} + \ldots + v_p a_{pn} \end{cases}$$

Example 1.4

for n=3, and p=2:

$$\begin{cases} f(u_1) = 1v_1 + 2v_2 \\ f(u_2) = -3v_1 + v_2 \\ f(u_3) = 1v_1 + 4v_2 \end{cases} \Longrightarrow \mathcal{M}_{23} = \begin{bmatrix} 1 & -3 & 1 \\ 2 & 1 & 4 \end{bmatrix}$$

Note 1.1

Let $A=(a_{ij})_{1 \leqslant i \leqslant n, 1 \leqslant j \leqslant p} \in \mathcal{M}_{p,n}(\mathbb{K})$:

- *A is the identity matrix :* $\forall i, \forall j$ *, if* $i = j$: $a_{ij} = 1$ *; if not:* $a_{ij} = 0$.

- *A is a null matrix* $\Leftrightarrow\ a_{ij} = 0_{\mathbb{K}}, \forall i = 1,...,n, \forall j = 1,...,p$
- *The opposite of A is:* $(-A) = (-\ a_{ij})_{1\leqslant i\leqslant n, 1\leqslant j\leqslant p}$
- *A is a diagonal matrix if:* $\forall 1 \leqslant i \leqslant n, 1 \leqslant j \leqslant p$, $\forall i \neq j$: $a_{ij} = 0$.
- *A is triangular superior matrix if:* $\forall i, \forall j\ i > j :\ a_{ij} = 0$
- *A is triangular lower matrix if:* $\forall i, \forall j$, *for* $i < j$: $a_{ij} = 0$

Notation

- We note by $\mathbf{M_{p,n}}(\mathbb{K})$ by the array set of n columns and p rows.
- If $dimE = dimF = n$, $\mathbf{M_{p,n}}(\mathbf{K}) = \mathbf{M_n}(\mathbf{K})$ represent the set of square matrices of order n.

1.2.1 Transpose, the sum and multiplication of matrices

In this subsection, all vector-spaces are of finite-dimension over the same field $\mathbb{K}$.

Transpose of a matrix

The transpose of A= (a_{ij}) is A^t = (c_{ij}) with, c_{ij}= $a_{ji}, \forall i = 1...p, \forall j = 1...n$.

Properties 1.1

1. *If:* $A = A^t$, *we said A is a symmetric matrix.*
2. *If:* $A = -A^t$, *we said A is a antisymmetric matrix.*
   And we have:
3. $(A + B)^t = A^t + B^t$.
4. $(\lambda A)^t = \lambda\ A^t$.
5. $(AB)^t = B^t\ A^t$

The sum of matrices

For even $A, B \in \mathcal{M}n, p(\mathbb{K})$.

The addition of A with B, is the matrix of the same type (n, p) noted:

$$A + B = (a_{ij} + b_{ij}).\forall i = 1...p, \forall j = 1...n.$$

The multiplication of matrices

Let $A \in \mathcal{M}_{n,p}(K)$, and let $B \in \mathcal{M}p,q(K)$, the multiplication of the two matrices A, B is defined by:

$$A \times B = C = (c_{ij}), \text{ with } \; c_{ij} = \sum_{k=1}^{p} a_{ik} b_{kj} \; \forall i = 1..n, j = 1..q$$

Note 1.2

Generaly, the product of two matrices don't commute $A \times B \neq B \times A$.

1.3 Toeplitz matrix definitions and properties

Toeplitz matrices are defined by the German mathematician *Otto Toeplitz (1881-1940)*.

In case T is square we have :

Definition 1.10

The matrix $[T]_{ij} = [t_{(i-j)}, i, j = 1, ..., n]$ *is a Toeplitz matrix, if it has the form:*

$$T_n = \begin{pmatrix} t_0 & t_{-1} & \cdots & \cdots & t_{-(n-2)} & t_{-(n-1)} \\ t_1 & t_0 & \cdots & \cdots & \cdots & t_{-(n-2)} \\ \vdots & \vdots & \ddots & & \vdots & \vdots \\ t_{(n-2)} & \cdots & \cdots & & t_0 & t_{-1} \\ t_{(n-1)} & t_{(n-2)} & \cdots & \cdots & t_1 & t_0 \end{pmatrix}$$

Example 1.5

For $n = 3$, *we have* $T_3 = [t_{i-j}, i, j = 1, 2, 3]$, *then the matrix* T_3 *defined in the form :*

$$T_3 = \begin{pmatrix} 7 & -1 & 0 \\ -3 & 7 & -1 \\ 2 & -3 & 7 \end{pmatrix} \textit{ is a Toepliz matrix.}$$

1.3.1 Algebraic structure of Toeplitz matrices

Let $\mathbb{K}$ be an abelian field, and $'n'$ a strictly positive integer.

$T_n \in \mathcal{M}_n(\mathbb{K})$ Toeplitz matrix of order n (square matrix $n \times n$, and the T elements are in $\mathbb{K}$)

Proposition 1.2

Let's $T = [t_{i-j}; i, j = 1, ..., n]$ *and* $S = [s_{i-j}; i, j = 1, ..., n]$ *are matrices of Toeplitz in* $\mathcal{M}_n(\mathbb{K})$ *, and be* λ *a scalar , we put :*

$$\begin{cases} T + S = (t_{i-j} + s_{i-j})_{1 \leq i,j \leq n} \\ \lambda T = (\lambda t_{i-j})_{1 \leq i,j \leq n} \end{cases}$$

Provided with these laws, the set of Toeplitz matrices $\mathcal{M}_n(\mathbb{K})$ *is a* $\mathbb{K}$*-vector space.*

Proof.

- The addition of two Toeplitz matrices is obviously a Toeplitz matrix .
- The product of a Toeplitz matrix by a scalar is obviously a Toeplitz matrix .

Or the set of Toeplitz matrices, $\mathcal{M}_n(\mathbb{K})$ with these two laws is a $\mathbb{K}$-vector space.

1.3.2 Determinant of a Toeplitz matrix

The determinant of a Toeplitz matrix T of order n is:

$$\det(T_n) = \sum_{i=1}^{n} (-1)^{i+j} . t_{i-j} . M_{i,j}$$

$M_{i,j}$is the minor of T_n (Obtained by deleting the row i and the column j of T_n). [41, 16]

Example 1.6

For $n = 3$*, the determinant:*

$$\begin{aligned} \det(T_3) &= \begin{vmatrix} t_0 & t_{-1} & t_{-2} \\ t_1 & t_0 & t_{-1} \\ t_2 & t_1 & t_0 \end{vmatrix} \\ &= t_0 \times \begin{vmatrix} t_0 & t_{-1} \\ t_1 & t_0 \end{vmatrix} - t_1 \times \begin{vmatrix} t_{-1} & t_{-2} \\ t_1 & t_0 \end{vmatrix} + t_2 \times \begin{vmatrix} t_{-1} & t_{-2} \\ t_0 & t_1 \end{vmatrix} \\ &= t_0(t_0^2 - t_1 t_{-1}) - t_1(t_{-1} t_0 - t_1 t_{-2}) + t_2(t_{-1} t_1 - t_0 t_{-2}) \end{aligned}$$

by applying to: $T_3 = \begin{bmatrix} 3 & -1 & 2 \\ -4 & 3 & -1 \\ 5 & -4 & 3 \end{bmatrix}$*, we obtain:*

$$\begin{aligned} \det(T_3) &= 3[3^2 - (-4) \times (-1)] - (-4)[(-1) \times 3 - (-4) \times 2] + 5[(-1) \times (-1) - (3 \times 2)] \\ &= 15 + 20 - 25 \\ &= 10 \end{aligned}$$

1.4 Algebraic operations on Toeplitz matrices:

1- Addition

Proposition 1.3

The addition of two Toeplitz matrices gives a Toeplitz matrix [33, 16].

2- Multiplication by a scalar

Theorem 1.2

The multiplication of a Toeplitz matrix by a scalar is a Toeplitz-matrix [47, 48].

3- Multiplication of two Toeplitz matrices

Theorem 1.3

The product of two Toeplitz matrix is not always a Toeplitz matrix [47, 48].

Example 1.7

Let, $T_3 = \begin{bmatrix} -1 & 4 & 5 \\ 3 & -1 & 4 \\ 2 & 3 & -1 \end{bmatrix}$ *and,* $R_3 = \begin{bmatrix} 3 & 0 & -7 \\ -1 & 3 & 0 \\ 2 & -1 & 3 \end{bmatrix}$ *be two Toeplitz matrix.*

$$\text{We have: } T_3 \times R_3 = \begin{bmatrix} -1 & 4 & 5 \\ 3 & -1 & 4 \\ 2 & 3 & -1 \end{bmatrix} \times \begin{bmatrix} 3 & 0 & -7 \\ -1 & 3 & 0 \\ 2 & -1 & 3 \end{bmatrix}$$

$$= \begin{bmatrix} 3 & 7 & 8 \\ 18 & -7 & -9 \\ 1 & 10 & -17 \end{bmatrix}$$

So, the product is not a toeplitz matrix .

1.4.1 Inverse of a Toeplitz matrix:

Theorem 1.4

Let T_n *be an invertible Toepliz matrix.*

The inverse of a Toeplitz matrix is not generally a Toeplitz matrix [47, 48].

Example 1.8

$T_3 = \begin{bmatrix} 3 & -1 & 2 \\ -4 & 3 & -1 \\ 5 & -4 & 3 \end{bmatrix}$, *the inverse is:*

$T_3^{-1} = \frac{1}{10} \begin{bmatrix} 5 & -5 & -5 \\ 7 & -1 & -5 \\ 1 & 7 & 5 \end{bmatrix}$, *show that, the inverse is not a toeplitz matrix.*

1.5 Circulant matrices

A circulant matrix is a particular case of a Toeplitz matrix, a Frobenius matrix (it is the generic matrix of multiplication by an element of group algebra $\mathbb{C}[\mathbb{Z}/n\mathbb{Z}]$ and also a particular case of Latin square.

The reduction of circulant matrices involves the formulas of discrete Fourier transformation. In numerical analysis, circulant systems can be solved very efficiently by fast Fourier transform.

Assum that $\mathbb{K}$ is a field.

1.5.1 Definitions

A circulant matrix A is an element of the set $\mathcal{M}_n(\mathbb{K})$ generated by the vector $V(a_1 a_2 \cdots a_n)$, where $a_1 a_2 \cdots a_n$ in this order are the elements of its first line, and the i^{th} line $(2 \leq i \leq n)$, is the target of V by the translation wich translate elements of V by $(i-1)$ times as fellowing :

$$A = \begin{pmatrix} a_1 & a_2 & \cdots & a_n \\ a_n & a_1 & \cdots & a_{n-1} \\ \vdots & \vdots & \ddots & \vdots \\ a_2 & a_3 & \cdots & a_1 \end{pmatrix} \tag{1.1}$$

And, we can write it:

$$A = \langle V \rangle = \langle a_1, a_2, \cdots, a_n \rangle = C(a_1, a_2, \cdots, a_n)$$

1.5.2 Determinant of circulant matrix

Theorem 1.5

Let $A = \begin{pmatrix} a_1 & a_2 & \cdots & a_n \\ a_n & a_1 & \cdots & a_{n-1} \\ \vdots & \vdots & \ddots & \vdots \\ a_2 & a_3 & \cdots & a_1 \end{pmatrix}$ *be matrix of order of complex element n.*
Thr circulant matrix has the determinant given by :

$$det(A) = \prod_{j=1}^{n} (a_1 + a_2 \zeta^j + a_3 \zeta^{2j} + ... + a_n \zeta^{nj})$$

Where $\zeta = e^{\frac{2\pi i}{n}}$ *is a primitive* n^{th} *roots of the unity. [25, 33, 34, 7]*

1.5.3 Properties of circulant matrices

We give here some important proprieties of circulant matrices, so we cite the following propositions:

Proposition 1.4

Let A, B *be two circulant matrices of* $\mathcal{M}_n(\mathbb{C})$*, then we have:*

The product of circulant matrices is commutative: $A \times B = B \times A$.

We can see the proof of the proposition in [25, 33, 34, 7].

Proposition 1.5

The product of two circulant matrices gives a circulant matrix also.

We can see the proof of the proposition in [25, 33, 34, 7].

Example 1.9

Let $A = \begin{bmatrix} 3 & -1 & 2 \\ 2 & 3 & -1 \\ -1 & 2 & 3 \end{bmatrix}$, *and* $B = \begin{bmatrix} 1 & 5 & 7 \\ 7 & 1 & 5 \\ 5 & 7 & 1 \end{bmatrix}$ *be two circulant matrices.*

So, $A \times B = B \times A$

$$= \begin{bmatrix} 3 & -1 & 2 \\ 2 & 3 & -1 \\ -1 & 2 & 3 \end{bmatrix} \times \begin{bmatrix} 1 & 5 & 7 \\ 7 & 1 & 5 \\ 5 & 7 & 1 \end{bmatrix}$$

$$= \begin{bmatrix} 1 & 5 & 7 \\ 7 & 1 & 5 \\ 5 & 7 & 1 \end{bmatrix} \times \begin{bmatrix} 3 & -1 & 2 \\ 2 & 3 & -1 \\ -1 & 2 & 3 \end{bmatrix}$$

$$= \begin{bmatrix} 6 & 28 & 18 \\ 18 & 6 & 28 \\ 28 & 18 & 6 \end{bmatrix}$$

Proposition 1.6

Let A be an invertible circulant matrix, then we have:
A^{-1} *is also a circulant matrix.*

We can see the proof of the proposition in [2, 22, 25, 33].

Example 1.10

Let $A = \begin{bmatrix} 3 & -1 & 2 \\ 2 & 3 & -1 \\ -1 & 2 & 3 \end{bmatrix}$ *be a circulant matrix,*

$det(A) = 52$, *so A is invertible then:*

$A^{-1} = \frac{1}{52} \begin{bmatrix} 11 & 7 & -5 \\ -5 & 11 & 7 \\ 7 & -5 & 11 \end{bmatrix}$, A^{-1} *is also a circulant matrix.*

1.6 Eliptic curve

In mathematics, an eliptic curve is a particular case of algebraic curve.

1.6.1 Definitions and properties

Definition 1.11

An eliptic curve E defined on $\mathbb{K}$*-field is a smooth curve given by a Weierstrass equation:*

$$E : y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6 \tag{1.2}$$

Coefficients a_1, a_2, a_3, a_4 *and* a_6 *are in* $\mathbb{K}$ *field.*

In the case of cryptography, the previous equation can be simplified by changing the variable and an equation of the form is most often used:

$$E : y^2 = x^3 + ax + b \tag{1.3}$$

where coefficients a, b are real numbers. Depending on the choice of these coefficients, the corresponding graphs have essentially two possible forms.

The discriminant of the curve

The quantity $\Delta = -16(4a^3 + 27b^2) \neq 0$ is called the discriminant of the curve: a discriminant other than zero indicates a curve without singularities (or even non-specific curve). The factor –16 may seem unnecessary at this stage but it is involved in the more advanced study of eliptic curves.

Example 1.11

Let two examples of eliptic curves,

$$E1 : y^2 = x^3 - x \;\; with \;\; \triangle > 0 \qquad E2 : y^2 = x^3 - x + 1 \;\; with \;\; \triangle < 0 \tag{1.4}$$

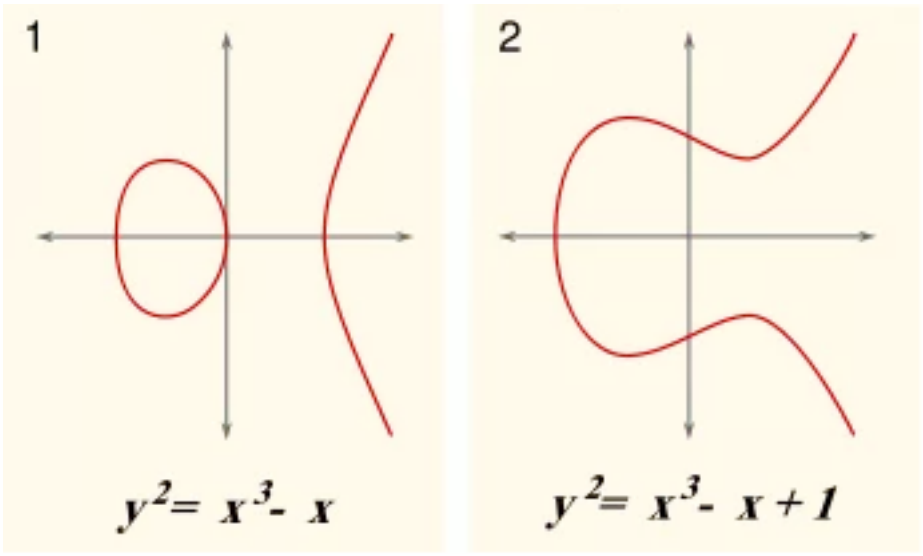


Figure 1.1: Examples of eliptic Curves

- *If the discriminant is positive, it has two components (as in the right image). This case corresponds to the fact that the cubic polynomial $x^3 + ax + b$ has exactly three distinct real roots; these roots are the abscisses of the three points of the eliptic curve on the $x-axis$.*
- *If the discriminant is negative, it has a single component (as in the left image). This case corresponds to the fact that the cubic polynomial $x^3 + ax + b$ has exactly one real root; this root is the abscissa of the eliptic curve point on the $x-axis$.*

Note 1.3

The equation curve: $y^2 = x^3$ has as a discriminant 0: it has a crossover point at the origin and is therefore not an eliptic curve.

More generally, the cubic polynomial: $x^3 + ax + b$ has a multiple roots if the discriminant Δ ewual zero; in this case, the corresponding curve is not eliptic.

1.6.2 Notion of point to infinity

It is assumed that two parallel lines cut to infinity...

Yes but (do you think in your heart...) is it the infinite «from the front» or the «from behind»? Before formalizing this rigorously, note that it would be very embarrassing if two parallel lines crossed in one point and two parallel lines crossed in two...

Therefore start to get used to the idea that there is only one infinite which is both «front» and «behind» (the top, and bottom of the y axis in the case of our eliptic curves).

Moreover, do you find that the notion «from below» and «from above» still has a lot of meaning when working in a finite field?

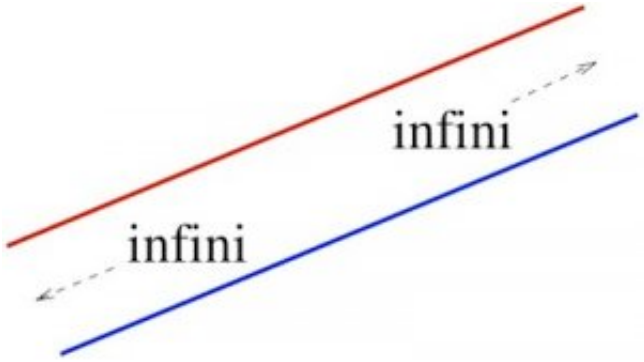


Figure 1.2: Illustration of notion of point to infinity

Notation

Eliptic curve $E(\mathbb{K})$, noted $E(\mathbb{Z}/n\mathbb{Z})$, is the set of the points $p = (x, y) \epsilon \mathbb{K}^2$, checking equation $(1, 9)$, plus a point the infinite note p_∞:

$$E(\tfrac{\mathbb{Z}}{n\mathbb{Z}}) = \{(x,y)\epsilon\ (\tfrac{\mathbb{Z}}{n\mathbb{Z}})^2\ ,\ y^2 = x^3 + ax + b\} \cup \{\ p_\infty\ \}$$

The point: p_∞ is called point to infinity.[15, 18]

- p_∞ is suposed the intrsection of all the vertical and paraleled lines.

1.6.3 The group law

Let $E(\mathbb{K})$ be an eliptic curve on a field ($\mathbb{K}$) .
There is a group law noted + on $E(\mathbb{K})$. This law exists in all characteristics, but we only consider the eliptic Curves defined on a field(it's characteristic different to 2 , 3) and given by a Weierstrass equation; the group law is based on the following construction:

Geometrical construction

Let E be an eliptic Curve and (L) a straight line of the plane.if (L) is tangent at one point to curve E or if (L) cuts E at two distinct points, then (L) cuts at a single other point.

Let P, Q be two points of the curve $E(\mathbb{K})$, we call the addition of points P with Q the point R obtained by the following construction schematized in figure 1.2

First you draw the right (PQ). The line (PQ) cuts the eliptic eurve E at the third point, the point $P+Q$ is the symmetric in relation to the $x-axis$ of this third point:

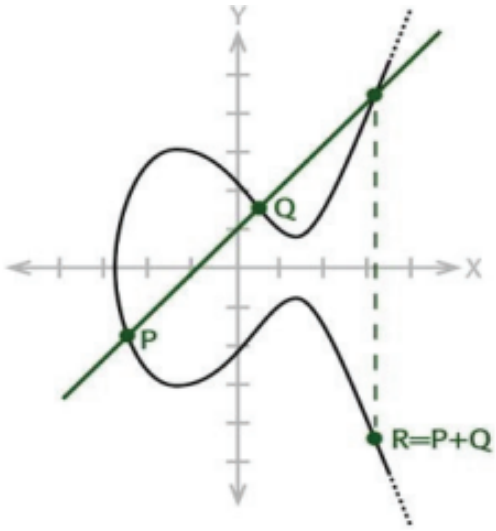


Figure 1.3: Group law on eliptic curves.

Theorem 1.6 *[45]*

All points of an eliptic Curve E provided with the law (+) check the following properties:

1. *The internal law:* $\forall P, Q \in E : P + Q \in E$.
2. *Existence of a identity element :* $\forall P \in E, P + P_\infty = P$.
3. *Commutativity of the law + ;* $\forall P, Q \in E, P + Q = Q + P$.
4. *The associativity of the law +:* $\forall P, Q, R \in E : (P + Q) + R = P + (Q + R)$.
5. *the + law is symmetrical :* $\forall P \in E, \exists -P \in E : P + (-P) = P_\infty$.

1.7 Algebraic aspect of group law

Let E be an equation of an eliptic curve:

$$(E): \quad y^2 = x^3 + ax + b \tag{1.5}$$

$P = (x_p, y_p)$ and, $Q = (x_q, y_q)$ two elements of $E(\mathbb{K})$.

The coordinates of the point $-P$ the inverse of the point P for the + law can be expressed according to the coordinates of the point P .

1.7.1 The Opposite of a point

Let (x_P, y_P) be the none-homogeneous coordinates of a point P of $E(\mathbb{K})$. Then its opposite $Q = -P$ has for coordinates.[15, 18]

$$\begin{cases} x_Q = x_P \\ y_Q = -y_P \end{cases}$$

the opposite of a point is defined by its symmetry for the x-axis. Thus, the opposite of the point (x, y) is the point $(x, -y)$.

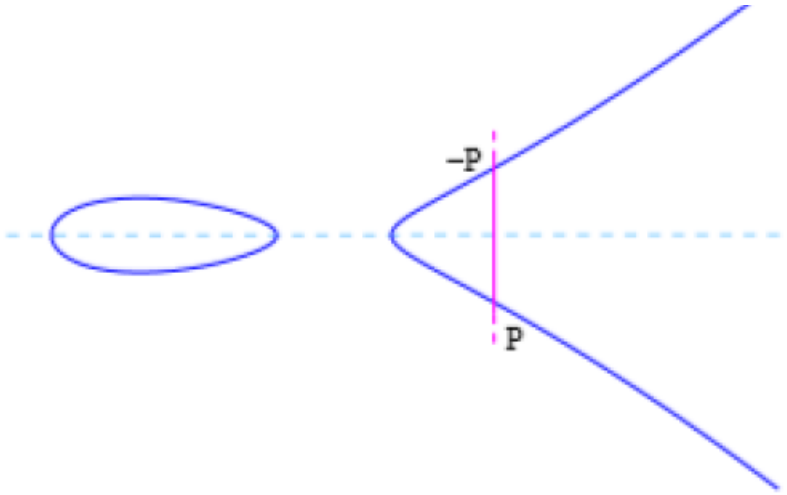


Figure 1.4: opposite of a point in eliptic curves

Proposition 1.7

The opposite of the point P noted −P, admits for coordinates (x_p , -y_p) thus, $P + (-P) = P_\infty$.

1.7.2 Tha addition of points in eliptic curve

Let $P = (x_p , y_p)$, and $Q = (x_q, y_q)$ be two separate points of an eliptic curve E($\mathbb{K}$) such as: P ≠ -Q.

To find the formulas giving the coordinates of the point R = P+Q with R(x_R , y_R) ,we seek to solve the system of two equation formed by the equation of the right (PQ) and the equation of the eliptic curve .

This system accurately reflects the fact that $-(P + Q)$ represent the third point of intersection of the eliptic curve and right (PQ)

We obtained the formulas or λ represents the slope of the line (PQ).

$$\begin{cases} \lambda = \frac{y_p - y_Q}{x_p - x_Q} \\ x_R = \lambda^2 - x_p - x_Q \\ y_R = \lambda(x_p - x_R) - y_p \end{cases} \tag{1.6}$$

1.7.3 Doubling of a point

To find the formulas giving the coordinates of point R=[2]P , we use the fact that - [2]P and the second point of intersection of curve E and tangent E at point P. We get the formulas or λ represents the slope from tangent to point P of the eliptic curve.

$$\begin{cases} \lambda = \frac{3x_p^2+a}{2y_p} \\ x_R = \lambda^2 - 2x_p \\ y_R = \lambda(x_p - x_R) - y_p \end{cases} \tag{1.7}$$

Example 1.12

Let $p = 257$ and $\mathbb{F}_p$ be the associated finite field.

Let $E(\mathbb{F}_p)$ be the eliptic equation Curve: $y^2 = x^3 + 1$.

$P = (8;16)$, and $Q = (19;101)$ are two rational points $\mathbb{F}_p$ of the eliptic curve E.

The coordinates of the points $-P, [2P]$ and $P + Q$ are given by:

$-P = (8;241)$, $[2P] = (20;169)$, and $P + Q = (209;113)$.

Multiplication of a point by integer

Multiplication of a point, rated $Q = k.P$, on an eliptic curve E when $k \in \mathbb{Z}^+$, and $P, Q \in E$.

