République Algérienne Démocratique et Populaire

Ministère De L'enseignement Supérieur Et De La Recherche Scientifique
Université Batna 2
Faculté des Mathématiques et Informatique
Département Informatique


# Introduction à la cryptographie

Support de cours pour les étudiants de troisième année Licence

Auteur : Dr R.DJELLAB

01/05/2018

République Algérienne Démocratique et Populaire

Ministère De L'enseignement Supérieur Et De La Recherche Scientifique
Université Batna 2
Faculté des Mathématiques et Informatique
Département Informatique

Table des matières

# Introduction

La sécurité de l'information est l'un pilier majeur lors de la mise en place de tout système d'information afin de préserver la ce dernier et d'éviter tout type de pertes, qu'elles soient matérielles, immatérielles, financières ou même humaines. Pour cela, et depuis très longtemps, des mécanismes et des techniques ont été mis en place ; parmi elles, les techniques cryptographiques.

La cryptographie, aussi appelée science du secret, ou l'art de cacher, est une branche d'une science plus large : la cryptologie. Elle permet, la cryptographie, de réaliser des transformations sur un message de telle sorte qu'il devienne « illisible » pour les entités non autorisées.

Le présent document, et sans prétende une complétude, aspire à présenter pour les étudiants de troisième année licence, un support de cours leur permettant de mieux aborder les notions de la cryptographie et de comprendre certains mécanismes de base sur lesquels reposent les techniques de chiffrement.

# 1. Sécurité et le besoin de la sécurité

Le besoin de sécuriser l'information c'est fait sentir de plus en plus à force que de nouvelles applications liées au développement technologique apparaissaient : e-learning, e-commerce, e-health…sans oublier la protection de la propriété intellectuelle, la politique, l'armement …tout cette panoplie d'applications et la diversité d'information qui y est manipulée a fait qu'un groupe de participants à une communication veulent maintenir les informations qui circulent au sein du groupe à l'abri de tout intrus pouvant représenter une éventuelle menaces. Une menace qui se traduirait par un vol ou un espionnage, modification et/ou falsification de l'information,…les conséquences, humaines et/ou matérielles, peuvent être alors très lourdes.

## 1.1. Définitions

Avant de s'attarder sur les menaces et les techniques de sécurité, nous allons d'abord revoir les définitions de deux concepts clés, à savoir *la sécurité informatique* et *l'information.*

En fait, le concept de *sécurité informatique* est défini comme suit [1][2]: *La protection accordée à un système d'information automatisé afin d'atteindre les objectifs applicables de préservation de l'intégrité, la disponibilité et la confidentialité des ressources du système d'information (comprenant le matériel, les logiciels, les firmware, informations/données et les télécommunications).*

Quant au concept d'*information*, il est à préciser qu'il peut prendre plusieurs formes, dépendant des besoins de la situation de communication.

La RFC 2828 définit l'*information* comme étant *tous faits et idées qui peuvent être représentés (codés) sous différentes forme de donnée* ; aussi la *donnée* est *l'information codée sous une certaine représentation physique, généralement sous forme de séquence de symboles ayant un sens ; spécialement en ce qui concerne l'information qui peut être manipulée et produite par un ordinateur.*

Cependant, dans la littérature du domaine, et suivant la définition de la sécurité informatique introduite en haut, aucune distinction n'est faite entre *information* et *donnée* [1].

On optera pour les besoins du sujet pour la définition donnée dans [3] : *L'information est toute quantité compréhensible*. Nous considérerons alors que sécuriser l'information revient, dans un premier temps, à cacher cette information, et à l'écrire sous une forme *incompréhensible* pour des entités non-autorisées.

La sécurité de l'information est ainsi élaborée contre tout changement ou lecture non-autorisée. En fait, Il faut distinguer entre deux types de sécurité, la sécurité inconditionnelle, et la sécurité computationnelle. La sécurité inconditionnelle est liée à la puissance de calcul de l'adversaire. Dans ce cas de figure, même si l'adversaire a une puissance de calcul infinie, la sécurité de l'information devra toujours être assurée. A la différence de la sécurité computationnelle, qui elle, est basée sur certaines hypothèses concernant l'impossibilité pratique, et non théorique, de calculer certaines opérations, tout en utilisant les meilleures méthodes possibles.

## 1.2. Objectifs de la sécurité

Par le terme « mesures techniques » on fait référence aux mesures où l'homme n'intervient nullement ou presque, car c'est bien l'homme qui mettra en place ces mesures là.

Ces mesures sont mises en place dans le but d'assurer les quatre piliers de la sécurité, reconnus dans la littérature du domaine, en l'occurrence la confidentialité ; l'intégrité ; l'authentification et la non-répudiation.

- Confidentialité : il s'agit de vérifier que l'information n'est accessible qu'aux entités (personnes ou machines) autorisées.
- Intégrité : il s'agit là de s'assurer que la donnée n'a pas changé durant sa transmission d'un point A vers un (ou plusieurs points)
- Authentification : lors de la réception de l'information il s'agit de pouvoir vérifier que celle-ci provient bien de la source qui prétend l'avoir envoyé.
- Non répudiation : le but ici est de prévenir le cas où une entité dénie tout engagement ou action préalable.

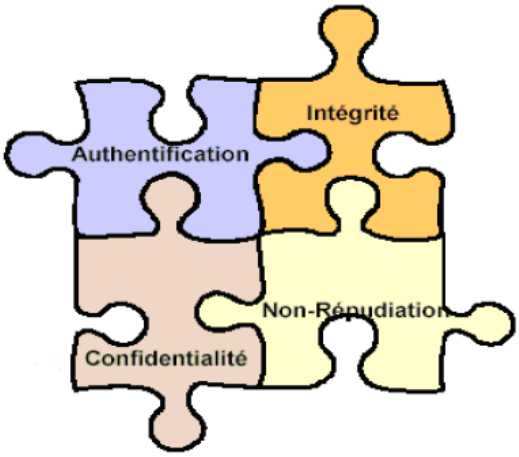


Figure 1 Principaux objectifs de la sécurité de l'information.

Ces objectifs sont nécessaires mais non suffisants dans certains cas, d'autres objectifs doivent être assurés également, il est alors possible de les résumés dans le tableau suivant :

| | |
|---|---|
| Identification | Corroboration de l'identité d'une entité (i.e : une personne, un ordinateur, ou une carte de crédit) |
| Autorisation | Délivrer, à une autre entité, la permission officielle de faire ou être quelque chose. |
| Validation | un moyen de fournir l'opportunité à une autorisation d'employer ou manœuvrer une information ou des ressources. |
| Control d'accès | Restriction de l'accès à des ressources, à des entités privilégiées. |
| Certification | Approbation d'information par une entité de confiance. |
| Timestamping | Enregistrant la période de la création ou l'existence d'information. |
| témoignage | Vérifiant la création ou l'existence d'information par une entité autre que le créateur. |
| Accusé de réception | Reconnaissance que l'information a été reçue. |

| | |
|---|---|
| Confirmation | Reconnaissance que le service a été fourni. |
| Propriété | Un moyen de fournir à une entité le droit légal d'employer ou transférer une ressource à d'autres entités. |
| Anonymat | Cacher l'identité d'une entité impliquée dans un certain processus. |
| Révocation | Rétraction de certification ou d'autorisation. |

**Tableau 1 Objectifs de la sécurité[3].**

Les techniques utilisées pour assurer les objectifs cités précédemment vont de la plus simple à la plus complexe. On parlera alors de chiffrement, signature numérique, de tatouage et d'empreinte digitale, de certificats …

La majorité de ces techniques utilisent une information particulière, en l'occurrence la « clé », un concept sur lequel nous reviendrons plus loin.

### 1.1. Mesures humaines

La sécurité de l'information nécessite toute une panoplie de techniques à mettre en place pour éviter au mieux de mettre en péril tout un système d'information.

Avant de passer aux techniques proprement dites, il est à signaler que la sécurité de l'information a, aujourd'hui, un volet « humain » à prendre au plus grand degré d'importance. En effet, à quoi servirai les meilleurs techniques si l'utilisateur même de l'information la mette en péril via des fausses manœuvres ou même des manœuvres mal intentionnées.

Certains experts préfèrent alors ne pas « éduquer » à la sécurité informatique des utilisateurs qui ne métrisent pas l'outil informatique car ceci mènerait automatiquement à de mauvaises manipulations.

D'autre part, la frontière d'un système d'information est devenue de plus en plus *perméable* avec les nouvelles technologies. La mobilité des utilisateurs du système, et donc des nœuds pouvant en constituer l'infrastructure, rajoute encore plus à la complexité de délimiter les frontières, et donc de gérer à bien la sécurité du tout. Un deuxième dispositif, est à prendre en considération afin d'assurer la sécurité de l'information, il s'agit de l'*externalisation* face à la *dépérimétrisation*[1]. Une solution proposée par la BP (***B****ritish* ***P****etroleum*) suivant laquelle une société n'aura plus à se soucier de la sécurité des postes de travail des clients, et même d'une partie des employés, ces derniers n'ayant accès qu'à une partie de l'information, celle dont ils ont besoins.

Cela rejoint en partie la première solution où l'on se soucie peu des utilisateurs inexpérimentés, et ouvre également la voie à une autre, celle de la sauvegarde de l'information.

En effet, même si une partie des utilisateurs n'ont accès qu'à une partie de l'information (celle dont ils ont besoin et sur demande) un système d'information n'est pas à l'abri de quelques défaillances, il est alors intéressant, même important, de réaliser des sauvegardes régulières sur des sites éloignés. NAS (***N****etwork* ***A****ttached* ***S****torage*) et SAN (***S****torage* ***A****rea* ***N****etwork*) sont des techniques modernes permettant une duplication de données à distance, en temps réel ou à intervalles rapprochés. Bien entendu, des

[1] Dépérimétrisation : dissolution du périmètre de sécurité.

tests sont à prévoir de temps à autre (rechargement et restauration de données stockées, redémarrage d'une application à distance…) cela permet en partie de vérifier la disponibilité des données.

1.2. Mesures techniques

1.2.1.1. Cryptographie et Chiffrement

Avant de passer au chiffrement, il est important de rappeler que c'est une science qui découle directement d'une science plus large, la cryptologie. En effet, la cryptologie renferme deux grandes disciplines scientifiques : la cryptographie et la cryptanalyse.

