Table des matières

Chapitre 1

Introduction à la sécurité de l'information

1.1 Qu'est-ce que la sécurité ?

La sécurité de l'inform ation est un processus ayant pour but de protéger les systèmes d'information contre les accès non autorisés, les usages non conformes, la divulgation, les pertes d'accès, les modifications ou destruction de données. La sécurité de l'information est présente dans plusieurs niveaux de la portée et de la vie de l'information.

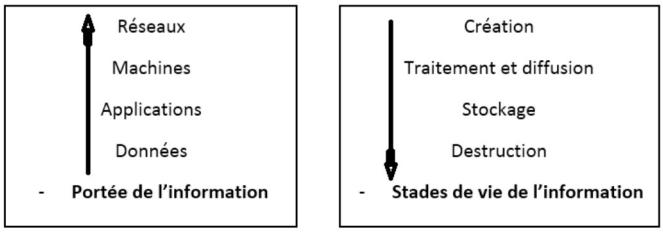

FIGURE 1.1 – Portée et stades de vie de l'information.

Classiquement le processus de sécurité de l'information est décomposé en trois aspects se référant à l'objet de sécurisation en spécifiant notamment ce qui doit être protégé. Cette vue de la sécurité est connue sous la trinité CIA (Confidentialité, intégrité et disponibilité).

Confidentialité : garantir que seuls les utilisateurs habilités (autorisés) ont accès à l'information.

Intégrité : la méthode pour garantir que le contenu d'une communication ou d'un fichier n'a pas été modifié et aussi que les données échangées sont exactes et complètes.

Authentification : elle consiste à assurer l'identité d'un utilisateur, c'est-à-dire de garantir à chacun des correspondants que son partenaire est bien celui qu'il croit être.

Cette décomposition (CIA) est aujourd'hui normalement insuffisante, car elle ne couvre pas bien certaines nouvelles menaces comme les virus informatiques ou les messages non sollicités,... En plus de CIA, on peut citer :

Disponibilité : assurer un accès continu aux informations et ne peut être bloquée ou perdue.

Auditabilité : garantir la traçabilité des accès et des tentatives d'accès et la conservation de ces traces comme preuves exploitables.

Non-répudiation : elle permet d'assurer qu'un message a bien été envoyé par une source spécifiée et reçu par un récepteur spécifié. Elle permet d'assurer qu'un émetteur ou un récepteur ne peut pas plus tard nier faussement qu'il a envoyé ou reçu un message.

1.2 Menaces et Attaques

Dans le domaine de la sécurité d'information, on rencontre les termes suivants :

Vulnérabilité : faute créée durant le développement du système, ou durant l'opération, pouvant être exploitée afin de créer une intrusion.

Intrusion : faute malveillante externe résultant d'une attaque qui a réussi à exploiter une vulnérabilité.

Menace : possibilités et probabilités d'attaque contre la sécurité. Une menace est définie par le processus d'attaque, par la cible et par le résultat (conséquences de la réussite d'une attaque).

Attaque : C'est n'importe quelle action qui a le but de menacer la sécurité des informations et de nuire au moins à l'une des propriétés de la sécurité informatique (disponibilité, confidentialité, intégrité, authentification,..). Il s'agit d'une tentative d'intrusion.

Les motivations des attaques sont de différentes sortes :

- obtenir un accès au système ;
- voler des informations, tels que des secrets industriels ou des propriétés intellectuelles ;
- glaner des informations personnelles sur un utilisateur ;
- récupérer des données bancaires ;
- s'informer sur l'organisation (entreprise de l'utilisateur, etc.) ;
- troubler le bon fonctionnement d'un service ;
- utiliser le système de l'utilisateur comme « rebond» pour une attaque c-à-d à attaquer une machine par l'intermédiaire d'une autre machine ;
- utiliser les ressources du système de l'utilisateur, notamment lorsque le réseau sur lequel il est situé possède une bande passante élevée.

1.3 catégories des attaques et menaces

Avec la popularité grandissante des réseaux, des échanges de données, et donc des transmissions entre individues, de nombreuses menaces émergèrent. Parmi celles-ci, on trouve diverses catégories :

Menaces/attques accidentelles : elles ne supposent aucune préméditation. Elles sont des bugs logiciels, des pannes matérielles, et autres défaillances incontrôlables.

Menaces/attaques intentionnelles : elles reposent sur l'action d'un tiers désirant s'introduire et relever des informations. Il existe deux types : passives ou actives.

Dans le cas d'une attaque passive, l'intrus va tenter de dérober (voler) les informations par audit (écoute), ce qui rend sa détection relativement difficile. En effet, cet audit ne modifie pas les fichiers, ni n'altère les systèmes.

Dans le cas d'une attaque active, la détection est facilitée, mais il peut être déjà trop tard lorsque celle-ci a lieu. Ici, l'intrus (espion) aura volontairement modifié les fichiers ou le système de communication en place pour s'en emparer.

