

Chapitre 2

Algorithmes cryptographiques

Sommaire :

2.	Terminologie.....	15
3.	Propriétés de sécurité.....	16
4.	Cryptographie moderne.....	17
4.1.	La cryptographie symétrique	18
4.2.	La cryptographie asymétrique	23
4.3.	Cryptographie hybride	27

1. Introduction

Pendant longtemps la science des secrets était utilisée seulement dans certains domaines plus au moins très sensibles (diplomatie, militaire), mais depuis l'avancement considérable des technologies actuelles en matière de traitement de données, de puissance de calcul et de réseaux de télécommunication, elle est devenue, une tâche critique dans un nombre important d'applications telles que l'historique médical, la sécurité sur internet, la sécurité des réseaux...etc.

Les premiers signes d'une cryptographie semblent remonter à près de 4000 ans, les inscriptions de hiéroglyphes retrouvés sur des tombes égyptiennes ont été apparemment modifiées pour en obscurcir le sens. Quoique qu'il en soit, les recherches archéologiques semblent montrer que les écritures "secrètes" sont apparues en même temps que l'invention de l'écriture elle-même.

Mais les faits les plus tangibles sont apparus au 5e siècle avant notre ère. En effet, on apprend que les Spartiates utilisaient des « scytales », bâtonnets autour desquels ils enroulaient une bandelette de parchemin. Puis ils écrivaient le long de la scytale. Une fois déroulée, le message inscrit sur la bandelette devenait incompréhensible. Le récepteur du message devait utiliser une scytale identique à celle de l'émetteur pour déchiffrer le message. Bien sûr, cette méthode étant très simple, elle devait être gardée secrète.

Au 20e siècle, l'exemple le plus connu est celui du décryptage de l'appareil (Enigma « Machine conçue par le chiffre allemand servant à crypter les messages entre nazis »), utilisé

par les allemands et les japonais. Ce décryptage a fortement joué dans la victoire des alliés lors de la seconde guerre mondiale. [13]

Aujourd'hui, l'usage de la cryptologie s'est banalisé. On le retrouve quotidiennement avec les cartes bleues, téléphones portables, Internet ou encore les titres de transport.

Dans ce chapitre nous allons détailler les grandes lignes des principes de la cryptographie. La principale distinction se fera entre les chiffrements de type symétrique et type asymétrique et autre type de chiffrement « hybride ».

2. Terminologies

Comme toute science, celle-ci possède son propre langage, étant donnée la relative jeunesse de cette science, et le fait qu'une très grande partie des publications dans ce domaine sont en langue anglaise, le problème de la terminologie francophone se pose, parfois par manque de traduction. Les termes les plus utilisés en cryptographie sont :

- ü **Chiffrement** : est le procédé grâce auquel on peut rendre la compréhension d'un document impossible à toute personne qui n'a pas la clé de déchiffrement.
- ü **Clé** : est un paramètre utilisé en entrée d'une opération cryptographique.
- ü **Déchiffrer** consiste à retrouver le texte original (aussi appelé clair) d'un message chiffré dont on possède la clé de déchiffrement.
- ü **Décrypter** consiste à retrouver le texte original à partir d'un message chiffré sans posséder la clé de déchiffrement.
- ü **Texte clair** (Clear text ou Plain text) : Caractères ou bits sous une forme lisible par un humain ou une machine.
- ü **Texte chiffré [Cipher text]** : Résultat de la manipulation de caractères ou de bits via des substitutions, transpositions, ou les deux.
- ü **Cryptologie** : étymologiquement la science du secret, ne peut être vraiment considérée comme une science que depuis peu de temps. Cette science englobe la cryptographie, l'écriture secrète et la cryptanalyse, l'analyse de cette dernière. On peut dire que la cryptologie est un art ancien et une science nouvelle.
- ü **Cryptographie** : est une des disciplines de la cryptologie s'attachant à protéger des messages (assurant confidentialité et/ou authenticité) en s'aidant souvent de secrets ou clés. Le mot cryptographie découle des mots grecs "krypto" (je cache) et "graphe" (le document).

- ü **Cryptanalyse** : L'analyse cryptographique ou Cryptanalyse a pour objet de percer écran logique derrière lequel sont cachées les informations chiffrées.