La cryptanalyse est la science qui traite de l'opération inverse de la cryptographie. Il s'agit de pouvoir reconstruire plus ou moins le texte en clair sans pour autant avoir accès à la clé de chiffrement. Il est possible de distinguer entre une cryptanalyse passive, où l'attaquant ne fait que « lire » les messages chiffrés sans y introduire une quelconque modification. Si par contre, il y a un quelconque changement de contenu dans ce cas de figure il s'agit le plus d'une cryptanalyse active.

La cryptographie quant à elle est reconnue comme étant *« l'art de sécuriser»* ; elle a été utilisé depuis très longtemps par l'homme sous forme de mécanisme permettant de faire passer des messages en secret surtout en période de guerre.

L'un des mécanismes les plus anciens " *Le Scytale*" . C'est une technique qui consistait à enrouler des bandelettes de papyrus sur un bâtonnet puis d'écrire longitudinalement sur le papyrus, une fois le message fini, les bandelettes sont déroulées puis envoyées à destination. Arrivées au destinataire, il aurait besoin du diamètre du bâtonnet initial pour enrouler une seconde fois ces bandelettes sur un bâtonnet de même diamètre et pouvoir lire enfin le message.


**Message crypté:** KTMIOILMDLONKRIIRGNOHGWT

**Figure 2 : Technique du Scytale.**

Plus récemment, *La cryptographie est la discipline qui permet d'écrire un message sous forme d'un texte chiffré, usuellement via une transformation appliquée sur un texte en clair en utilisant une clé, dans le but de protéger un secret contre des adversaires, des intercepteurs, des intrus, des indiscrets, des espions, ou simplement contre des attaquants, des adversaires ou des ennemis. La cryptographie professionnelle se charge non seulement de la protection du texte en clair mais aussi de la clé de chiffrement, plus généralement elle se charge de la protection du crypto-système en entier*.

Formellement, le processus de chiffrement d'un message $m$ consiste en la transformation d'un message $m$ en $m'$ via une fonction de chiffrement $\mathcal{E}$, et en utilisant une clé $\mathcal{K}$ dite de chiffrement.

L'opération inverse est le déchiffrement[2]. Elle consiste à retrouver à partir du message $m'$ le message initial $m$ en utilisant une fonction de déchiffrement $\mathcal{D}$ et une clé de déchiffrement $K'$.

On notera alors :

$$\mathcal{E}(m)_K = m'$$

$$\mathcal{D}(m')_{K'} = m$$

Il est possible que $K=K'$, on parlera alors de chiffrement symétrique. Autrement, et si $K \neq K'$, il s'agira d'un chiffrement asymétrique.

1.2.1.2. Taxonomie des algorithmes de chiffrement suivant le procédé appliqué au message

1.2.1.2.1. Transposition

Il s'agit de changer les positions des caractères constituant le message de sorte à en former un autre message ayant ou non un sens.

Si le changement de position se fait de sorte à ce que le nouveau message ait un sens, il s'agit plutôt d'anagramme.

Il en existe des populaires sous forme de mot ou même de phrase comme :

| Mot | Phrase |
|---|---|
| Argent⇨gérant | Rien n'est établi⇨Albert Einstein |
| Chien⇨Niche | Dur notaire⇨Ordinateur |
| Star⇨Tsar | Tout commença dans l'eau⇨Le commandant Cousteau |

Sinon le changement de position peut se faire en utilisant un mot clé. L'ordre se fait alors suivant l'ordre alphabétique des caractères constituants le mot clé comme le montre l'exemple suivant :

| G | R | A | I | N |
|---|---|---|---|---|
| 2 | 5 | 1 | 3 | 4 |
| L | A | C | R | Y |
| P | T | O | G | R |
| A | P | H | I | E |

| A | G | I | N | R |
|---|---|---|---|---|
| 1 | 2 | 3 | 4 | 5 |
| C | L | R | Y | A |
| O | P | G | R | T |
| H | A | I | E | P |

[2] Il est à noter que le déchiffrement et le décryptage sont deux notions différentes, le déchiffrement consiste à retrouver le texte en clair à partir du texte chiffré en utilisant la clé de déchiffrement, normalement connue par le/les destinataires légitimes ; le décryptage consiste à retrouvé le texte en clair et non forcement en utilisant la clé de déchiffrement.

| | | | | |
|---|---|---|---|---|
| E | S | T | L | A |
| R | T | D | E | C |
| A | C | H | E | R |

| | | | | |
|---|---|---|---|---|
| T | E | L | A | S |
| D | R | E | C | T |
| H | A | E | R | C |

Tableau 2 Exemple de chiffrement par transposition.

Le texte à chiffrer est :la cryptographie.

Le texte chiffré est alors "CLRYAOPGRTHAIEPTELASDRECTHAERC".

1.2.1.2.2. Substitution

Il s'agit de remplacer les caractères du message par d'autres caractères appartenant au même alphabet, et là on parlera de substitution monoalphabétique, ou d'un alphabet différent, et on parlera alors de substitution polyalphabétique.

| | | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| **Chiffrement** | **Message à crypter** | c | r | y | p | t | o | g | r | a | p | h | i | e | **Déchiffrement** |
| | **Rang des lettres** | 3 | 18 | 25 | 16 | 20 | 15 | 7 | 18 | 1 | 16 | 8 | 9 | 5 | |
| | | 5 | 20 | 2 | 18 | 22 | 17 | 9 | 20 | 3 | 18 | 10 | 11 | 7 | |
| | **Message crypté** | e | t | b | r | v | q | l | t | c | r | j | k | g | |

Tableau 3 : Exemple de chiffre de César avec un décalage de +2.

Le message à chiffrer est : *cryptographie*

Le message crypté est : *etbrvqltcrjkg*

1.2.1.3. Taxonomie des algorithmes de chiffrement suivant la/les clé(s)

Le chiffrement est considéré comme clé de voute de la sécurité de l'information. Suivant le type de la clé de chiffrement/déchiffrement, il est possible de distinguer entre deux types de chiffrement :

1.2.1.3.1. Chiffrement symétrique

Un algorithme de chiffrement symétrique, est un algorithme de chiffrement où les opérations de chiffrement et de déchiffrement se font en utilisant la même et unique clé. Ainsi, Alice (Alice et Bob étant les émetteur/récepteur traditionnels du processus de chiffrement dans la littérature du domaine) chiffre le message $m$ en $m'$ en utilisant la clé $K$ ; Lorsque Bob reçoit le message $m'$ il le déchiffre en utilisant la même clé $K$.

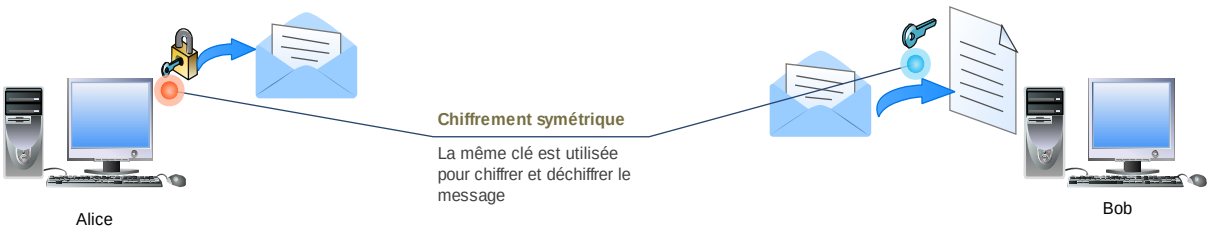


Figure 3 Chiffrement symétrique.

La confidentialité, aussi bien que l'authentification dans ce cas de figure, ne sont assurées que si la *distribution sécurisée* de la clé de chiffrement, au préalable de tout échange, est assurée. En effet, la confidentialité du transfert entre les deux protagonistes légitimes est assurée si l'on s'assure qu'une tierce entité non légitime ne détient pas d'une manière ou d'une autre la clé de chiffrement $\mathcal{K}$ et qu'il lui est donc impossible de déchiffrer $m'$. Pour ce qui est de l'authentification, cette dernière peut être assurée de par le fait de la sécurité de la distribution de la clé, car si seule Alice détient la clé $\mathcal{K}$, Bob en déchiffrant le message $m'$ via cette même clé $\mathcal{K}$ s'assure en même temps que c'est bien Alice qui l'a chiffré. La distribution sécurisée de la clé de chiffrement est une condition nécessaire et non suffisante pour assurer l'authentification d'un message envoyé, d'autres techniques dédiées sont utilisées pour l'assurer (e.g : signature numérique).

Pour ce qui est de l'intégrité du message envoyé, la sécurité de la clé n'est pas seule garante. Pour assurer l'intégrité d'un message envoyé, toujours en utilisant un chiffrement symétrique, il est possible d'avoir recours à un contrôle d'erreur externe ou interne.

Les figures suivantes schématisent les cas de contrôle d'erreur externe et interne :

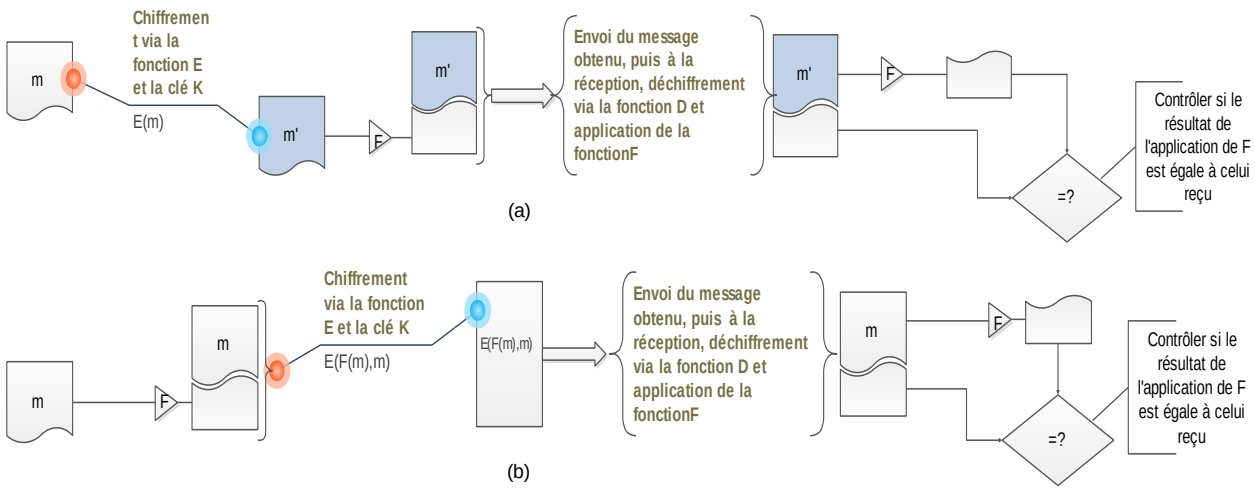


Figure 4 Contrôle d'erreur.