This operation is called the multiplication by scalar , which is considered the most important transaction on eliptic curves.

That this is a crucial operation in cryptographic protocols based on the previous curves.

The multiplication of points by scalar can be considered as a series of consecutive points additions: $Q = k.P = P + P + ... + P$. ($P$ repeat k times)

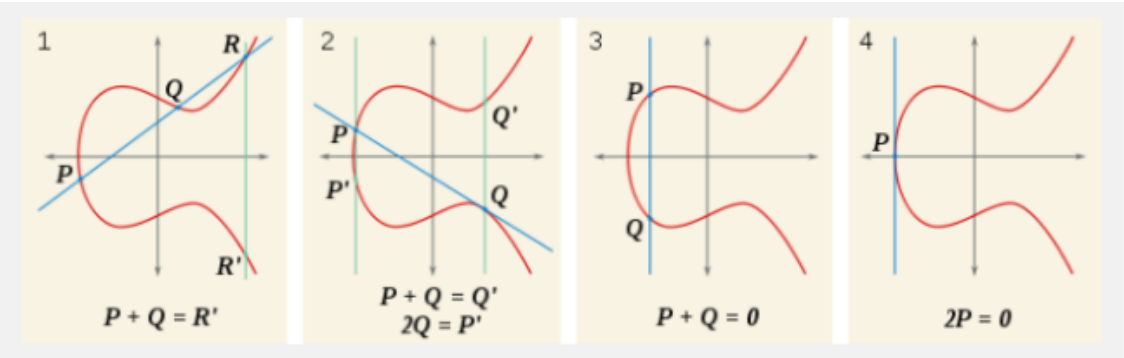


Figure 1.5: Possible additions of two points of an eliptic Curve

Theorem 1.7

The set of the points in real coordinates of the eliptic curve (including the point to infinity), equipped with precedent law of composition, forms a commutative group. [15, 18]

Chapter 2

Cryptology

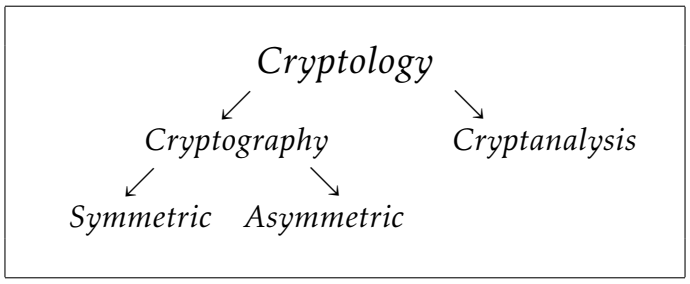
In this chapter, we will do An overview of cryptology such as definition and keywords, cryptanalysis, the purpose of cryptography, some classic algorithms (Caesar's encryption, Hill's cipher...) and tools necessary for the implementation of cryptology mechanisms and systems.

2.1 Cryptology

Definition 2.1

Cryptology is a word composed of two elements: "crypto" which means hidden, and "logos" which means word.

Cryptology is the science of secret messages. Contains ***Cryptography****, The art of making a message unintelligible, and* ***Cryptanalysis*** *art of finding the clear hidden message.*



2.2 Cryptography

Definition 2.2

Cryptography is one of the disciplines of cryptology that seeks to protect messages by often using secrets or keys with the uses of some mathematics technical.

Applications of Cryptography [23]

Cryptography is used in many areas, in the protection of our privacy, such as security in payment portals, secure messaging platforms (social networks). Here are some applications:

Figure 2.1: Applications of Cryptography

1. **SSL/TLS Intrnet encryption:**

   Internet is secure through the cryptography, because you were able for encryption of ower data flow. From browser identification to server authentication, cryptography, in general, have simplified ower navigation online.

2. **Digital Signatures:**

   The world needed a secure channel to transmit essential documents, so digital contracts became important. Cryptography helps provide an authentication layer. So we can be sure of original data, confidentiality then the integrity of ower documents.

3. **Online banking servives:**

   Payment applications and online banking would be considered after the fact, if not secured by data encryption. Cryptography has allowed authentication systems for individuals before allowing them to hold transactions and detect credit card fraud.

4. *Secure chate services:*

   To ensure that no one other than the emitter or the recptteur can read messages in the mail (social network applications, such as: whatsApp, Telegram...) have now adopted an encryption protocol. This is a big step forward from the SMS era, where safety has always been a challenge. Because of cryptography, we have a plethora of communication platforms to use.

5. **Encrypt ower Emails:**

   Through encryption algorithms foexample PGP (PGP= Pretty Good Privacy), ower emails are encrypted all times, because a large amount of secrets infor-

mation going through your inbox, have a secure and absolute communication system.

6. **Crypto-Currency:**

   Cryptocurrency are the most sought after commercial markets, and because of astronomical rise in interest rates thanks to blockchain technology. completely decentralized, secure and tamper-proof systems have found their way into today's digital world because of cryptography.

   So, many different area where cryptography has found its role, and its implementation.

2.3 Components of a cryptosystem

Cryptosystem

Definition 2.3

A cryptosystem is a term used in cryptography to refer to a set contains cryptographic algorithms and all possible incial text, encrypted texts, and encrypted keys.

The components of cryptosystem

The various components of a cryptosystem are:

- **The plain text:** This is the informaion that will be protected during the transmission.
- **The encryption algorithm:** It's the mathematical process to produce encryption for all data in clear and key encryption. It's a cryptographic algorithm that makes the plain text and an encrypted keys to input and to produce encrypted text.
- **Encrypted text:** This is the scrambled party of the plain text crated by the encryption algorithm with a specific encrypted key. Encrypted text is not protected. It circulates on a publical channal. It can be intercepted by anyone with can access to this channal.
- **The decryption algorithm:** This is the mathematical process, which produces a single clear text for every given digit and decrypted keys. It's the mathematics algorithm that makes a number and a decrypted key as an entry, and produces plain text. The decryption algorithm can reverses the encrypted algorithm and is therefore related to it.
- **The encryption keys:** This is a value that the sender must known it. The sender enters the encrypted key with the encrypted algorithm and the plain text to calculate the encrypted data.
- **The decryption keys:** This is a known value by receiver. A decryption keys are somtime lied to the encrypted keys, and it are not always identicals. Receiver enters a decrypted key into the decrypted algorithm with encryption to calculate original text.

2.4 Mechanisms of cryptography

An encryption system or cryptosystem will refer to the description of an encryption/decryption process. It consists in conveying a message that is only understandable by the recipient. For this, he shares a secret with the sender of message. The "clear" message was transmited using an "encryption alghoritm" configured by a "key" into an "encrypted text" coded message and the coded message is transformed using a "decryption function" configured by a "key" into a clear message.

2.4.1 Some basic principles in cryptography

1. **performance:** [8] A secure protocol is better than an effective protocol.
   Forexample: Stopwatch attack on the cards the chip.

2. **simplicity:**[8] A protocol should never try to do more than it is supposed to do.
   Forexample: Extension of identification protocols.

3. **The Weak Link:**[8] A protocol is never as sure as its weakest component.
   Forexample: Lyon University WiFi 1.

4. **Paranoid reasoning :**[8] A protocol with a weakness, too Small as it is, is a protocol that is no longer assur.
   Forexample: The WEP protocol.

5. **security model:** A protocol is never perfect. The key is to achieve the desired level of safety.
   Forexample: WiFi of Lyon University.

2.5 Symmetric and Asymmetric Cryptography

Cryptography divided into two disciplines **Symmetrical** and **Asymmetric cryptography** :

Symmetrical encryption

Symmetrical encryption (Known as secret encryption) uses a same key to encrypt and decrypt messages. The sender and reisiver must share this common key.

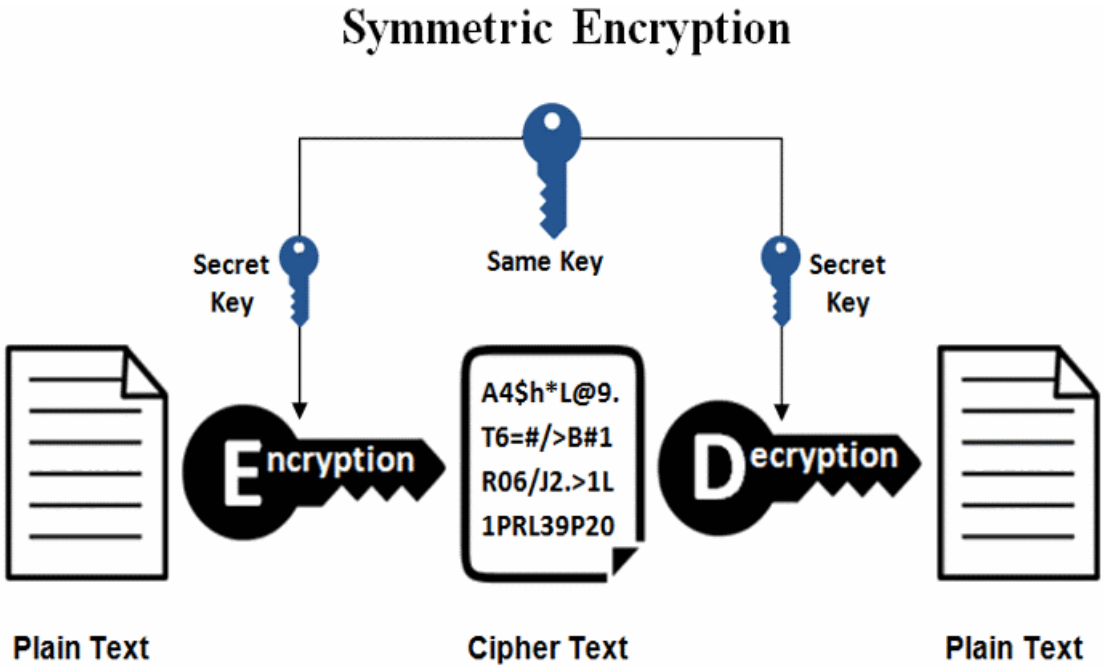


Figure 2.2: Symmetric encryption

Asymmetric encryption

The asymmetric encryption required two diffrent keys to function. First, a public for order to encrypt ower data. Second, a private or secret key using for decrypting of data.

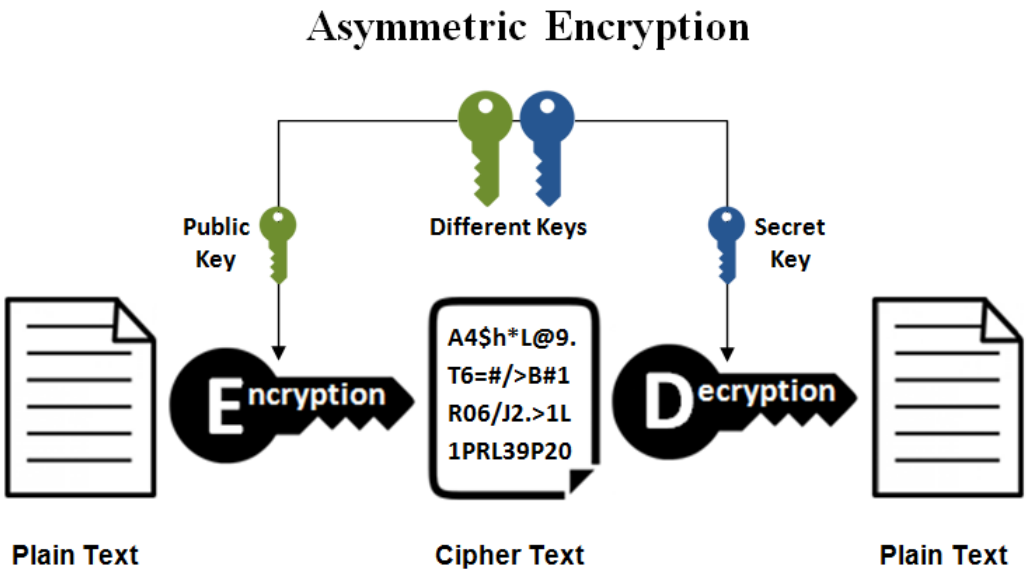


Figure 2.3: Asymetric encryption

In summary, a synthesis of these two methods of cryptography is described in the table below :

Symmetrical encryption	Asymmetric encryption
Same keys to encrypt and decrypt.	A different key for encryption and decryption.
Fast in execution.	Slow to run due to the high computational load.
Used for mass data transmission.	Used for secret key exchange...
AES, *DES*, *3DES* and *RC4*.	*Diffie-Hellman*, *RSA*...

Table 2.1: Comparison Symmetric and Asymmetric encryption

2.6 Advantages and Inconveniences

Advantages and Inconveniences of symmetrical encryption

Advantages

- It is easy to set up and can be done in few time.
- It is simpler, used by all ages and backgrounds.

Inconveniences

The secret key must be shared with the recptor. If the secret key is encrypted with the user's password, then make sure that password is not easy to guess.

If you use the same secret key for all of your email encryption and someone spies on that secret key, all of your previous encrypted emails will be compromised.

Advantages and Inconveniences of Asymmetric encryption

Advantages

- It is not necessary to force the sender to shared the secret keys as symmetric encryption. So we eliminating the need sharing keys.
- Requires a digital signature that authenticates the identity of the recipient.
- It guarantees that the message is not modified during its translation.

Inconveniences

It takes a long time, and it required much more works. Generaly, you can only send the encryption emails, if the other person has maked pairs of keys. So to speak, that the other person must be well informed....

2.7 Cryptanalysis

Security of a cryptosystem is in fact basing on the analysis of the complexity of the defined algorithms and on the computational powers available for an attack.

Cryptanalysis is somehow opposed to cryptography, it is the study of the weaknesses of cryptographic systems, it is usually carried out by an intruder who implements methods to find secret information such as the key, clear message from information considered public (cryptogram, algorithms), cryptanalysis is one of the disciplines of cryptology.

In the cryptanalysis it is assumed that man is weak and easily welded, so the strength of a system must rest on the strength of the principle used.

If the purpose of cryptography is to develop methods of protection, the purpose of cryptanalysis is instead to break these protections.An attempt to cryptanalyze a system is called an attack, and it can lead to different results.

We can resum this in the folloning definition:

Definition 2.4

Cryptanalysis *is decrypted encrypted information without using the key. Cryptanalysis provides an interesting combination of analytical reasoning, implementations of mathematical tools, model research, determination and luck. These cryptanalyses are also called hackers.*

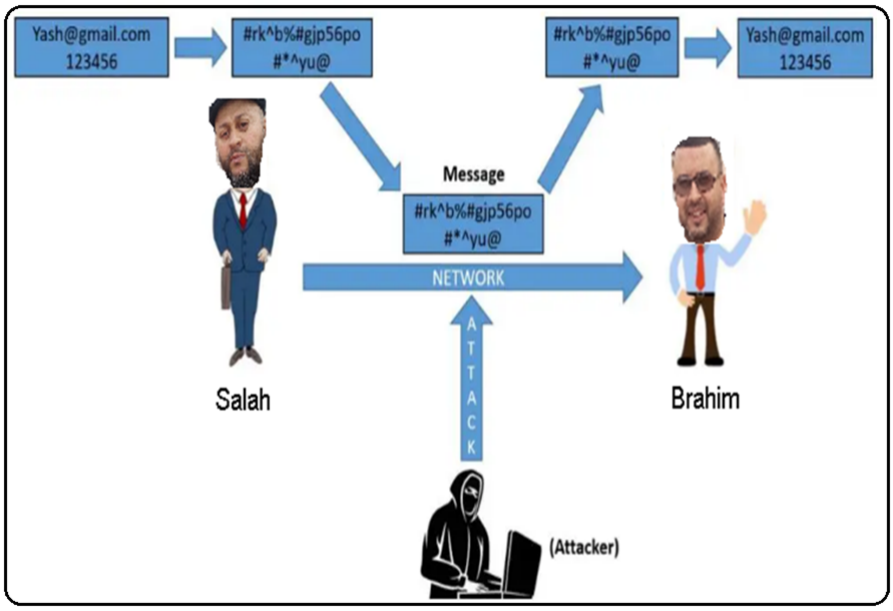


Figure 2.4: Cryptanalysis decryption with out key

2.7.1 Classicals attacks :

The attacker knows the encryption and decryption algorithms [8, 20]

- **Brute force attack:** It is a method used in cryptanalysis to find a password or key. It is about testing, one by one, all possible combinations.

- **Encrypted text attack only :** the attacker has only one or more encrypted messages that he wants to decrypt. This is the most difficult type of attack.
- **Clear text attack known :** [8, 20] the attacker has examples of clear messages with corresponding encrypted messages, or a clear part of an encrypted message. The purpose is to obtain information about the key.
- **Clear text attack selected :** the attacker can get the encrypted version of a number of clear messages chosen, either before the attack (offline attack), or as and when (online attack). The goal is still to get information about the key.
- **Selected Encrypted Text Attack :** The attacker can get the encrypted version of a number of selected clear messages, and also the clear version of a number of selected encrypted messages. There is still a distinction between offline and online attacks.

2.7.2 Other types of attacks:

- **Pre-calculation attack :**[8] It is for the attacker to pre-calculate information and use it to identify messages or keys. This requires more work but also allows more flexibility. An extreme case is the exhaustive search.
- **Differentiation attack :** This is an attack that differentiates the encryption protocol used from a perfect encryption protocol. This covers the aforementioned attacks and all future attacks!
- **The model of Dolev-Yao :**
  It is a formal system using to demonstrate the properties of interactive protocols of cryptography.

  vulnerable environment: It is assumed that the attacker dispose is very intelligent and has many ways to modify the network communications. It is assumed that the attacker :

  - can get all messages circulating on the network ;
  - is a legitimate user of the network ;
  - may initiate communication with all members of the network;
  - can send a message to all members of the network by pretending to be someone else. However, the attacker is not all-powerful. Presumably, between other than the attacker:
  - cannot guess a random integer;
  - cannot guess the private key corresponding to a the public one.

Success scale[8]

- Full breaking : The attacker discovers the key.
- Global deduction: the attacker discovers functions equivalent to encryption and decryption functions without knowing the key.

- Local deduction: the attacker can decrypt one or more new encrypted messages.
- Deduction of information: the attacker gets information about the key or about encrypted messages.

evaluation criteria

- Time: the number of base operations required
- Space: the maximum amount of memory required
- Data: the number of clear/encrypted messages required.

2.7.3 The problem of discret logarithm

Let G be a cyclic group of order n , and let g be one of its generators.

The discret logarithm of G in the base g, is the application, log_g defined by:

$$\begin{aligned} log_g : & G \to \frac{Z}{nZ} \\ & x \mapsto log_g(x) = y \end{aligned}$$

It is therefore an isomorphism of groups, of reciprocal application $x \to g^x$. For some groups G, the calculation of log_g is trivial: for example for $G = (\frac{Z}{nZ}, +)$.

However, if $G = (\frac{Z}{pZ})^*$, where 'p' is a prime number, finding a 'G' generator is not easy: you need to know how to factor $p-1$ to guarantee the result. And the calculation of discrete logarithm seems very difficult. [19, 26]

Example 2.1

Let $(\frac{Z}{7Z})^* = \{1, 2, 3, 4, 5, 6\}$.
Noting that 3 and 5 are generators of this group.
So we can define a discrete logarithm at base 3 and base 5 as follows:

x	1	2	3	4	5	6
$log_3(x)$	6	2	1	4	5	3
$log_3(x)$	6	4	5	2	1	3

Table 2.2: Discrete logarithm of $(\frac{Z}{7Z})^*$

Algorithms to calculate discrete logarithm

It is always possible, to calculate the discrete logarithm of x, to enumerate the elements: $g^0, g^1, g^2, ..., g^i, ...$, until we get x. However, if this method is quite reasonable for small groups, it is totally imaginable when the cardinality of the group increases.

There are several algorithms for calculating D-L:

- Shanks' giant-step baby-step algorithm.
- Pollard ζ algorithm.
- The Pohlig-Helman algorithm.
- The index calculation algorithm.

We will indicate in the following one of these algorithms which is the algorithm of baby-step giant step due from Shanks.

Shanks' giant-step baby-step algorithm.

the equation: $g^y = x\ mod(p)$ .....(1).....(looking for y).

This equation is solved according to Shanks [26]
as follows: we write: $y = au + b$, with: $u = \lceil\sqrt{p}\rceil$, and: $0 \leq a, b \leq u - 1$, where $\lceil\sqrt{p}\rceil$ is the smallest rational integer p.

Equation (1) becomes:
$g^{au} = xg^{-b}\ mod(p)$.

Two lists are then created, thus constituting the so-called 'no giant, no baby'.

Giant step g^{au}	**Baby step** xg^{-b}
1	x
g^u	xg^{-1}
g^{2u}	xg^{-2}
g^{3u}	xg^{-3}
...	...
...	...
...	...
...	...
...	...
$g^{(u-1)u}$	$xg^{-(u-1)}$

Table 2.3: Shanks' giant-step baby-step algorithm.

The creation of lists uses $\bigcirc(\sqrt{p})$ operations and their consultation has a $\bigcirc(\sqrt{p}Logp)$ [19]

Example 2.2

$p = 23, g = 11, x = 14$.
So, $u = 5$ *, the two lists are then:*

Suite g^{au} *:*$1, 5, 2, 10, 4$ *with:* $0 \leq a \leq 4$.

Suite xg^{-b} *:*$14, 18, 10, 3, 17$ *with :* $0 \leq b \leq 4$. *There is equality for* $a = 3$ *and* $b = 2$ *where* $y = 17$.

Complexity of algorithms: [20]

The complexity of algorithms for calculating discrete logarithm is expressed according to the size of group G (card G). But because the machine (processor) works in binary, we will consider the group size in $log_2(p)$.

Also a polynomial complexity is in $\bigcirc ln(rp)$, r real , and an exponential complexity is in $\bigcirc(pr) = \bigcirc(e^{r.lnp})$. We naturally define a complexity under exponential as being of the form $\bigcirc(e^{clna+\circ(1)p})$ where has $a < 1$ and $c \in \mathbb{R}$c R. The problem of discrete logarithm is a generally difficult problem, that is not resolvable in polynomial time. So we built cryptosystems based on this problem (like protocols: Elgamal, ...).

2.8 Cardinality of an eliptic Curve over finite field

Let $\mathbb{K} = F_q$ be a finite field, with q elements, and let E be an eliptic curve defined on this field. An important first result concerning the number of the points of an eliptic Curve on a finite field is the following:

Theorem 2.1 ***(Hasse)*** *[45]*
If E is an eliptic curve on the finished field, F_q, then we have:

$$q + 1 - 2\sqrt{q} \leq cardE(F_q) \leq q + 1 + 2\sqrt{q} \tag{2.1}$$

2.8.1 Counting the points of an eliptic Curve on a finished field

In this part we will show that it is easy to calculate the cardinal of an $E(Fq^n)$ Curve if we know its cardinal for $E(Fq)$. Then we will give an algorithm that allows us to calculate $CardE(Fp)$ for a primer p.

Theorem 2.2 *[17]*
Let $CardE(F_q) = q + 1 - \varepsilon$.

We put: $x^2 - \varepsilon x + q = (x - \alpha)(x - \beta)$, when $\alpha, \beta \in \mathbb{C}$.
So: $CardE(F_q^n) = q^n + 1 - (\alpha^n + \beta^n)$.

Example 2.3

Consider the eliptic Curve E: $y^2 = x^3 + 2$; defineded on F_7, then a simple calculation shows that:
Card $E(F_7) = 9$, and $\varepsilon = 7 + 1 - 9 = -1$, then we have the following polynomial:

$$x^2 + x + 7 = (x - \tfrac{-1-\sqrt{-27}}{2})(x - \tfrac{-1+\sqrt{-27}}{2})$$

We can therefore calculate the cardinal of any group $E(F_7^n)$. for example if $n = 60$:

$$(\tfrac{-1-\sqrt{-27}}{2})^{60} + (\tfrac{-1+\sqrt{-27}}{2})^{60} = 1804985852611988480600 6498$$

and therefore:

$$\begin{aligned} CardE(F_7^{60}) &= 7^{60} + 1 - 180498585261198848060064 98 \\ &= 508021860739623365322188179602357975652549718829504. \end{aligned}$$

With this theorem we can very quickly calculate the cardinality of a group $E(F_p^n)$ of the moment we know Card $E(F_p)$.

The Schoof algorithm [18]

The Schoof algorithm is an effective algorithm for counting eliptic Curve points on finite fields. It has applications in cryptography on eliptic curves, where it is used to construct eliptic curves having a cardinal divisible by a large prime number.

The algorithm was published by *René Schoof* in 1985, which was a major breakthrough in the first polynomial deterministic algorithm for point counting. Before this algorithm, only methods of exponential complexity were known for this problem, such as the naive algorithm and the no baby no giant algorithm. . Its complexity is $O(ln8p)$ [9]. Thus we can calculate Card $E(F_p^n)$ with the last theorem. Schoof evaluated the order of an $E(F_p)$ group as: $p+1-t$, where t is a root of a *Frobenius* equation [9].

q	$E(F_q)$	$CardE(F_q)$	Time (sec)
23	$y^2 = x^3 + 2x + 6$	17	0.000000
29	$y^2 = x^3 + 22x + 16$	37	0.054945
31	$y^2 = x^3 + 5x + 3$	41	0.054945
37	$y^2 = x^3 + 8x + 14$	47	0.000000
41	$y^2 = x^3 + 8x + 4$	43	0.274725
43	$y^2 = x^3 + 27x + 22$	29	0.000000
47	$y^2 = x^3 + 38x + 6$	37	0.054945
53	$y^2 = x^3 + 5x + 12$	43	0.054945
59	$y^2 = x^3 + 4x + 49$	53	0.000000
61	$y^2 = x^3 + 31x + 49$	61	0.054945
67	$y^2 = x^3 + 2x + 56$	37	0.000000
71	$y^2 = x^3 + 57x + 14$	47	0.054945
73	$y^2 = x^3 + 33x + 34$	79	0.000000
79	$y^2 = x^3 + 75x + 6$	61	0.054945
83	$y^2 = x^3 + 3x + 78$	67	0.000000
89	$y^2 = x^3 + 54x + 52$	103	0.054945
97	$y^2 = x^3 + 32x + 33$	97	0.054945

Table 2.4: Schoof Performance Program

Improvements to the Schoof algorithm

In the '90s years, *A. O. L. Atkin* and *then Noam Elkies* proposed improvements to the original *Schoof* algorithm by restricting the set $S = \{l_1, l_2, ..., l_s\}$ of first taken into

consideration. These first were subsequently called first of *Atkin* and *Elkies* respectively. A first l is said of *Elkies* if the characteristic equation of Frobenius $\Phi^2 - t\Phi + q = 0$ splits in $\mathbb{F}_l$ *Atkin* showed how to combine the information obtained by the first *Atkin* with that obtained by Elkies in order to design an effective algorithm, called the *Schoof–Elkies–Atkin* (or SEA) algorithm.. The first problem in this algorithm is to determine if a first data point comes from l and from Elkies or Atkin. To this end, we study the factorization properties of the modular polynomial, an object derived from the theory of modular forms and eliptic curves on complexes.