3. Propriétés de sécurité

Le but de la cryptographie traditionnelle est d'élaborer des méthodes permettant de transmettre des données de manière confidentielle par chiffrement, mais la cryptographie moderne est de traiter plus généralement des problèmes de sécurité des communications et de fournir un certain nombre de services de sécurité :

- 3.1. Confidentialité** : est un service qui sert à cacher le contenu de l'information à tous sauf pour ceux qui sont autorisés, le secret est un terme synonyme de confidentialité de vie privée.

Il y a de nombreuses approches servant à rendre l'information confidentielle, que ce soit des méthodes physiques ou des algorithmes mathématiques qui rendent des données inintelligibles.

- 3.2. Intégrité des données** : est un service qui empêche l'altération non autorisée des données, pour assurer l'intégrité de données, il faut avoir la capacité de détecter n'importe quelle manipulation même minime par des parties non autorisées, la manipulation de données inclut des actes tels que l'insertion, l'effacement et la substitution.

- 3.3. Authentification des divers acteurs** : est un service lié à l'identification, cette fonction s'applique à toutes les entités qui échangent l'information et à l'information elle-même, deux parties entrant dans une communication doivent s'identifier l'un l'autre, l'information livrée sur un canal doit être authentifiée quant à son origine, sa date d'origine, le contenu des données, la date et l'heure d'envoi, etc.

Pour ces raisons cet aspect de cryptographie est d'habitude subdivisé en deux classes principales : authentification d'entité et authentification d'origine de données. L'authentification d'origine de données fournit implicitement l'intégrité de données (si un message est modifié, la source a changé).

- 3.4. Non-répudiation d'un contrat numérique** : est un service qui empêche une entité de nier des obligations précédentes ou des actions. Quand les conflits surgissent en raison d'une entité niant que certaines actions ont été prises, le moyen de résoudre cette situation est nécessaire, par exemple, une entité peut autoriser l'achat d'une propriété (terrain, action boursières,...) par une autre entité et plus tard nier que

l'on a accordé une telle autorisation, une procédure impliquant un tiers de confiance est nécessaire pour résoudre ce conflit.

3.5. Signature numérique : la norme ISO 7498-2 définit la signature numérique comme 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 et protégeant contre la contrefaçon (par le destinataire, par exemple) ", la mention "protégeant contre la contrefaçon " implique que seul l'expéditeur doit être capable de générer la signature. [14]

Une signature numérique fournit donc les services d'authentification de l'origine des données, d'intégrité des données et de non-répudiation.

3.6. Certificat numérique : est une chaîne de caractères, signée par l'AC (L'autorité de certification), et qui contient au moins les informations suivantes :

- ü Le nom d'utilisateur.
- ü Les clés publiques de l'utilisateur.
- ü Les noms des algorithmes dans lesquels ces clés publiques sont utilisées.
- ü Le numéro de série du certificat.
- ü Les dates de début et de fin de validité du certificat.
- ü Le nom de l'AC.
- ü Les restrictions qui s'appliquent à l'usage du certificat. [15]

3.7. L'autorité de certification : l'organisme qui assure la délivrance et le renouvellement des certificats, la diffusion des listes de révocation et des clés publiques.

4. Cryptographie moderne

La cryptographie moderne s'attaque en fait plus généralement aux problèmes de sécurité des communications, le but est d'offrir un certain nombre de services de sécurité comme la confidentialité, l'intégrité, l'authentification des données transmises et l'authentification d'un tiers, pour cela, on utilise un certain nombre de mécanismes basés sur des algorithmes cryptographique.

Nous allons voir, quelles sont les techniques que la cryptographie fournit pour réaliser ces mécanismes :

4.1. La cryptographie symétrique

La cryptographie symétrique, aussi connue sous le nom de cryptographie à clé secrète ou cryptographie conventionnelle, est la plus ancienne historiquement. Elle est extrêmement répandue à cause de ses performances remarquables, elle suppose qu'au moins deux personnes partagent la connaissance de la même clé secrète, ce qui leur confère donc un rôle symétrique, elle s'appuie principalement sur les fonctions booléennes et les statistiques.