Les auteurs de ces attaques sont notamment les hackers (agissant souvent par défi personnel), les concurrents industriels (vol d'informations concernant la stratégie de l'entreprise ou la conception de projets), les espions, la presse ou encore les agences nationales.

1.4 Buts des attaques/menaces

Il existe plusieurs objectifs pour les attaques/menaces :

- **Interruption :** vise la disponibilité des informations (dénis de service,. . .)
- **Interception :** vise la confidentialité des informations (capture de contenu, analyse de trafic,. . .).
- **Modification :** vise l'intégrité des informations (modification, rejet, . . .).
- **Fabrication :** vise l'authenticité des Informations (Masquerade).

1.5 Exemple d'attaques/menaces d'informations

Il existe un nombre énorme d'attaques qui menacent les systèmes d'informations :

1.5.1 Attaques de Dénis de Services (Denial Of Service - DOS)

L'attaque DOS est une attaque informatique ayant pour but de rendre indisponible un service, d'empêcher les utilisateurs légitimes d'un service de l'utiliser.

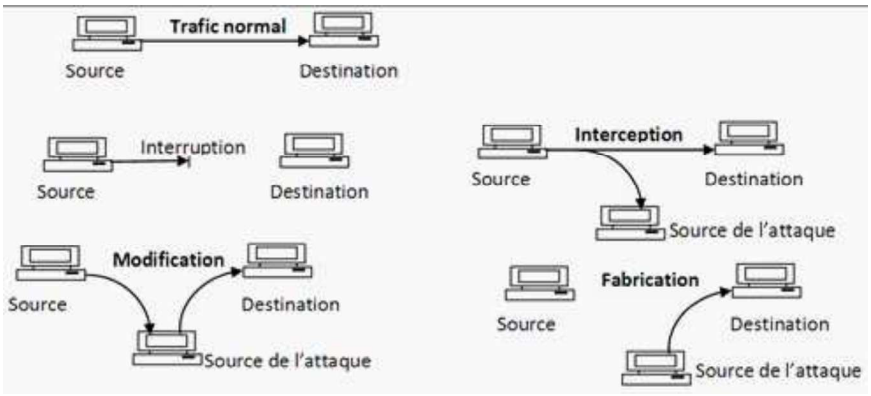

FIGURE 1.2 – Buts des attaque.

1.5.2 L'analyseur réseau (sniffer)

Le sniffer est un dispositif permettant d'écouter le trafic d'un réseau, c'est-à-dire de capturer les informations qui y circulent par exemple voler un mot de passe.

1.5.3 Attaque par logiciels malveillants

- Le virus : c'est un programme qui se reproduit en s'insérant partiellement dans d'autres fichiers.

- Le ver (anglais worm) : est un programme qui se propage d'ordinateur à ordinateur via un réseau comme l'Internet.

- Cheval de Troie (trojan en anglais) : un programme qui semble effectuer une fonction utile, mais qui a une fonction illicite non déclarée (cachée).

- Logiciel espion (spyware) : Logiciel qui collecte des informations à partir d'un ordinateur et les transmet à un autre système espion.

- Logiciel de publicité indésirable (Adware) : logiciel de publicité indésirable qui peut générer des annonces pop-up ou la redirection d'un navigateur à un site commercial.

- La bombe logique : est un cheval de Troie qui est capable de se déclencher suite à un événement particulier (date système, activation distante, ...).

- Le hoax : un hoax (canular) est un courrier électronique contenant une fausse information. Si certains sont inoffensifs, d'autres peuvent être dangereux.

- Le spam : le spamming consiste à envoyer des messages appelés "spam" à une ou plusieurs personnes. Ces spams sont souvent d'ordre publicitaire.

- Le pishing : consiste à soutirer des informations confidentielles (comme les codes bancaires) auprès des clients par usurpation d'identité.

- Le ransomware : est un logiciel qui chiffre les données, les «prend en otage» et ne donne le mot de passe que lorsque la rançon a été versée.

-...

1.6 Mécanismes de défense contre les attaques

Un mécanisme de défence est l'ensemble de procédures ou dispositifs qui sont conçu pour détecter, prévenir ou récupérer les attaques qui menacent la sécurité des informations, on peut citer :

Chiffrement : Algorithme généralement basé sur des clefs et transformant les données.

Signature numérique : Données ajoutées pour vérifier l'intégrité ou l'origine des données.

Bourrage de trafic : Données ajoutées pour assurer la confidentialité.

Notarisation : Utilisation d'un tiers de confiance pour assurer certains services de sécurité.

Contrôle d'accès : Vérifie les droits d'accès d'un acteur aux données. N'empêche pas l'exploitation d'une vulnérabilité.

Antivirus : Logiciel censé protéger unsystème contre les logiciels néfastes.

Le pare-feu (firewall) : Un élément (logiciel ou matériel) du réseau informatique contrôlant les communications qui le travers.