2.8.2 Discrete Logarithm Problem on eliptic Curves

We have seen the different operations we can perform on eliptic curves, including scalar multiplication, which is frequently used during cryptographic calculations. In this section, we explain why scalar multiplication was the key to ensuring security of an eliptic-based cryptosystem.

The level of safety of ECC depends heavily on their difficulty in solving the discret logarithm problem , using eliptic curves. We assume that 'g' is the generator of a cyclic group 'G' of the order n, if the composition law of the group is multiplicative, any element e can be written as $e = g^k$ where $k \in \mathbb{Z}$.

We choose, on an eliptic curve defined in a finite first field $E(F_p)$, a point 'P' of order n as the generator of ower cyclic group $\langle P \rangle$, another point $Q \in \langle P \rangle$.

The problem of discrete logarithm on eliptic curves (ECDLP) is to find $k \in [0, n-1]$ satisfactory $Q = kP$.

The most naive solution to solve this problem is to calculate exhaustively $1P, 2P, 3P...$ until we find Q, but the calculation can become extremely long if the value of k is large enough. It is therefore extremely difficult to recover the value of k from Q acal proof that the ECDLP is insoluble, but the resolution of such a problem is still considered impossible, taking into account the current state of computer technologies [15].

2.9 Obejectfs of Cryptography and Cryptanalysis

Cryptography objectfs [11]

Cryptography is generally used to secure information, in particular for the following properties:

- **Confidentiality (or Secret):** only the recipient must be able to decrypt the messages. It must not be possible for another person to obtain meaningful information from what they observe.
- **Integrity:** Recipient must determine if the message has been modified (in their transmission).
- **Authentication:** The recipient must confirm and verify the authenticity of the sender.
- **Non-repudiation:** as a result of points 2 and 3 the sender cannot deny being the author of the message.

- **Non-replayability (anti-replay):**the message cannot be sent several times without the recipient being able to distinguish it.
- **Proof of delivery :** the sender must have a means of proving that the recipient has received the message.

Cryptanalysis objectfs

Find attacks to break the protections set up using cryptography.

2.10 Classical cryptography

2.10.1 Scytal

Scytal rolled up with a blank strip. After wrapping the belt on the scytal, the message was written with a letter on each circumvolution. To decipher it, the recipient had to have a stick of the same diameter as the one used for encoding. It was then enough to wrap the scytal around this stick to get the message in clear [8].

Figure 2.5: Scytal rolled up with a blank strip.

Example 2.4 *[42]*

Encrypting

It is assumed that the stem allows to write 4 letters vertlcalement and 5 letters horisonement. The plain text for is written as follows:

*"**I am hurt very badly help**". For encryption, write through the leather:*

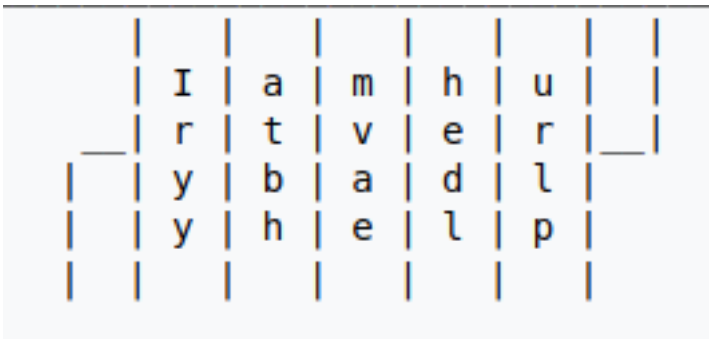


Figure 2.6: Encryption with Scytal

So the encrypted text becomes: *"**Iryyatbhmvaehedlurlp**" after the unfolding.*
The decrypting

For decryption, wrap the tape around the rod and read through. The encryped is: "Iryyatbhmvaehedlurlp", every fifth letter will appear at the same line, so that the original text becomes: "I am hurt very badly help".

2.10.2 Caesar cryptogram :

Caesar's encryption is an offset of letters: to encrypt a message, 'A' becomes 'D', 'B' becomes 'E', 'C' becomes 'F',... Here table with the original alphabet at the top and , in correspondence with the alphabet for encryption below.

To also take into account the last letters of the alphabet, it is better to represent the alphabet on a ring. This shift is a circulant shift on the letters of the alphabet
To decipher Caesar's message, simply shift the letters in the other direction, D is deciphered in A, E in B, ... [9]

Encrypt and decrypt :

We associate to each of the 26 letters from A to Z, a number of 0 to 25. In mathematical terms, we define a bijection :

$$f : \{A, B, C, ..., y, Z\} \longrightarrow \{0, 1, 2, ..., 25\}$$

by :

$$A \longmapsto 0 \ , B \longmapsto 1, \ ... \ , Z \longmapsto 25$$

Caesar's encryption is simply an addition in $\mathbb{Z} = 26\mathbb{Z}$ Let's fix an integer k which is the offset (for example k = 3 in the Cesar example above) and define the Caesar offset encryption function k which goes from the whole $\mathbb{Z} = 26\mathbb{Z}$ in itself :

$$C_k : \begin{cases} \mathbb{Z}/26\mathbb{Z} \longrightarrow \mathbb{Z}/26\mathbb{Z} \\ x \longrightarrow x + k (mod 26) \end{cases}$$

To decipher, nothing simpler! Just go the other way, that is to say here to subtract(if the result is negative add 26 to the result). The decoding function of shift k Caesar is :

$$D_k : \begin{cases} \mathbb{Z}/26\mathbb{Z} \longrightarrow \mathbb{Z}/26\mathbb{Z} \\ x \longrightarrow x - k \end{cases}$$

Example 2.5

If the key $k = 3$,

A	T	T	A	Q	U	E		A	U		M	A	T	I	N	(clear message)
0	19	19	0	16	21	4		0	21		12	0	19	8	13	(Clear Message Letter Val)
3	22	22	3	19	24	7		3	24		15	3	22	11	16	(Result of the add mod 26)
D	X	X	D	T	Y	H		D	Y		P	D	X	L	Q	(encrypted message)

Table 2.5: Example for Caesar encryption

Letter permutations

In the permutation codes we share the text in blocks, we keep the same alphabet but we change the place of the letters 'inside a block (we swap them)[**?**].

Example 2.6

B	o	n	j	o	u	r	$\longrightarrow$	j	n	o	b	r	u	o
1	2	3	4	5	6	7	$\longrightarrow$	4	3	2	1	7	6	5

Table 2.6: Example one: encryption with permutation

Example 2.7

ATTAQUE AU MATIN $\rightarrow$ *DAADECV DC WDASI*

if the permutation is :

$A \rightarrow D$	$B \rightarrow R$	$C \rightarrow K$	$D \rightarrow X$	$E \rightarrow V$	$F \rightarrow H$	$G \rightarrow L$
$H \rightarrow N$	$I \rightarrow S$	$J \rightarrow O$	$K \rightarrow P$	$L \rightarrow Q$	$M \rightarrow W$	$N \rightarrow I$
$O \rightarrow T$	$P \rightarrow J$	$Q \rightarrow E$	$R \rightarrow U$	$S \rightarrow Z$	$T \rightarrow A$	$U \rightarrow C$
$V \rightarrow F$	$W \rightarrow B$	$X \rightarrow Y$	$Y \rightarrow G$	$Z \rightarrow M$		

Table 2.7: Example two: encryption with permutation

Frensh			
A	9,42%	N	7,15%
B	1,02%	O	5,14%
C	2,64%	P	2,86%
D	3,39%	Q	1,06%
E	15,87%	R	6,46%
F	0,95%	S	7,90%
G	1,04%	T	7,26%
H	0,77%	U	6,24%
I	8,41%	V	2,15%
J	0,89%	W	0,00%
K	0,00%	X	0,30%
L	5,34%	Y	0,24%
M	3,24%	Z	0,32%

Table 2.8: Frequency of appearance of French letters.

Cryptanalysis of letter permutation

Using the frequency of appearance of French letters:
In all languages the letters appear with different frequencies: for example the *'e'* is a most used letter of French and english. Below are the frequencies of letters and groups of letters. These frequencies are calculated from newspaper or book articles

English			
E	12,70%	TH	THE
T	9,10%	HE	ING
A	8,20%	IN	AND
O	7,50%	ER	HER
I	7,00%	AN	ERE
N	6,70%	RE	ENT
S	6,30%	ED	THA
H	6,10%	ON	NTH

Table 2.9: Frequency of appearance of English letters.

2.10.3 Vigenère encryption:

Vigenère's figure uses multiple alphabetic substitutions per shift:

- You choose a word as your key.
- the rank of each letter of the key defines an offset to apply letter correspondence
  $\rightarrow numbers:\quad A=0\quad ;\quad B=1\quad ;\quad ...\quad ;\quad Z=25$
  Addition on the letters: $J+W=F(9+22 mod 26=5)$

Example 2.8

The key word is : ***CLE***

D	C	O	D	E	(clear message)
3	2	14	3	4	(message letter val)
C	L	E	C	L	(repeat encryption key)
2	11	4	2	11	(val de lettre de la clé)
5	13	18	5	15	(result of the addition mod 26)
F	N	S	F	P	(encrypted message)

Table 2.10: Example 1 of Vignére encryption

The deciphering principle

To decipher: we take the first letter of the message and the key and subtract their values, if the result gives a negative number, we add 26 to the result (because 26 is the number of letters of the alphabet), the result corresponding the rank in the plain letter alphabet.

Example 2.9

F(=5) and key C(=2) and subtract it(5-2 =3), the letter of rank 3 is D So :

F	N	S	F	P	(encrypted message)
5	13	18	5	15	(message letter val)
C	L	E	C	L	(encryption key)
2	11	4	2	11	(key letter val)
3	2	14	3	4	(result of subtracting it mod 26)
D	C	O	D	E	(clear message)

Table 2.11: Example 2 of Vignére encryption

How to decipher without knowing the key?[43]

1. **KASISK testI :**
   Consists in locating repetitions of letters in the text.
   The coincidence index is an indicator used in cryptanalysis to evaluate the overall distribution of letters in an encrypted message for a given alphabet. Under the formula:

$$I_c = \sum_{i=A}^{Z} \frac{n_i(n_i-1)}{N(N-1)}$$

   with :

   - n_i : The number of repitions of the letter i that appears in the message.
   - N : Total number of letters of the message.

   Note 2.1
   If the lower the index, the greater the number of the alphabet used.

2. **Friedman test :**
   This method for determine the length of the key, and is based on the coincidence index between two texts .
   Note p_i the frequency of the letter L = A ,... ,Z. So, we have:

$$I_c = \sum_{i=A}^{Z} p_i$$

   It follows that the I_c of a text (sufficiently long) in French is 0,078.

Theorem 2.1

The Vigenère encryption protocol with a key their length equal or greater than the message's length, and used once and only once, is totally sure.

2.10.4 Hill Encryption :

Hill Encryption uses the alphabet, and a square matrix $mathcalM$ of order n composed of integers is calling: **The encryption Matrix** .

$n = 2$, so $\mathcal{M}$ of size 2×2,this matrix acts on the vectors of length 2 as follows [8] :

$$\left(x, y\right)\begin{pmatrix} a & b \\ c & d \end{pmatrix} mod 26 \equiv (ax + cy, bx + dy) mod 26$$

By reducing the numbers modulo 26, we deduce an action on the pairs of letters [8].

Example 2.10

For example for the Matrix $M = \begin{pmatrix} 3 & 21 \\ 5 & 8 \end{pmatrix}$

$RE \longrightarrow (17,4) \longrightarrow^{\times M} (71,389) \longrightarrow^{mod 26} (19,25) \longrightarrow TZ$

so :

Key $:M = \begin{pmatrix} 3 & 21 \\ 5 & 8 \end{pmatrix}$ *invertible*

Text message *:* $RENDEZVOUSCESOIR$

RE $(17,4)$ $\times M$ $mod 26$	ND $(13,3)$ $\times M$	EZ $(4,25)$ $\times M$	VO $(21,14)$ $\times M$	US $(20,18)$ $\times M$	CE $(2,4)$ $\times M$	SO $(18,14)$ $\times M$	IR $(8,17)$ $\times M$
(19,25) TZ	(2, 11) CL	(7, 24) HY	(3, 7) DH	(20, 18) US	(0, 22) AW	(20, 22) UW	(5, 18) FS

Table 2.12: Example of Hill Encryption

Nnumber of keys

$(2^2-1)(2^2-2)(13^2-1)(13^2-13) = 157248$ *matrix (in this example)*

Special case

The AA digram corresponds to the vector (0.0) and therefore is always coded on itself for any matrix $\mathcal{M}$. There are several methods to overcome this problem.

How to decrypt by Hill?

Deciphering requires knowing the matrix and the alphabet used. The calculations involve concepts of matrix calculation like matrix inversion and arithmetic calculation like modular inversion.

For decryption:

- first calculate the inverse of the matrix(md 26, where 26 the letters of the alphabet), which requires the matrix to be inverted.

- The decryption then consists in re-encrypting the encrypted message using the inverted matrix.

$$(x,y)\begin{pmatrix} a & b \\ c & d \end{pmatrix}^{-1} mod 26 \equiv \frac{1}{ad-cb}\begin{pmatrix} d & -b \\ -c & a \end{pmatrix} mod 26$$

Cryptanalysis of Hill's encryption

- **Attack by digrams:**
  Consider the digrams that appear most often

ES	*DE*	*LE*	*EN*	*RE*	*NT*	*ON*	*ER*	*TE*
3,3 %	2,4 %	2,3 %	2,1 %	1,9 %	1,7 %	1,6 %	1,5 %	1,5 %

Table 2.13: Digrams that appear most often

- **Clear text attack known:** If we know a part of the clear text and its encrypted version, we can deduce information about the key, or even the entire key.

- **Partial information attack:** In particular, if we can guess a part of the clear message, we can deduce information about the key.

2.11 Modern cryptography

The purpose of this party is to give a brief overview of the organization of modern cryptology. Obviously this overview is far from complete. Its interest is to make people understand the various elements to which we will then develop.

2.11.1 Algamel cryptosystem

In 1985, Algamal proposed a public key encryption algorithm.

This algorithm addresses the problem of the confidentiality of messages sent, and its effectiveness is based on calculating difficulty of the discrete logarithm problem.

A person called Salah, asks an other person Brahim to send him confidential messages.

Description of the cryptosystem

A description is given below:

- If we take a prime number $'p'$, and generator $'g'$ of the group $(\frac{Z}{pZ})^*$.
- Common data: p and g.
- Private Salah Key: $x \in (\frac{Z}{pZ})^*$.
- Salah Public Key: $y = g^x mod\ p$.

Encryption:

Let $'m'$ be a message to be encrypted by Brahim.
This message m is coded as an element of $(\frac{Z}{pZ})^*$.

- Brahim selects an element $k \in (\frac{Z}{pZ})^*$ then calculates R and S:

$$\begin{cases} R = g^k mod(p) \\ S = m.y^k mod(p) \end{cases} \tag{2.2}$$

An encrypted $'m'$ is the pair $(R; S)$.

Decryption:

- Only Salah is able to find $'m'$ from the cipher, according to his knowledge of x.

He calculates:

$$\begin{cases} y^k = g^{xk} = R^x mod(p) \\ m = \frac{S}{R^x} mod(p) \end{cases} \tag{2.3}$$

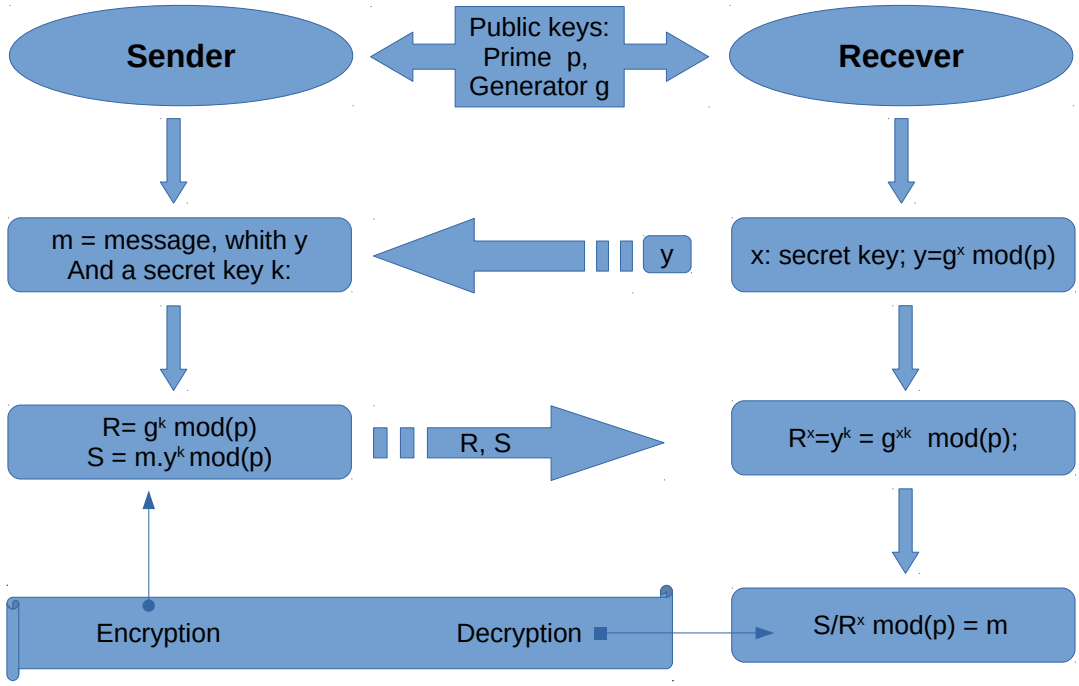


Figure 2.7: The Algamel cryptosystem

Example 2.11

Put the following dictionary:

a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s
01	02	03	04	05	06	07	08	09	10	11	12	13	14	15	16	17	18	19

t	u	v	w	x	y	z	!	space	?
20	21	22	23	24	25	26	27	28	29

Table 2.14: The encoded dictionary

- ***Step 1:***

  - *Salah chooses* $p = 31 =$ *prime number,*
    and $'g = 11'$ *is a generator of* $(\frac{Z}{31Z})^*$.
  - *Salah calculates* $y = g^x mod 31 = (11)^{10} = 5$ *, for* $x = 10$ *(x Salah secret key).*

  So Salah publishes $(p, g, y) = (31, 11, 5)$ *and keeps his secret key* $x = 10$.

- ***Step 2:***

  Brahim wants to send Salah the following message:

  $\dashrightarrow\dashrightarrow m =$ *Il fait beau!*

Encryption

- *Brahim converts this message to an integer sequence m of* $(\frac{Z}{31Z})^*$.
- *So* $m =$ *Il fait beau!* $= 091228060109202802050121 27$
- *Brahim selects an element* $k = 8$ *from* $(\frac{Z}{31Z})^*$ *then, it calculates R and S:*

$$\begin{cases} R = g^k mod(p) = 11^8 mod(31) = 19 \\ S = m.y^k mod(p) = (091228060109202802050121 27).5^8 mod(31) \\ \qquad\qquad = (091228060109202802050121 27).25 mod(31) \\ \qquad\qquad = 082118262508041821012529 24 = S \end{cases}$$

Brahim sends Salah the pairwise cipher $(R; S)$.

- ***Step 3:***

Decryption

Salah receives the pairwise cipher $(R; S)$ *and decrypt it using his secret key* $x = 10$ *by calculating:*

$$\begin{cases} y^k = g^{xk} = R^x mod(p) = 19^{10} mod(31) = 25 mod(31) \\ m = \frac{S}{R^x} mod(p) = \frac{(082118262508041821012529 24)}{25} mod(31) \\ \qquad = (082118262508041821012529 24).(5) mod(31) \\ \qquad = 091228060109202802050121 27 mod(31) \\ \qquad = 091228060109202802050121 27 \\ \qquad = m = \text{Il fait beau!} = \textit{The initial message.} \end{cases}$$

2.11.2 RSA cryptosystem

RSA (Rievest, Schamir, Adleman) is an asymmetrical algorithm in cryptography, used for encryption and decryption of messages using modern machines .

RSA algorithm includes private and public keys that can be published to anyone, as it is used for encryption of plain text to encrypted text.

The generation of the RSA algorithm key is what makes it so docure and reliable today.

The key generation process of the RSA algorithm involves five steps:

- Chosing of two prime numbers p, and q.
- Calculation of: $n = p \times q$.

- Calculation the euler $\Theta = (p-1)(q-1)$.
- Choose e ,$1 < e < q$.
- Message Encryption : $C = m^e mod n$, where m is the message to encrypt.

  Message Decryption: $m = c^d$ where: $d = e^{-1}$

Example 2.12

- *choose two primes* $(p,q) = (3,7)$.
- *compute* $n = p \times q = 3 \times 7 = 21$.
- *compute euler* $\Theta = (p-1)(q-1) = 2 \times 6 = 12$.
- *choosing 'e = 7'* ,$1 < e \leq q$.
- ***Message Encryption :***

  Let $m = 4$ *be a message to encrypt:*
  $C = m^e mod n$, *where m is the message to encrypt.*
  So, $C = 4^7 mod 21 = 16384 mod 21 = 4$

- ***Message Decryption:***

  $m = c^d mod n$ *where:* $d = e^{-1} mod 7 = 7^{-1} mod 12 = 7$
  So, $m = c^d mod n = 4^7 mod 21 = 1638 mod 21 = 4$ *the initial message.*

2.11.3 Diffie-Hellman Protocol

This protocol allows for two entities that are never met to build a common secret key known to them alone and unknown to who conquers, even an indiscreet that would listen to their communication . Need a one-way trap function: a good candidate is discrete logarithm [46]:

1. Salah and brahim chose a big finite prime number p, and a small number g strictly than p.
2. Salah chooses a random number a, raises g to power a, and tells Brahim g^amod p , number that we note A. It sends A to Brahim .
3. Similarly, Brahim chooses a random number b, and does the same; he transmits the number $B = g^b$ mod p .
4. Salah, by raising the number B received from Brahim to power a, gets g^{ba} mod p.
5. Brahim makes the analogous calculation with the number A received from Salah and gets g^{ab} mod p, which is the same result (same K keys) $k = g^{ab} mod p$

6 At the end of the protocol, Salah and Brahim both know the number g^{ab} [mod p] but not aymen . Since it is difficult to reverse the xponentiation in a finite field (or on an eliptic curve), that is to say to calculate the discrete logarithm, aymen cannot discover, therefore cannot calculate g^{ab} (mod p).

Example 2.13

1. *Salah and brahim chose prime number* $p = 23$, *and a base* $g = 5$.
2. *Salah chooses secret number* $a = 6$.
3. *He send to Brahim the value* $A = g^a mod p = 5^6[23] = 8$.
4. *Brahim chooses a secret number* $b = 15$.
5. *Brahim sends to salah the value* $B = g^b mod p = 5^{15}[23] = 19$.
6. *Salah can now calculate the secret key* $B^a mod p = 19^6[23] = 2$.
7. *Brahim also calculate the secret key* $A^b mod p = 8^{15}[23] = 2$
   same key $k = 2$

Chapter 3

Quantum mechanics and Chaos theory in Cryptography

Quantum mechanics is a branch of theoretical physics that has succeeded quanta theory and wave mechanics to study and describe the fundamental phenomena at work in physical systems, especially at the atomic and subatomic scales.

It was developed in the 1920s by a dozen European physicists to solve problems that classical physics failed to explain, such as the radiation of the black field, the photoelectric effect, or the existence of spectral lines. It proved fruitful in various results and applications: it made it possible in particular to elucidate the mystery of the structure of the atom, and more generally it proved to be the general framework for describing the behaviour of elementary particles, to form the foundation of modern physics.

Quantum cryptography is an attempt to implement quantum mechanics predicates to ensure the confidentiality, the integrity and non-interception of ower data transmissions. It is also a sub-domain of quantum computing.

3.1 Quantum mechanics in cryptography

Quantum Mechanics: a formulation proposed in the 1920s, which allows the study of systems of atoms and systems of particles at low energies, their structures and their interactions with external environments. Two features of these systems: - Possible energy values are imposed; - any measure brings an uncontrollable disturbance. The scientist "talks" about quantum systems

This formulation is simple, its development is fast for the connoisseur of the notions of probability, vector space, and mathematical operators.

Software currently allows numerical resolutions of mathematical equations!

It is useful to recall here the postulates of quantum mechanics. We present it in a purely axiomatic way, without “explanation” on the physical origins because we will only use some postulates.

3.1.1 The mathematical framework of mechanics quantum.

Quantum mechanics is presented in a space of Hilbert, that is to say a functional space L^2 equipped with a scalar product.