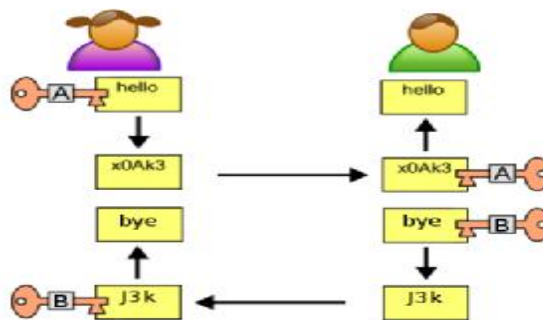


Figure 2.1 principe générale de cryptographie symétrique. [13]

- ✓ **Services offerts par la cryptographie symétrique :** la cryptographie symétrique répond aux objectifs de confidentialité car les messages étant encryptés, l'intégrité est également garantie, car une modification sur le message par un tiers engendrait un résultat de déchiffrement incohérent.

La structure du fichier étant corrompue, l'authentification des participants est basée sur le fait qu'ils sont les seuls à partager le secret de la clé, ces éléments sont valables dans la mesure où la clé secrète est préservée.

- ✓ **Inconvénients de la cryptographie symétrique :** Le problème majeur dans la cryptographie à clé secrète réside dans la distribution des clés.

Avec le passage à l'ère numérique, ce sont désormais des suites de bits qui sont chiffrés, Distingue deux types d'algorithme symétrique de chiffrement :

- 4.1.1. Chiffrement par bloc :** le message clair est découpé en une multitude de blocs relativement grands (par exemple 128 bits) et on opère des opérations bien choisies sur les blocs.

Les algorithmes de chiffrement par bloc sont nombreux et variées, Nous ne pouvons pas parler de tous les algorithmes, Nous nous occupons de certains algorithmes importants et nécessaire comme (AES, IDEA).

✓ Algorithme AES (Advanced Encryption Standard)

Le développement de l'AES a été instigué par le NIST (National Institute of Standards and Technology) le 2 janvier 1997. L'algorithme a été choisi il y a peu de temps : il s'agit de l'algorithme Rijndael (prononcer "Raindal"). Cet algorithme suit les spécifications suivantes.

Ø l'AES est un standard, donc libre d'utilisation, sans restriction d'usage ni brevet.

Ø c'est un algorithme de type symétrique

Ø c'est un algorithme de chiffrement par blocs

En termes décimaux, ces différentes tailles possibles signifient concrètement que:

3.4×10^{38} clés de 128-bit possibles

6.2×10^{57} clés de 192-bit possibles

1.1×10^{77} clés de 256-bit possibles [17]

Fonctionnement

L'algorithme prend en entrée un bloc de 128 bits (16 octets), la clé fait 128, 192 ou 256 bits. Les 16 octets en entrée sont permutés selon une table définie au préalable. Ces octets sont ensuite placés dans une matrice de 4x4 éléments et ses lignes subissent une rotation vers la droite. L'incrément pour la rotation varie selon le numéro de la ligne. Une transformation linéaire est ensuite appliquée sur la matrice, elle consiste en la multiplication binaire de chaque élément de la matrice avec des polynômes issus d'une matrice auxiliaire, cette multiplication est soumise à des règles spéciales selon $GF(2^8)$ (groupe de Galois ou corps fini). La transformation linéaire garantit une meilleure diffusion (propagation des bits dans la structure) sur plusieurs tours.

Finalement, un XOR entre la matrice et une autre matrice permet d'obtenir une matrice intermédiaire. Ces différentes opérations sont répétées plusieurs fois et définissent un « tour ». Pour une clé de 128, 192 ou 256, AES nécessite respectivement 10, 12 ou 14 tours. [18]