Détection d'intrusion : Repère les activités anormales ou suspectes sur le réseau surveillé.
Journalisation (logs) : Enregistrement des activités de chaque acteur.
Analyse des vulnérabilités (Security audit) : Identification des points de vulnérabilité du système.
Dans la plupart du temps, et pour atteindre un niveau acceptable de sécurité, plusieurs mécanismes sont utilisés en même temps.

Chapitre 2

Concepts de cryptographie et de cryptanalyse

2.1 Définitions et terminologies

Chiffrer : transformer à l'aide d'une convention secrète, appelée clef, des informations intelligibles pour des tiers n'ayant pas la connaissance du secret.

Déchiffrer : retrouver les informations claires, à partir des informations chiffrées en utilisant la convention secrète de chiffrement.

Clef : paramètre d'un algorithme de chiffrement ou de déchiffrement, sur lequel repose le secret. On distingue deux types de clefs : les clefs secrètes et clefs publiques (les couples, clef privée).

Texte en claire (plaintext) : données intelligibles, dont la sémantique est compréhensible.

Texte chiffré (ciphertext, cryptogramme) : données obtenues par application d'un algorithme de chiffrement. Le contenu sémantique de ces données n'est pas compréhensible.

La cryptologie : est l'ensemble formé de la cryptographie et de la cryptanalyse.

La cryptographie : le mot «cryptographie» du grec kryptos (caché) et le verbe graphein (écrire) peut être assimilé à «l'étude des écritures secrètes». C'est la science qui utilise les mathématiques pour chiffrer, crypter, coder et déchiffrer des données.

Un algorithme (fonction) cryptographique : est l'ensemble des fonctions (mathématiques ou non) utilisées pour le chiffrement et le déchiffrement.

La cryptanalyse : est la science de la reconstitution du texte en clair sans connaître la clef. Une cryptanalyse réussie peut fournir soit le texte en claire, soit la clef. Une tentative de cryptanalyse est appelée **attaque** et les cryptanalystes sont appelés **attaquants**.

Un cryptosystème : est l'ensemble des deux méthodes de chiffrement et de déchiffrement utilisable en sécurité. Il dépend de paramètres (clefs) qui doivent pouvoir être modifiés aisément et fréquemment.

Décrypter : retrouver l'information intelligible, à partir de l'information chiffrée sans utilisée la convention de chiffrement.

Protocole : description de l'ensemble des données nécessaires pour mettre en place le mécanisme de cryptographie : ensemble des messages clairs, des messages cryptés, des clés possibles, des transformations.

Signatures : Chaine de caractères associées à un message donné et le caractérisant.

un cryptographe : est une personne qui conçoit des cryptosystèmes ;

un cryptanaliste : est une personne qui tente de casser les cryptosystèmes.

2.2 Algorithmes cryptographiques

Un algorithme cryptographique est une fonction mathématique utilisée pour le chiffrement et le déchiffrement.

Jusqu'aux années 1970 les algorithmes de cryptographie utilisés consistaient à enchaîner **des permutations et des substitutions** sur des ensembles de petite cardinalité (taille). C'est ce qui est connu aujourd'hui sous le nom de **la cryptographie classique**.

Les algorithmes de chiffrement actuels reposent sur des résultats en algèbre (étude des corps de nombres, courbes elliptiques, chaos, ...) et sur des problèmes algorithmiquement difficiles comme la décomposition d'un nombre entier

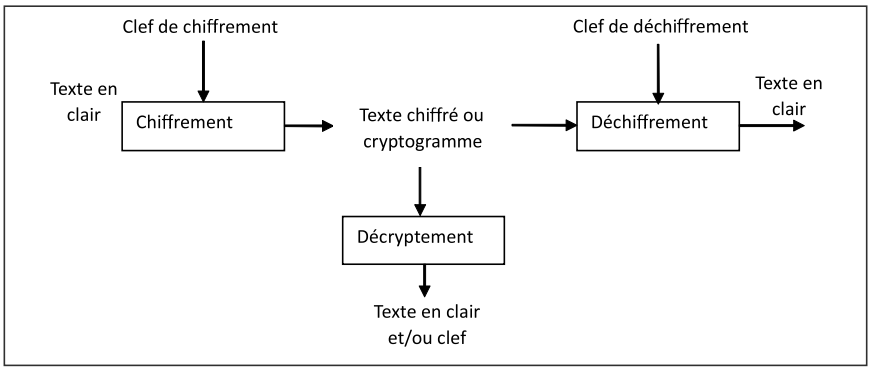

FIGURE 2.1 – chiffrement et déchiffrement avec une clef.

en facteurs premiers.

Il est possible de résumer la philosophie de la cryptographie moderne par le principe de **Kerckhoffs 1883**. "la sécurité d'un système de chiffre ne doit pas dépendre du secret de l'algorithme mais seulement du secret de la clé. En particulier un attaquant est supposé connaître le cryptosystème".Les principes fondamentaux d'un algorithme de cryptographie sont basés sur deux notions essentielles, énoncées par Shannon :

- La confusion vise à rendre le texte aussi peu lisible que possible. Ceci peut se faire par une substitution systématique de symboles, ou par un algorithme de codage aussi complexe que l'on veut.