Definition 3.1 $\mathbb{H}$ *is a space of Hilbert if:*

- $\mathbb{H}$ *is a space* L^2 *, that is* $\forall f \in L^2, f$ *:*
  $A \subset \mathbb{R}^3 \times \mathbb{R} \to \mathbb{C}$, f *is measurable and summatable square,*

$$\int_A |f(x)|^2 dx < \infty \tag{3.1}$$

- $\mathbb{H}$ *is complete, any Cauchy sequel straight is converging.*
- $\mathbb{H}$ *is equipped with a scalar product, defined by:*

$$\langle f|g\rangle = \int_A f(x) \times \overline{g(x)} dx, \forall f, g \in \mathbb{H} \tag{3.2}$$

The elements of this space are called wave functions, and noted:
$\psi : A \to \mathbb{C}$

Note

Note that $\langle|\rangle$ is a good hermitic scalar product, that is, it checks the following properties:

$\forall\ f, g, h \in \mathbb{H}, \forall \alpha, \beta \in \mathbb{C}$

- $\langle f|\alpha g + \beta h\rangle = \alpha\langle f|g\rangle + \beta\langle f|h\rangle$
- $\langle f|g\rangle = \langle g|f\rangle^*$
- $\langle f|f\rangle > 0$
- $\langle f|f\rangle = 0 \Leftrightarrow$ f is the null function

The ratings of Dirac

Any Ψ wave function is associated with a vector, noted $|\Psi\rangle$ and called a *ket*. This state vector belongs to space ε, called space of states. It's a subspace of Hilbert's space.

The existence of a scalar product also allows us prooving that the dual of ε, $\varepsilon^* = linearapplication : \varepsilon \to \mathbb{C}$, is isomorphic to ε.

An element of ε is actually associated with a wave function (or *ket*) and is noted: $|\Psi\rangle$.

Theorem 3.1

ε^* is isomorphic to ε .

Indeed, $\forall|\Psi\rangle, |\phi\rangle \epsilon \varepsilon$, we have $\langle\phi|\psi\rangle \equiv (|\phi\rangle, |\psi\rangle)$ where $(,)$ is the product scalar in ε.

The action of $\langle\phi|$ on $|\psi\rangle$ is noted $\langle\phi|\psi\rangle$, it is also the scalar product.

3.1.2 Postulates

- ***Axiome 1***

  Any quantum state can be described as ket. State space is a complex vector space. In particular, the principle of superposition is derived:

$$\forall |f\rangle, |g\rangle \epsilon \varepsilon, \forall \alpha, \beta \in \mathbb{C} : \frac{\alpha|f\rangle + \beta|g\rangle}{\|\alpha|f\rangle + \beta|g\rangle\|} \in \varepsilon \tag{3.3}$$

  remark 1
  Always standardize kets to always have a total probability of 1.

- ***Axiom 2***

  Any physical quantity is represented by an observable, that is a linear operator,
  $A : \varepsilon \to \varepsilon$*, auto-assistant (equal to its hermitic conjugate;* $A = A^{\tau}$ *) for which there is always an orthonormed base of* ε *formed by its own kets.*

  The only physically measurable quantities are given by the values own from A. Either A an observable, $A = A^{\tau} \equiv (A^T)^*$*, or* $\lambda_i, |v_i\rangle$ *all of its eigenvalues and associated eigenvectors.*

  Therefore, $A|v_i\rangle = \lambda_i|v_i\rangle$ *with* $\lambda_i \in \mathbb{C}$*.*

- ***Axiom 3***

  Probability calculation axiom (discrete case). The probability to measure λ_i *is given in:*

  $P(\lambda_i) = |\langle v_i|\psi\rangle|^2$*, when* $|\psi\rangle$ *= State of the considered system .*

  remark 2

  This entry is only valid if the base is discrete (the spectrum is discrete) and where eigenvalues are not degenerated, that is to say where the dimension of all the clean subspaces is 1. We will only need thereafter this case, which is why we limit ourselves to it.

  remark 3*[44]*

  This axiom justifies the normalization of kets:

  $|\langle v_i|\psi\rangle|$ *is the i component of* $|\psi\rangle$ *on the basis* $|v_i\rangle$*.*

- ***Axiom 4: Effect of a measurement on a quantum state.***

  At time t, let $|\psi(t)\rangle$ *be a state and* $\lambda_i, |v_i\rangle$ *the spectrum of A. If a measurement of A is made at that moment, the state is projected on the proper vector corresponding to the measurement.*

$$|\psi(t)\rangle \rightarrow |\psi^{'}(t)\rangle = |v_i\rangle$$

This axiom, central for quantum cryptography, finally tells us that if a measurement is made, and we measure λ_i (with a probability $P(\lambda_i)$), immediately after, we know that the outgoing state is $|v_i\rangle$; because if we redo this measure again and if the state has not changed over time, we are sure to find λ_i .

$$P(\lambda_i) = |\langle v_i|v_i\rangle|^2 = 1 \tag{3.4}$$

- ***Axiom 5: Evolution of a state over time.***

  Temporal evolution $|\psi(t)\rangle$ is described by a linear differential equation, known as the Schrödinger equation:

$$ih\frac{d}{dt}|\psi(t)\rangle = H(t)|\psi(t)\rangle \tag{3.5}$$

  where, H is an observable representing the energy of a system, called hamiltonian; $H = H^{\tau}$.

  For example, for a particle of mass m , $H = -\frac{h^2}{2m}\Delta$

After this axiomatic list, let us consider an example of a direct relationship with quantum cryptography.

3.1.3 Quantum cryptography

The quantum cryptography uses the properties of physics(quantum) to establish protocols in cryptography. The information carrier is then the photon – encoded via polarization, its phase or its amplitude.

3.1.4 Polarized photon and its quantum properties

In reality, all photons that constitute a ray of light have their own polarizations. When these have polarizations aligned in the same direction, we say that the light is polarized linearly. [9].

1. *A photon can be polarized in all directions: horizontally, vertically, diagonally,*
2. *A photon polarized on an angle axis 'a' passing through 'b' axis polarizing filter has a probability equal $=\cos^2(b-a)$ to pass filter [9, 13]. So:*
   - *When the filter is oriented precisely in the photon polarization axis '$(b = a)$', the photon will pass through the filter*

$$(probability = \cos^2(b-a) = \cos^2(0) = 1).$$

- *When the filter oriented at* 90^0 *from polarization axis '*$(b = a + 90')$*, the photon will be stopped by this filter*

$$(probability = \cos^2(b-a) = \cos^2(90) = 0).$$

- *When the filter oriented at* 45 *from the photon polarization axis '*$(b = a + 45)'$*, the photon will have a* 50% *probability to pass the filter*

$$(probability = \cos^2(b-a) = \cos^2(45) = \frac{1}{2}).$$

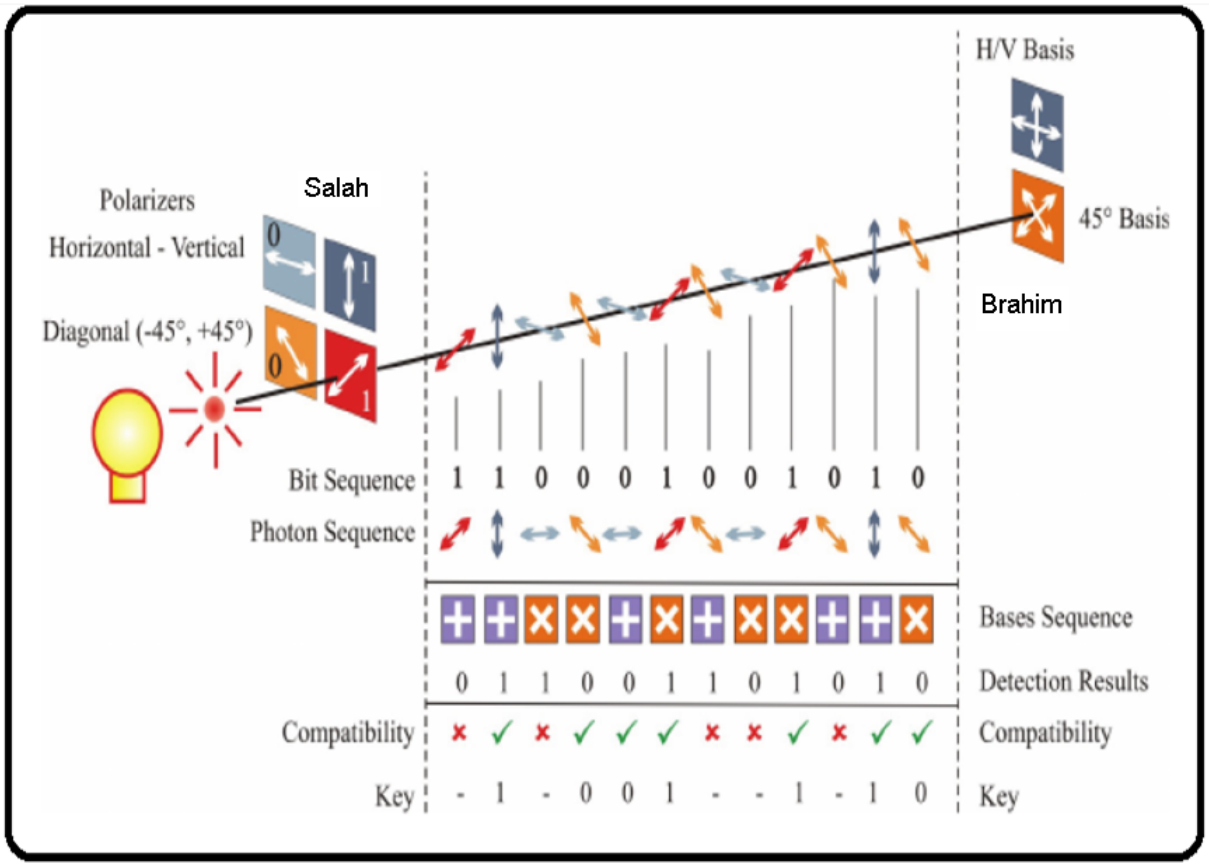


Figure 3.1: System using *BB*84 to shared a Quantum Key

3. *The quantum properties used by quantum cryptography are properties are still in the classical domain: [13, 14]:*

   - *If the probability of passing the different filter of 0 and 1, the passage of an individual photon through this filter is fundamentally unpredictable and indeterminist.*
   - *The bias axis is not known only by using a bias filter (or more generally, if in fact a measurement, the result of which is YES-NO). No direct measurement, giving an angle of the photon polarization axis as example.*

- *We cannot know the initial polarization axis of the photon in all cases, unless the axis is oriented at* 0^0 *or* 90^0*, but if it is oriented at* 45^0 *for example no way to know the initial polarization axis concerning the photon.*

3.1.5 Protocols for transmission keys

Indeed, it is a set of protocols allowing to distribute an encryption key between two remote interlocutors, while ensuring the security of transmission thanks to the laws of quantum physics and information theory. When two people want to communicate secretly (sender called the «Salah» and the «Brahim» receiver the spy being called «Med») they send each other coded messages. To decipher them, both people must have the "key" to decipher them. Initially, only Salah has it.

And it must not be intercepted when it is sent to Brahim. This is where quantum cryptography comes in. Salah sends the key in the form of photons emitted one by one into an optical fiber, a technological feat particularly difficult. Brahim receives these photons and measures their properties. They are the ones that will allow him to reconstitute the key. To capture it, Med must also observe these photons without leaving a suspicious trace.

Quantum physics explains that it is impossible to observe a photon without changing its properties. This is the famous Heisenberg uncertainty principle. In other words, Salah and Brahim can, by exchanging information by a standard channel, immediately detect any attempted espionage.

we find two modes for polarisation of photon:

- *Mode 1:* 10 *is encoded by a* 0^0 *polarization axis photon and* 11 *by a* 90^0 *polarization photon;*
- *Mode 2:* 10 *is encoded by a* 45^0 *polarization axis photon and* 11 *by a* 135^0 *polarization photon.*

The emitter emits the photon key per photon, randomly choosing the polarization mode at each emitted photon, and notes for each bit the chosen polarization mode.

With a polarizing filter(the receiver), it can be oriented at will to 0^0 *or* 45^0*. Before the expected arrival of a photon, it positions the filter, also randomly, at* 0^0 *or* 45^0*. At the expected time of arrival of the photon, he observes the result (if the photon has passed or not passed the filter), as well as the chosen orientation of the filter.*

Two possible cases for each bit:

- *Both persons have chosen, the same mode , randomly. This happens on average every other time. In this case, the received photon is representative of the emitted bit and can be translated directly into bit.*
- *Both persons have chosen a separate orientation of* 45^0*, in this case the received photon is random and no information can be extracted.*

After transmission of all the bits (minimum $2Nbits$ *for a* $N-bit$ *key), the transmitter communicates to the receiver, by a means (classic channal), the polarization mode used for each bit. So the receiver can know which bits have the same polarization orientation. It knows that these bits are non-random. So it knows some* $Nbits$ *on average for* $2Nbits$ *transmitted.*

Example 3.1

Salah sends 2000 photons randomly choosing the bases and polarization of each photon. Brahim measures the 2000 photons he receives; Espion measured some of these photons and therefore induced some errors.

Then, Salah and Brahim compare their bases and eliminate the ones that are not the same. Brahim chose the wrong base once in two, he them thus remains 1000 photons. For example, they use 250 photons to calculate their probability of error. They communicate the results through the public channel, and find P error .

Communication of these results is not a problem if they reject the exposed photons to build the key. Suppose 25 photons out of those 250 are fake when they used the same base.

So:

$$P_{error} = \frac{25}{250} = 0.1$$

If this probability is less than a terminal that will be calculated, they will use the remaining 750 photons for the key. Otherwise, they know Eve has too much information and they start the protocol again.

So we have, by quantum mechanics only, a safe way to transmit a key (or at least if we manage to send it, we are sure that Espion does not have enough information to be able to use it).

3.2 Chaos Theory in cryptography

Chaotic cryptography is recent and has demonstrated security reliability as long as it has demonstrated high resistance to cryptanalysis.

In this paragraoh, we will show how to exploit chaos theory for cryptography and secure transmission. Also, we will focus on simple polynomial mapping that presents a chaotic behavior that results from the simple non-linear dynamic equation. This type of mapping is called a logistics map.

3.2.1 The Chaos theory

If a butterfly flaps its wings in South Africa, can it cause a tornado in Algiers?

Chaos theory attempts to answer such confusing questions. The discovery of randomness within seemingly stable physical systems has become a science proclaiming that the Universe is far more unpredictable than we had imagined.

This "Overview" of chaos explains how chaos manifests itself in a series of events, from the fluctuations of animal populations to the ups and downs of the financial market. He also analyzes the roots of chaos in modern mathematics and physics, and explores the links between chaos and complexity, the unifying theory that suggests that any complex system evolves from a few very simple rules.

Definition 3.2

Chaos is a complex non-linear phenomenon, which depends on several parameters and is characterized by extreme sensitivity to the initial conditions.

Chaotic systems are systems whose trajectories evolve in a bounded region with a stable character but without converging to a fixed point or a limiting cycle. These trajectories that remain dense in this region are very sensitive to the initial conditions.

The solutions of nonlinear differential equations cannot be calculated with analytical accuracy because there is no analytical resolution method for these equations,except for certain particular classes.They are then determined numerically and the behavior of the system is analyzed by simulation.

3.2.2 Properties of Chaotic systems

Among the main features that evoke chaotic behavior, the following properties may be used:

- ***Determinism and unpredictability:***

  In the case of deterministic systems, theoretically knowledge of initial state of the input, and of the model predicts their future state. However, it is difficult to calculate the theoretical analytical solution of some non-linear systems, which is the case for deterministic chaotic systems, because they are characterized by sensitivity to initial conditions, which a simple measurement error or a simple rounding leads to different solutions, which make them unpredictable, so predictability is no longer related to determinism.

- ***The sensitivity to the initial conditions:***

  The sensitivity to the initial conditions is one of the fundamental characteristics of the chaotic systems explained by Lorenz in his famous quote "the butterfly effect". A slight variation of initial conditions on a chaotic system results in two trajectories that are initially close, then diverge exponentially, then the two trajectories are incomparable, making chaotic systems unpredictable in the long run. It is therefore clear that the slightest error or inaccuracy on the initial condition does not allow us to decide at all times that it will be the trajectory actually followed. To illustrate this property, we take as an example the Lorenz system described by the folowing system:

$$\begin{cases} x^{'} = & a(y-1) \\ y^{'} = & b-y-xz \\ z^{'} = & xy-cz \end{cases} \tag{3.6}$$

With: (x,y,z)*: state vector.* (a,b,c)*: are the parameters of the system of Lorenz.*
$(a=10;b=28;c=83)$*: are the values of the parameters for which the system has a chaotic behavior.*
For two very close initial conditions:

$$\begin{cases} (x_{01},y_{01},z_{01}) = (0.1,0.1,0.1). \\ (x_{02},y_{02},z_{02}) = (0.1001,0.1001,0.1001) \end{cases}$$

We get the figure:

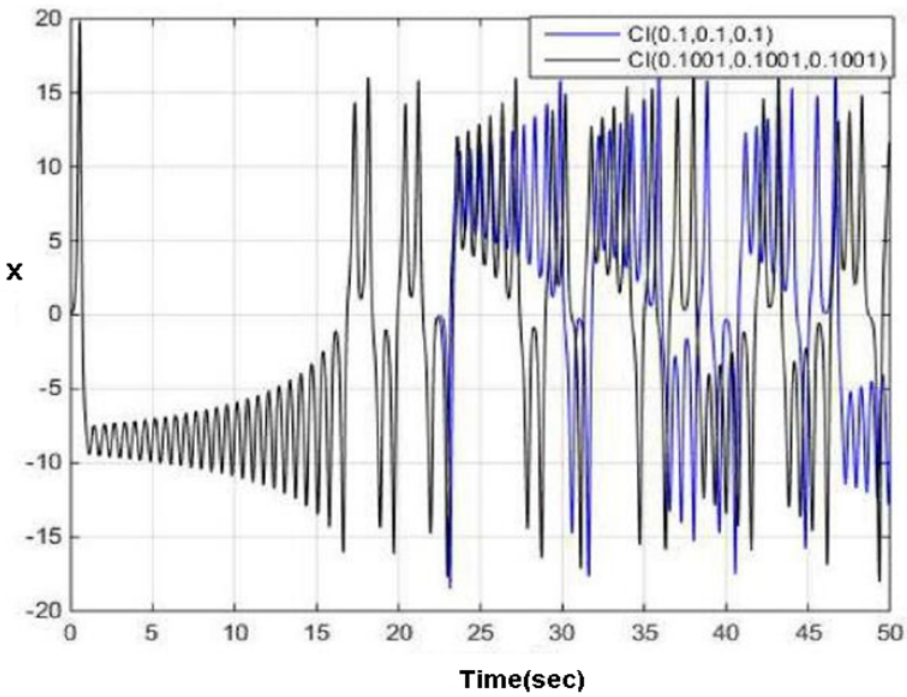


Figure 3.2: Evolution over time for two initial conditions very close.

Figure (3.2) illustrates the sensitivity to the initial conditions of chaotic systems for two very close initial conditions. Initially the two phase trajectories evolve in the same way, then they diverge.

- ***Randomness:***
  Although chaotic systems are deterministic, all states of a chaotic system have random aspects, as can be seen in Figure (4.2). No periodicity is apparent.

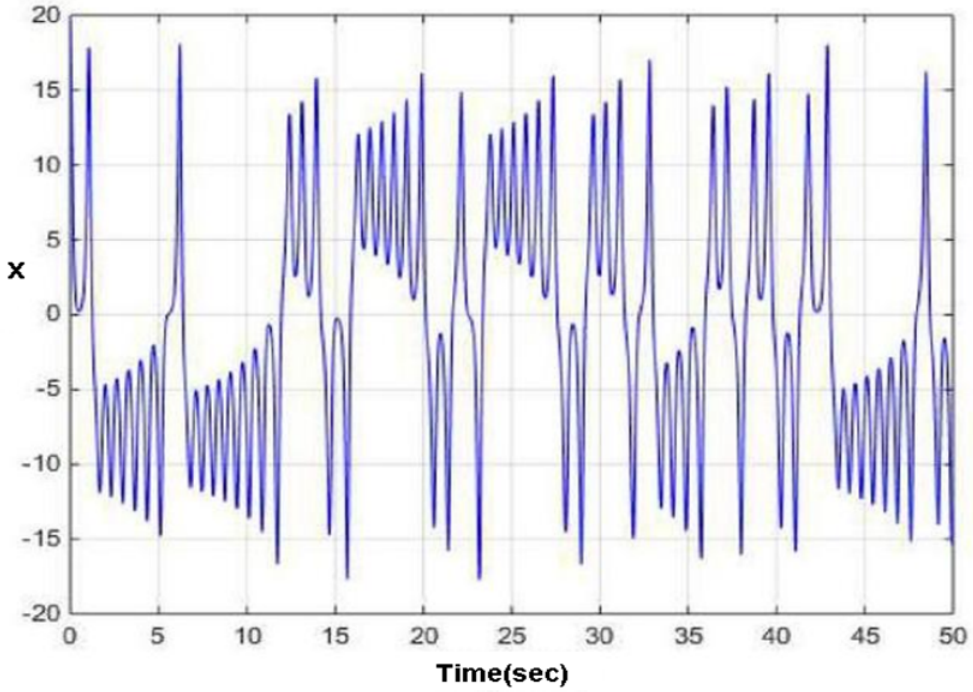


Figure 3.3: The random aspect of Lorenz's system.

- ***Strange attractor:***
  When Edward Lorenz graphically undertook the solution of his system (3.1) by means of his computer, drawing two curves with two sets of initial conditions very close, he expected the two curves to diverge, but to his surprise, the two curves were more or less identical, they looked like two butterfly wings.

  Physicist David Ruelle, who studied the issue, called this figure a "strange attractor," noting that the trajectories never intersect, and although they seem to evolve randomly, they form indisputably recognizable figures.

  Therefore, when the regime of a system is chaotic, the corresponding attractor is a strange attractor that has different topological properties than a simple attractor. A strange attractor is characterized by its catchment area and fractal dimension.

- ***Solution Limitation:***

  All solutions of chaotic systems are globally limited solutions. [27] Indeed, the trajectory of the chaotic system observed in phase space remains confined to a well-defined region (strange attractor), after a transient period of variable duration.

  Chaotic systems can be described as stable if their initial conditions are taken in the basin of attraction, that is, the trajectories do not diverge towards infinity but converge on the strange attractor.

In the study of non-linear systems the following situations occur: - Asymptotic stability: trajectories converge to a fixed point. - Stability limit (sinusoidal oscillatory response): trajectories converge towards a limiting cycle. - Stability limit (bounded response): trajectories converge towards a strange attractor. - Instability: Diverging trajectories to infinity.

3.2.3 Path to Chaos

Varying a system parameter can change its behavior. It can change from a stationary state to a periodic state and become chaotic. There are several scenarios that describe the transition from fixed point to chaos. Evolution is done by discontinuous changes called bifurcation.

Feigenbaum rediscovered a road to chaos that had been discovered in the 1960s by Myberg. This route is called the "period doubling cascade". This scenario is observed with the logistic sequence. This is the best known example of a none-linear system for which a bifurcation diagram can be drawn.

His equation is given as follows.

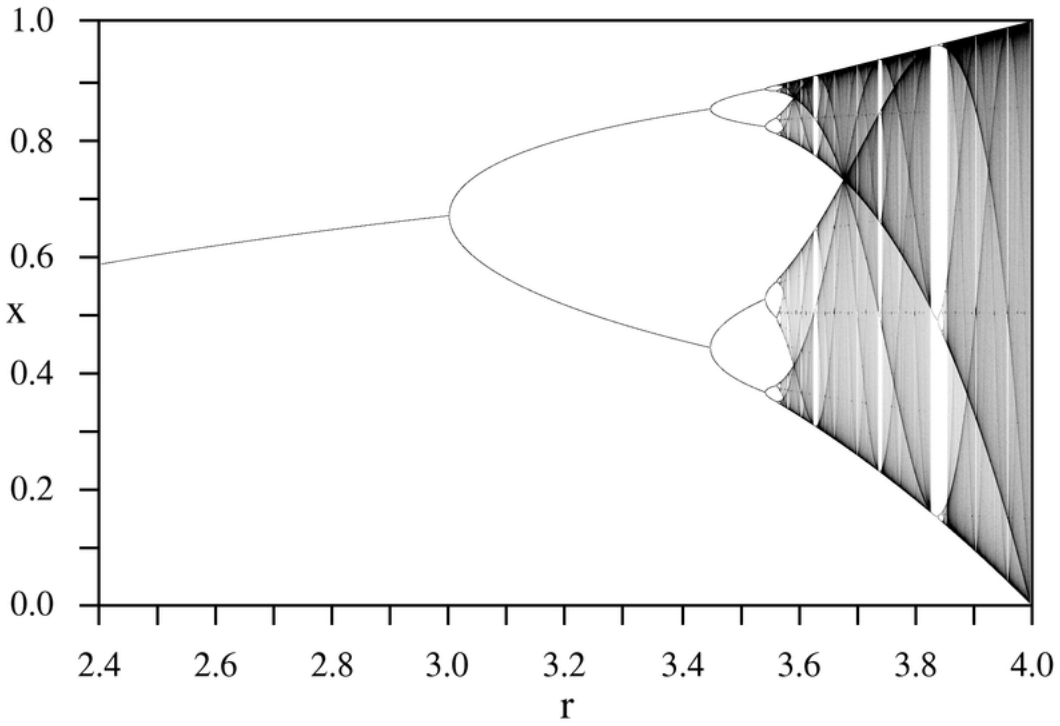


Figure 3.4: Diagram of bifurcation in the logistic map.

3.2.4 The logistic maps

En mathématiques, une suite logistique est une suite réelle simple, mais dont la récurrence n'est pas linéaire.

It's reccurence is given by:

$$x_{n+1} = \mu x_n(1 - x_n) \;\; ; \;\; 3 < \mu < 4 \tag{3.7}$$

This reccurence was popularized by the biologist Robert in 1976.

Depending on the value of the parameter μ *(*$0 \leq \mu \leq 4$ *to ensure that the values of* x *remain in* $[0;1]$*), it generates either a convergent sequence, a series subjected to oscillations, or a chaotic sequence.*

If $\mu \simeq 3.57$*, the chaos settles. A slight variations in the inicial value lead to a radically different difference.*

3.2.5 The sensitivity to initial conditions

A very small changes in the initial conditions can gives radically different in their final state, we see this in the following example (see Figure 3.5).