Dans le cas d'un contrôle d'erreur interne, *(a)* sur la figure ci-dessus, on rajoute un bloc résultant de l'application de la fonction $\mathcal{F}$ au message $m$. Le tout est soumis à l'algorithme de chiffrement $\mathcal{E}$ en utilisant la clé $\mathcal{K}$. Une fois le message arrivé à destination, le récepteur exécute l'opération inverse, c-à-d qu'il déchiffre le message reçu ; en extrait le message initiale $m$, et le bloc qui lui a été rajouté ; le récepteur soumet le message $m$à la fonction $\mathcal{F}$, et compare le résultat au bloc extrait. Si les résultats sont identiques alors l'intégrité a probablement était préservée.

Dans le deuxième cas, *(b)* sur la figure précédente, il s'agit de la même idée, à la différence que le bloc de vérification est rajouté après le chiffrement de $m$ et non avant comme c'est le cas dans *(a)*. La fonction $F$ est alors appliquée à $E(m)$ au lieu d'être appliquée directement à $m$.

1.2.1.3.2. Chiffrement asymétrique

Dans le cas du chiffrement asymétrique il s'agit d'utiliser une paire de clés (publique/privée) et non plus d'utiliser une seule clé pour les opérations de chiffrement/déchiffrement. Généralement, la clé publique est utilisée pour le chiffrement alors que la clé privée est utilisée pour le déchiffrement. Ainsi, Bob distribue sa clé publique $K_P$ à un ensemble d'entités. L'entité voulant communiquer avec Bob (soit Alice cette entité) chiffre le message $m$ en utilisant la clé publique de Bob. A la réception du message chiffré, Bob utilisera sa clé privée $K_S$ pour le déchiffrer.

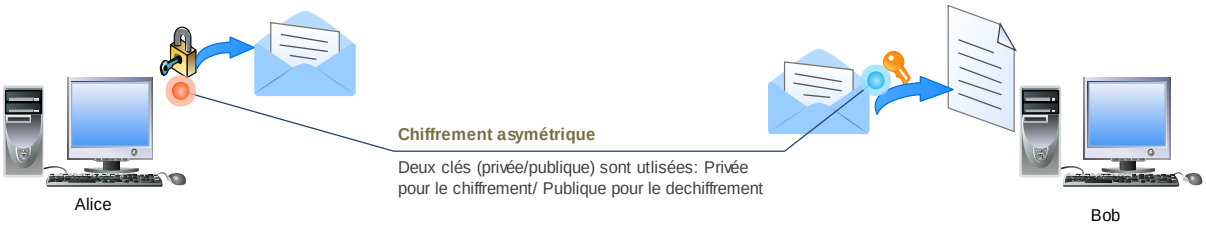


**Figure 5 Chiffrement asymétrique.**

Les algorithmes de chiffrement asymétrique sont basés sur la difficulté de résoudre des problèmes mathématiques. En général, il s'agit de fonction à sens unique ; une fonction à sens unique est une fonction facile à calculer dans un sens, mais difficile à calculer dans l'autre sens (avec la puissance de calcul actuelle), telle que la factorisation des grands nombres (e.g : RSA).

La confidentialité d'un message chiffré via un algorithme de chiffrement est basée sur la difficulté de résoudre ces problèmes mathématiques dans un temps acceptable en usant de la puissance de calcul actuelle.

Quant à l'authentification, il est possible d'intervertir les rôles des clés pour l'assurer. La clé privée serait utilisée pour le chiffrement alors que la clé publique servirait au déchiffrement. Ainsi Alice chiffre un message $m$ en utilisant sa clé privée $K_S$ et le diffuse à tous les destinataires légitimes ayant sa clé publique $K_P$. Bob, l'un des destinataires légitimes (ainsi que tous les autres destinataires potentiels), déchiffre le message d'Alice avec la clé publique de cette dernière, et *vérifie* par là même l'authenticité d'Alice. Alice est la seule à avoir la clé privée et donc la seule à avoir pu chiffrer le message $m$.

1.2.1.3.3. Hybridation

La sécurité lors de l'utilisation d'un algorithme de chiffrement symétrique est fortement liée à la distribution de la clé de chiffrement/déchiffrement qui doit être distribuée de façon sécurisée avant même d'entamer tout échange. Les algorithmes de chiffrement asymétriques quant à eux ne souffrent pas de cette problématique, du fait qu'ils peuvent servir à la génération et distribution même des clés. Cependant, les algorithmes de chiffrement asymétriques sont gourmands en termes de temps de calcul, ce qui implique une certaine lenteur.

En pratique, il est possible de prévoir une hybridation des deux types d'algorithmes de chiffrement (voir ci-dessous Figure 6); on utilisera alors un algorithme de chiffrement asymétrique pour *distribuer* une clé au lieu de chiffrer un message. La clé ainsi distribuée est celle d'un algorithme de chiffrement symétrique.

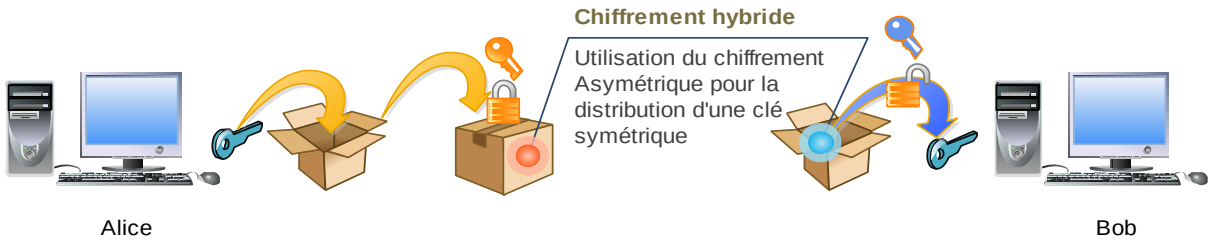


Figure 6 Hybridation: Distribution de clé symétrique via un chiffrement asymétrique.

1.2.1.4. L'Authentification

L'authentification et l'identification sont deux concepts très liés. Si l'authentification est le fait d'apporter une preuve d'une identité, l'identification est la vérification que cette identité est bien existante.

Plus simple : Si on répond à la question « Qui est qui ? » ⇨ c'est l'identification

Si on répond à la question « Est-ce que X est bien X ? » ⇨ c'est l'authentification

1.2.1.4.1. Techniques d'authentification

Plusieurs techniques existent pour apporter une preuve d'identité est donc une authentification. On en détermine les suivantes :

| Ce que je sais | Ce que j'ai | Ce que je suis |
|---|---|---|
| Une information que l'on est seul à avoir ou à connaitre | Un objet (ou autre) que nous seul possédons | Ce qui fait partie de moi, de ma biométrie et qui est unique |
| Le mot de passe<br>Code PIN<br>Schéma | Clé USB<br>Carte à puce<br>QR code | L'authentification biométrique : Empreinte, Iris, Rétine, visage, la voix, la démarche, ADN, la palme de la main… |

1.2.1.4.1.1. La signature numérique

Tirée du concept même de la signature manuscrite, qui est censée être unique à une personne donnée, la représentant et permettant de là même à l'identifier, la signature numérique suit plus ou moins le même principe. En effet, il ne s'agit pas seulement de quelque chose d'unique au signataire et indépendant à l'information signée, mais il s'agit plutôt de techniques utilisées afin de *lier* l'identité d'une entité à une information, ce qui implique la transformation du message, et de certaines informations jugées secrètes et connues par le signataire, un *tag* représentatif dit *signature*.

Selon la norme ISO 7498-2, la signature numérique est définie comme étant « *des données ajoutées à une unité de données, ou transformation cryptographique d'une unité de données, permettant à un destinataire de prouver la source et l'intégrité de l'unité de données …* »

Plus formellement, la signature numérique peut être définit comme suit :

- Soit $\mathcal{M}$ l'ensemble des messages pouvant être signé ;
- Soit $\mathcal{S}$ l'ensemble des signatures ;
- $S_A$ est une transformation de l'ensemble des messages $\mathcal{M}$ vers l'ensemble des signatures $\mathcal{S}$. $S_A$ est la transformation de signature de l'entité $\mathcal{A}$. $S_A$ est gardée secrète par l'entité $\mathcal{A}$.
- $V_A$ est une transformation de l'ensemble $\mathcal{M} \times \mathcal{S}$ vers l'ensemble {vrai, faux} . $V_A$ est une transformation de vérification de la signature de l'entité $\mathcal{A}$. $V_A$ est publique et est utilisée par les autres entités pour vérifier les signatures crées par l'entité $\mathcal{A}$.
- $S_A$ et $V_A$ offrent un *schéma de signature numérique* pour l'entité $\mathcal{A}$.

La signature numérique permet d'éviter le problème de *personnification*[3], et donc de vérifier l'authentification d'une information signée. En effet, l'expéditeur légitime ayant une signature unique, puisqu'elle est liée à des données privées, est le seul à pouvoir la déposer sur l'information.

Vu que la signature numérique est liée à des données privées, un expéditeur ayant signé un message ne peut nier l'avoir fait. La signature numérique permet donc d'assurer l'un des principaux buts de la sécurité de l'information, en l'occurrence la non-répudiation.

D'un point de vue pratique, l'utilisation des algorithmes de chiffrement, tel que les algorithmes de chiffrement à clé publique, où le fait même de chiffrer le message via la clé privée constitue une forme de signature, puisque seul le possesseur de cette clé est habilité à l'utiliser. Les destinataires légitimes pourront vérifier cette *signature* en déchiffrant le message via la clé publique.

A noté cependant qu'un tel schéma n'assure pas la confidentialité, car tous les correspondants ayant la clé publique peuvent déchiffrer le message. De plus et vu l'inconvénient rencontré lors de l'utilisation de tels algorithmes, en l'occurrence la lenteur induite par les calculs, il est plus judicieux si une partie seulement du message est chiffrée. Cette partie est une masse plus réduite du message, mais représentative de ce dernier (aussi dite empreinte du message).