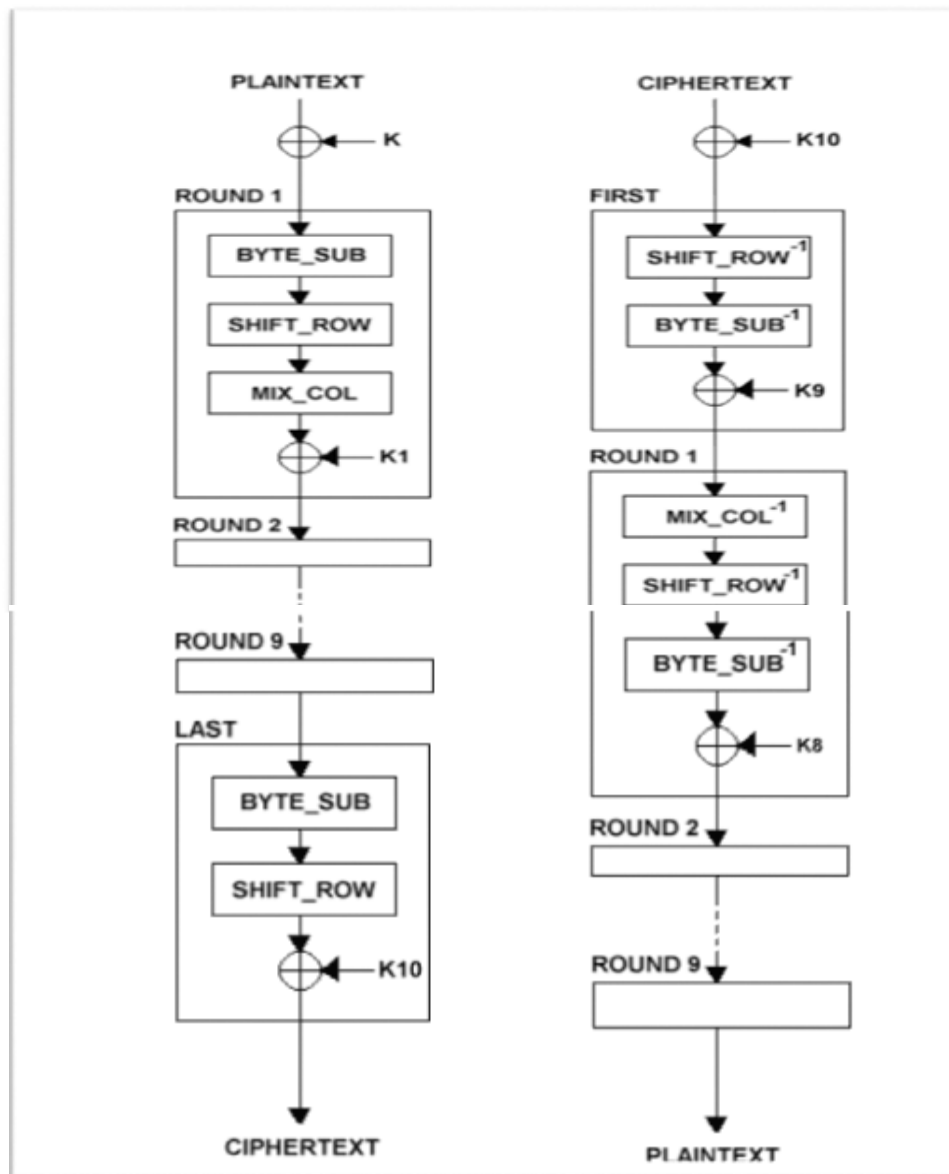


Figure 2.2 chiffrement et déchiffrement par AES. [17]

Pour une étude détaillée de l'AES, voir le cours : [16]

- ▼ **Algorithme IDEA** (International Data Encryption Algorithm) : Autre solution de chiffrement par blocs de 64 bits basé sur huit étages facilement réalisable en matériel ou en logiciel, les opérations utilisées sont des opérations arithmétiques:

- Ø Ou exclusif \oplus
- Ø Addition modulo \boxplus 216
- Ø Multiplication modulo $2^{16}+1$ \boxtimes [19]

- ✚ **Fonctionnement** : Le bloc d'entrée de 64 bits est divisé en 4 blocs de 16 bits A, B, C et D. Les 8 premières sous-clés sont directement tirées de la clé principale. Les 8 clés suivantes sont obtenues de la même façon, après une permutation à gauche de 25 bits, et ainsi de suite. [13]