Those graphs correspond to the variation of same sequence (x_n) *showed in* (3.7)*. If we fixe the parameter* $\mu = 3.90$ *and take two initial values* x_0 *and* x_0' *withe a little changing in its values (in the ordre of* 10^{-2} *). In our exemple we have choice* $x_0 = 0.100$ *and* $x_0' = 0.99$*.*

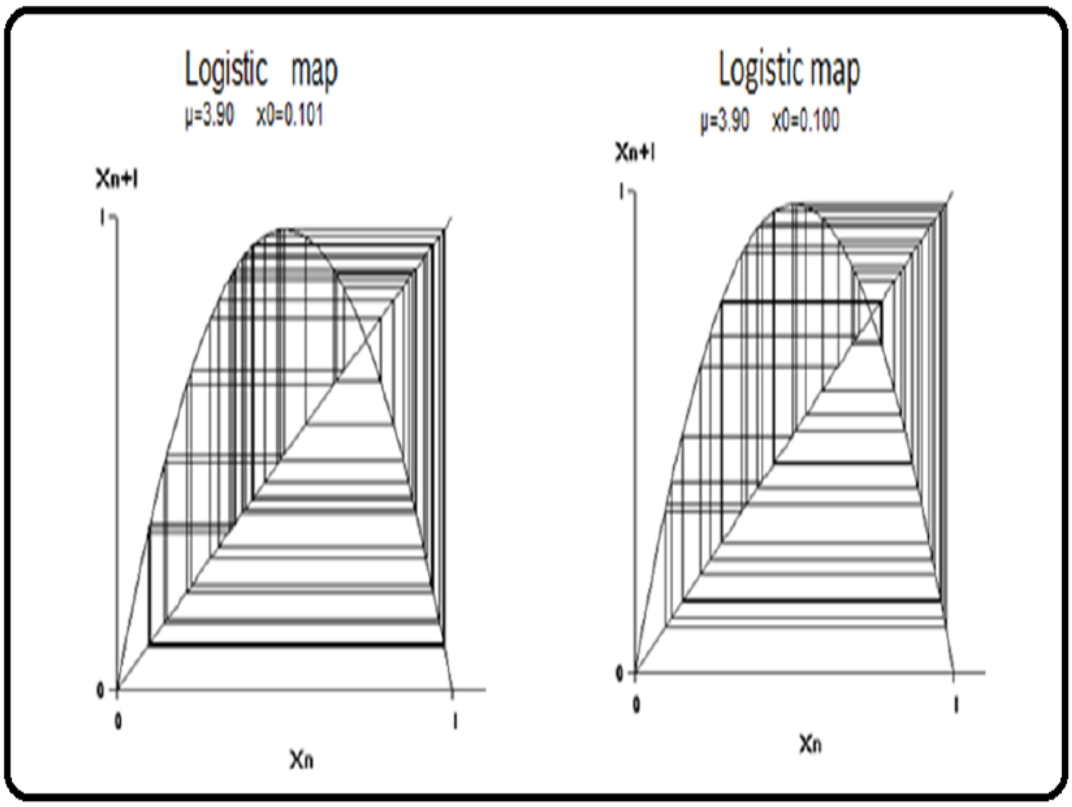


Figure 3.5: Different states of a same logistic map changing in their initial state

In Figure 3.5, we show that the two logistic map trajectories move away from the beginning until some orders n for the first case and n' for the other, and we get a chaotic phenomenon. [10].

Chapter 4

Key exchange protocols

After the presentation of Chaos and quantum theory and that based on elytic curves and matrices and their most used protocols in cryptography, we pass in this chapter to present a some famous protocols for charing keys that combines many types of cryptography to have a highly secure key.

4.1 Shamir's secret sharing Protocol

The sharing of secret used to secure a (sensitive) data in a distributed way, it allows to decentralize the risk, this system consists in sharing the secret S and sending the shares $S_1, S_2, ..., S_n$ to the persons concerned $P_1, P_2, ..., P_n$ so that certain subsets of these persons (authorized groups) can recover the secret.
All authorized groups are called "access structures".

Secret sharing at threshold k

Let n, k be two positive integers with $k \leq n$.

• *(k, n) threshold secret sharing is a special scheme which enables to distribute n shares and reconstruct the secret from k shares or more while no group of $(k-1)$ or fewer can do so.*

Perfect scheme

• *A perfect (k, n) threshold secret sharing must involve the two properties:*

1. *Correctness (recoverability): Any set of at least k shares can reconstruct the secret.*
2. *Secrecy (perfect privacy): any fewer than k shares get absolutely no information on the secret.*

In [3, 4], it is proved that Shamir's scheme is not always perfect.

The sharing of secret by Shamir's protocol

The first secret sharing by threshold scheme was proposed by Ali Shamir in 1979. Based on the principle of polynomial interpolation of Lagrange in a two-dimensional plane, this diagram has been the basic subject of the majority of contemporary research work in the domain of sharing ryptographic secrets.

Shamir's method consists in: The distributor D chooses a finished field $K = F_p$ *of cardinal p prime* $(p \neq 2)$ *with* $k \leq n \leq p-1$.
Let $P = \{p_1, p_2, ..., p_n\}$ *all participants*

Secret Distribution Phase

D considers a secret $S \in F_p$ *and randomly selects* $k-1$ *coefficients* $a_1, ..., a_{k-1} \in F_p$ *and forms the polynomial:*

$$f(x) = a_{k-1}x_{k-1} + ... + a_1x + a_0; with \quad a_0 = S.$$

D selects n separate elements $x_1, ..., x_n \in F_p - \{0\}$ *respective participant(public) indices* $\{p_1, p_2, ..., p_n\}$ *then calculates the unit* $S_i = f(x_i)$ *and transmits to* p_i , $1 \leq i \leq n$.

Reconstruction's Phase

The k participants combine their share to obtain the secrets by resolving a linear syetem.

Example 4.1

Let the Shamir system of threshold $k = 3$ *and* $K = F_5$.
Put $f(x) = x^2 + 2x + S, S \in K$. *Let's take* $S = 3$.

x_i	1	2	3	4
$f(x_i)$	1	1	3	2

To calculate S from the 3 units: $s_1 = 1, s_2 = 1, s_4 = 2$
Put: $f(x) = a_2x^2 + a_1x + S$

$$\begin{cases} f(1) = 1.....(1) \\ f(2) = 1.....(2) \\ f(4) = 2.....(3) \end{cases} \Rightarrow \begin{cases} (1)+(2) : 3a_1 + 2S = 2 \\ (1)+(3) : 2a_2 + 2S = 3 \\ (2)+(3) : a_1 + 2S = 3 \end{cases} \Rightarrow \{a_1 = 2a_2$$

so the secret key: $S = a_0 = 3$

4.2 Lagrange's secret sharing Protocol

Secret Reconstruction Phase

k or more participants can calculate S if we solv a system of linear equations or we use the Lagrange- interpolation method: $x_{i_1}, ..., x_{i_k}$ *and their respective shares:* $S_{i_1}, ..., S_{i_k}$ *The formula:*

$f(x) = \sum_{j=1}^{k} S_{i_j}.l_j$; *when :* $l_j = \prod_{h \neq j} \frac{x - x_{i_k}}{x_{i_j} - x_{i_k}}$ *This is called the Lagrange interpolation formula. S is calculated by:*

$$S = f(0) = \sum_{j=1}^{k} S_{i_j}.l_j(0).$$

Example 4.2

The previous example:

x_i	1	2	3	4
$f(x_i)$	1	1	3	2

By Lagrange interpolation:

Put: $f(x) = S_1 l_1 + S_2 l_2 + S_4 l_4$; *when:*

$$l_1 = \frac{(x-2)(x-4)}{(1-2)(1-4)}$$

$$l_2 = \frac{(x-1)(x-4)}{(2-1)(2-4)}$$

$$l_4 = \frac{(x-1)(x-2)}{(4-1)(4-2)}$$

So; $S = f(x) = 1.\frac{1}{3}(0-2) + 1.(\frac{-1}{2})(0-1)(0-4) + 2.(\frac{1}{6})(0-1)(0-2) = 3 \Rightarrow S = 3$

4.3 Protocol of Diffie-Hellman to exchange Keys

In cryptography, Diffie-Hellman protocol, named according its authors Diffie Whitfield and Hellman Martin, is a method published in 1976, whereby two agents, can agree on a number (which they can use as a key to encrypt the next conversation) without a third agent named Eve being able to discover the number, even after listening to all their exchanges. This idea earned the two authors the Turing Prize in 2015.

Principle explained with colors

Let's first give an intuitive explanation by making an analogy with colors. The goal is for Salah and Brahim to agree on a secret color, without Emine being able to know it. This explanation is pictorial and has no practical meaning, but allows to understand the essence of the protocol of Diffie-Hellman. It is assumed that agents can mix colors, but that it is difficult (especially for Eve!) to extract the colors used to make a mixture. The principle is as follows.

1. *Salah and Brahim first choose a common painting, here yellow. This color is known by all, including the intruder Emine.*

2. *Salah chooses another secret color (here red). He mixes the common paint and its secret color and gets orange. Salah sends the orange color to Brahim. The orange color is known to Emine.*

3. *Brahim does the same: he chooses a secret color (here cyan) which he mixes with the common paint and he gets blue. Brahim sends his blue color to Salah. The blue color is known to Emine.*

4. *Salah takes the received color (blue) which he mixes with its secret red color. He gets a brown color.*

5. *Brahim takes the received color (orange) and mixes it with its secret cyan color. He gets the same brown color.*

At the end of the protocol, Salah and Brahim have the same brown color, which represents the shared secret color. Assuming it is difficult for Emine to extract the colors used to get the public colors orange and blue, Emine does not know the final brown color.

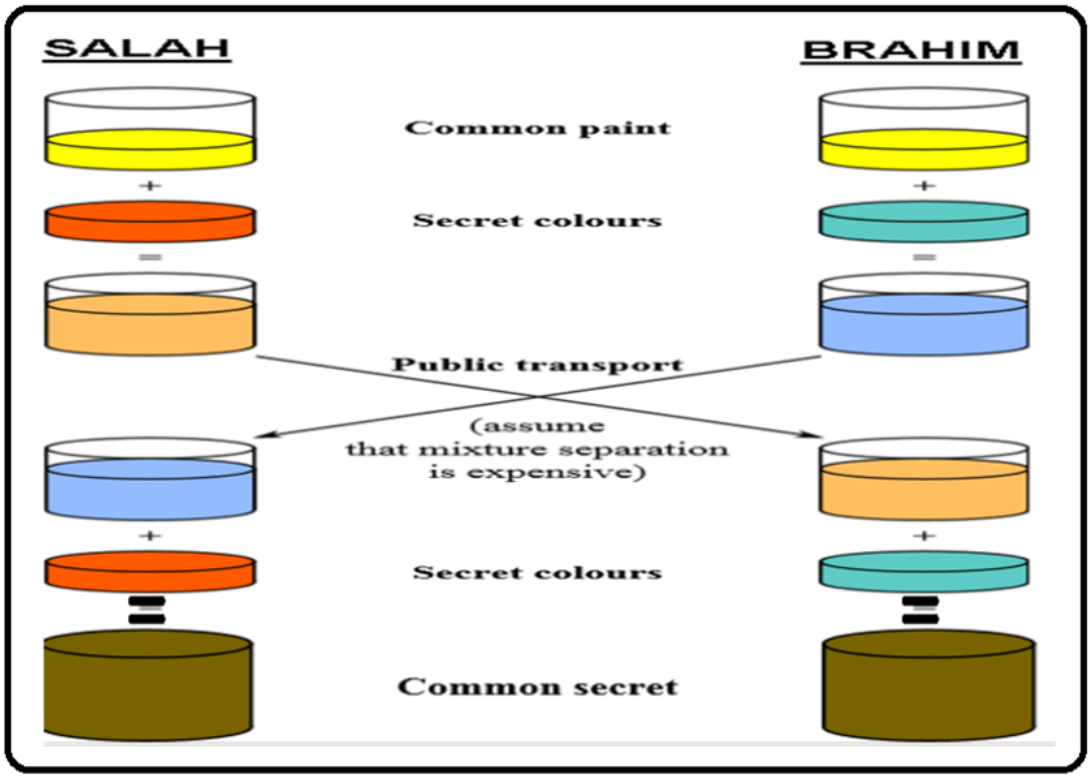


Figure 4.1: Conceptual illustration of Diffie-Hellman system

4.3.1 The protocol of Diffie-Hellman on $\frac{\mathbb{Z}}{p\mathbb{Z}}$

In the original principle described below, a prime number p is chosen. The «colors» are modulo p numbers. The mixture of two colors consists in raising a number to a certain power modulo p. To find the colors used in a mixture is to reverse the exponentiation, which is a difficult algorithmic problem.

Original principle

We describe the original principle:

1. *Salah and Brahim choose p = a prime number, and g = a generator of the group $\frac{\mathbb{Z}}{p\mathbb{Z}}$ strictly smaller than p (they may also, as shown in the figure 5.2, decide on this choice only at the time of the exchange and communicate it to each other in plain language, which does not improve Emine's chances);*
2. *Salah chooses a = random number , and sends Brahim the number $A = g^a mod[p]$ ("g power a modulo p");*
3. *Similarly, Brahim randomly selects a number b, and transmits the number $B = g^b mod[p]$;*
4. *Salah, with the number B received from Brahim, calculates $B^a mod[p]$. So he gets the number: $g^{ba} mod[p]$;*
5. *Brahim does the analog calculation with the number A received from Salah: $A^b mod[p]$. It gets $g^{ab} mod[p]$, which is the same number as Salah.*

At the end of the protocol, Salah and Brahim both get the number $g^{ab} mod[p]$ but not Emine. Since it is difficult to reverse exponentiation in a finite field (or on an eliptic curve), that is, to calculate discrete logarithm, Emine cannot discover or calculate $g^{ab} mod[p]$. Salah and Brahim found a common secret key without ever exchanging it and without anyone being able to calculate it.

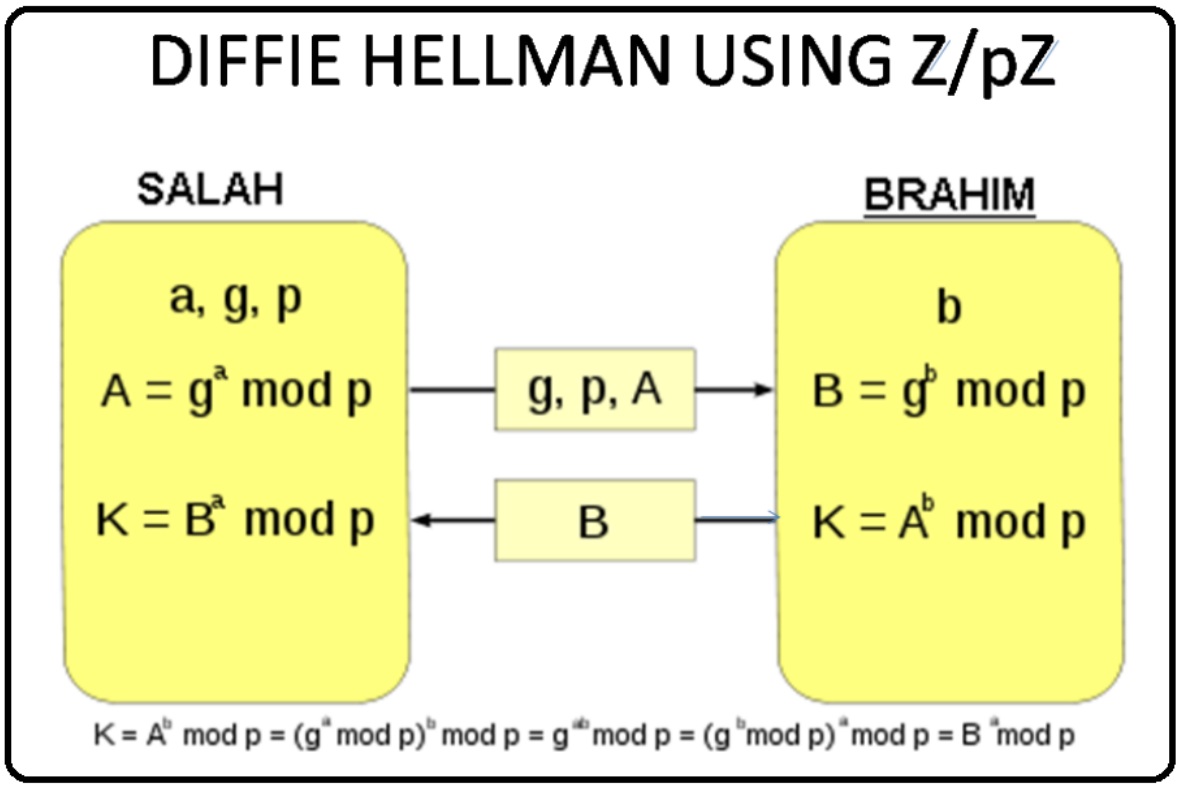


Figure 4.2: Principle of Diffie-Hellman system (the chosen group here is $\frac{\mathbb{Z}}{p\mathbb{Z}}$)

In the description above, Salah and Brahim work in the finite field $\frac{\mathbb{Z}}{p\mathbb{Z}}$, they will exchange modulo p numbers. Generally, the Diffie-Hellman protocol is generalized to a cyclic finite group (instead of agreeing on a prime number, they agree on a finite group). This finite group may be a finite field, of which they only use multiplication, or an eliptic curve.

Salah			Brahim		
Secret	Calculate	Public	Public	Calculate	Secret
		p, g	p, g		
a					b
	$A = g^a[p]$	A	(receives)	$B = g^b[p]$	
		(receives)	B		
	$B^a[p] = (g^b[p])^a[p]$			$A^b[p] = (g^a[p])^b[p]$	

Table 4.1: Principle of a Diffie-Hellman key exchange

Example 4.3

1. *Salah and Brahim choose p = prime number and g =a generator. In our example, we take p = 23 and g = 5.*

2. *Salah chooses a private number a = 6, Brahim also chooses a private number b = 15*

3. *Salah sends to Brahim* $A = g^a[p] = 5^6[23] = 8$
4. *Brahim sends to Salah* $B = g^b[p] = 5^{15}[23] = 19$
5. *Salah can now calculate the secret key:* $B^a[p] = (g^b[p])^a[p] = 19^6[23] = 2$
6. *Brahim does the same and gets the same key as Salah:*$A^b[p] = (g^a[p])^b[p] = 8^{15}[23] = 2$

4.3.2 Diffie-Hellman Protocol on Eliptic Curves

Eliptic Curve Cryptography (ECC) is a public cryptographic system. The fundamental advantage of using eliptic curves for cryptographic purposes is that they appear to offer a significant level of security for a key size much smaller, which reduces processing costs.

In 1976, the Diffie-Hellman system was introduced by Diffie and Hellman to solve the problem of key distribution. The Diffie-Hellman system depends on the difficulty of calculate the discrete logarithms.

The Diffie-hellman system on elliptic curves (ECDH) is based on the problem of discrete logarithm on eliptic curves (ECDLP). This section presents the implementation of the ECDLP by Diffie-Hellman protocol for key exchange on an unsecured channel.

The shared of a key by ECC between two persons Brahim and Salah works as follows:

1. *Brahim select* d_A *= integer lower than "p". This is the private key (of Brahim). Brahim generates a public key:* $P_A = d_A.G$*, the public key = a point of* $E(a, b)$*.*
2. *The user(Salah) selects also a secret key* d_B *and he calculates the public key:* $P_B = d_B.G$*.*
3. *The Brahim user generates the private key from Salah's public key:* $K = d_A.P_B$*. Similarly, Salah generates the secret key from Brahim's public key:* $K = d_B.P_A$*.*

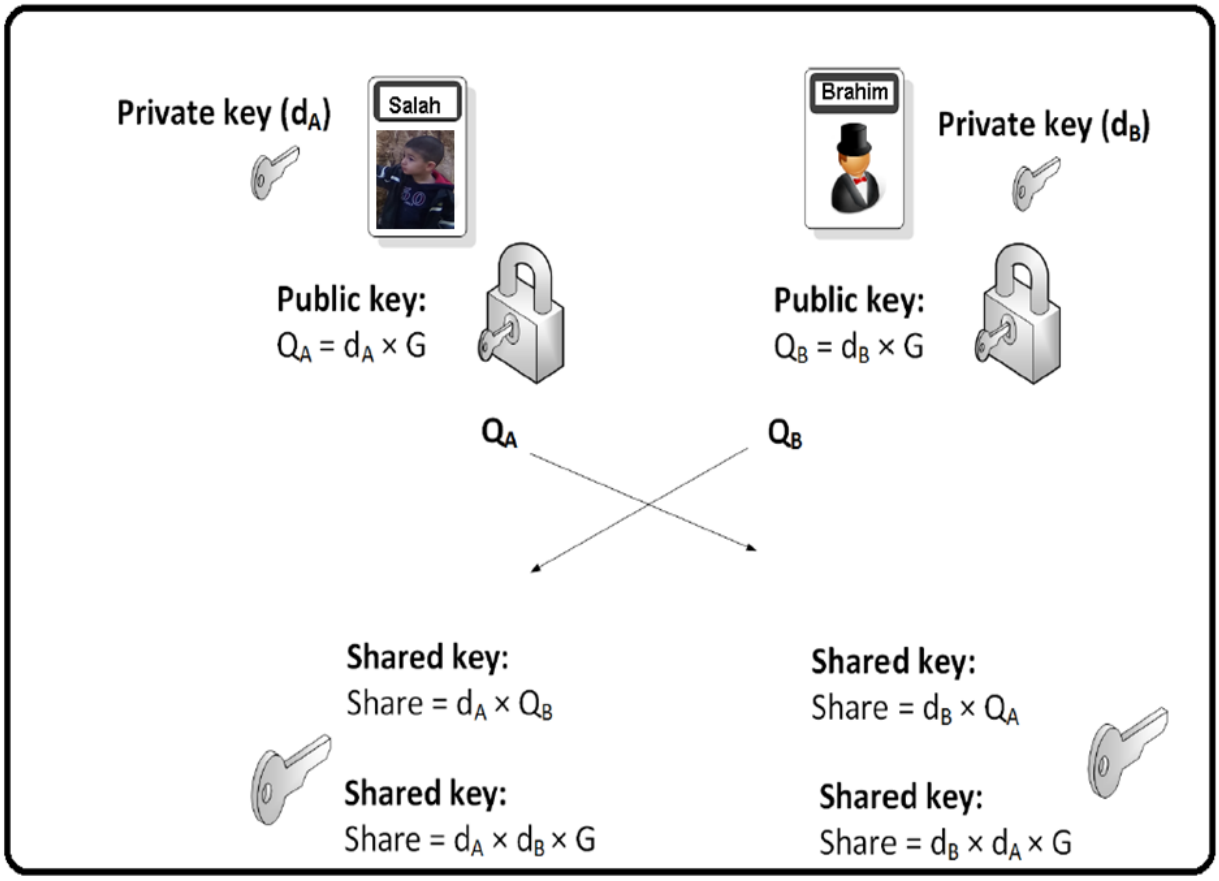


Figure 4.3: Diffie-Hellman exchange protocol using eliptic curves

Example 4.4

Messages are transmitted from the Brahim user to the Salah on eliptic curve $E_{(a,b)}(p) : y^2 = x^3 + ax + b$ *. We take* $p = 23, a = 1, b = 1$

We use point $G = (3,10)$ *was used as a generator of* $E_{(a,b)}(p)$*. The communication between users Brahim and Salah in the following steps:*

1. *Brahim select an integer "*$d_A = 4$*" lower than "23". This is the user's private key (Brahim). Brahim generates public key:* $P_A = d_A.G = 4.(3,10) = (17,3)$*, the public key is a point in* $E(a,b)$*.*

2. *The user(Salah) chooses a secret key* $d_B = 2$ *and calculates the public key* P_B*:* $P_B = d_B.G = 2.(3,10) = (7,12)$*.*

3. *The Brahim user generates the private key from Salah's public key:* $d_A.P_B = 4.(7,12) = (13,16) = K$*.*

   Similarly, Salah generates the secret key from the Brahim public key: $d_B.P_A = 2.(7,12) = (13,16) = K$ *.*

So $K = (13,16)$ *is a point in curve* $E(F_{23})$ *which is a common secret point of Brahim and Salah that will be used in symetric cryptsystem.*

Advantages and inconveniences

This makes the difference between eliptic curve based encryption algorithms versus integer based algorithms like RSA or El-Gamal is that, to overcome them, it is necessary to solve the problem of discret logarithms on the set of the eliptic curves, and not an analogous problem on integers.

These groups are more difficult to manipulate, they can differ a lot from each other if we change the parameters. Thus, solving proble of discret logarithms on eliptic curves is considered to be a more difficult problem than the similar problem in integer modulo n. Therefore, it is estimated that a 200-bit key (which measures, for eliptic curve, the size of the finite field K of that curve).

Calculations on eliptic curves are not very complicated to perform, this is a good advantage for smart cards where there is little power, and where the size of the key has a big influence on the performance.

The inconveniences are two fold. On the one hand, the theory of eliptic functions is complex, and still relatively recent. It is not out of the question that hatches get around the problem of discret logarithms. On the other hand, eliptic curve cryptography technology has been the subject of numerous patents around the world. This can make its use very expensive.

Discrete Logarithm Problem on Eliptic Curves

We have seen the different operations we can perform on eliptic curves, including scalar multiplication, which is frequently used during cryptographic calculations.

If someone spied on their exchange, they must know $E(a,b,K), P, K_AP, K_BP$ to be able to calculate K_AK_BP and a problem similar to the discrete logarithm problem must be solved but on an eliptic curve, what is not obvious it is necessary to be able to calculate K_A knowing P and K_AP. -Discrete logarithm is already difficult to resolve in well-known groups $(\frac{Z}{pZ})^*$. For groups of eliptic curves, this is even more difficult....