L'utilisation d'empreinte réduit considérablement le temps nécessaire au chiffrement. L'empreinte, elle, est générer via une fonction de hachage, puis elle est chiffrée via un algorithme de chiffrement (e.g : RSA). La propriété d'unicité de la signature numérique est ainsi renforcée grâce à l'utilisation des fonctions de hachage caractérisées par la propriété de *non-collision*[4], ce qui permet par conséquence d'assurer l'intégrité du message.

[3] Personnification : Une entité, non-autorisée, se fait passer pour une autre qui l'est.
[4] Non-collision : deux entrées différentes d'une fonction de hachage n'ont pas la même sortie.

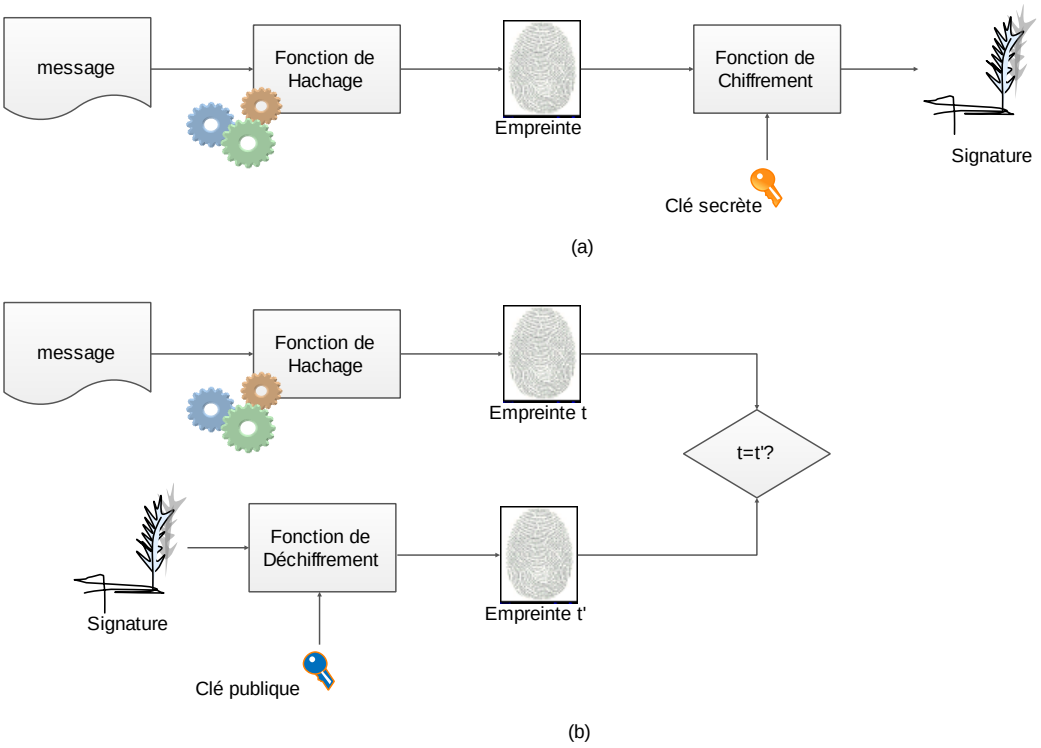


**Figure 7 Illustration de la signature numérique via une fonction de hachage : (a) génération de la signature ; (b) phase de vérification de la signature.**

#### 1.2.1.4.1.2. Le tatouage numérique

Apparu au 13ième siècle, le tatouage numérique (aussi dit *watermarking*) servait comme tags d'authentification pour les supports imprimés, son équivalent numérique sert plutôt à vérifier le copyright. Le plus ancien tatouage retrouvé, remonte à 1292 et fut retrouvé dans la ville de *Fabriano* en *Italie*, qui a joué un rôle important dans l'industrie et la fabrication du papier, domaine où les artisans usaient des tatouages pour marquer leur produit et éviter toute confusion.

L'utilisation de la technique du tatouage a vite pris de l'ampleur, et dispose aujourd'hui de son équivalente numérique, toujours dans le but d'assurer l'authentification de l'information hôte du tatouage.

Le tatouage numérique est défini comme étant une méthode qui permet d'identifier la source ou le propriétaire du copyright d'un signale digitale ou analogique, qui est inclus dans le signale même, afin de garder la trace de provenance ou afin de déterminer le propriétaire du copyright.

Le processus de tatouage numérique se compose de deux phases, à savoir la phase intégration du tatouage et la phase recouvrement (ou extraction) du tatouage. L'entrée de la première phase est constituée de la donnée à tatouer, d'une clé (publique ou privée, et l'on parlera, respectivement, de tatouage à clé publique et tatouage à clé privée) et du tatouage en soit (appelé aussi marque qui est une information de copyright). Le tatouage peut être soit un nombre, une image (un logo) ou encore un texte.

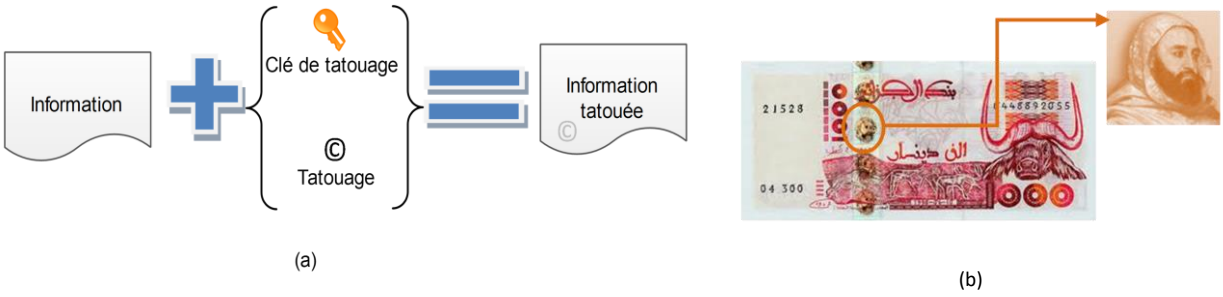


**Figure 8 Tatouage numérique : (a) Schéma général de tatouage ; (b) Tatouage sur un billet d'argent**

### 1.3. Clé et principe de KERCKHOFFS

Au départ, la sécurité de l'information dépendait des techniques de chiffrement utilisées pour *cacher* l'information. Ces techniques se résumaient en quelques manipulations et algorithmes, et se compliquaient au fur et à mesure qu'elles étaient découvertes. Il s'avère par la suite que la sécurité de l'information, ne dépendait pas seulement de ces dits algorithmes, qui se devaient d'être secrets, mais plutôt d'une information particulière qui contribue à la transformation de l'information dans le but de la cacher. Il s'agit de la clé.

L'importance de la clé dans le processus de chiffrement est renforcée par le principe de KERCKHOFFS. Ce dernier, introduit par Auguste KERCKOFFS en 1883; stipule que la sécurité d'un système ne doit pas dépendre seulement de l'algorithme de chiffrement, mais plutôt du choix de la clé de chiffrement. En fait, KERCKHOFFS énumérait un certain nombre de conditions, qui sont au nombre de six (06), et que doit remplir un système de cryptographie opérationnel. La condition portant sur l'importance de la clé faisant partie de cette énumération.

Les six conditions dans leur version originale sont comme suit :

*1° Le système doit être matériellement, sinon mathématiquement, indéchiffrable ;*

*2° Il faut qu'il n'exige pas le secret, et qu'il puisse sans inconvénient tomber entre les mains de l'ennemi ;*

*3° La clé doit pouvoir en être communiquée et retenue sans le secours de notes écrites, et être changée ou modifiée au gré des correspondants ;*

*4° Il faut qu'il soit applicable à la correspondance télégraphique ;*

*5° Il faut qu'il soit portatif, et que son maniement ou son fonctionnement n'exige pas le concours de plusieurs personnes ;*

*6° Enfin, il est nécessaire, vue les circonstances qui en commandent l'application, que le système soit d'un usage facile, ne demandant ni tension d'esprit, ni la connaissance d'une longue série de règles à observer.*[5]

### 1.3.1. Gestion et distribution de clé dans un groupe

Vu l'importance de cette information, qui est la clé, plusieurs algorithmes et protocoles ont été proposé, surtout dans le contexte de groupe de communication, où l'opération de gestion de clé devient très difficile au fur et à mesure que le nombre de participants dans le groupe augmente.

En 2005 Yacine Chellal et al. proposent une nouvelle taxonomie que nous adoptant ici. Dans cette taxonomie on distingue entre deux classes de clé : clé commune par groupe TEK (***T**raffic **E**cryption **K**ey*) où tous les membres du groupe partagent la même clé, et clé indépendante par sous-groupe.

#### 1.1.1.1.1. Première classe

Les auteurs regroupent dans cette classe des protocoles de distribution de clé où les membres du groupe partagent la même TEK. Ils distinguent entre 3 sous-classes :

Dans la première sous-classe, dite *centralisée*, il est toujours question d'une seule entité qui gère et distribue la clé. Suivant la technique utilisée pour distribuer la TEK, les auteurs distinguent entre 3 sous-catégories :

- ✓ Clé par paire : dans cette première sous-catégorie, une clé KEK est partagée entre le serveur de clé et chaque membre du groupe.
- ✓ Diffusion de secret : l'approche se base sur la diffusion du message au lien d'une communication secret point-à-point.
- ✓ Hiérarchie de clé : l'approche permet de diminuer le nombre de messages lors de l'opération de rekeying.

La deuxième sous-classe est celle des approches *décentralisées*. Pour éviter les goulots d'étranglement en lesquels peuvent se transformer les entités centrales de gestion de clé des protocoles de la classe précédente. On y distingue également des sous-catégories :

- ✓ Orientée adhésion : où le rekeying ce fait à chaque fois qu'un membre rejoint ou quitte le groupe.
- ✓ Orientée temps (Systématique) : le rekeying ce fait à chaque intervalle de temps. Ainsi les membres quittant le groupe auront toujours l'accès au contenu sécurisé jusqu'à la fin de l'intervalle temporelle. Et les nouveaux membres n'y auront pas immédiatement accès, mais devront attendre le début d'une session pour obtenir la nouvelle clé et donc avoir accès au contenu sécurisé.