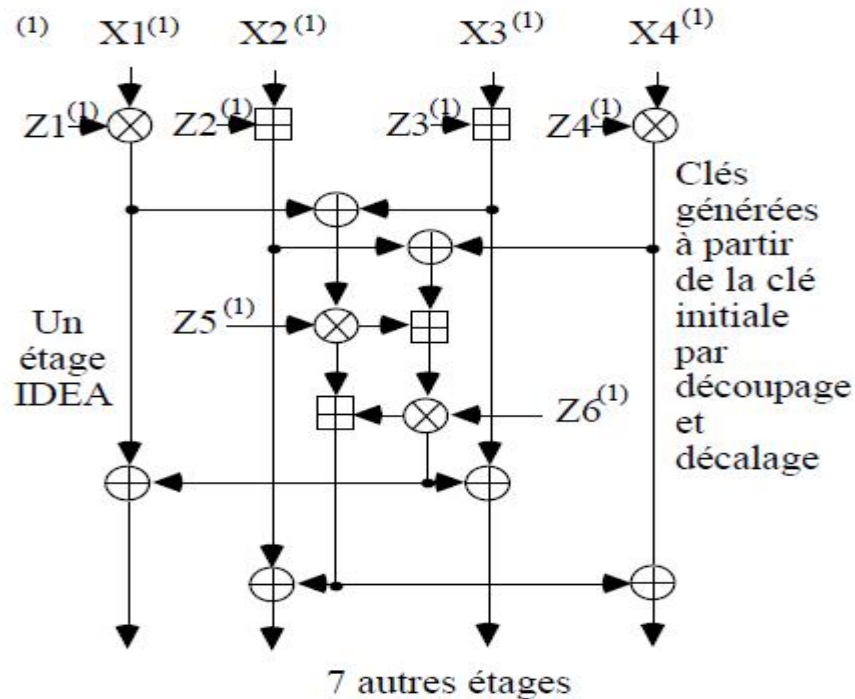


Figure 2.3 chiffrement par IDEA. [19]

✚ Les avantages

- Ø IDEA est considéré par les spécialistes comme l'un des meilleurs cryptosystème à clé privée.
- Ø La longueur de clé est élevée (128 bits).
- Ø La vitesse de chiffrement et de Déchiffrement peut-être élevée au moyen de circuits spéciaux. Circuits à 55 Mb/s et 177 Mb/s En logiciel sur 386 33Mhz: 880 Kb/s.
- Ø Les attaques semblent difficile mais le système est assez récent (1990). [19]

4.1.2 Chiffrement par flot (Stream Cipher): le message clair est considéré comme un flot de bits (ou d'octets), et il est combiné avec un autre flot de bits (ou d'octets) généré de façon pseudo- aléatoire.

Nous choisissons un algorithme de chiffrement par flot très connu (RC4).

✓ Algorithme RC4 (Rivest Cipher 4)

RC4 fonctionne de la façon suivante :

La clef RC4 permet d'initialiser un tableau de 256 octets en répétant la clef autant de fois que nécessaire pour remplir le tableau. Par la suite, des opérations très simples sont effectuées, les octets sont déplacés dans le tableau, des additions sont effectuées, etc. Le but est de mélanger autant que possible le tableau. Au final on obtient une suite de bits qui parait tout à fait aléatoire, par la suite on peut extraire des bits par conséquent pseudo-aléatoires qui peuvent être utilisés pour chiffrer les données via un XOR.

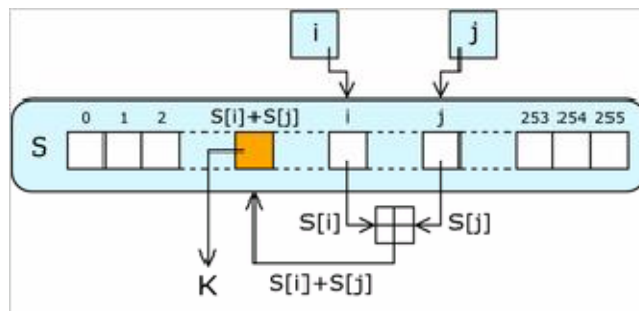


Figure 2.4 principe cryptographie RC4. [24]

✚ Étapes :

1. Générer deux tables P et K de taille 256 octets.
2. Initialiser la première table P par les entiers de 0 à 255 (table d'états).
3. Remplir la deuxième table K avec la clé secrète.
4. Permuter pseudo-aléatoirement la table P en utilisant la clé secrète.
5. Permuter pseudo-aléatoirement la table P avec elle-même.
6. Additionner la séquence ainsi obtenue de la table P avec le flux des données.