- La diffusion vise à rendre chaque élément d'information du ciphertext dépendant d'un nombre aussi grand que possible d'éléments d'information du plaintext. Ceci rend la découverte de l'algorithme, ou de la clef de cet algorithme, en principe plus difficile.

2.3 Types et modes d'algorithmes

Il existe deux modèles de base d'algorithmes : l'algorithme de chiffrement par blocs et l'algorithme de chiffrement en continu.

- Les algorithmes de chiffrement par blocs manipulent des blocs de texte en clair et de texte chiffré.

- Les algorithmes de chiffrement en continu manipulent des flots de textes en clair et de textes chiffrés bit par bit ou octet par octet.

Un mode de cryptographie combine en général un algorithme cryptographique, une sorte de rétroaction et des opérations simples.

a) Carnet de codage électronique (CCE)

Le mode CCE est la méthode la plus évidente pour utiliser un algorithme de chiffrement par blocs : Un bloc de texte en clair se chiffre en un bloc de texte chiffré.

b) Mode de chiffrement avec chaînage de blocs (CCB)

Le chaînage utilise une méthode de rétroaction car les résultats du chiffrement du bloc précédent sont réutilisés comme entrées pour le chiffrement du bloc courant. Chaque bloc chiffré dépend non seulement du bloc de texte en clair mais aussi de tous les blocs de texte en clair qui précèdent celui-ci.

c) Mode de chiffrement à rétroaction (CR)

Un bloc chiffré peut être utilisé en tant que chiffrement autosynchrone en continu. Avec ce mode, le chiffrement ne peut pas commencer avant qu'un bloc complet de données ait été reçu.

d) Mode de rétroaction de sortie (RS)

Le mode de rétroaction de sortie est une méthode qui consiste à utiliser un algorithme de chiffrement par blocs comme un algorithme de chiffrement synchrone en continu.

2.4 Cryptanalyse

Les cryptanalystes sont les ennemis des cryptographes, puisque leur but est de casser un algorithme de cryptographie afin d'en permettre le décodage par une tierce personne. On distingue un certain nombre de méthodes de base utilisée par les cryptanalystes pour arriver à leurs fins :

- L'attaque à texte chiffré seulement : le cryptanalyste dispose un texte chiffré de plusieurs messages, tout ayant chiffrés avec le même algorithme. La tâche du cryptanalyse est de retrouver le texte en clair du plus

grand nombre de messages possible ou mieux encor de retrouver la ou les clefs qui ont été utilisées pour chiffrer les messages ce qui permettrait de déchiffrer d'autres messages chiffré avec ces mêmes clefs.

- L'attaque à texte en clair connu : le cryptanalyse a non seulement accès aux textes chiffrés de plusieurs messages mais aussi aux textes en clairs correspondants. La tâche est de retrouver la ou les clef (s) utilisées pour chiffrer ces messages ou un algorithme qui permet de déchiffrer n'importe quel nouveau message chiffré avec la même clef.

- L'attaque à texte en clair choisi : non seulement le cryptanalyse a accès aux textes chiffrés et aux textes en clair mais de plus il peut choisir les textes en clair à chiffrer. Cette attaque est plus efficace que l'attaque à texte en clair connu car le cryptanalyste peut choisir des textes en clair spécifiques qui donneront plus d'informations sur la clef. La tâche consiste à retrouver la ou les clefs utilisées pour chiffrer ces messages ou un algorithme qui permette de déchiffrer n'importe quel nouveau message chiffré avec la même clef.

- L'attaque à texte en clair choisi adaptative : c'est un cas particulier de l'attaque à texte en clair choisi. Non seulement le cryptanalyste peut choisir les textes en clair mais il peut également adapter ses choix en fonction des textes chiffrés précédents. Dans une attaque à texte en clair choisi, le cryptanalyste est juste autorisé à choisir un grand bloc de texte en clair au départ tendis que dans une attaque à texte en clair adaptative, il choisit un bloc initial plus petit et ensuite il peut choisir un autre bloc en fonction du résultat pour le premier et ainsi de suite.

- L'attaque à texte chiffré choisi : Le cryptanalyste dispose de la machine permettant de décoder le ciphertext. Son but est de retrouver l'algorithme ou la clef, qui est à la base de la génération du ciphertext.

- L'attaque à clef choisie : le cryptanalyste peut choisir la clef, il est seulement au courant de quelques relations entre différentes clefs. cette méthode est difficile et n'est pas très pratique.

2.5 Structure générale d'un cryptosystème

Les composants pricipaux d'un cryptosystème sont :
- Une fonction de cryptage C_K
- Une fonction de décryptage D_K
- Une clef K

L'émetteur désire envoyer un message M. Il utilise la clef Kpour produire le message encrypté $C_K(M)$. Le récepteur doit ensuite pouvoir à l'aide de $D_K$et de $C_K(M)$reconstituer le message M.