[5] Kerckhoffs disait lui-même : « *Tout le monde est d'accord pour admettre la raison d'être des trois derniers desiderata ; on ne l'est plus, lorsqu'il s'agit des trois premiers.* »

La dernière sous-classe est celle de la distribution par *accord*. Suivant la topologie virtuelle des membres du groupe, cette classe est subdivisée en :

- ✓ Coopération orientée anneau : où les membres sont disposés dans un anneau virtuel.
- ✓ Coopération orienté hiérarchie : où c'est plutôt une structuration hiérarchique qui est adoptée.
- ✓ Coopération orienté diffusion : qui se base sur la diffusion de messages secrets et distribution des calculs pour aboutir à la clé de groupe.

1.1.1.1.2. Deuxième classe

La seconde grande classe est celle des TEK communes par sous-groupe. Dans cette classe il est question d'éviter les problèmes liés au phénomène 1-effects-n, qui risque d'apparaitre dans les approches à TEK commune suite à une dynamique des membres du groupe (ajout, départ ou expulsion). En effet, avec une TEK commune, l'ajout (ou le départ) d'un membre implique une mobilisation des tous les membres du groupe pour l'établissement d'une nouvelle clé, et ce afin de garantir la confidentialité passée (respectivement future).

Dans cette classe les auteurs regroupent deux principales sous-classes :

- ✓ Orienté dynamique de membre : où le renouvellement de la clé se fait à chaque fois qu'un membre rejoint ou quitte le groupe (ou est expulsé du groupe);
- ✓ Orienté temps : où il est question de renouveler les clés de façon périodique ;

Il est clair que la classe orientée dynamique ne saurait être adaptée à des groupes où la dynamique est assez forte, où l'adhésion et le départ des membres est assez fréquent, car cela prendrait beaucoup de temps au à réaliser des renouvellements de clé. Quant à la seconde classe, orientée temps, deux cas peuvent se présenter : Le premier étant qu'un membre quitte le groupe avant l'échéance, dans ce cas, si le membre est un malveillant il pourra toujours écouter le trafic car la clé ne peut être changer avant ladite période de changement, ainsi la confidentialité future n'est nullement assurée. Le deuxième cas est qu'un nouveau membre adhère au groupe avant la période de changement de clé. Le nouveau ne pourra pas accéder à la communication tant qu'il n'aura pas la nouvelle clé et devra rester ainsi en instance jusqu'à ce que le changement de clé soit opéré.

| | Centralisée | | Décentralisée | Accord de clé distribuée | |
|---|---|---|---|---|---|
| **TEK Commune** | Paires Point-à-Point | Hiérarchie de clé | | Coopération en anneau | Coopération hiérarchique |
| | GKMP<br>Poovendran et al.<br>Dunigan and Cao | LKH<br>OFT<br>Canett et al.<br>ELK<br>CFKM | SMKD<br>IGKMP<br>Hydra<br>MARKS<br>KRONOS<br>DEP | Ingemarson et al.<br>GDH | DH-LKH<br>D-LKH<br>D-OFT<br>D-CFKM |
| **TEK Indépendante par sous-groupe** | | | Iolus<br>KHIP<br>Cipher Sequences<br>Yang et al. | | |

| | |
|---|---|
| | Proxy<br>Encryption<br>SIM-KM |

Tableau 4 Exemple Taxonomie des protocoles des protocoles de gestions de clé de groupe [37].

### 1.4. Le quantique

La puissance de calcul des machines étant en perpétuelle augmentation, le risque de casser les systèmes de sécurité et de plus en plus grand, de ce fait, il devient important de penser à des outils, sinon des machines puissantes permettant d'avoir une sécurité inconditionnelle et ne dépendant pas de la puissance de calcul de l'espion.

L'informatique quantique peut justement offrir cette sécurité inconditionnelle de par les principes sur lesquelles elle repose et que nous détaillons dans la suite de cette section.

En fait, « information quantique » est en soit un terme générique utilisé pour désigner la théorie de traitement et de la transmission de l'information utilisant les spécificités de la mécanique quantique.

#### 1.4.1.Principes de la mécanique quantique

La mécanique quantique est régie par un nombre de principes, plus ou moins déroutants, et échappant quelquefois à la logique à laquelle nous sommes habitués dans notre monde *macroscopique*.

##### 1.4.1.1. Le Qubit

Par analogie à l'informatique dite classique, l'informatique quantique a aussi un support d'information, ce dernier étant dit le Qubit (noté également qbit). Mais à la différence du bit classique, qui ne prend que les valeurs 0 ou 1 suite à la mesure de ce dernier, le qbit lui, peut, suite à une mesure, révéler les valeurs 0 ou 1 (correspondants respectivement aux états |0> et |1>) ou, plus encore, être dans un état dit de superposition, qui est un état de combinaison linéaire des deux autres états.

##### 1.4.1.2. L'intrication quantique

Relevant de la science-fiction pour certains, le principe de l'intrication quantique stipule que quand deux qubits sont intriqués s'ils sont séparés de quelques micromètres ou des kilomètres, donc arbitrairement éloignés, ces deux qubits, et donc ces deux systèmes, continuent à former un tout, une entité indissociable.

Le principe d'intrication quantique permet de réaliser ce qu'on appelle la téléportation. Mais il s'agit de téléportation de l'information et non de matière !

En effet, pour réaliser une téléportation quantique d'une information d'une particule ***A***, il est nécessaire d'utiliser une paire auxiliaire de particules intriquées ***B***, ***C***. Une particule des deux paires sera gardée par Alice alors que l'autre sera au niveau de Bob. Puis une série d'opérations quantiques sera appliquée pour préparer le système.

#### 1.4.1.3. La superposition quantique

Il est souvent difficile de concevoir l'état de superposition quantique de par l'absence d'une analogie dans le monde réel à un niveau microscopique, ceci dit, cela n'en diminue pas plus l'importance de ce phénomène.

Un exemple qui pourrait nous faire comprendre le phénomène de superposition et de voir le qubit comme une pièce de monnaie. Une pièce de monnaie peut être en position pile ou face. Mais pour une pièce de monnaie *imparfaite* qui balance il y a un état intermédiaire. Un qubit est alors en un *continuum* d'états entre |0> et |1>.

##### 1.4.1.3.1. Chat de Schrödinger

E. Schrödinger (1887-1961) explique le concept de superposition quantique par une expérience de pensée (émise en 1935) qui lui doit même son nom. L'expérience s'annonce comme suit :

Soit un chat enfermé dans une boite avec un dispositif qui libère un poison dans le cas où il détecte la désintégration d'un atome radioactif. Si l'on suppose que l'atome à une chance sur deux de se désactiver alors, le chat aurait une chance sur deux d'être vivant. Ayant la boite fermée, il serait impossible de connaitre exactement l'état du chat sans l'ouverture de la boite.

Il est donc possible, en dehors de toute mesure, et suivant les concepts de la mécanique quantique, de considérer le chat comme mort et vivant au même instant $t$.

#### 1.4.1.4. Le principe d'incertitude de Heisenberg

Le principe d'incertitude de Heisenberg est une autre révolution du monde quantique qui révoque le principe de déterminisme de la mécanique classique, prouvant encore une fois, que le monde microscopique, ou de l'infiniment petit, à ses propres lois.

Elaboré en 1927 par Heisenberg (1901-1979), le principe est également appelé principe d'indéterminisme. Suivant ce principe il sera impossible d'avoir simultanément, et exactement, les valeurs de deux observables. Si l'on mesure la vitesse d'une particule à un instant donné, il est impossible de connaitre *exactement* sa position à ce même instant. Réciproquement, s'il s'agit de mesurer sa position en premier, il ne sera possible d'en mesure exactement la vitesse. Ce qui nous permet de dire qu'il est impossible de reproduire un système quantique suite à une mesure. Ceci nous mène directement ou principe suivant, celui du non-clonage.

#### 1.4.1.5. Le non-clonage

Il est tout à fait facile de réaliser une copie d'un bit classique. En plus du fait que la copie du bit aurait la même valeur que le bit originel, la copie, elle, qui ne se fait que suite à une mesure, n'entrainerai aucune perturbation ni changement de valeur du bit originel. Cependant, il est difficile de réaliser une telle opération aussi « simple » qu'elle puisse paraitre sur un qubit. En effet, mesurer un qubit entrainerai inévitablement une modification de l'état de ce dernier, car, étant dans une superposition d'états, la mesure de ce dernier lui imposerai la prise de valeur 0 ou 1, au lieu des *deux à la fois*. Une caractéristique bien propre au qubit que lui confère le principe fondamental de non-clonage (non-clonning en Englais).

Il serait donc, selon la théorie du non-clonage, impossible de réaliser une copie d'un qubit, cela s'explique par le fait que pour le copier, il faudrait tout d'abord connaitre son état, et pour se faire il faut le mesurer, sauf qu'en le mesurant il perdra son état initial.

### 1.4.2.La distribution de clé quantique

L'accroissement de la vitesse de calcul des machines actuelles peut mettre en péril les algorithmes de chiffrement actuels, ce qui remet en cause la sécurité des systèmes qui se basent sur ces algorithmes-là. Et comme la clé est l'élément le plus important, suivant le principe de KERCKHOFFS, il est judicieux de penser à une technique qui nous permettrait d'avoir une clé sûre.

L'une des applications de la mécanique quantique est justement la distribution de clé. Une technique permettant d'avoir une clé totalement aléatoire qu'il serait possible d'utiliser à des fins cryptographiques comme le chiffrement avec un simple XOr.

Un des protocoles phares de la distribution de clé quantique on cite le BB84.

Ce protocole connu par la simplicité de l'idée mais aussi par la sécurité qu'il offre, fut conçu par Charles Bennett et Gilles Brassard et présenté lors d'une conférence en Inde en 1984 (d'où son acronyme BB84) dans leur fameux papier « Quantum Cryptography: Public-key Distribution and Coin Tossing ».

Charles Bennett et Gille Brassard avaient exploité dans leur papier un principe très important de la physique quantique, à savoir le principe d'incertitude. Ils y rappellent que dans le contexte de la théorie de l'information classique, il est convenu que toute communication peut être passivement écoutée et même copiée, par tout tiers ignorant même la signification de l'information transmise. Cependant, si l'information est codée sous forme d'états quantiques non-orthogonaux, tel que les photons polarisés, le canal de transmission ne peut être écouté, ni que l'information soit copiée sans que cela n'entraine des perturbations menant à la détection de l'espion par les utilisateurs légitimes du canal de transmission.