4.3.3 Diffie-Hellman Protocol using Circulant matrices

Either Brahim and Salah two people communicated between them on a secure channel, Brahim and Salah use the protocol of Diffie-Hellman scheme to obtain a shared secret key that difinites by a matrix, and this matrix use for cipher and decrypt images this key is extracted as follows:

Let K be a public random matrix of order n, then:

1. *Brahim chooses two circulant matrices M_1 and M_2 of order n;*
2. *Salah chooses two circulant matrices M_3 and M_4 of order n;*
3. *Brahim calculates: $M_1KM_2 = K_1$ and sends K_1 to Salah;*
4. *Salah calculates: $M_3KM_4 = K_2$ and sends K_2 to Brahim;*
5. *Brahim calculates : $M_1K_2M_2 = C_{Brahim}$;*
6. *Salah calculates : $M_3K_1M_4 = C_{Salah}$;*

and we get: $C_{Brahim} = C_{Salah} = C$: the same key.

Proof

As we have M_1, M_2, M_3 and M_4 are circulant matrices; and from the property of the commutativity of the multiplication of circulant matrices, we obtain:

$M_1M_3 = M_3M_1$ *and* $M_2M_4 = M_4M_2$, *so:*

$$C_{Brahim} = M_1K_2M_2 = M_1M_3KM_4M_2 = M_3M_1KM_2M_4 = M_3K_1M_4 = C_{Salah} = C.$$

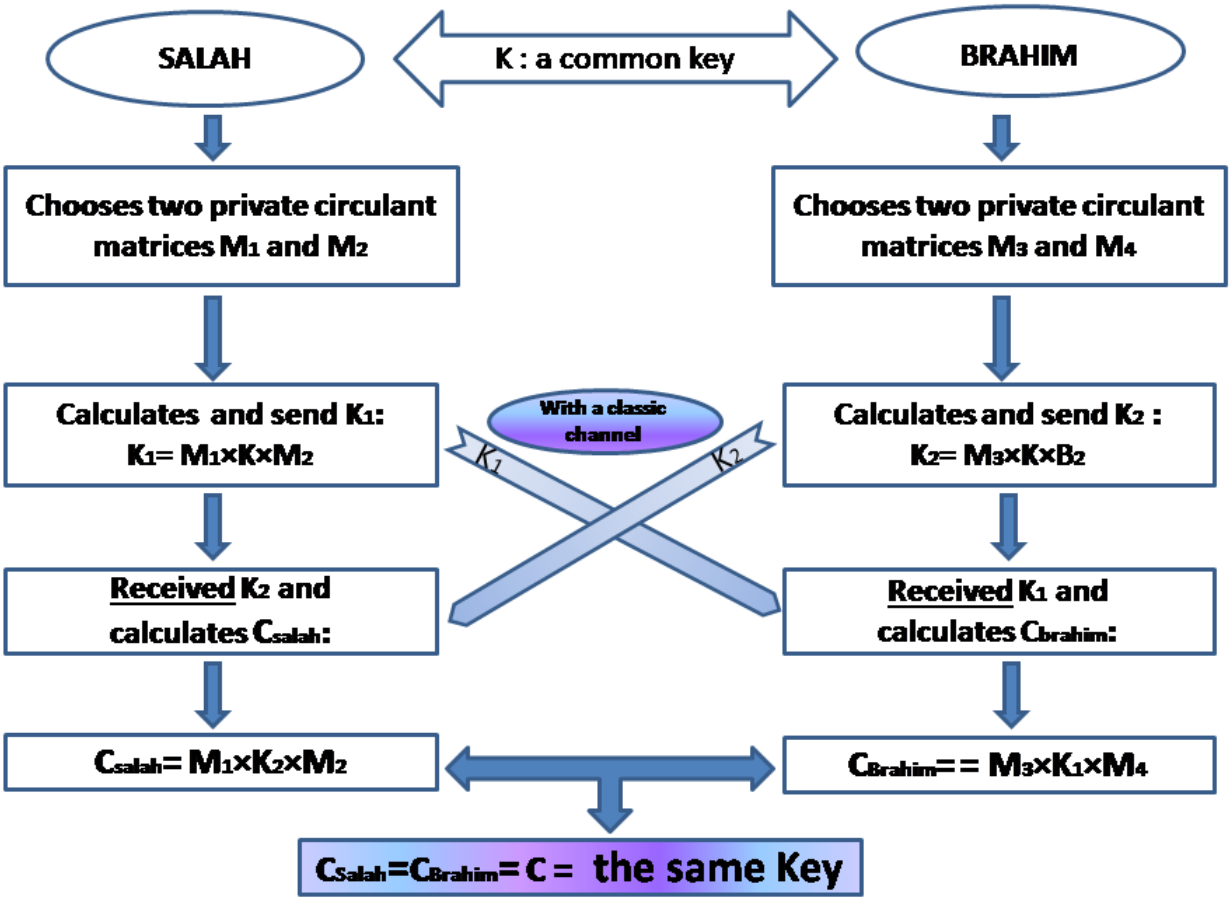


Figure 4.4: Principle of Diffie-Hellman system using circulant matrices

Advantages and inconveniences

- ***Advantages:***
  - *the calculations are very easy*
  - *the difficulty is how to find the private key from a product of three or more matrices*
  - *Select many private keys large enough to achieve greater security*
  - *there are no problems with the calculations even if the order of the matrices is large enough (because: the product of the circulant matrices is commutative)*

- ***inconveniences:***
  - *If you use many of the private matrices, you get a lot of time to do calculations*
  - *If we have the matrix of order n then we have n unknown pixel since each matrix depends on vector of order n.*

Example 4.5

Let's be the folowing four circulant matrices:

$$M_1 = \begin{bmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \\ 2 & 3 & 1 \end{bmatrix}, M_2 = \begin{bmatrix} 4 & 2 & 1 \\ 1 & 4 & 2 \\ 2 & 1 & 4 \end{bmatrix}, M_3 = \begin{bmatrix} 6 & 5 & 4 \\ 4 & 6 & 5 \\ 5 & 4 & 6 \end{bmatrix} \text{ and, } M_4 = \begin{bmatrix} 3 & 4 & 5 \\ 5 & 3 & 4 \\ 4 & 5 & 3 \end{bmatrix}$$

.

And we choose :

$$K = \begin{bmatrix} 2 & 1 & 3 \\ 4 & 5 & 6 \\ 7 & 2 & 4 \end{bmatrix}$$

.

1. *Brahim chooses two private circulant matrices M_1 and M_2 of order 3;*
2. *Salah chooses two private circulant matrices M_3 and M_4 of order 3;*
3. *Brahim calculates: $M_1KM_2 = K_1$ and sends K_1 to Salah:*

$$K_1 = \begin{bmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \\ 2 & 3 & 1 \end{bmatrix}.\begin{bmatrix} 2 & 1 & 3 \\ 4 & 5 & 6 \\ 7 & 2 & 4 \end{bmatrix}.\begin{bmatrix} 4 & 2 & 1 \\ 1 & 4 & 2 \\ 2 & 1 & 4 \end{bmatrix}$$
$$= \begin{bmatrix} 195 & 157 & 173 \\ 154 & 119 & 140 \\ 167 & 150 & 173 \end{bmatrix}$$

4. *Salah calculates: $M_3KM_4 = K_2$ and sends K_2 to Brahim:*

$$K_2 = \begin{bmatrix} 6 & 5 & 4 \\ 4 & 6 & 5 \\ 5 & 4 & 6 \end{bmatrix}.\begin{bmatrix} 2 & 1 & 3 \\ 4 & 5 & 6 \\ 7 & 2 & 4 \end{bmatrix}.\begin{bmatrix} 3 & 4 & 5 \\ 5 & 3 & 4 \\ 4 & 5 & 3 \end{bmatrix}$$
$$= \begin{bmatrix} 631 & 677 & 648 \\ 693 & 740 & 715 \\ 641 & 698 & 677 \end{bmatrix}$$

5. *Brahim calculates : $M_1K_2M_2 = C_{Brahim}$:*

$$C_{Brahim} = \begin{bmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \\ 2 & 3 & 1 \end{bmatrix}.\begin{bmatrix} 631 & 677 & 648 \\ 693 & 740 & 715 \\ 641 & 698 & 677 \end{bmatrix}.\begin{bmatrix} 4 & 2 & 1 \\ 1 & 4 & 2 \\ 2 & 1 & 4 \end{bmatrix}$$
$$= \begin{bmatrix} 31564 & 31612 & 31684 \\ 24724 & 24787 & 24829 \\ 29360 & 29429 & 29411 \end{bmatrix}$$

6. *Salah calculates :* $M_3K_1M_4 = C_{Salah}$*:*

$$C_{Salah} = \begin{bmatrix}6 & 5 & 4\\ 4 & 6 & 5\\ 5 & 4 & 6\end{bmatrix}.\begin{bmatrix}195 & 157 & 173\\ 154 & 119 & 140\\ 167 & 150 & 173\end{bmatrix}.\begin{bmatrix}3 & 4 & 5\\ 5 & 3 & 4\\ 4 & 5 & 3\end{bmatrix}$$
$$= \begin{bmatrix}31564 & 31612 & 31684\\ 24724 & 24787 & 24829\\ 29360 & 29429 & 29411\end{bmatrix}$$

And we get: $C_{Salah} = C_{Brahim} = C$*: the same key.*

4.4 BB84 Key Exchange Protocol

[ref BB84] In cryptography, the BB84 protocol is the first quantum key exchange mechanism to have been formalized, and in fact the first protocol in quantum cryptography. It was published in 1984 by Charles Bennett and Gilles Brassard1. The BB84 protocol has inspired many variants, which are based on the same fundamental principles: E90, E91, B92, SSP99, SARG04. If it is different from Ekert's protocol, both constructions are actually compatible and there are variants of BB84 using the principle of entanglement, especially to resist some of the known attacks.

4.4.1 Polarization and measurement

The BB84 protocol is based on the concept of linear polarization of a photon: a photon can be emitted with polarization on a given axis.

the photon with a probability $cos^2(\theta)$ *, where* θ *measures the angular deviation between the photon polarization axis and the filter's main axis.*

Thus, a filter exactly aligned with the photon polarization axis is transparent, while a filter forming a right angle with this axis is opaque; if the angle is 45° the probability that the photon passes the filter is 50 % . If this happens, the collapse of the wave packet ensures that the photon is now aligned with the filter axis, regardless of its previous polarization.

So we define two bases, noted + and $\times$ *, the latter corresponding to a rotation of the first by* 45^0*. Mathematically, we can fix:*

$$+ = \begin{cases}\overrightarrow{e}^{+}_{0} = (1,0)\\ \overrightarrow{e}^{+}_{1} = (0,1)\end{cases} \quad \text{, and: } \times = \begin{cases}\overrightarrow{e}^{\times}_{0} = (\frac{1}{\sqrt{2}}, \frac{1}{\sqrt{2}})\\ \overrightarrow{e}^{\times}_{1} = (\frac{-1}{\sqrt{2}}, \frac{1}{\sqrt{2}})\end{cases}$$

Suppose a photon emitted according to $\overrightarrow{e}^{+}_{0}$*, and a filter aligned according to* $f \in \{\overrightarrow{e}^{+}_{0}, \overrightarrow{e}^{+}_{1}, \overrightarrow{e}^{\times}_{1}\}$*, then the probability of measuring the photon is:*

$$\begin{cases}1 & (f = \overrightarrow{e}^{+}_{0})\\ 0 & (f = \overrightarrow{e}^{+}_{1})\\ \frac{1}{2} & (f = \overrightarrow{e}^{\times}_{0}, \overrightarrow{e}^{\times}_{1})\end{cases}$$

and after the measurement the photon (if not absorbed) is polarized according to f *.*

Procedure

The BB84 protocol consists of several steps, and allows two participants, Salah and Brahim, to establish a common cryptographic key.

One assumes an established communication channel, on which it is possible to emit selected polarization photons, the Salah and Brahim reference frames having been calibrated beforehand.

In the first step, Salah selects a random sequence of bits; for each bit $b \in \{0,1\}$, he randomly selects a base $t \in \{+,\times\}$ and emits a photon polarized according to e_b^t.

For his part, Brahim selects a base of random reception $r \in \{+,\times\}$ for each photon, and aligns its filter to e_1^r . The following illustration shows this first step in action:

Bit of Salah (b)	0	1	1	0	1	0	0	1
Base of Salah (t)	+	+	×	+	×	×	×	+
Polarisation of photon (e_b^t)	→	↑	↖	→	↖	↗	↗	↑
Base of Brahim (r)	+	×	×	×	+	×	+	+
Photon received by Brahim	→	↖ or ↗	↖	↖ or ↗	↑ or →	↗	↑ or →	↑

Table 4.2: Illustration an example of the first step of BB84 protocol

In the second step, Brahim sends Salah a list of the bases used at the reception. Salah responds by indicating which bases Brahim has correctly chosen, and only the corresponding photons are conserved2.

In the example above, this corresponds to the sequence →, ↖, ↗, →, that is to say to bits 0, 1, 0, 1. This sequence is called the "reconciled" or "breached" key.

Bit of Salah (b)	0	threw	1	threw	threw	0	threw	1
Base of Salah (t)	+		×			×		+
Polarisation of photon (e_b^t)	→		↖			↗		↑
Base of Brahim (r)	+		×			×		+
Photon received by Brahim	→	threw	↖	threw	threw	↗	threw	↑

Table 4.3: Illustration an example of the second step of BB84 protocol

In the third step, Salah and Brahim agree on a subset of the reconciled key that they will publicly reveal. They then compare whether they got the same bits in this subset: if so, they use the rest of the key to derive a cryptographic key.

If there is a disagreement, it can mean a transmission problem or an attempt to listen along the channel. Indeed, the non cloning theorem guarantees that in case of listening, the spy forces the photon on a basis (which is not necessarily that of Salah).

Thus, if the spy correctly guesses the base of Salah with a 50 % probability, then 25 % of the bits of the reconciliation key will disagree. In general, by sacrificing n displaystyle n n bits of the reconciliation key, Salah and Brahim can detect a possible spy on the channel with a $1-(\frac{3}{4})^n$ probability.

Thus, by building a long reconciliation key, one can achieve a sufficient level of security by sacrificing enough bits

Chapter 5

Application of key exchange for images encryption

Symmetric encryption is based on the use of the same key to encrypt and decrypt messages. The security of this solution is based on the fact that the key is known only by the sender and receiver of the message.

The importance of the key in an encryption algorithm; and the restrictions it implies. The key also needs to be able to take enough value so that a comprehensive attack-systematic testing of all the keys—is far too long to be carried out. This is called computational security.

In this chapter we proposed an improvement of an algorithm known in the field of key exchange (Diffie-Hellman protocol); we exchanged and built keys: the first is in the form of a circulant square matrix of order n generer by the terms of a logistic map after exchanging parameters has crossed a quantum chanal, using BB84 a known protocol in the quantum domain [10].

Then we use the first key to create a second key by using the circulant matrices because of their good properties especially that concerning the commutativity of the multiplications of these matrices.

This last key was used in the encryption and decryption of digital images.

5.1 Digital image theory

The image is a representation of an object by the graphic or plastic arts: sculpture, photography, drawing, film, etc...

Digital image editing is the manipulation of digital images using existing software such as Adobe Photoshop or Corel Paint.

*Image processing is a discipline of computer science and applied mathematics that studies digital images and their transformations, with the aim of improving their quality or extract information from it. [**?**, 29]*

5.1.1 Pixel and pixel per bit (Bpp)

Pixel

Contraction of the English expression "Picture elements": image elements, the pixel is the smallest point of the image, it is a calculable entity that can receive a structure and a quantification.

A digital image consists of a set of points called pixels (abbreviation for PICture Element) to form an image. All of these pixels are contained in a two-dimensional array comprising the image.

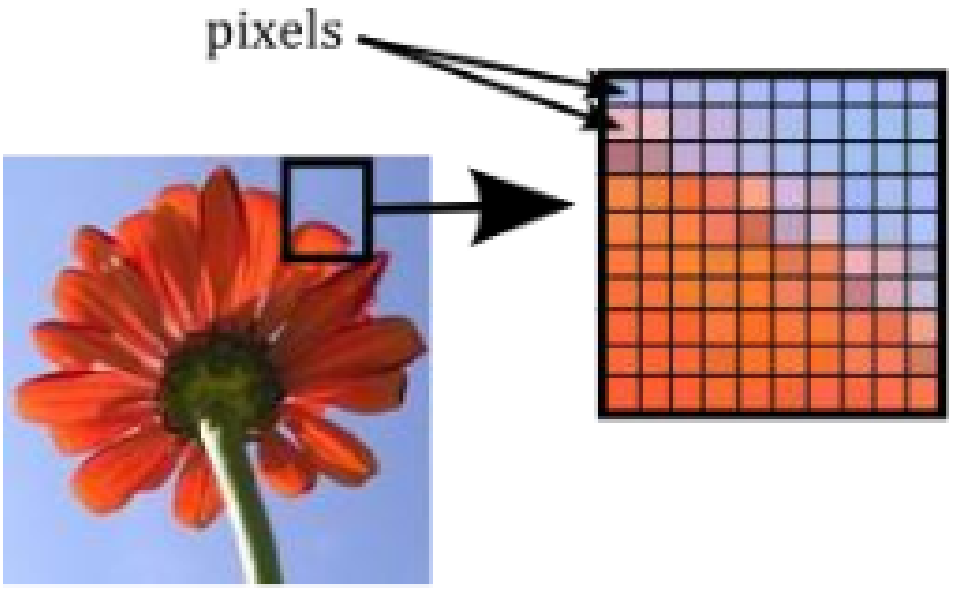


Figure 5.1: Presentation of Pixel

The definition of an image *is the number of pixels composing an image: it is the number of columns of the image that multiplies its number of rows [31]. For example: An image with 10 columns and 11 rows will have a definition of* 10x11 *meaning* 110 *pixels.*

Pixel per bit (Bpp)

It depends on the number of bits in an single pixel, ,It relies to the number of different colors , and the depth of every color.

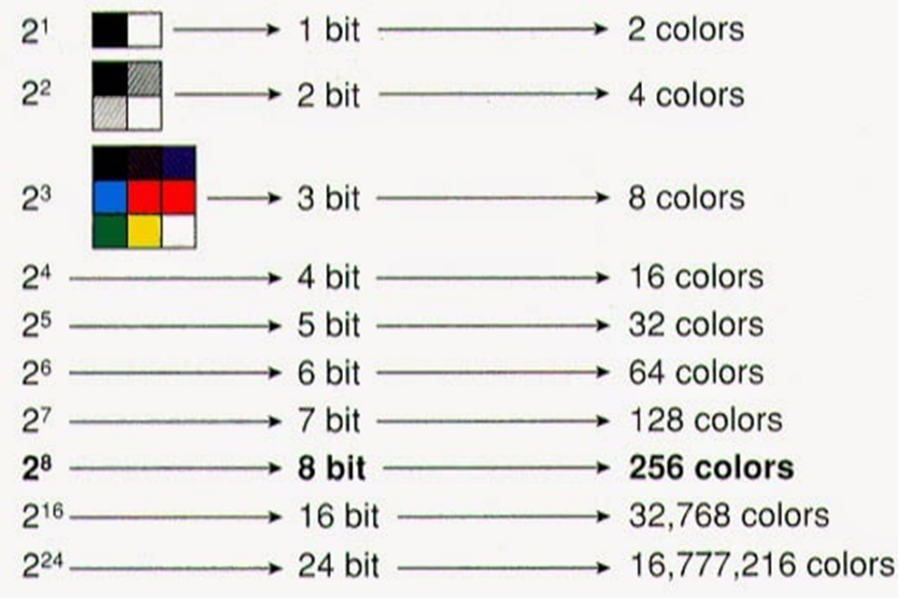


Figure 5.2: Pixel per bit representation (Bpp)

Interpreting Mathematics:

- *An image = matrix of numbers, which represents a signal.*
- *There are some tools for handling this signal. From a human perspective.*
- *An image contains several semantic information. The content must be interpreted at beyond the value of numbers. [50]*

Natural image ⟶ Several means of acquisition camera, microscope, tomography, infrared, satellite, ... Artificial image ⟶Several tools for image synthesis, virtual reality, scientific visualization, ...

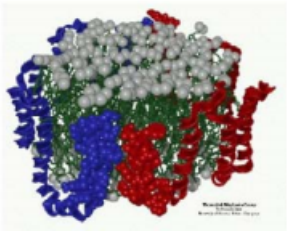


Figure 5.3: (a) Natural image (b) Artificial image (c) Artificial image

5.1.2 Types of digital images

In reality there are (03) three main types of images:



Figure 5.4: (a) Grayscale images (b)binary images (c)color images

- ***Grayscale images:***
  The gray level reverts to the light intensity value in a point. The pixel color can take values from black to white through a finite number of intermediate levels [11]. The depth of Bit (or color depth) is defined by the number of bits used to represent each pixel in grayscale. The greater the number, the greater the possible levels.

- ***Binary images:***
  They are simpler images, a pixel takes only two values: black or white. This is the type of image used to analyze a text composed of a single color. Each pixel is represented by a bit (0/1) with in general (0 for black, zero intensity and 1 for white, maximum intensity) [28, 50].

- ***Colour images:***
  The color representation is done in the same way as the monochrome images with however some peculiarities. In fact, we must first choose a representation model. We can represent the colours using their primary components. The systems emitting light (computer screens,...) are based on the principle of additive synthesis: the colors are composed of a mixture of red, green and blue (Model R.V.B.). [29, 30]

- ***Color image in RGB space:***
  Red-green-blue (RGB) refers to an optical processing system, an electronic display system, or an analog video signal coding system, or a computer colour coding system.

  Each pixel of a color image contains three numbers (r, v, b), each number is an integer between 0 and 255. [29]

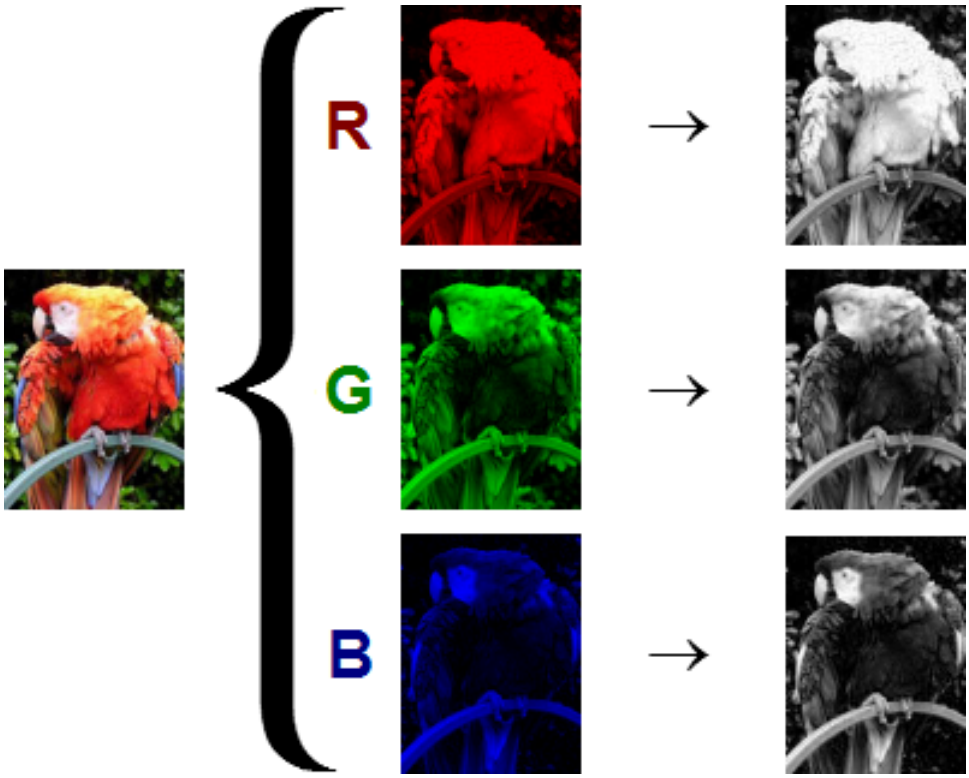


Figure 5.5: Colorful image in RGB space

RGB color model

RGB color model is an additive colour mixing method, which means that different light colours combine to form other colours. Additive synthesis generally uses three colored lights: one red, one green and one blue (RGB for red, green, blue). The addition of these three coloured lights in suitable proportions gives white light. The absence of light gives black.

Figure 5.6: Additive color synthesis

Acquisition of Digital Images

General operation to acquire a digital image is illustrated in the following figure:

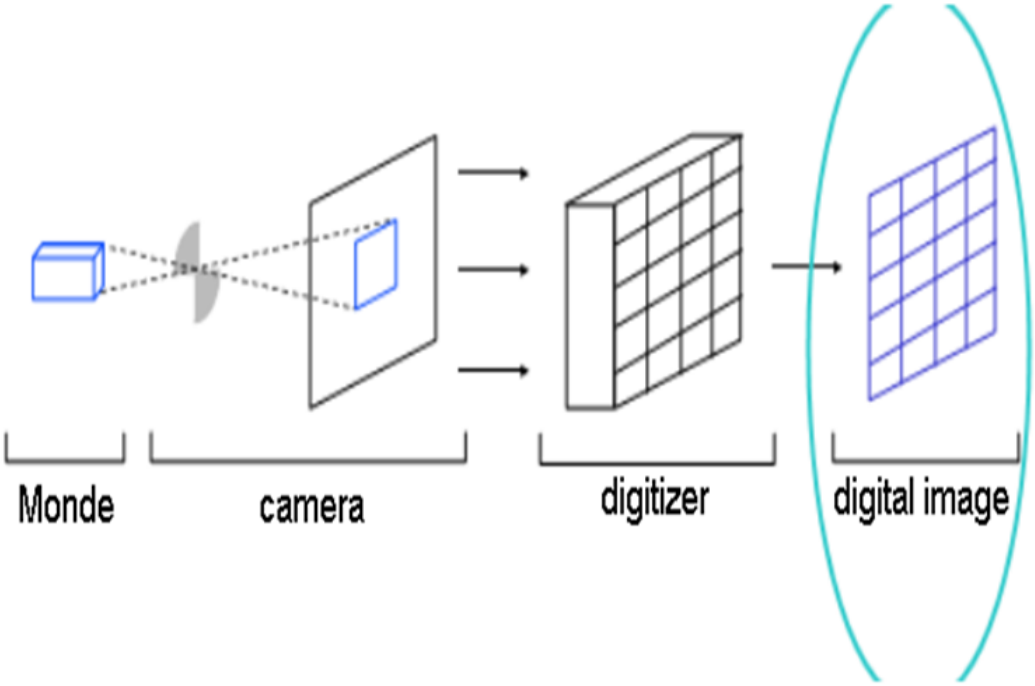


Figure 5.7: General process to acquire a digital image

5.1.3 How we convert an Image to a matrix

To convert an image to a matrix we should firstly Identifies the size of the Image (how many pixels in image).then, recognize the type of this image.