✚ Génération de la permutation :

```

◆ Pour i de 0 à 255
    P[i] := i ;
◆ Finpour

j := 0 ;
◆ Pour i de 0 à 255
    j := (j + P[i] + K[i mod |K|]) mod 256;
    Échanger (P[i], P[j]);
◆ Finpour
  
```

✚ Génération de la séquence :

```

i := 0 ;
j := 0 ;
♦ Tant_que générer une sortie:
    i := (i + 1) mod 256;
    j := (j + P[i]) mod 256;

    /* permutation de P */
    Échanger (P[i], P[j]);
    S = P [(P[i] + P[j]) mod 256];

    /* chiffrement du message M */
    C = S  $\oplus$  M
♦ Fintant_que. [25]

```

4.2. La cryptographie asymétrique

Le principe d'un code asymétrique (aussi appelé à clé publique) est que, contrairement au code symétrique, les deux interlocuteurs ne partagent pas la même clé. En effet, la personne qui veut envoyer un message utilise la clé publique de son correspondant, celui-ci déchiffre alors ce message à partir de sa clé privée que lui seul connaît, on voit ici que contrairement à un codage symétrique, le chiffrement et le déchiffrement se font par des opérations complètement différentes.

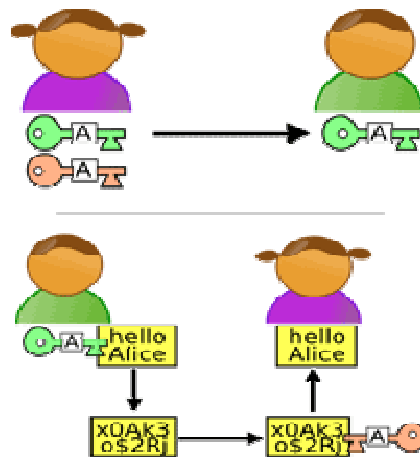


Figure 2.5 principe générale de cryptographie asymétrique. [13]

Cette technique permet de répondre à la problématique du partage sécurisé des clés publiques entre des correspondants. En effet, en cas d'interception de la clé publique) et d'un message codé par cette clé, l'intercepteur ne pourra pas

retrouver le message d'origine, car il lui manque la clé privée possédée par le vrai destinataire du message codé.

4.2.1. Algorithme RSA :(Rivest, Shamir, Adleman)

RSA est le premier système de chiffrement à clé publique, il a été conçu en 1977 par Rivest, Shamir et Aldeman du MIT (Massachusetts Institute of Technology). Rapidement devenu un standard international, la technique RSA a été commercialisée par plus de 400 entreprises et l'on estime que plus de 400 millions de logiciels l'utilisent. [20]

RSA peut être utilisé pour assurer :

- Ü La confidentialité : seul le propriétaire de la clé privée pourra lire le message chiffré avec la clé publique correspondante.
- Ü La non-altération et la non-répudiation : seul le propriétaire de la clé privée peut signer un message (avec la clé privée). Une signature déchiffrée avec la clé publique prouvera donc l'authenticité du message.

Fonctionnement

Soit p et q deux grands nombres premiers. Il est très difficile de retrouver ces deux nombres en connaissant leur produit $n = p * q$

- Ü Pour le calcul des clés publique et privée, il faut choisir deux grands nombres premiers p et q .
- Ü On calcule le produit $n = p * q$. On choisit un grand nombre e premier avec $(p-1) * (q-1)$.
- Ü On calcule ensuite un nombre d tel que $e * d = 1 \text{ mod } (p-1) * (q-1)$.
- Ü Le couple (n, e) est la clé publique, d est la clé privée.
- Ü Le message chiffré s s'obtient en calculant : $y = x^e \text{ modulo } n$
- Ü Pour déchiffrer le message il suffit de calculer : $z = y^d \text{ modulo } n$ qui vaut x puisque $y^d = x^{ed} = x \text{ modulo } n$. [21]

Fiabilité

La sécurité de l'algorithme RSA repose sur la difficulté à factoriser n . Pour décrypter le message, il est nécessaire de trouver d connaissant e , ce qui nécessite de recalculer $(p-1) * (q-1)$. Et donc de connaître p et q , les deux facteurs premiers de n .

la factorisation d'un entier (de très grande taille) en facteurs premiers est extrêmement difficile, cette opération nécessitant une capacité de calcul très importante. Pour exemple en 2010, l'INRIA et ses partenaires ont réussi à factoriser

une clé de 768 bits. Il leur a fallu deux ans et demi de recherche, et plus de 10^{20} calculs. C'est à ce jour le meilleur résultat connu de factorisation. [21]

4.2.2. Algorithme El GAMAL

Est un algorithme de cryptographie asymétrique basé sur les logarithmes discrets. Il a été créé par Taher Elgamal(1985), cet algorithme est utilisé par le logiciel libre GNU PrivacyGuard, de récentes versions de PGP, et d'autres systèmes de chiffrement, et n'a jamais été sous la protection d'un brevet contrairement à RSA. Il peut être utilisé pour le chiffrement et la signature électronique. L'algorithme DSA du NIST est basé sur ElGamal.