#### 1.1. Phases d'échange du BB84

Le déroulement du protocole de distribution de clé quantique BB84, comme décrit par ses concepteurs, passe par deux phases principales. La première consiste en un échange sur un canal quantique ; la seconde s'effectue sur un canal classique. Cette dernière étape permet aux participants à la communication de décider si oui ou non il y a eu espionnage et donc l'utilisation ou non du bit obtenu suite à l'échange quantique. Le résultat de ces échanges est une suite de bits aléatoires qui peut être utilisée ultérieurement à des fins cryptographiques comme le chiffrement via le One Time Pad.

##### 1.1.1.Première phase : échange quantique

Durant cette première phase, les deux protagonistes, Alice et Bob, s'échangent des qubits sur le canal quantique. Concrètement les qubits peuvent être des photons polarisés. Alice choisit alors une chaine de bit aléatoire et une séquence de bases de polarisation (rectilinéaire que l'on note **+** ou diagonale que l'on note **x**). Alice prépare des photons polarisés suivant l'une des deux bases de polarisation utilisées dans le protocole puis les envoie à Bob. Chaque photon polarisé représente un bit de la

séquence, suivant qu'une polarisation à 0° ou à 45° traduit un 0, et qu'un photon polarisé à 90° ou 135° traduit un 1.

A chaque envoi, Bob tente de mesurer correctement le qubit envoyé par Alice en choisissant aléatoirement l'une des deux bases de polarisation utilisées, traduisant ainsi à chaque fois les photons reçus en 0 et 1. Bob a une chance sur deux de mesurer correctement le qubit parce que toute tentative de mesurer un photon dans une polarisation qui n'est pas celle dans laquelle il a été préparé, lui fait perdre automatiquement l'information qu'il porte produisant une information tout à fait aléatoire.

### 1.1.2.Seconde phase : échange classique

La deuxième étape du protocole de distribution de clé quantique, tel introduit par ses concepteurs, se fait sur un canal classique susceptible d'être écouté.

Alice et Bob déterminent alors quels sont les photons qui ont été reçus et ceux ayant été correctement mesurés. Un photon correctement mesuré signifie que Bob a utilisé la bonne base de polarisation pour le mesurer, évitant toute perturbation et récupérant ainsi la valeur transmise par Alice.
Nous illustrons le processus ci-dessus décrit dans la figure suivante.

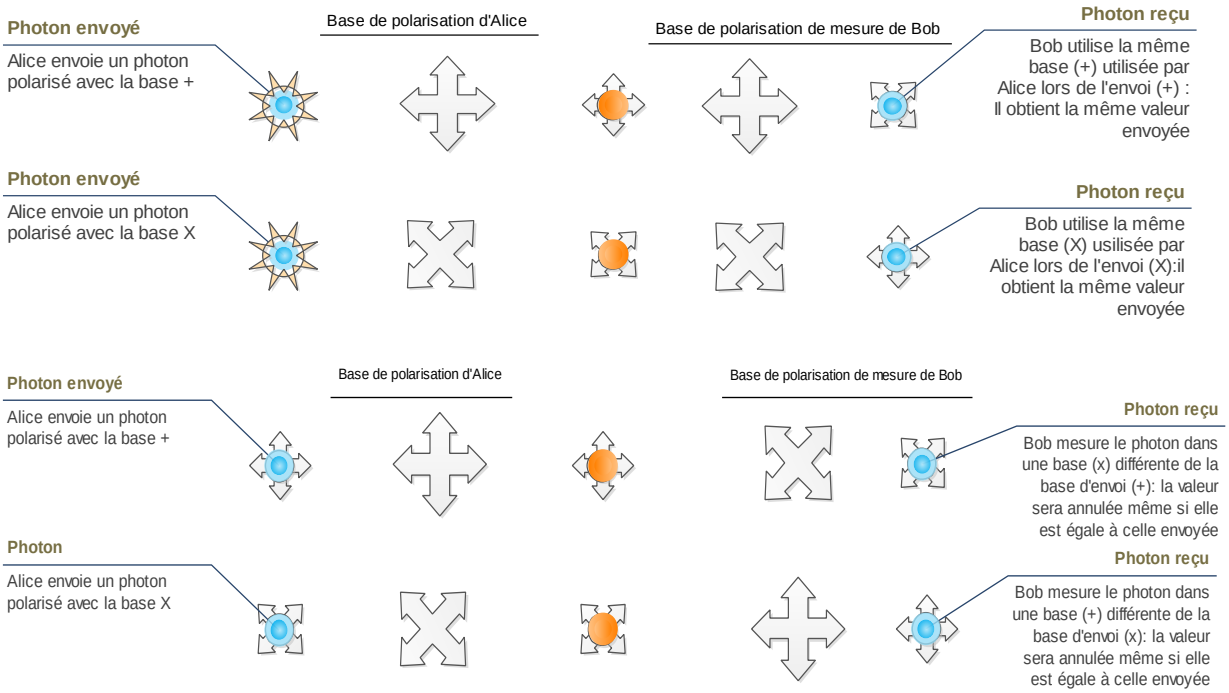


**Figure 9 Echange quantique du BB84 sans éspion [18]**

Voici un exemple explicatif de cet échange :

| | | | | | | | | | | | | | | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| Bits Alice | 1 | 0 | 0 | 1 | 1 | 0 | 1 | 0 | 1 | 0 | 1 | 1 | 1 | 0 | 1 | 0 | 1 | 0 | 0 | 1 | 1 | 0 | 1 | 0 | 1 | 0 |
| Base Alice | + | x | x | x | + | x | + | + | x | + | + | x | x | + | x | + | + | + | x | x | + | + | + | x | + | x |
| Base Bob | x | + | x | + | x | x | x | + | x | + | x | + | + | + | + | x | x | + | + | + | x | + | + | x | + | + |
| Bits Bob | 1 | 0 | 0 | 0 | 0 | 0 | 1 | 0 | 1 | 0 | 1 | 0 | 1 | 0 | 0 | 1 | 1 | 0 | 0 | 1 | 1 | 0 | 1 | 0 | 1 | 0 |

| Décision | × | × | ✓ | × | × | ✓ | × | ✓ | ✓ | ✓ | × | × | × | ✓ | × | × | × | ✓ | × | × | × | ✓ | ✓ | ✓ | ✓ | × |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|

Tableau 5 Exemple de distribution de clé quantique via BB84 sans la présence d'Eve.

Le tableau est un exemple d'échange de clé quantique entre Alice et Bob. Nous désignons par ✓ le fait que Bob utilise la bonne base de polarisation pour mesurer le photon envoyé par Alice et donc qu'il réussisse à récupérer la valeur binaire qu'il porte, cette dernière fera partie de la clé finale. Le symbole × désigne le fait que Bob utilise une base différente, et donc que la valeur du photon ainsi mesurer sera écartée, et ne figurera pas dans la clé finale. Si l'on nomme K, la chaine obtenue suite à cet échange, alors K=00010000101.

Le schéma **Error! Reference source not found.**sur la Figure 10. récapitule les différentes étapes du BB84 dans sa version standard.

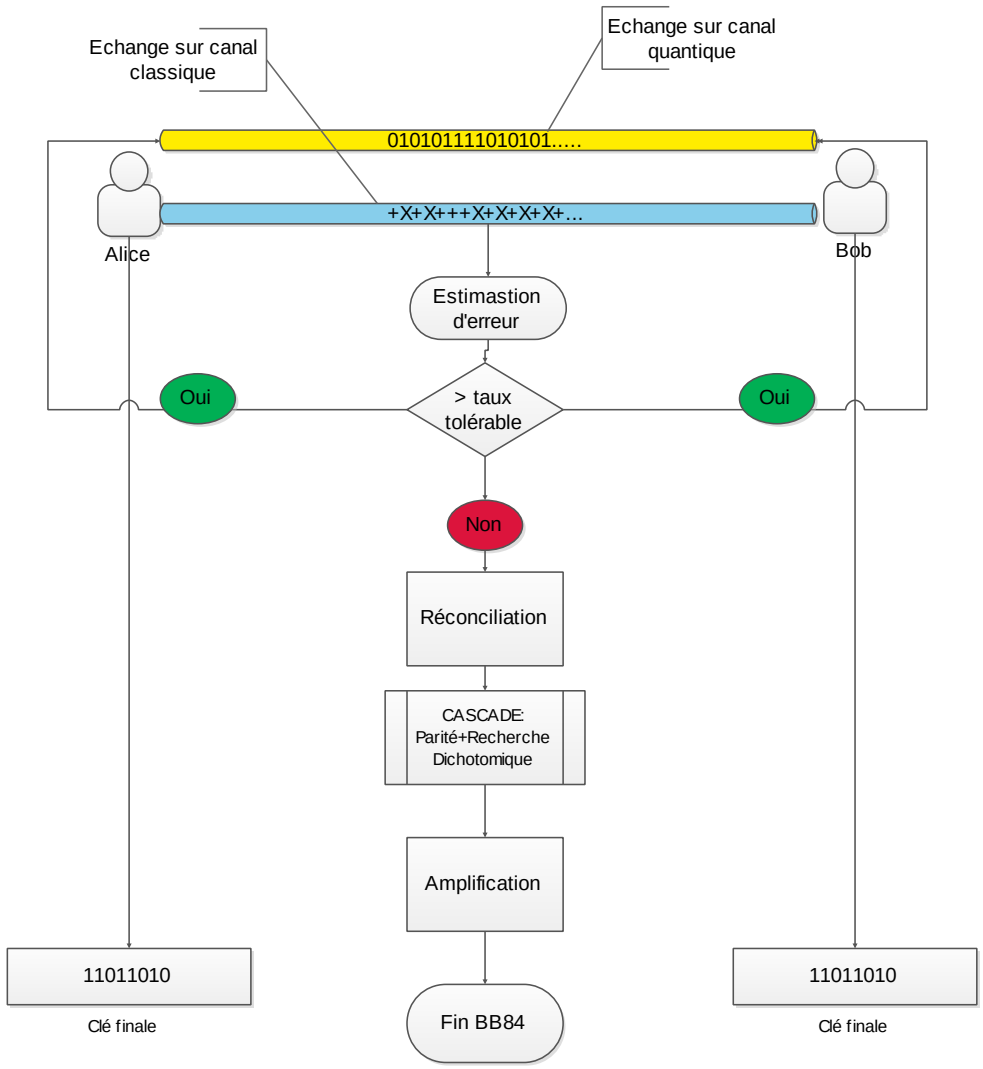


Figure 10 Schéma récapitulatif des étapes du BB84 [18].