Binary Image:

*Consist of only two colors black and white, the best wat to describe it would be in a binary form meaning we can only use one or zero to describe the color (*0 *stand for black and* 1 *stands for white. and if we focus on our image and start filling in the values all the white pixels will become one and all the white pixels will become* 0*. and if we keep only the numbers in image we can see our matrix.[***?***]*

Example 5.1

●	○	○	○	○		1	0	0	0	0
○	●	○	○	○		0	1	0	0	0
○	○	○	○	●		0	0	0	0	1
○	○	○	●	○		0	0	0	1	0
●	○	○	○	○	⟹	1	0	0	0	0
○	●	○	○	○		0	1	0	0	0
○	●	○	○	○		0	1	0	0	0
○	●	○	○	○		0	1	0	0	0
●	○	○	○	○		1	0	0	0	0

Greyscale Image :

When image has many different colors and all are shades of gray in thi case the best color formay to describe this image would be grayscale so the grayscale format is using numbers any where from 0 to 255 to describe the itensity of black where onceagain 0 is black and 255 is white so it is the highet contrast with black .

- *black --→ 0*
- *white --→ 255*
- *gray --→ 1 – 254*

So ,we want to find out how we represent a color that's only 50 black which is the color we see in the very center for image .

*To calculate this we would have to devide our number of avaible values by two and because zero also represents a color which is black our tota number of avaible values would be 256 rather than 255 there-for 50 black in grayscale is represented by the value 128 which we can now also fill in but let's try to calculate a slightly more complicated percentage let's say we want to find out what black would look like first we subtract 15 percent and we get 85 percent then we will devide 100 by 85 to get the ratio, we need and then we will do the exact values by 1.1776 which is the ration we just got and the result is 217.68 which we can definitely round up and get 218. [**?**]*

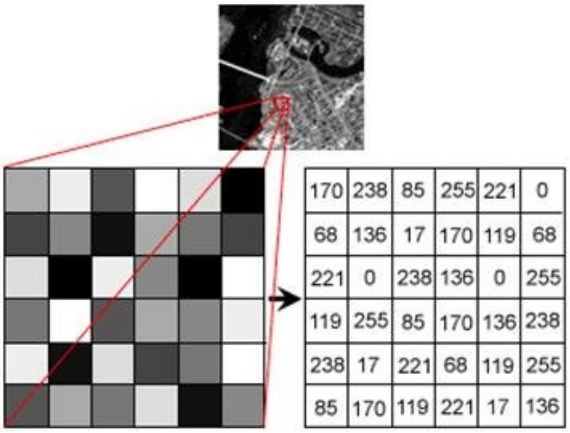


Figure 5.8: Figure represent how convert a greyscale Image to a matrix

RGB Image:

RGB stands for red, green and blue and it measures itensity of each of these colors on a particular pixel here we are also using values from[0-255] the only different is will be cheking across three different color channels and not just one .Let's say that we want to find out how we describe the color white in RGB , white represented by a set of 3 values 255 for red ,255 for green 255 for blue .

In this particular order ths is very important the same thing for black represented by a set of 3 values 0 for red ,0 for green 0 for blue .When ever we see an RGB color mix consisting of 3 identical values for example RGB777 , RGB505050 you will always be looking at a shade of gray and this is because no color is overpowering the other .

But if we want to represent the color green it will be (0, 200, 20) where 0 is red , 200 is green , 20 is blue .

Every RGB image has 3 different color channels we will need to multiply the Image by the amount of channels we get a single matrix with 3 dimensions first dimension holds the value for the red channel second dimension holds the value for green channel and third dimension hold the value for blue channel.

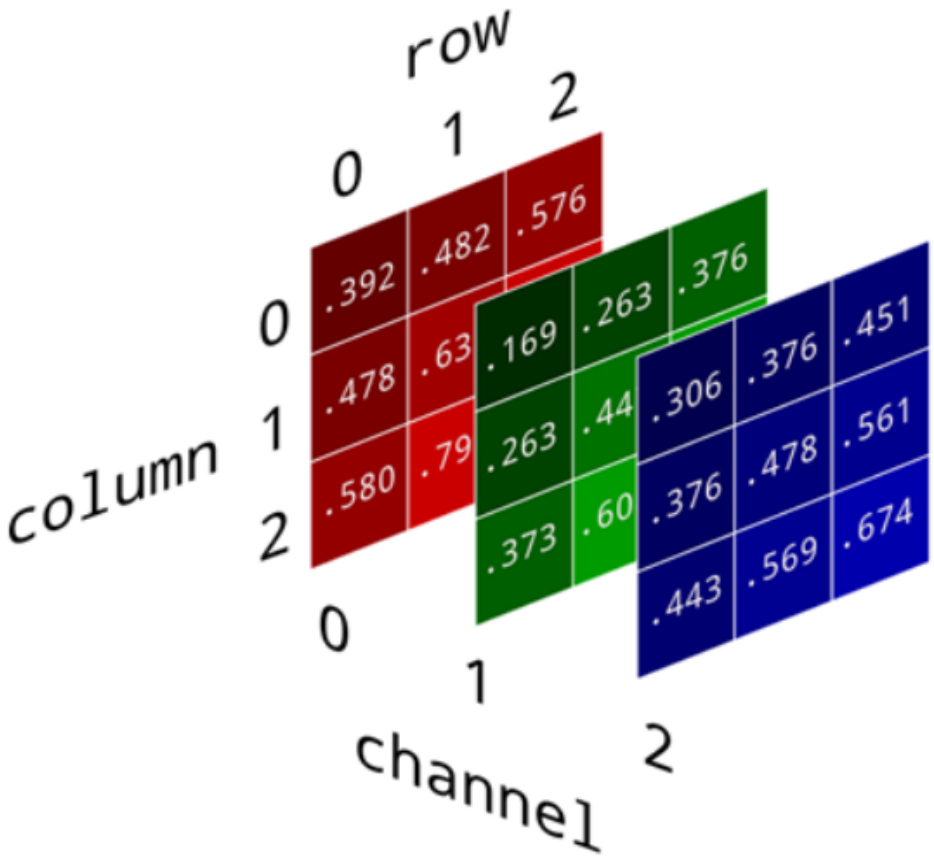


Figure 5.9: Figure represent how convert a RGB Image to a matrix

5.1.4 Image representation:

- *An image I is an LxH dimension matrix.*
- *Each element has an integer value in the range* $[N_{min}, N_{max}]$.
- *Number of bits required the representing grayscale in the "N" range is "K".*
- *The relationship between "K" and "N" is:* $N = 2^K$.
- *The representation of an image is by a number of bits b given by:* $b = L.H.K$

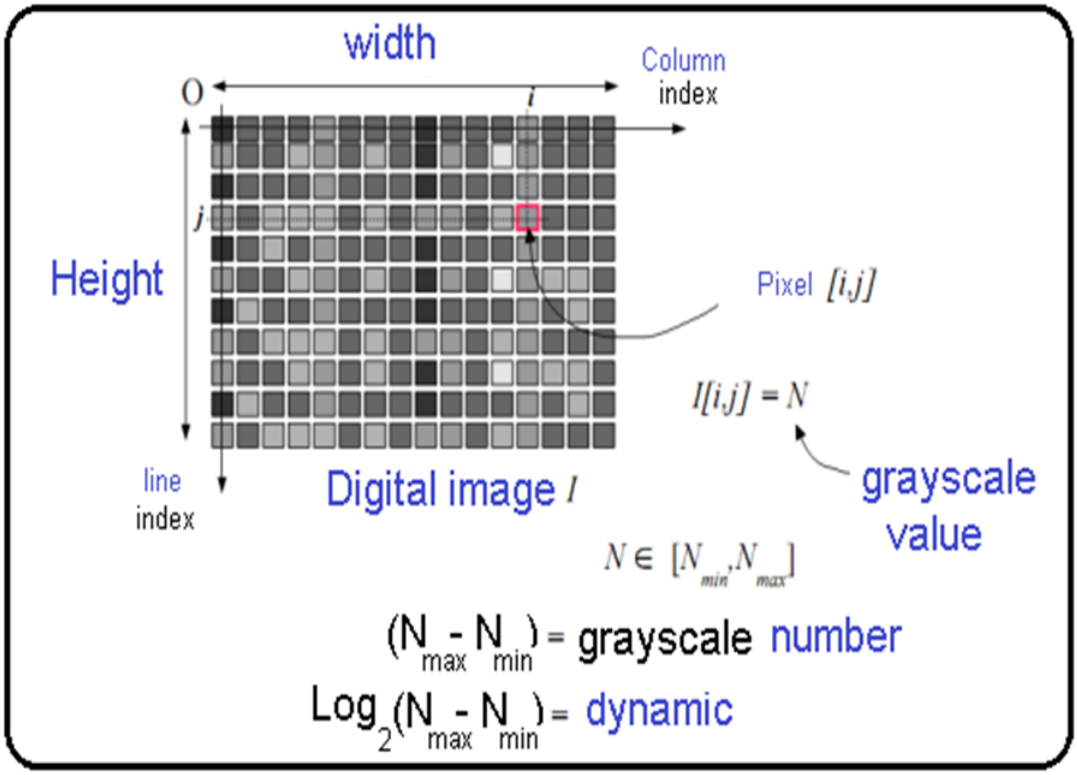


Figure 5.10: Image representation

We can distinguish between resolution mode and images:

1. *Spatial resolution: is the smallest discernible detail.*
2. *Tone resolution (grayscale): is the smallest discernible change.*

An image therefore has a spatial resolution of LxH pixel and a resolution of gray tones of K bits or N levels or tones.

5.1.5 The Matrix Images

A matrix image (or bitmap) is an image consisting of a set of points: the pixels. Each point has position and color information. Bitmap image format: BMP, GIF, PCX, JPEG, TIFF.

Digital photos and scanned images are of this type. [31, ?]

Advantages of matrix images

- *Bitmap images can easily be created and stored in an array of pixels representing the image.*
- *Easy to read/write pixel by image as a grid.*
- *Bitmap images can easily be displayed on a screen or be im- award-winning.*

Inconveniences of matrix images [28, 29]

- *Files can be very large (need for compression).*
- *Scale change problem (effect of stair steps or blur with interpolation).*
- *Image dimensions must be provided for interface resolution output (screen, printer).*

5.1.6 The Vector Images

Vector images are composed of geometric shapes that can be described mathematically. For example, a line will be defined by 2 points, a circle by a center and a radius. The processor is responsible for "translating" these forms into information interpretable by the graphics card (Word images, Publisher, CorelDraw - WMF format, CGM, etc). [31]

Advantage of Vector images

- *Suitable for storing images composed of geometric shapes.*
- *Can be easily resized.*
- *Ability to expand indefinitely without losing original quality.*
- *take up less space than a bitmap image.*

Inconveniences of Vector images [28, 29]

- *Difficult to store complex images such as photographs.*
- *Displaying a vector image may take longer than displaying a bitmap image of equal complexity.*

Figure 5.11: Matrix image and Vector image

5.2 Programming language (Matlab)

Matlab(or: Matrix Laboratory) is a scientific computational programming-language designed to make matrix computation simple to program and efficient in time.

Matlab and a software (for a fee) offering a graphical interface to a Matlab code editor, and a debugging tool to run programs in step-by-step mode. Matlab offers different frameworks (for a fee, called toolbox), offering advanced features to easily perform complex tasks (e.g., differential equation toolbox, aerospace toolbox).

Different use of of Matlab

- *Design, test and implement control systems.*
- *Collect, analyze and explore data, and automate testing.*
- *Design, optimize and test mechatronic systems.*
- *Used to devel algorithms .*
- *Makes simpler interfaces for the user.(graphical interface and in several applications like API Application Programming Interface), in cryptography...*

Simulink

The integration of virtual systems reduces reliance on prototyping hardware, and gives engineers virtual access to the system at any stage of the product development cycle. You can

use Simulink to model, simulate and analyze complex virtual systems that include physical hardware, embedded software, algorithms, and the environment in which the system operates.

5.3 Our first proposed scheme

We use a logistic maps, choosing two arbitrer parameters μ, x_0 with x_0 the initial term of the logistic map 3.7. *Using a quantium channal, applying the BB*84 *protocol, we exchange the encrypted key (μ, x_0). So, prospecters arrive to create a same circulant matrix generated by the vector $\langle x_1, x_2, \cdots, x_n \rangle$, when $(x_1, x_2, \cdots, x_n)$ are the terms of the logistic map.* (3.7).

Then, we work to generate an other key using the circulant matrices by applying the Diffie-Hellman protocol to obtain a second shared key that will be used to encrypt and decrypt of text or images.

And using the same idea we can using several logistic maps to get a good level of security.

Two intelocutors want to share some information:

First step:

Through the quantium channal

1. **With one logistic map:**

   - *Let $\mu(3 < \mu < 4)$ and, x_0 be two parameters, where, x_0 represente the initial term of the sequence* (3.7)*, this parameters will be exchanged between interlocutors through a quantium canel appliying the BB*84 *protocol.*
   - *After we have shared (μ, x_0), we use the logistic map given in* (3.7) *for calculating the n terms $x_1, x_2, \cdots, x_n$.*
   - *Then we create the folowing matrix*

$$Q = \langle (x_1, x_2, \cdots, x_n) \rangle = \begin{pmatrix} x_1 & x_2 & \cdots & x_n \\ x_n & x_1 & \cdots & x_{n-1} \\ \vdots & \vdots & \ddots & \vdots \\ x_2 & x_3 & \cdots & x_1 \end{pmatrix}$$

2. **Using three logistic maps:[1, 2]**

   - *Let $\mu_1, x_0^1, \mu_2, x_0^2 \mu_3$, and x_0^3 be six parameters, where, $\{\mu_i : 3 < \mu_i < 4$ forr $i \in \{1, 2, 3\}\}$ and $\{x_0^i : i \in \{1, 2, 3\}\}$ are the initial terms of sequences defiend in* (3.7)*, these parameters will be exchanged between the two interlocutors through a quantium channal appliying the BB*84 *protocol.*
   - *After we have shared those six parameters, we introduce the formula of logistic map defined in* (3.7) *to get the n terms of each sequence:*

$$\{x_1^1, x_2^1, \cdots, x_n^1\} \ , \ \{x_1^2, x_2^2, \cdots, x_n^2\} \ \text{ and } \ \{x_1^3, x_2^3, \cdots, x_n^3\}$$

- *So, we can generate the matrix:*

$$Q = \begin{pmatrix} x_1^1 & x_1^2 & x_2^2 & \cdots & \cdots & x_{n-2}^2 & x_{n-1}^2 \\ x_1^3 & x_2^1 & x_n^2 & \cdots & \cdots & x_{2n-4}^2 & x_{2n-3}^2 \\ x_2^3 & x_3^3 & x_3^1 & \cdots & \cdots & x_{3n-7}^2 & x_{3n-6}^2 \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots & \vdots \\ \vdots & \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ x_{\frac{n^2-5n+4}{2}}^3 & x_{\frac{n^2-5n+6}{2}}^3 & x_{\frac{n^2-5n+8}{2}}^3 & \cdots & \cdots & x_{n-1}^1 & x_{\frac{n^2-n}{2}}^2 \\ x_{\frac{n^2-3n+2}{2}}^3 & x_{\frac{n^2-3n+4}{2}}^3 & x_{\frac{n^2-3n+6}{2}}^3 & \cdots & \cdots & x_{\frac{n^2-n}{2}}^3 & x_n^1 \end{pmatrix}$$

In the fist and cecond case, we arrived to create a matrix Q wich will be ower first private commun key between the two interlocutors; then with this key, we will working for creating a second other key through a classical channal with applying the famous protocol Diffie-Hellman.

So, we have creating a matrix Q, in fellowing table (see Table 5.1), we resume the time required using 1 logistic map using Matlab software-2009 on PC intel(R) C(TM) i5-3470CPU@3.20GHz.

Size of the first key Q	225×225	256×256	400×400	500×500	512×512	960×960
Time required (second)	0.010919	0.013829	0.076993	0.152158	0.164088	1.277364

Table 5.1: Time required to implement the proposed key Q generation method.

Second step:

Using a classical channal

- *Let Q be the last matrix obtained during ower first exchange.*
- *Both the two interlocutors choose similary circulant matrices C_1 and C_2, of the same order n.*
- *Each interlocutor send to the other a cipher matrix S_1 and S_2 using a classical channal where:*

$$\begin{cases} S_1 = C_1 Q \\ S_2 = C_2 Q \end{cases} \tag{5.1}$$

- *The first interlocutor received S_2 and he calculates :*

$$K_1 = C_1 S_2$$

Similary the second interlocutor received S_1 and he calculates:

$$K_2 = C_2 S_1$$

And we have the folowing result:

Result:
The two interlocutors get the same key K, such that:

$$K = K_1 = K_2$$

Proof.

We know that the product of circulant matrices commute seen in Lemma 1.4, this gives:

$$K_1 = C_1 S_2 = C_1 C_2 Q = C_2 C_1 Q = C_2 S_1 = K_2$$

The following diagram resum how to create the commun keys through a quantum and classical channals.

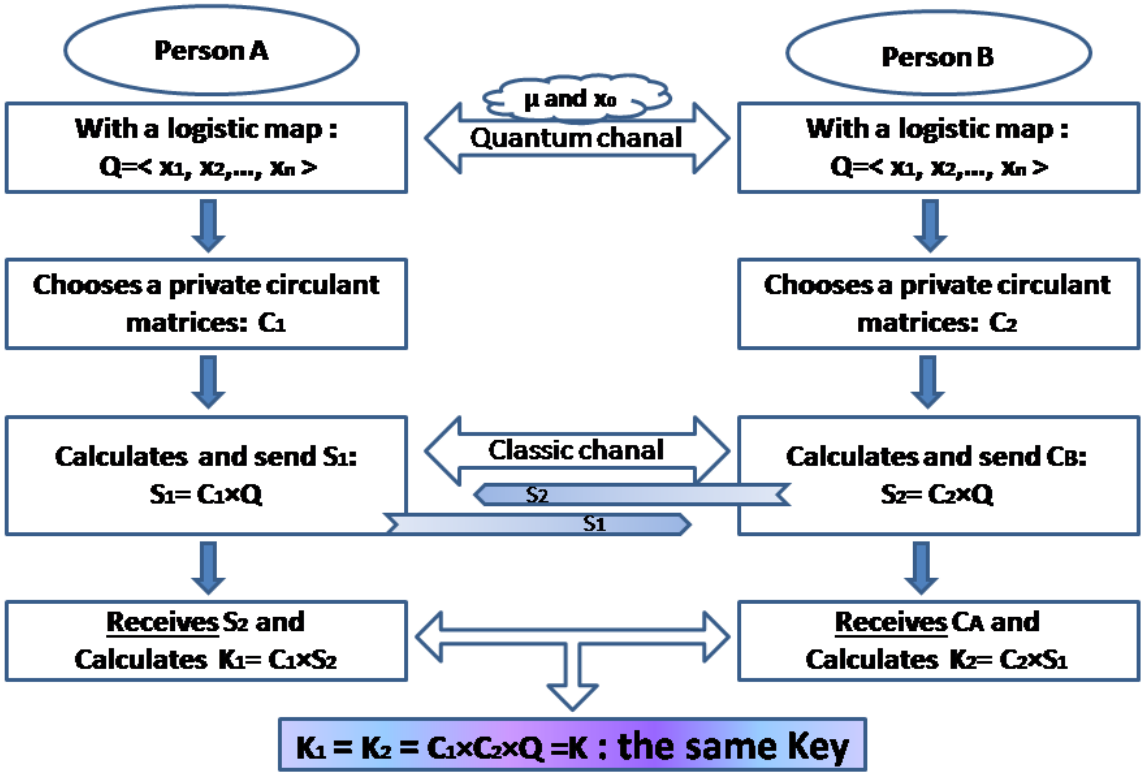


Figure 5.12: Illustration of the construction of a common key K.

We have creating a matrix K wich will be the private commun key between the the two interlocutors, this key will be used for encryption or decryption of text or images. [1, 2]

The fellowing table (see Table 5.3), resume the time required to create the key K using Matlab software-2009 on PC-intel(R) Cr(TM) i5-3470CPU@3.20GHz.

Size of the second key K	225×225	256×256	400×400	500×500	512×512	960×960
Time required (secod)	0.026830	0.029325	0.164801	0.337485	0.365084	2.803810

Table 5.2: Time required to implement the proposed key K generation method.

Third step:

Encryption and Decryption of some images

Let I be an image of size $n \times n$ pixel, If some one want to send the image to an other person, he must convert it to a matrix of order n. Let G be the converted matrix, Q and K are the exchanged keys obtained previousely.

We take an image named I of size $n \times n$. if a person want send I to an other person , first he must to convert I to a matrix G of same order n.

Then we take the shared keys obtained previousely : Q and K.

Encryption:

The first person calculates and sends the folowing encrypted matrix

$$H = KGQ$$

Decryption:

The second person receives H and he calculates

$$H' = K^{-1}HQ^{-1}$$

so he decrypt H and gets the intial matrix G and converted them to obtain the initial image I.

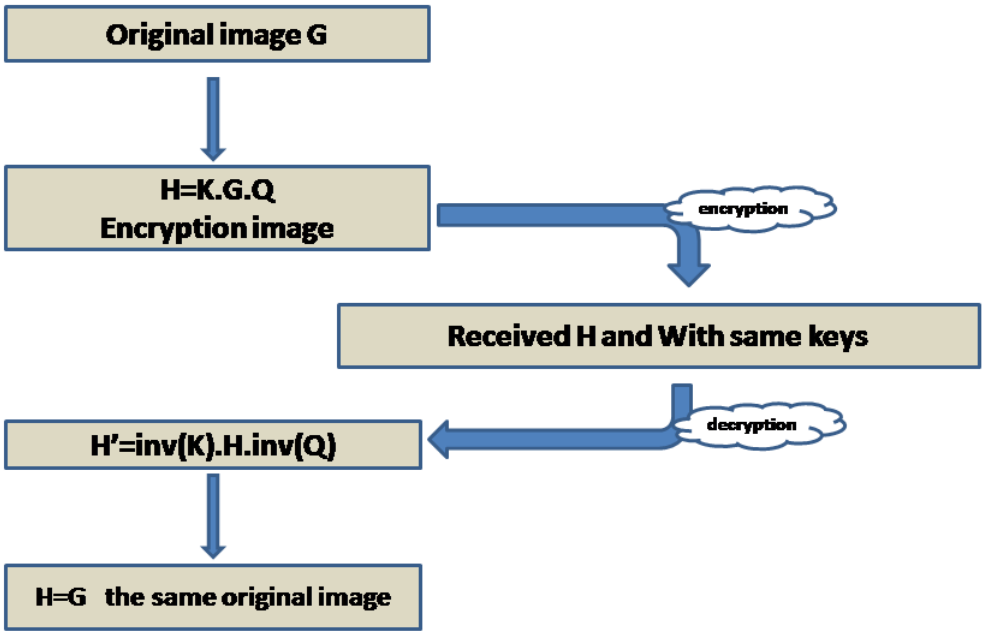


Figure 5.13: Illustration of the encrypt and decrypt operation

5.4 Analysis of safety and performance

Key Space Analysis

The total number of possible keys an attacker must try to break for an encryption system is called key space and it must be large enough to prevent attacks by brute force. For an algorithm to be resistant to brute force attacks, the key space must be greater than 2^{100}*. [31]*

We test the security of some proposed scheme, we choose a key space $n = 256$ *or* $n = 512$*. The secret key* K *is random because the interlocutors use arbitrary circulant matrices* (C_1 *and* C_2) *when sharing keys* K*. If we take the proposed key generation methode with*

$$x_i \in \{0, \cdots, 255\}; \quad (x_i \text{ are the composants of the key } K)$$

This its request 256^{256} *possible case to get the key* K*, and* 10^{60} *possible case to obtain the key* Q *(if we take ten digits decimal after the comma) using 3 logistic maps. The logistic map is of dimenssion one it has intersting proprieties: periodicity , sensitivity of intial values, but its security is low, so we have choosing in this phase 3 logestic maps to generate the key* Q*. And we get that the key space size of our proposed scheme is greater then* $256^{256} \times 256^{256} \times 10^{60}$ *(in the formula* $K = C_1 C_2 C Q$*) and key space is large enough for a brute force attacks.*

5.4.1 Tests to encrypt and decrypt some images

In the encryption and decryption of digital images, it is necessary to test some properties to see the efficiency and the level of security of the proposed system, among its properties:

- ***Histogram****;*
- ***Entropy****;*
- ***Correlation****.*

5.4.2 Histogram analysis (statistical attack)

An image histogram represents the transport of the image pixels by tracing the number of pixels at each gray scale level. The redundancy of plain text must be hidden in the distribution of encrypted text and this distribution must logically be uniform [31].

So histogram analysis is the most popular and effective way to test the uniformity of values (invulnerability to statistical attacks). Thus, for an encrypted image, it is necessary for an encrypted image to have a uniform distribution of pixel values on both axes [31], that is, good encryption must produce encrypted images with a uniform histogram as much as possible.