Fonctionnement

Algorithme d'ElGamal se compose de trois composants : le générateur principal, l'algorithme de chiffage, et l'algorithme de déchiffrage

Le générateur principal fonctionne comme suit :

- Le destinataire du message, Alice (comme il est de coutume en cryptologie) choisit deux paramètres non-secrets : un nombre premier p et une racine primitive de p , i.e. Un nombre g dont les puissances modulo p engendrent $\mathbb{Z}_p^* \setminus \{0\}$.
- Elle choisit aléatoirement un nombre a dans l'intervalle $[1, \dots, p-2]$ et calcule $\alpha = (g^a \bmod p)$.
- Elle publie sa clé (p, g, α) et garde secrète sa clé a .
- Bob, qui désire envoyer un message m à Alice, l'exprime sous la forme d'un nombre entre 0 et $p-1$ (quitte à le décomposer en sous-blocs de la bonne longueur).Il choisit aléatoirement un nombre b dans l'intervalle $[1, \dots, p-2]$ et calcule $\beta = (g^b \bmod p)$.

Les travaux d'algorithme de chiffage et déchiffrage comme suivant:

- Il chiffre alors son message m en $m' = \alpha^b \cdot m \bmod p$. Il transmet enfin à Alice le couple (β, m') .
- Pour déchiffrer le message de Bob, Alice détermine le nombre $x = p - 1 - a$. Elle calcule $\beta^x \cdot m' \bmod p$ et retrouve le message m initial. [22]

✚ Efficacité

Le chiffage sous ElGamal exige deux élévations à une puissance, cependant, ces élévations à une puissance sont indépendant du message et peuvent être calculées en avant du temps si besoin en est. Le déchiffage exige seulement une élévation à une puissance (plus une division, qui est en général beaucoup plus rapide). À la différence de dans RSA et Rabin systèmes, déchiffage d'ElGamal ne pouvez pas soyez accéléré par l'intermédiaire du Chines de reste.

4.2.3. La cryptographie sur courbes elliptiques (ECC)

Définition : Une courbe elliptique a pour équation générale (forme de Weierstrass) :

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6 \quad (2.1)$$

Lorsque les coordonnées (x, y) sont définies sur un corps de caractéristique strictement supérieur à 3, alors on peut réécrire l'équation de la courbe sous la forme :

$$y^2 = x^3 + ax + b \quad (2.2)$$

Pour utiliser les courbes elliptiques en cryptographie, il faut trouver un problème difficile (tel que la factorisation d'un produit en ses facteurs premiers dans le cas du RSA). Considérons l'équation

$$Q = kP, \text{ Où } Q, P \in E_p(a, b) \text{ et } k < p. \quad (2.3)$$

Il est facile de calculer Q connaissant k et P, mais il est difficile de déterminer k si on connaît Q et P. Il s'agit du problème du logarithme discret pour les courbes elliptiques $\log_P(Q)$.

Dans une utilisation réelle, le k est très grand, rendant l'attaque par force brute inutilisable (rappelons qu'a priori, l'attaque par force brute est toujours possible).

✚ ECC pour l'échange de clés

Soit un grand entier premier q et les paramètres a et b satisfaisant l'équation

$$y^2 \bmod q = (x^3 + ax + b) \bmod q, \text{ cela nous permet de définir } E_q(a, b).$$

Prenons ensuite un point de départ $G(x_1, y_1)$ dans $E_q(a, b)$ dont l'ordre n est élevé. L'ordre n d'un point sur une EC est le plus petit entier positif tel que $nG = O$.

$E_q(a, b)$ et G sont rendu publiques.

L'échange d'une clé par ECC entre deux entités Alice et Bob se déroule comme suit :

- Alice choisit un n_A inférieur à n qui sera sa clé privée. Alice génère alors sa clé publique $P_A = n_A \times G$.
- Bob choisit un n_B inférieur à n qui sera sa clé privée, Bob génère alors sa clé publique $P_B = n_B \times G$.