### 1.5. Les menaces :

Nous allons nous intéresser à présent aux menaces informatiques. Nous essayons dans cette section d'en faire un survol et en citer les plus connues sans prétendre à une exhaustivité.

Les vers

Les virus

Chaval de Troie

Bombe logique

Spam et scam

Logiciel d'espionnage

### 1.6. Les attaques

Malgré les avancées perçues dans le domaine de la sécurité, certaines brèches subsistent encore et la sécurité doit être montée pour renforcer la vulnérabilité envers des menaces d'attaques que peuvent montrer nombres des protocoles de communication. En fait, il est possible de distinguer entre deux types d'attaques [5] :

#### 1.6.1.Attaques passives

Une attaque passive est une attaque où l'adversaire n'applique aucune modification aux informations. On distinguera entre observation et accès non autorisé :

*Observation non autorisée* : Où un observateur indiscret observe seulement des informations (chiffrées ou non) qui transitent sur un réseau par exemple ;

*Accès non autorisés* : Où l'intrus lit des informations mémorisées sur un ordinateur, ou écoute un trafic sur un réseau.

#### 1.6.2.Attaques actives

Dans une attaque de ce type par contre, l'attaquant modifie les informations, on distinguera également plus d'un cas :

*Le contrôle non autorisé d'un système* ; Où l'attaquant prend totalement le contrôle d'une machine ;

*La modification de l'information* ; que ce soit au niveau d'une machine ou lors de sa transmission ;

*L'accès à des services/ressources* (e.g temps de calcul, logiciel, …) auxquelles l'attaquant n'a pas le droit ;

*Le refus de service* (*Denial-of-services*) aux utilisateurs légitimes qui en ont normalement le droit.

La sécurité de l'information ne peut être réduite à des aspects purement techniques, liées le plus à l'informatique, qui en constituent certes une bonne partie, mais pas la totalité de la problématique. En effet, d'autres aspects rentrent en jeu, on citera les aspects juridiques, sociales, ergonomiques, et même psychologique et organisationnels [7]

# Séries de TDs

République Algérienne Démocratique et Populaire

Ministère de l'Enseignement Supérieur et de la Recherche Scientifique

Université Batna-2

Faculté des Mathématiques et de l'Informatique

Dép. Informatique

# TD Nº 01

***Exercice 01 :***

A- Soient les messages suivants :

1- « 90% of the time is spent in 10% of the code. » Dixit Robert Sedgewick

2- Il existe 10 types de personnes ceux qui comprennent l'informatique et les autres.

3- Instead of thinking about things, think about possibilities.

4- « Un problème sans solution est un problème mal posé. » Dixit Albert Einstein

Si l'on sait qu'une transmission sécurisée entre Alice et Bob se fait via le chiffre de César, avec une clé de chiffrement K=3 ; et que$\forall\, c \in M_i \; alors \; c \in \{\overline{A-Z}; \overline{a-z}; \overline{0-9}\}$, calculer alors les $M_i'$ correspondants tel que $M_i' = C_k(M_i)$.

B- Si pour des raisons de sécurité, Alice et Bob décident de changer la clé de chiffrement K=-3 ; et décident de continue leur échange, quels seraient alors les $M_i'$ correspondants aux messages suivant :

1- « Si tu révèles ton secret au vent, tu ne dois pas lui reprocher de le révéler à l'arbre. » Dixit Gibran Khalil Gibran.

2- « Il faut toujours se réserver le droit de rire le lendemain de ses idées de la veille. » Dixit Napoléon Bonaparte

***Exercice 02 :***

Alice et Bob décident de changer de méthode de chiffrement. Ils optent pour un chiffrement par transposition, et utilisent la clé **K**=*grain*.

1- « La valeur d'un homme tient dans sa capacité à donner et non dans sa capacité à recevoir » Dixit Albert Einstein

2- « Cookie : Anciennement petit gâteau sucré, qu'on acceptait avec plaisir. Aujourd'hui : petit fichier informatique drôlement salé, qu'il faut refuser avec véhémence. » Dixit Luc Fayard

Alice et Bob s'échange les messages suivants en utilisant toujours la même technique mais avec la clé **K**=*crypto*. Retrouver alors les messages en clair :

République Algérienne Démocratique et Populaire

Ministère de l'Enseignement Supérieur et de la Recherche Scientifique

Université Batna-2

Faculté des Mathématiques et de l'Informatique

Dép. Informatique

1- «efinn□oiartmqa□ulemtiianutsraiiu□□angenmte□u□lpaicasnsece□□da□ullcoupne□tet□re □□upslp□ietteuptl□sen□tilngleit□□□□□□» Dixit Bernard Werber

2- «uopnr□gemrma□rfionmuiaqteta□if□u□cqeeso□uv□ail□uvi□edztfe□□dapei□ra□cse□qo □uveuuvso□lu□eqz'a□ifls□□s□e» Dixit Loi Murphy

République Algérienne Démocratique et Populaire

Ministère De L'enseignement Supérieur Et De La Recherche Scientifique
Université Batna 2
Faculté des Mathématiques et Informatique
Département Informatique

# TD N° 02

***Exercice 01 :***

Soit le tableau en face.

| | 1 | 2 | 3 | 4 | 5 |
|---|---|---|---|---|---|
| 1 | a | b | c | d | e |
| 2 | f | g | h | i /j | k |
| 3 | l | m | n | o | p |
| 4 | q | r | s | t | u |
| 5 | v | w | x | y | z |

Le chiffrement avec ce tableau se fait comme suit : Chaque lettre est codée par le numéro de sa ligne||numéro de colonne.

Alice et Bob ont utilisé ce tableau, et le résultat du chiffrement de leur conversation était le suivant :

Alice : « 41451531 154344 1315 13232421214215?»

Bob : «13'154344 3115 13232421214215 1415 353431541215»

Alice : «414524 154344 353431541215?»

Bob : «13'154344 4533 232443443442241533 22421513 »

Alice: « 1544 4324 3433 1543431154112444 453315 5111422411334415 11511513 323444 133115 "4315134542244415"»

1- Découvrez la conversation d'Alice et Bob.

2- En utilisant les résultats de la question précédente, chiffrer le message suivant.

M= « Avant de vouloir qu'un logiciel soit réutilisable, il faudrait d'abord qu'il ait été utilisable - Ralph Johnson».

***Exercice 02 :***

En utilisant le chiffre de Vigenère (voir la table au verso) et le mot clé K= « sécurité » chiffrez le message suivant :

1- L'intégrité est une composante essentielle de la sécurité. Et pas seulement en informatique !

2- UNIX is basically a simple operating system, but you have to be a genius to understand the simplicity.

***Exercice 03 :***

Décidant que toutes les clés utilisées jusqu'à maintenant lors de leur communication, n'ont pas été sûre, Alice et Bob veulent générer une clé secrète. Ils utilisent pour cela le protocole Diffie-Helleman, avec les paramètres suivants : p=11, w=7. Alice utilise a=3 et Bob utilise b=6.

1- Quelle est la clé obtenue après calcul ?

Une troisième personne, Charles, rejoins Alice et Bob. Les trois décident de renouveler leur clé avec les données suivantes : p=23, w=3, a=6, b=4, et c=3

2- Calculer la nouvelle clé.

| Mot clé | Message en clair | | | | | | | | | | | | | | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | a | b | c | d | e | f | g | h | i | j | k | l | m | n | o | p | q | r | s | t | u | v | w | x | y | z |
| a | a | b | c | d | e | f | g | h | i | j | k | l | m | n | o | p | q | r | s | t | u | v | w | x | y | z |
| b | b | c | d | e | f | g | h | i | j | k | l | m | n | o | p | q | r | s | t | u | v | w | x | y | z | a |
| c | c | d | e | f | g | h | i | j | k | l | m | n | o | p | q | r | s | t | u | v | w | x | y | z | a | b |
| d | d | e | f | g | h | i | j | k | l | m | n | o | p | q | r | s | t | u | v | w | x | y | z | a | b | c |
| e | e | f | g | h | i | j | k | l | m | n | o | p | q | r | s | t | u | v | w | x | y | z | a | b | c | d |
| f | f | g | h | i | j | k | l | m | n | o | p | q | r | s | t | u | v | w | x | y | z | a | b | c | d | e |
| g | g | h | i | j | k | l | m | n | o | p | q | r | s | t | u | v | w | x | y | z | a | b | c | d | e | f |
| h | h | i | j | k | l | m | n | o | p | q | r | s | t | u | v | w | x | y | z | a | b | c | d | e | f | g |
| i | i | j | k | l | m | n | o | p | q | r | s | t | u | v | w | x | y | z | a | b | c | d | e | f | g | h |
| j | j | k | l | m | n | o | p | q | r | s | t | u | v | w | x | y | z | a | b | c | d | e | f | g | h | i |
| k | k | l | m | n | o | p | q | r | s | t | u | v | w | x | y | z | a | b | c | d | e | f | g | h | i | j |
| l | l | m | n | o | p | q | r | s | t | u | v | w | x | y | z | a | b | c | d | e | f | g | h | i | j | k |
| m | m | n | o | p | q | r | s | t | u | v | w | x | y | z | a | b | c | d | e | f | g | h | i | j | k | l |
| n | n | o | p | q | r | s | t | u | v | w | x | y | z | a | b | c | d | e | f | g | h | i | j | k | l | m |
| o | o | p | q | r | s | t | u | v | w | x | y | z | a | b | c | d | e | f | g | h | i | j | k | l | m | n |
| p | p | q | r | s | t | u | v | w | x | y | z | a | b | c | d | e | f | g | h | i | j | k | l | m | n | o |
| q | q | r | s | t | u | v | w | x | y | z | a | b | c | d | e | f | g | h | i | j | k | l | m | n | o | p |
| r | r | s | t | u | v | w | x | y | z | a | b | c | d | e | f | g | h | i | j | k | l | m | n | o | p | q |
| s | s | t | u | v | w | x | y | z | a | b | c | d | e | f | g | h | i | j | k | l | m | n | o | p | q | r |
| t | t | u | v | w | x | y | z | a | b | c | d | e | f | g | h | i | j | k | l | m | n | o | p | q | r | s |
| u | u | v | w | x | y | z | a | b | c | d | e | f | g | h | i | j | k | l | m | n | o | p | q | r | s | t |
| v | v | w | x | y | z | a | b | c | d | e | f | g | h | i | j | k | l | m | n | o | p | q | r | s | t | u |
| w | w | x | y | z | a | b | c | d | e | f | g | h | i | j | k | l | m | n | o | p | q | r | s | t | u | v |
| x | x | y | z | a | b | c | d | e | f | g | h | i | j | k | l | m | n | o | p | q | r | s | t | u | v | w |
| y | y | z | a | b | c | d | e | f | g | h | i | j | k | l | m | n | o | p | q | r | s | t | u | v | w | x |
| z | z | a | b | c | d | e | f | g | h | i | j | k | l | m | n | o | p | q | r | s | t | u | v | w | x | y |