En autre terme, on doit avoir pour tout message M.

$$D_K(C_K(M)) = M$$

La connaissance de $C_K$et $D_K$ne doit être possible que si l'on connaît la clef K. Cette clef doit être tenue secrète par l'émetteur et le récepteur.

Un tel système exigeant une clef unique est appelé cryptosystème conventionnel ou cryptosystème à clef simple et peut schématiser sur la figure ci-après.

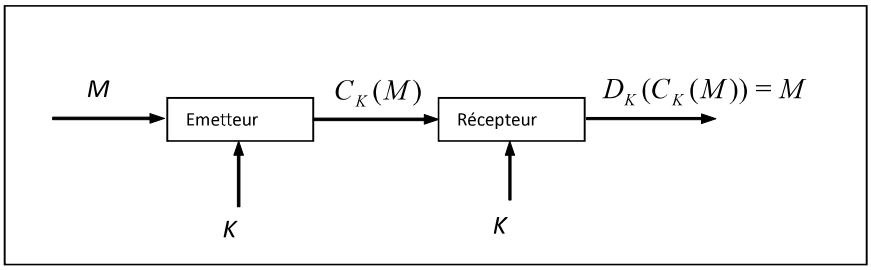

FIGURE 2.2 – Crypto système à clef simple.

2.6 Exemples de crypto-systèmes conventionnels

2.6.1 Chiffre monoalphabétique

Formellement, un chiffre monoalphabétique et une application bijective des lettres de l'alphabet des messages clairs sur les lettres de l'alphabet des cryptogrammes.

chiffrement par décalage

Le chiffrement par décalage (addition), aussi connu comme le chiffre (code) César est une méthode de chiffrement très simple utilisée par Jules

César dans ses correspondances secrètes. Ce chiffre est définie par l'application suivante : Si la clef $K_C = 3$, on décale l'alphabets de trois lettres :

a b c d e f g h i j k l m n o p q r s t u v x z y z
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

FIGURE 2.3 – Code de César.

Example 1 *Texte en clair : jijel*
Avec la clef $Kc = 3$ *le cryptogramme vaut : MLMHO*
Cryptogramme déchiffré avec la même clef $(K_d = -3)$ *: jijel*

Le chiffrement par translation

Soit $A = Z^{26}$ l'anneau des entiers $modulo26$. Il faut commencer par associer les lettres de l'alphabet aux entiers de manière simple et bijective : $a : 0, b : 1, ...z : 25$.

L'espace des clefs est également égal à A. Pour chiffrer un texte à l'aide d'une clef K, il faut :
- Lui associer une suite de nombres de A par la correspondance.
- Pour tout nombre x de$A$ calculer $C_K(x) = x + K \bmod 26$

Example 2 *Texte en clair : université de jijel*
Avec la clef$k = 5$ *le cryptogramme vaut : zsnajwxnyj ij onojq*
Cryptogramme déchiffré avec la même clef : université de jijel

La faiblesse des codes précédents et des systèmes analogues est que la fréquence des lettres est conservée ce qui permet une cryptanalyse aisée par analyse de fréquences ou par l'exploration de l'espace de toutes les clefs possibles (recherche exhaustive).

2.6.2 Les chiffres polyalphabétiques

Le chiffrement de Vigenère

Inventé en 1586 par le diplomate français Blaise de Vigenère, l'idée de ce système repose sur l'utilisation de plusieurs système mono-alphabétiques. L'algorithme de chiffrement se déroule comme suit :
- Le cryptogramme d'un bloc de $(m > 1)$ chiffres est donné par : $e_k(x_1, x_2, ..., x_m) = (x_1 + k_1, x_2 + k_2, ..., x_m + k_m)$
- Le déchiffrement d'un bloc de m chiffres du cryptogramme s'obtient par l'opération inverse : $d_k(y_1, y_2, ..., y_m) = (y_1 - k_1, y_2 - k_2, ..., y_m - k_m)$

L'espace des clefs est de cardinalité 26^m et peut donc être rendu suffisamment grand pour rendre impossible une cryptanalyse par essai systématique de toutes les clefs même pour de petites valeurs de m. Le cryptogramme d'une même lettre peut prendre m valeurs possibles ce qui rend l'attaque «**fréquentielle**» sensiblement moins performante.
- Texte en clair : **jijel**
- La clef de $(m = 5)$chiffres : $1, 2, 3, 4, 1$ donne le cryptogramme : **kkmim**
- Le cryptogramme déchiffré à l'aide de la même clef $(m = 5)$chiffres : $-1, -2, -3, -4, -1$: **jijel**

On s'aperçoit que la lettre (m) en position 3 et 5 n'ont pas le même cryptogramme.

2.7 Chiffrement à clef secrète et à clef publique

Le type de relation qui unit les clés K_e $(clef - chiffrement)$et K_d $(clef - déchiffrement)$permet de définir deux grandes catégories de systèmes cryptographiques :
- Les systèmes à clefs secrètes ou symétriques : (DES, AES, IDEA, Blowfish,...).
- Les systèmes à clefs publiques ou asymétriques : (RSA, El-Gamal, un cryptosystème elliptique,...).