We have examined using the histogram of test images, Camera-men(size 256×256*) and Barbara(*512×512*), and we find that their histogram is uniform and considerably different to the histogram of simple images.(see Figure 5.14). [1, 2]*

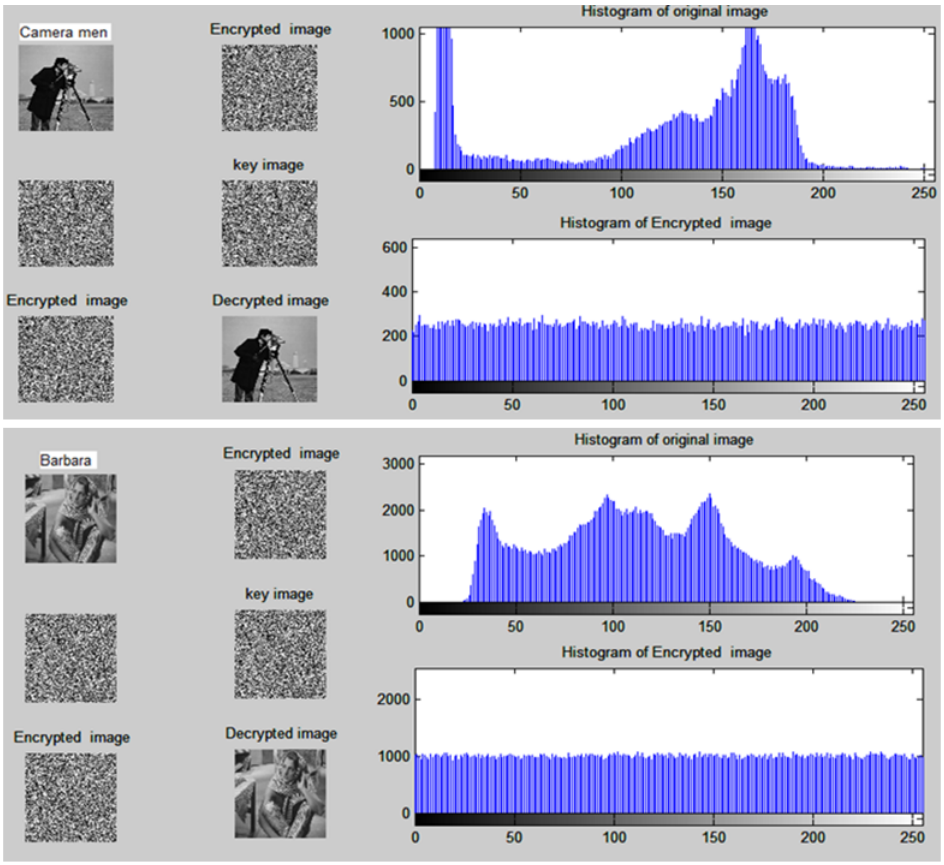


Figure 5.14: Application for encryptins and decryption of two images and their correspended histogram.

5.4.3 Entropy analysis of information

The entropy of a system is interpreted as an indicator to measure and characterize the amount of disorder in the system. It can measure the distribution of pixel values in the image. A good encrypted image has an entropy very close to 8. In other words, it represents the information needed to define the system states [31].

Entropy is defined by known formulas in the digital image encryption domain.

In the folowing table we find entropy results of analysis of some images [1]:

Encrypted images	images	size	μ	x_0	Entropy
Pepper		225×225	3.67	0.87	7.9966
Camera men		256×256	3.21	0.67	7.9977
Lena		256×256	3.57	0.47	7.9973
Im 400		400×400	3.57	0.47	7.9988
Im 500		500×500	3.47	0.33	7.9994
Barbara		512×512	3.59	0.41	7.9994
Im 960		960×960	3.30	0.28	7.9998

Table 5.3: Entropy values for a selection of encrypted images.

5.4.4 Correlation analysis

A strong correlation exists between the adjacent pixels in each clear image. A secure encryption algorithm should produce encrypted images whose correlation of adjacent pixels is very low. Typically, 1000 or 2000 pixels are selected for correlation analysis and correlation is calculated in horizontal, vertical and diagonal directions.

The correlation coefficient is calculated using the following formula:

$$r_{xy} = \frac{cov(x,y)}{\sqrt{D(x)D(y)}}, \text{ such as: } cov(x,y) = \sum_{0}^{N} \frac{(x_i - E(x))(y - E(y))}{N},$$

$$\text{and } D(x) = \sum_{0}^{N} (x_i - E(x))^2, \; E(x) = \sum_{0}^{N} \frac{x_i}{N}$$

Where, x and y represent the intensity values of two adjacent pixels. N is the number of pixels in the current analysis sample. $D(x)$ and $E(x)$ represent the variance and expectation of the current sample. [31]

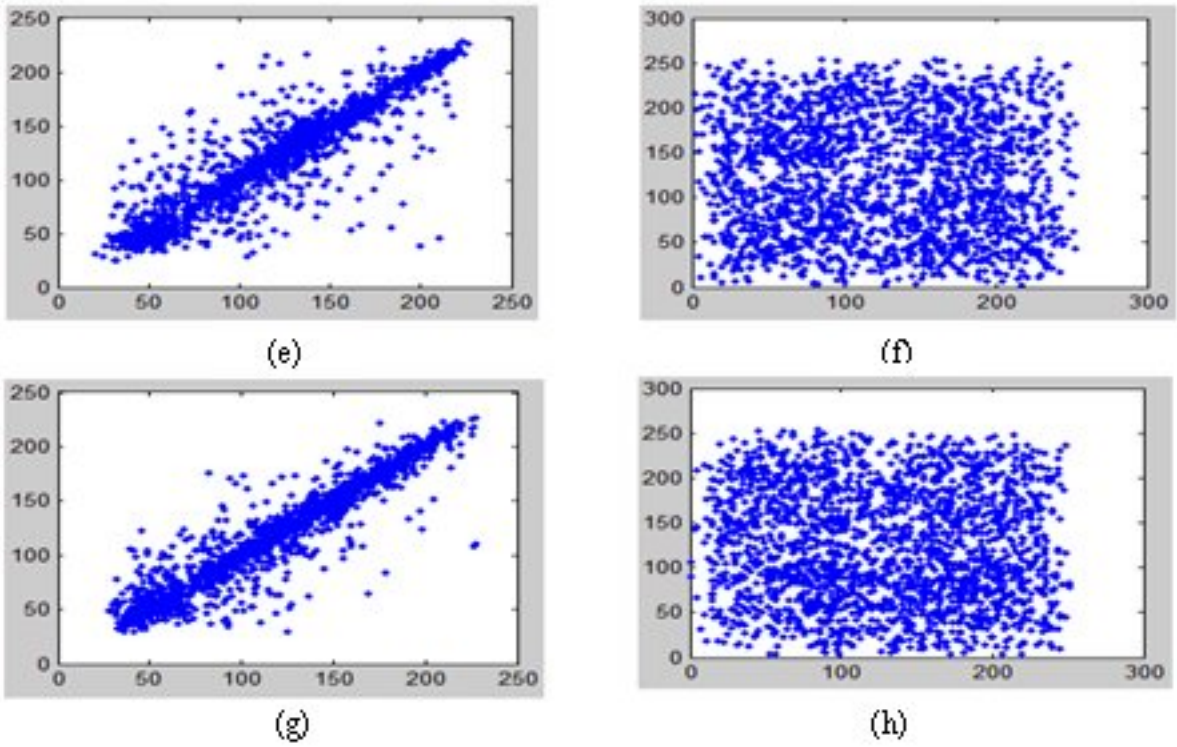


Figure 5.15: Correlation of two adjacent pixels [40].

- *We show in (a) and (b) the horizontal distribution of 2 adjacent pixels in the initial and decipher image.*
- *We show in (c) and (d) the vertical distribution of 2 adjacent pixels in the initial and decipher image.*
- *We show in (e) and (f) the diagonal distribution of 2 adjacent pixels in the initial and decipher image.*
- *We show in (g) and (h) the anti-diagonal distribution of 2 adjacent pixels in the initial and decipher image.*

5.5 Our second proposed scheme

Let $E_{(a,b)}(p)$ be an eliptic curve on the fine field F_p.
And let $R(x_R, y_R)$ a point of $E_{(a,b)}(p)$.

Through a quantium channal using the BB84 protocol, we can sharing the encryptions keys a, b, p, x_R and y_R.

So, the two interlocutors create a same Toeplitz matrix using $R(x_R, y_R)$ a point of $E_{(a,b)}(p)$.

Then, with this Toeplitz matrix, we can create and shared a second new key using the set of circulant matrices using the exchange protocol of Diffie-Hellman protocol to get this second commun key, this last key will be used encrypt and decrypt of ower data.

Two interlocutor want to exchange infomations:

First step:

Through a quantium channal

Using an eliptic curve

1. *Let $E_{(a,b)}(p)$ be an eliptic curve on the fine field F_p.*

   And let $R(x_R, y_R)$ a point of $E_{(a,b)}(p)$.

   Through a quantium channal and using the BB84 protocol, we can sharing the encryption a, b, p, x_R and y_R.

2. *After having exchanged a, b, p, x_R and y_R, we calcul points: $2R, 3R, 4R, \cdots, nR$ using formul defined in section (elliptic curve), for getting the n points of $E_{(a,b)}(p)$.*

3. *We create the following square Toeplitz matrix*

$$T_n = \begin{pmatrix} x_R & x_{2R} & x_{3R} & x_{4R} & \cdots & \cdots & x_{(n-1)R} & x_{nR} \\ y_{2R} & x_R & x_{2R} & x_{3R} & x_{4R} & \ddots & \ddots & x_{(n-1)R} \\ y_{3R} & y_{2R} & x_R & x_{2R} & x_{3R} & x_{4R} & \ddots & \vdots \\ \vdots & \ddots & \ddots & \ddots & \ddots & \ddots & \ddots & \vdots \\ \vdots & \ddots & \ddots & \ddots & \ddots & \ddots & \ddots & \vdots \\ \vdots & \ddots & \ddots & \ddots & \ddots & \ddots & \ddots & \vdots \\ y_{(n-1)R} & y_{(n-2)R} & \ddots & \ddots & \ddots & \ddots & x_R & x_{2R} \\ y_{nR} & y_{(n-1)R} & y_{(n-2)R} & \cdots & \cdots & \cdots & y_{2R} & x_R \end{pmatrix}$$

So, we succeeded to create a matrix T_n, it is the first secret commun key between the two interlocutors; this key T_n will be used to create a second key through a classic channal with applying the famous protocol of Diffie-Hellman.

Note.

We can also write:

$$T_n = (T_{ij}) = (T_{i-j}) \begin{cases} x_R & \text{if, } i = j \\ x_{(j-i+1)R} & \text{if, } i < j \\ y_{(i-j+1)R} & \text{if, } i > j \end{cases}$$

Second step:

Through a classic channal

- *Let T be the matrix obtained during ower first exchange.*
- *Both the two interlocutors choose two private circulant matrices of same order n.*

  let C_1 and C_1 the two circulant matrices choosed by the first interlocutor and C_3,C_4, choosed by the second interlocutor.
- *Each interlocutor sends to the other the folowing matrice s S_1 and S_2 through a classic channal with:*

$$\begin{cases} S_1 = C_1 T C_2 \\ S_2 = C_3 T C_4 \end{cases} \tag{5.2}$$

- *The first interlocutor received S_2 and calculates :*

$$K_1 = C_1 S_2 C_2$$

And with same procedure the second interlocutor received S_1 and he calculates :

$$K_2 = C_3 S_1 C_4$$

Proposition 5.1

The two interlocutors obtain a similar key K, that is:

$$K = K_1 = K_2$$

Proof.

Acording to the proprety(product of circulant matrices commute) seen in Lemma 1.4 we obtain:

$$K_1 = C_1 S_2 C_2 = C_1 C_3 T C_4 C_2 = C_3 C_1 T C_2 C_4 = C_3 S_1 C_4 = K_2 = K.$$

The following diagram resum how to create a commun keys through the two channals (quantum and classical).

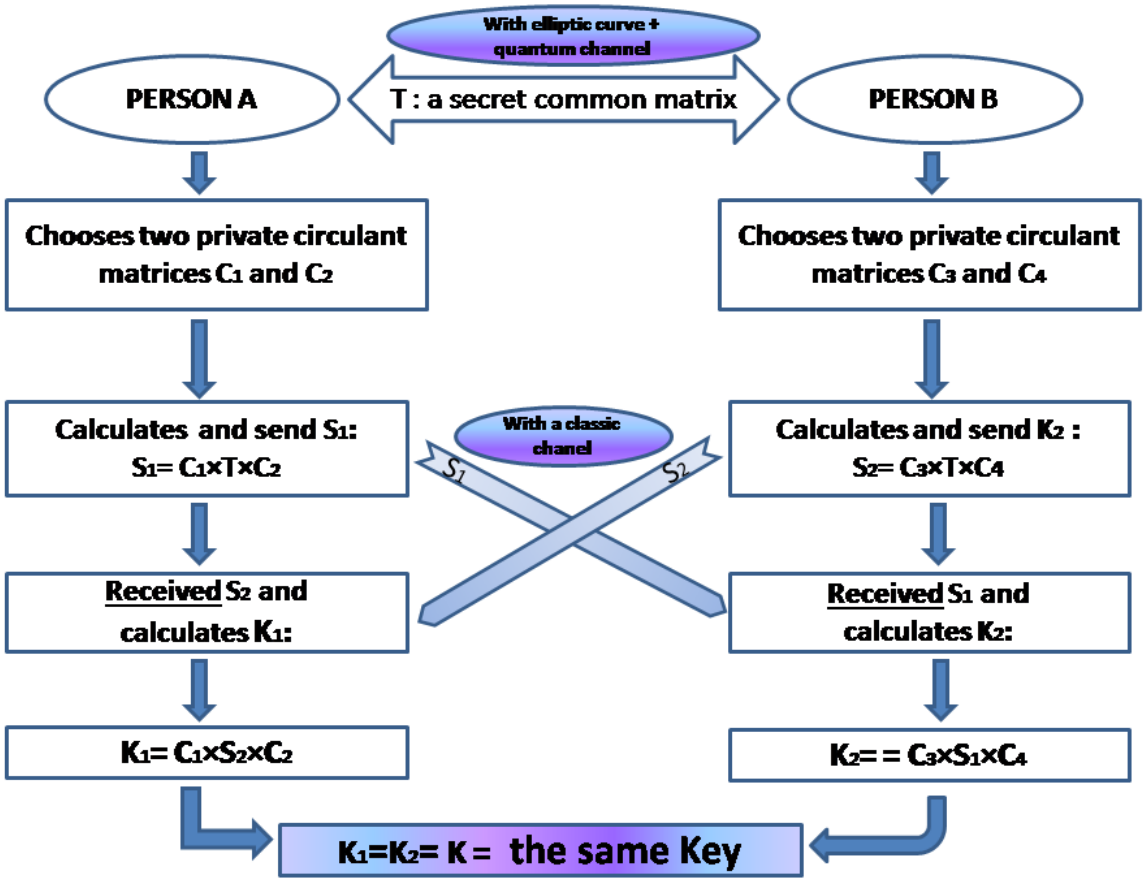


Figure 5.16: Illustration of the construction of a common key C.

We have managed to build a matrix K wich will be the secret commun key between the interlocutors; It will olso be used to encrypt and decrypt a text or image.

In the last chapter, we have proposed a new image encryption method that uses a good algebraic property which is the comutativity of multiplication of circulant matrices and the sensitivity of the chaotic maps. And we have representing a simple algorithm to generated some matrices from a random vector; through the experiment results and security analysis, we find that our proposal scheme has good encryption. Furthermore, and it resists to several known attacks.

Conclusion and perspectives

Through this study, we found that encryption techniques and algorithms still need to increase their security level against attackers, which is called the cryptoanalysis domain. This latter is the result of successive decryptions that have prompted man to develop increasingly elaborate techniques. The sensitivity of the information helped, the man was forced after long trusting simple substitutions (disk to encrypt, Scytale...) to move to more complex systems.

Since the advent of computer encryption techniques have taken a big step: the appearance of the first computer networks and the multiplication of data exchanges in digital form have forced mathematicians to completely revolutionize encryption systems (AlGamel, Mc-Eliece, DLP, RSA...).

The problem of discrete logarithm on eliptic curves (DLP) is a evidence of the complexity of recent encryption techniques in the world computing. Today, we find ourselves with systems accessible to the greatest number and whose complexity was unimaginable fifty years ago. It is no longer a secret subject but it is academic research launched around the world. This democratization of cryptography is no longer limited to the exchange of strategic data. Despite all the improvements, these systems are still not inviolable.

The battle of encryption between those who try to protect the data and those who try to hijack it has still good days ahead of it.

We remain amazed by the upheaval of the world's cryptology in thinking that every technological development in communication profoundly affects the world of cryptography.

Today, with the emergence of powerful computers and the performance of new computational algorithms, cryptography based on algorithmic mathematical and logical theories has become vulnerable. Alongside this problem, a new form of information protection is being implemented through physical processes according to the laws of quantum mechanics. Thus, quantum physics is used by cryptography to make our information inviolable. This is the very basis of our current memory work. Our goal is to study the basics, the principles, the characteristics of this quantum cryptography on fiber optic networks. However, this security technology presents several technological challenges in order to be well integrated in a standard and homogeneous way into equipment deployed in large-scale telecommunications networks.

We can extrapolate this idea by asking ourselves what the future of secure encryption will be if, one day, computers were to be replaced by new technology? Will digital communications stop? What forms will it take? Because its evolution will forever impact the world of cryptography.

Bibliography

[1] Adoui Salah, Brahim Benzeghli, and Lamnouar Noui.: *SHARING KEYS USING CIRCULANT MATRICES AND LOGISTIC MAPS THROUGH QUANTUM CHANNAL.,Advances in Mathematics: Scientific Journal,* **11(2022), no.12**, *page 1361–1378, the Union of researchers of Macedonia, 2022.*

[2] Adoui Salah.: *Circulant matrices and logistic maps to share keys.,3rd Intrnational Conference on Mathematics and Its Applications, page 35, Fsac Casablanca, Marroco,February 28-29 2020.*

[3] *LEMNOUAR Noui. Security limitations of Shamir's secret sharing. Journal of Discrete Mathematical Sciences and Cryptography, 2022, p. 1-13.*

[4] *LEMNOUAR Noui. A Novel Method for the Analysis of Privacy of Shamir's Scheme. May 2023,DOI: 10.13140/RG.2.2.36797.84967*

[5] *L. NOUI. Algèbre, Notion fondamentales, Presses de l'université de Batna, 1998.*

[6] *L. NOUI. Algèbre linéaire, Presses de l'université de Batna, 1999.*

[7] Lin Fuyong. *The inverse of circulant matrix. Applied Mathematics and Computation,* ***217****(21):8495–8503, 2011.*

[8] Shafi Goldwasser and Silvio Micali.: *Probabilistic encryption. J. Comput. Syst. Sci.,* ***28****(2):270–299, 1984.*

[9] Azeem Iqbal, Muhammad Aslam, Aslam Hafiza, and Sahar Nayab.: *Quantum cryptography: A brief review of the recent developments and future perspectives.* ***03*** *2016.*

[10] Ali Kanso and Nejib Smaoui.: *Logistic chaotic maps for binary numbers generations. Chaos, Solutions and Fractals,* ***40****(5):2557–2568, 2009.*

[11] Akinori Kawachi and Harumichi Nishimura.: *Communication complexity of private simultaneous quantum messages protocols, 2021.*

[12] Manish Kumar, Sunil Kumar, Rajat Budhiraja, M.K. Das, and Sanjeev Singh.: *A cryptographic model based on logistic map and a* $3-d$ *matrix. Journal of Information Security and Applications,* ***32****:47–58, 2017.*

[13] Álvaro Navarrete, Margarida Pereira, Marcos Curty, and Kiyoshi Tamaki.: *Practical quantum key distribution that is secure against side channels. arXiv: Quantum Physics, 2020.*

[14] Guihua Zeng. Quantum private communication.*: Quantum Private Communication by Guihua Zeng, Springer and Higher Education Press, ISBN: 978-3-642-03295-0,* ***01*** *2010.*

[15] D.R. Hankerson, S.A. Vanstone, and A.J. Menezes.*: Guide to elliptic curve cryptography. Springer-Verlag New York Inc, 2004.*

[16] Robert M. Gray. Toeplitz and Circulant Matrices :A review. http ://ee.stanford.edu/gray/Toeplitz.*: Deptartment of Electrical Engineering, Stanford University.*

[17] René SCHOOF , J. Théorie Nombres Bordeaux, 7. Counting points on elliptic Curve over finite fields. Pages 219-254, 1995.

[18] R. Schoof. Elliptic curves over finite fields and the computation of square Roots mod p. Mathematics of Computation, Vol. 44, pages 483-494, 1985.

[19] D-E. Knuth. The art of computer programming, vol.3, sorting and searching, Addison-Wesley. Reading, MA,1973.

[20] J-Y. Enjalbert. Jacobiennes et cryptographie. Thèse de Doctorat de l'université de limoges, 2003.

[21] Bernard le Stum . Algèbre linéaire et bilinéaire , version du 1 er décembre 2016 . [2] Nicolas Jacon , cours d'algèbre , licence mathématiques 2 me année semestre 1 , univ de Franche comté .

[22] Emmanuel Bresson, Olivier Chevassut, David Pointcheval, and Jean Jacques Quisquater.*: Provably authenticated group diffie-hellman key exchange.,In Proceedings of the 8th ACM Conference on Computer and Communications Security,* **CCS '01***, page 255–264, New York, NY, USA, 2001. Association for Computing Machinery.*

[23] https://www.simplilearn.com/tutorials/cryptography-tutorial/what-is-cryptography

[24] David Kahn, The Codebreakers : A Comprehensive History of Secret Communication from Ancient Times to the Internet, Revised and Updated, New York, Scribner, 1996.

[25] David Canright, Jong H. Chung, and Pantelimon Stanica.*: Circulant matrices and affine equivalence of monomial rotation symmetric boolean functions.,Discrete Mathematics,* **338***(12):2197–2211, 2015.*

[26] D. Shanks. Five number-theortic algorithms, proceeding of the second manitoba conference on numerical mathematics, pages 51-70, 1972.

[27] Int.J.Open Problems Compt.Math.,Vol.4,No.2,June 2011 ISSN 1998-6262 ; Copyright °c ICSRS Publication,2011 www.i-csrs.org

[28] GABRIEL Perye. Le traitement numérique des images. PhD thesis, hal-00690096, 2011.

[29] Léon Robichaud, L'image numérique Pixels et couleurs, support de cours, Département d'histoire, Université de Sherbrooke.

[30] Lepec. Les Graphiques sur Ordinateurs. PhD thesis, 1991.

[31] Aissam Djemaa, Aissa Boubednikh, Réalisation d'un Système de Cryptage des Images Numérique basé sur le Chaos ,Master en Informatique Spécialité : Réseau et Sécurité. 2021

[32] MOHAMED EL KHATTABI. LES STRUCTURES ALGEBRIQUES. PhD thesis, Université SIDI MOHAMED BEN ABDELLAH, 12 juin 2013.

[33] A. Carmona, A.M. Encinas, S. Gago, M.J. Jiménez, and M. Mitjana.*: The inverses of some circulant matrices.,Appl. Math. Comput.,* **270(C)***:785–793, November 2015.*

[34] A. Carmona, A.M. Encinas, M.J. Jiménez, and M. Mitjana.*: The group inverse of some circulant matrices.,Linear Algebra and its Applications,* ***614****:415–436, 2021. Special Issue ILAS 2019.*

[35] S.Chantel Gleghorn, application of generalized and circulant matrices to iterated function on integers. Angelos State Universitu, San Angelo.

[36] FRANCOIS DUMAS. ALGEBRE : GROUPES ET ANNEAUX I. PhD thesis, Université de Blaise Pascal, 2007.

[37] T. Moreau et M. Chavance. Rappels de calcul matriciel. Octobre 2006.

[38] Emmanuel Royer. Chapitre2 Matrices. PhD thesis, Université Blaise Pascal , Département de mathématiques et informatique, 2005.

[39] $http://bmm.univ-lyon1.fr/bmm/data/cours/algebre_lineaire/al1_tout.pdf$

[40] Abd Samad Hasan Basari, BSc Mathematics, MSc (IT-Edu), PhD (ICT)Professor at Universiti Tun Hussein Onn Malaysia.

[41] Mukherjee, Bishwa Nath; Maiti, Sadhan Samar (1988), "On some properties of positive definite Toeplitz matrices and their possible applications", Linear Algebra and Its Applications.

[42] Russel, Frank (1999). Information Gathering in Classical Greece. U. Michigan Press.

[43] C.H. Meyer, "Ciphertext/Plaintext and Ciphertext/Key Dependencies vs. Number of Rounds for Data Encryption Standard," AFIPS Conference Proceedings, 47, 1978.

[44] Dramaix Florence, van den Broek Didier, Wens Vincent; La Cryptographie Quantique Printemps des Sciences 2003.

[45] René SCHOOF, J. Théorie Nombres Bordeaux, 7. Counting points on elliptic Curve over finite fields. Pages 219-254, 1995.

[46] Shor, Pierre (1997). « Algorithmes en temps polynomial pour la factorisation principale et les logarithmes discrets sur un ordinateur quantique ». Revue SIAM sur l'informatique.

[47] O. Toeplitz, Zur Transformation der scharen bilinearer Formen von unendlich vielen Veränderli- chen, Nachr. der kgl. Gesellschaft der Wissenschaften zu Göttingen, Mathematisch-physikalische Klasse, (1907), pp. 110–115.

[48] Zur theorie der quadratischen und bilinearen Formen von unendlich vielen Veränderlichen, Math. Ann., 70 (1911), pp. 351–376.

[49] BENCHERAB Loubna, CHELLEF Somia, L'échange des clés et la cryptographie Chaotique ,Mémoire de fin d'étude de Master 2, Spécialité : Cryptographie et sécurité. 2021

[50] FELLOUSSI Ihcene, MATRICES AND CRYPTOSYSTEMS ,MASTER MEMORY; Option :functional analysis and operator theory. 2021