- Alice génère la clé secrète $K = n_A \times P_B$ et Bob génère la clé secrète $K = n_B \times P_A$.
[26]

✚ ECC pour chiffrer des données

Même si la cryptographie par courbes elliptiques est souvent employée pour l'échange d'une clé symétrique, elle est aussi utilisée pour chiffrer directement les données. Voici un exemple de cryptosystème les utilisant :

Il faudra ici encoder le texte clair m comme un point P_m de coordonnées (x, y) . C'est ce point qui sera chiffré, il faut ici aussi rendre publique un point G et un groupe elliptique $E_q(a, b)$. Les utilisateurs doivent également choisir une clé privée et générer la clé publique correspondante.

Pour chiffrer le message, Alice détermine aléatoirement un nombre entier positif k et produit C_m comme un couple de points tel que :

$$C_m = \{kG, P_m + kP_B\} \quad (2.4)$$

On remarquera l'utilisation de la clé publique de Bob, pour déchiffrer, Bob devra multiplier le premier point par sa clé privée, et soustraire le résultat au second point reçu : [26]

$$P_m + kP_B - n_B(kG) = P_m + k(n_BG) - n_B(kG) = P_m \quad (2.5)$$

✚ **Efficacité** : L'avantage d'effectuer les opérations sur les courbes elliptiques plutôt que sur Z_p^* est qu'il n'existe à ce jour pas d'attaque générale du log discret sur le groupe des points d'une courbe elliptique.

Certaines courbes ont été attaquées mais seul l'algorithme rho de Pollard (qui fonctionne sur tous les groupes et est optimal) fonctionne sur toutes les courbes. Il garantit donc le niveau de sécurité sur les courbes elliptiques. [42]

4.3. Cryptographie hybride

Cette technique a été introduite afin de profiter des avantages des deux types de chiffrement cités précédemment (symétrique/asymétrique), c'est à dire la rapidité de traitement des messages codés par cryptographie symétrique et la puissance du chiffrement des messages par cryptographie asymétrique.

Le principe est assez simple. La communication entre A et B se fait par système cryptographique symétrique, ce qui rend la communication assez rapide à chiffrer et déchiffrer. Mais la lacune de la sécurité de transmission de la clé symétrique de

chiffrement/déchiffrement est palliée par un chiffrement de cette clé, qui lui est asymétrique. [13]

Le schéma ci-dessous présenté la manière d'utilisation de cryptographie hybride :

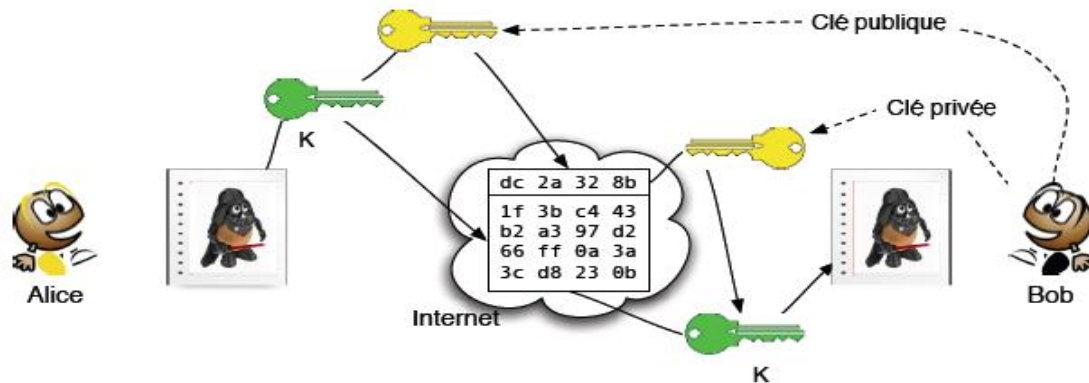


Figure 2.6 Principe générale de cryptographie hybride. [23]

5. Conclusion

Dans ce chapitre, nous avons présenté plusieurs techniques et quelques théories de La cryptographie qui vont nous permettre de comprendre cet axe de recherche, nous avons tout d'abord évoqué les notions formelles de sécurité et leurs implications, ensuite abordé les différents types de classifications des algorithmes de chiffrement et leurs contextes d'applications.

Ce chapitre a introduit aussi les principaux algorithmes de cryptage symétrique (par flot et par bloc) et asymétrique.