2.7.1 Chiffrement à clef secrète

Les algorithmes à clefs secrètes (symétriques) sont des algorithmes où la clef de chiffrement peut être calculée à partir de la clef de déchiffrement ou vise versa. Dans la plupart des cas, la clef de chiffrement et la clef de déchiffrement sont identiques. Voici le schéma qui illustre le principe du chiffrement à clef secrète :

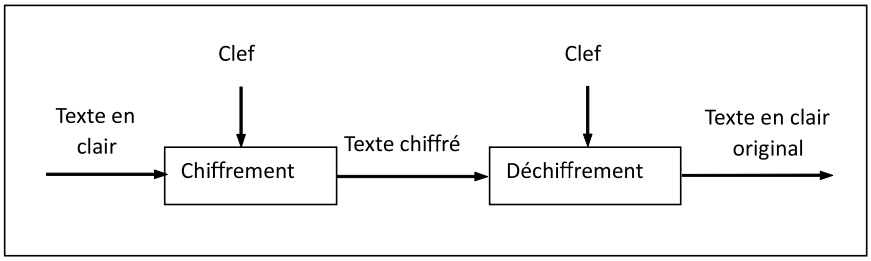

FIGURE 2.4 – Ciffrement à clef secrète.

Chiffre de Vernam

Le chiffre de Vernam ou one-time pad (à masque jetable) représente une solution presque parfaite au problème du chiffrement. Il a été inventé en 1917 et a été utilisé par des espions pendant la Seconde Guerre Monidale. Il s'agit d'un système de chiffrement à clé secrète où la taille de la clé est identique à celle du message clair. Une fois utilisée, la clé est effacée et n'est pas réutilisée.

Example 3 *on a la table de fonction XOR* $[1XOR1 = 0; 1XOR0 = 1; 0XOR1 = 1; 0XOR0 = 0]$ *et la table ASCII suivante :*

Character	ASCII
a	97
b	98
c	99
d	100
e	101
f	102
g	103
h	104
i	105
j	106
k	107
l	108
m	109

Character	ASCII
n	110
o	111
p	112
q	113
r	114
s	115
t	116
u	117
v	118
w	119
x	120
y	121
z	122

Character	ASCII
A	65
B	66
C	67
D	68
E	69
F	70
G	71
H	72
I	73
J	74
K	75
L	76
M	77

Character	ASCII
N	78
O	79
P	80
Q	81
R	82
S	83
T	84
U	85
V	86
W	87
X	88
Y	89
Z	90

Character	ASCII
0	48
1	49
2	50
3	51
4	52
5	53
6	54
7	55
8	56
9	57

FIGURE 2.5 – Code ASCII.

Example 4 *Le message à envoyer M = Gra en code ASCII M =71 114 97, en binaire M =01000111 01110010 01100001*

La clef de chiffrement K =11000001 01110000 11011110

Le message chiffré $C = M \quad XOR \quad K$ *=10000110 00000010 10111111*

Le message chiffré $M_d = C \quad XOR \quad K$ *=01000111 01110010 01100001*

Le réseau de Feistel

Cette structure a été inventé en 1973 (par Horst Feistel). Un chiffrement de Feistel est un chiffrement itératif opérant sur des blocs de $2N$ bits. Transformant toute fonction en permutation. Dans ce système de chiffrement, un bloc de texte en clair est découpé en deux ; la transformation du tour (rond) est appliquée à une des deux moitiés, et le résultat est combiné avec l'autre moitié par ou exclusif. Les deux moitiés sont alors inversées pour l'application du tour suivant. L'avantage cet algorithme est que la fonction de chiffrement et la fonction de déchiffrement sont similaires.

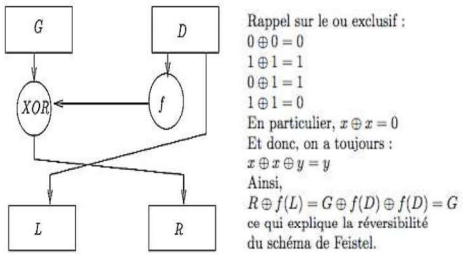

FIGURE 2.6 – Structure de Feistel.

Entrée	f_1	Sortie	Entrée	f_2	Sortie
00	→	01	00	→	11
01	→	11	01	→	00
10	→	10	10	→	00
11	→	01	11	→	01

FIGURE 2.7 – Les deux fonctions f1 et f2.

Example 5 *On va utiliser les deux fonctions $f_1$et f_2 pour chiffrer le message $M = 1101$. Les deux fonctions $f_1$et f_2 ne sont pas des bijection ($f_1(00) = f_1(11) = 01$;**Une application est bijective si etseulement si tout élément de son ensemble d'arrivée a un et un seul antécédent**). G désigne la moitié gauche du message à chiffrer, D la moitié droite :*

Etape de chiffrement

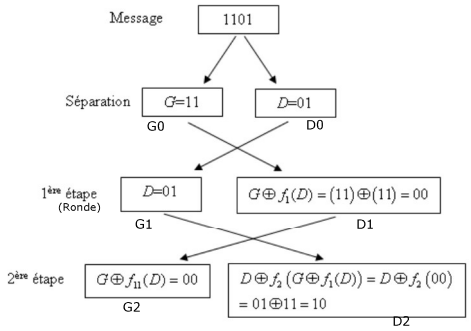

FIGURE 2.8 – Chiffrement du message d'entrée.