République Algérienne Démocratique et Populaire

Ministère De L'enseignement Supérieur Et De La Recherche Scientifique
Université Batna 2
Faculté des Mathématiques et Informatique
Département Informatique

# TD Nº 03

***RSA :***

1. Choisir *p* et *q*, deux nombres premiers distincts ;
2. calculer leur produit *n* = *pq*, appelé *module de chiffrement* ;
3. calculer ϕ(*N*) = (*p* - 1)(*q* -1) (c'est la valeur de l'indicatrice d'Euler en *N*) ;
4. choisir un entier naturel *e* **premier** avec ϕ(N) et strictement inférieur à ϕ(N), appelé *exposant de chiffrement* ;
5. calculer l'entier naturel *d*, inverse de *e* modulo ϕ(*N*), et strictement inférieur à ϕ(*N*), appelé *exposant de déchiffrement* ; *d* peut se calculer efficacement par l'algorithme d'Euclide étendu.

Chiffrement : $M' = M^e \ mod \ N$

Déchiffrement : $M \ \ = M'^d \ mod \ N$

***Inverse modulo et Euclide étendu (****Exemple introductif*[6]***):***

**Définition : *u*** est un inverse de ***a*** modulo ***n*** s'il existe un entier  tel que

Soit deux nombres 120, 23, alors :

Dans ce cas, le reste obtenu à l'avant-dernière ligne donne le PGCD égal à 1 ; c'est-à-dire que 120 et 23 sont premiers entre eux. Maintenant présentons autrement les divisions précédentes :

| |
|---|
| **120 ÷ 23 = 5 reste 5** |
| **23 ÷ 5 = 4 reste 3** |
| **5 ÷ 3 = 1 reste 2** |
| **3 ÷ 2 = 1 reste 1** |
| **2 ÷ 1 = 2 reste 0** |

| **Reste** | **=** | **Dividende** | **-** | **Quotient** | **×** | **Diviseur** |
|---|---|---|---|---|---|---|
| **5** | **=** | **120** | **-** | **5** | **×** | **23** |
| **3** | **=** | **23** | **-** | **4** | **×** | **5** |
| **2** | **=** | **5** | **-** | **1** | **×** | **3** |
| **1** | **=** | **3** | **-** | **1** | **×** | **2** |
| **0** | **=** | **2** | **-** | **2** | **×** | **1** |

Il est possible de possible de représenter les résultats de la manière suivante :

| **r** | | | | | | | | | | | | | **=** | **u** | **×** | **a** | **+** | **v** | **×** | **b** |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| **120** | | | | | | | | | | | | | **=** | **1** | **×** | **120** | **+** | **0** | **×** | **23** |

[6] https://fr.wikipedia.org/wiki/Algorithme_d%27Euclide_%C3%A9tendu dernière consultation 07.05.2016 à 23 : 19

| | | | | | | | | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| **23** | | | | | | | | | | | | | **=** | **0** | **×** | **120** | **+** | **1** | **×** | **23** |
| **5** | **=** | **120** | **-** | **5** | **×** | **23** | | | | | | | **=** | **1** | **×** | **120** | **+** | **-5** | **×** | **23** |
| **3** | **=** | **23** | **-** | **4** | **×** | **5** | **=** | **1×23** | **-** | **4** | **×** | **(1×120 - 5×23)** | **=** | **-4** | **×** | **120** | **+** | **21** | **×** | **23** |
| **2** | **=** | **5** | **-** | **1** | **×** | **3** | **=** | **(1×120 - 5×23)** | **-** | **1** | **×** | **(-4×120 + 21×23)** | **=** | **5** | **×** | **120** | **+** | **-26** | **×** | **23** |
| **1** | **=** | **3** | **-** | **1** | **×** | **2** | **=** | **(-4×120 + 21×23)** | **-** | **1** | **×** | **(5×120 - 26×23)** | **=** | **-9** | **×** | **120** | **+** | **47** | **×** | **23** |

Suivant la définition précédente 1=(-9)*120+47*23 est de la forme 1=a*u+n*v, ceci signifie que -9 est l'inverse pour la multiplication de 120 modulo 23, parce que 1 = -9 × 120 (mod 23).

---

**Exercice 01 :**

1- Soit deux participants dans un groupe de communication, Alice et Bob qui veulent communiquer de manière secrète. Ils décident d'utiliser le chiffrement RSA.

   a. Quel est le type de ce chiffrement ?

2- Alice et Bob choisissent p=3 et q=11. Alice choisit e=3 comme clé de chiffrement.

   a. Calculer la clé de déchiffrement d'Alice

3- Bob chiffre le message suivant M=162705, après l'avoir codé en blocs de deux nombres.

   a. Calculer le résultat du chiffrement de chaque bloc.

   b. Quel est le résultat final de chiffrement.

   c. Décoder le message reçu par Bob et vérifier que c'est bien celui envoyé par Alice

**Exercice 02 :**

Considérons le système RSA utilisé par Alice et Bob avec p=19 et q=23.

1- Calculer **N** ;

2- Calculer l'exposant **d** associé à e=9 et e=14 ;

3- Calculer l'exposant **d** associé à e=17.

**Exercice 03 :**

Alice et Bob calculent une clé via un échange quantique. Ils obtiennent les résultats suivants :

| | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| **Base Alice** | + | x | x | X | + | x | + | + | x | + | + | x | x | + | x | X | x | + | + | + | x | x | + | + | + | x | + | x |
| **Valeur Alice** | 1 | 0 | 0 | 1 | 1 | 0 | 1 | 0 | 0 | 1 | 1 | 1 | 0 | 0 | 1 | 1 | 1 | 0 | 1 | 0 | 0 | 1 | 1 | 0 | 1 | 0 | 1 | 0 |
| **Base Bob** | x | + | x | + | x | X | x | + | + | X | x | + | + | + | + | + | + | x | x | + | + | + | x | + | + | x | + | + |
| **Valeur Bob** | 1 | 0 | 0 | 0 | 0 | 0 | 1 | 0 | 1 | 1 | 1 | 0 | 1 | 0 | 1 | 1 | 0 | 1 | 1 | 0 | 0 | 1 | 1 | 0 | 1 | 0 | 1 | 0 |

a. Calculer la clé **K** obtenue par Alice et Bob suite à cet échange.

b. Si l'on sait que l'équivalent décimal de la clé **K** a été utilisée pour chiffrer le message **M** suivant via le chiffre de César, calculer alors le résultat du chiffrement **M'**

M= « il vaut mieux viser la perfection et la rater que viser la médiocrité et l'atteindre »

# Travaux cités


[1] **Willam, Stallings.** *Cryptography and Network security Principles and practice.* New York : Pearson, 2011. 978-0-13-705632-3.

[2] **NIST.** An Introduction to Computer Security:The NIST Handbook. Special Publication 800-12.

[3] **Alfred, J. Menezes, Paul C, van Oorschot et Scott A, Vanstone.** *Handbook of Applied cryptography.* s.l. : CRC Press, Août 1996. 0849385237.

[4] **Henk C.A., van Tilborg.** *Encyclopedia of cryptography and security.* s.l. : Springer, 2005. 978-0387-23483-0.

[5] **Martin, Bruno.** *Codage, cryptographie et applications.* s.l. : Presses polythechniques et universitaires romandes, 29 avril 2004. 2880745691.

[6] **Hassler, Vesna.** Introduction to communication security. [auteur du livre] Sklavos Nicolas et Zhang Xinmiao. *Wireless security and cryptography: Specification and implementation.* s.l. : CRC Press, 2007.

[7] **Laurent, Bloche et Christophe, Wolfhugel.** *Sécurité informatique: principes et méthodes.* Paris : Edition Eyrolles, 2007. 2-212-12021-4.

[8] **Stefan, Katzenbeisser et Fabien A.P., Petitcolas.** *Information Hiding Techniques for Steganography and Digital Watermarking.* Boston-Londre : Artech House, 2000. 1-58053-035-4.

[9] **Frédéric, Grosshans.** *Communication et cryptographie quantique avec variables continues.* Paris : Institut d'optique Laboratoire Charles Fabry, Université Paris XI UFR Scientifique d'Orsay, 2002. 7080.

[10] *La cryptographie militaire.* **Kerckoffs, Auguste.** s.l. : Journal des Sciences Militaires, Janvier-Fevrier 1883, Vol. 9, pp. 5-38 161-191.

[11] *Group Key Management Protocols: A Novel Taxonomy.* **Yacine, Challal et Hamida, Seba.** 1, 2005, INTERNATIONAL JOURNAL OF INFORMATION TECHNOLOGY, Vol. 2, pp. 105-118. 1305-2403.

[12] **Le Bellac, Michel.** *Physique quantique.* 2e édition. s.l. : CNRS Edition, 2007. ISBN 978-2-271-06584-1.

[13] **Michael A, Nielsen et Isaac L, Chuang.** *Quantum Computation and Quantum Information.* New York : Cambridge University Press, 2010. 978-1-107-00217-3.

[14] **Louis-Gavet, Guy.** *La physique quantique.* Paris : Eyrolles, 2012. 978-2-212-55276-8.

[15] *A single quantum cannot be cloned.* **Wootters, William K. et Zurek, Wojciech H.** 5886, 28 October 1982, Nature, Vol. 299, pp. 802-803. doi:10.1038/299802a0.

[16] **Gharout, Said.** Sécurité des communications dans les groupes dynamiques. Compiègne, France : UTC Université des Technologie Compiègne, 2009. Thèse de Doctorat.