Le message chiffré est obtenu en permutant G_2 et D_2: $M_{chiffré} = 1000$.
Etape de déchiffrement (processus inverse)
Le messge déchiffré est donc : $M_{déchiffré} = 1101$.

Algorithme DES (Data Encryption Standard)

Le DES est un système de chiffrement par blocs a été publié en 1975 utilisé par IBM et la N.S.A.(National Security Agency, le service de sécurité intérieure américain). Cet algorithme est basé sur les réseaux de Feistel (16 rondes), il chiffre les données par blocs de 64 bits avec une clef de 56 bits. Les grandes lignes de l'algorithme sont :

Le message, au prélable converti en binaire, est découpé en blocs $B_i$de $64bits$(8 octets). La clé K, elle, comporte $56bits$. Pour chaque bloc B_i, on applique l'algorithme DES :

1) On effectue une permutation initiale des bits du bloc B_i. On appelle alors G_0 et D_0 les parties de $32bits$ droite et gauche du bloc obtenu.

2) On répète 16 fois l'étape de permutation et de substitution (appelées rondes) :

$Gi = D_{i-1}$

$D_i = G_{i-1} \quad XOR \quad f(D_{i-1}, K_i)$ (XOR est représenté par + sur le schéma ci-après)

où Ki est un bloc de 48 bits de la clé K, et f une fonction composée successivement d'une expansion de bits, d'un XOR, d'une réduction de bits, et d'une permutation de bits.

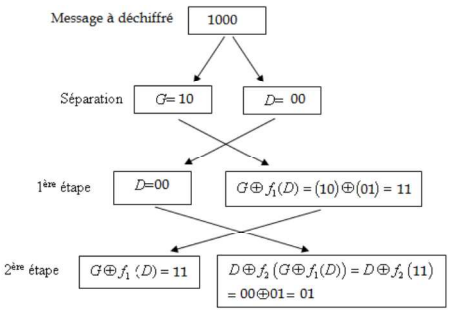

FIGURE 2.9 – Déchiffrement du message chiffré.

3) On recompose un bloc $B\prime_{16}$ en recollant D_{16} et G_{16} dans cet ordre.
4) On effectue la permutation inverse de la permutation initiale (1).

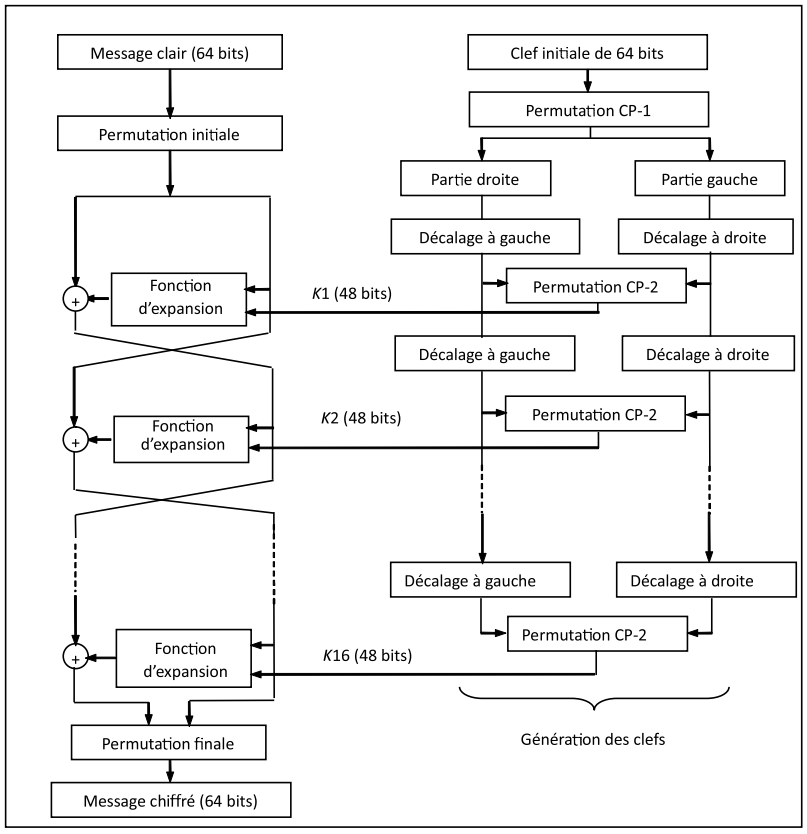

FIGURE 2.10 – Schéma de DES.

Cet algorithme est à la base d'autres cryptosystèmes plus récents comme AES, IDEA, FEAL,CAST, RC5, BLOW-FISH.

2.7.2 Chiffrement à clef publique

Le chiffrement à clef publique (asymétrique) utilise deux clefs séparées et distinctes, l'une publique, l'autre maintenue secrète. La source peut utiliser la clef publique pour encrypter le message, alors que le destinataire utilisera la clef secrète pour décrypter le message. La première est souvent divulguée sur le réseau afin que tout participant puisse chiffrer mais la deuxième reste en général secrète pour qu'une seule personne (ou machine) puisse le déchiffrer.

Voici quelques exemples des standards les plus utilisés :
- Algorithme DIFFIE-HELLMAN

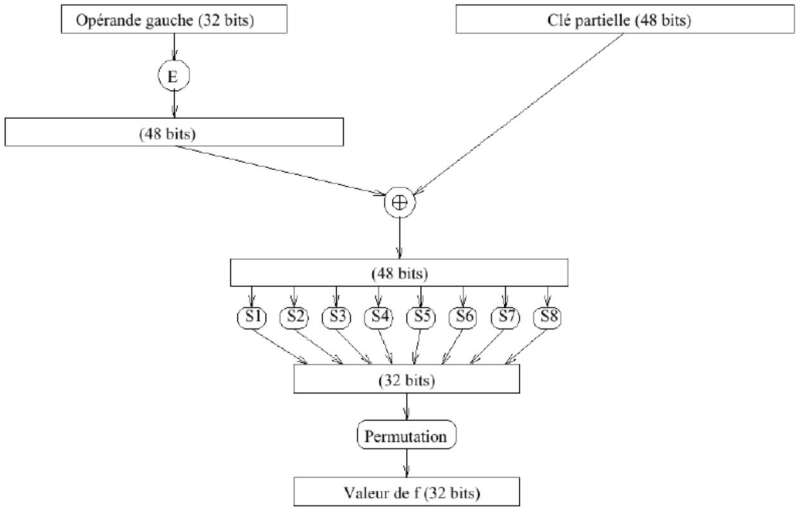

FIGURE 2.11 – La fonction f de DES.

- RSA c'est l'algorithme à clef publique le plus répandu, et la plus populaire.
- ELGAMEL basé sur la difficulté présumée du logarithme discret. Utilise 1024 bits pour être en sécurité.

Aspects mathématiques relatifs aux algorithmes à clef publique

Fonction à sens unique Une fonction à sens unique est une fonction mathématique relativement aisée à calculer mais considérablement plus difficile à inverser. En d'autre terme, étant donné x, il est facile à calculer $f(x)$, mais étant donné $f(x)$ il est extrêmement difficile de déduire x. Ces fonctions sont des éléments de base de la plupart des protocoles à clef publique.

Nombre premier Un nombre premier est un entier strictement supérieur à 1, qui admet exactement deux diviseurs distincts. Si p est un nombre premier, alors ses seuls diviseurs sont 1 et p.

Algorithme d'Euclide Soit x et y deux entiers. L'algorithme d'Euclide est un moyen de trouver le $gcd(x, y)$ (PGCD - grand diviseur commun) même si leurs facteurs premiers ne sont pas connus.

Pour trouver le $gcd(x, y)$, $x > y$ on divise y par x et on écrit le quotient et le reste de la division comme ci-dessous.

$$\begin{aligned} y &= q_1 \times x + r_1 \rightarrow x = q_2 \times r_1 + r_2 \rightarrow r_1 = q_3 \times r_2 + r_3 \rightarrow ... \\ r_n &= q_{n+2} \times r_{n+1} + r_{n+2} \rightarrow r_{n+1} = q_{n+3} \times r_{n+2} + r_{n+3} \rightarrow r_{n+2} = q_{n+4} \times r_{n+3} + r_{n+4}. \end{aligned}$$

Où r_{n+4} est le dernier reste non nul, qui représente le $gcd(x, y)$. égal à 1 si x et y sont premiers entre eux.

Algorithme d'Euclide étendu Il est possible de modifier l'algorithme d'Euclide afin qu'il détermine, outre le grand diviseur commun d de x et y, deux nombres entiers a et b tels que $a \times x + b \times y = d$.

On va partir de la dernière équation du système précédent pour écrire $1 = r_{n+2} - q_{n+4}\ r_{n+3}$.

Dans laquelle on peut remplacer r_{n+3} par l'expression $r_{n+1} - q_{n+3} \times r_{n+3}$ (on utilise ici l'avant dernière division euclidienne). On obtient une relation entre r_{n+2} et r_{n+1}.

Il suffit alors de continuer le procédé en remplaçant r_{n+2} à l'aide de l'antépénultième division euclidienne. On obtient ainsi de proche en proche des relations pour les couples d'entiers (r_{n+4}, r_{n+3}), puis (r_{n+2}, r_{n+1}),... et à la fin (x, y).

Modulo d'un nombre élevé à une puissance Dans la plupart des algorithmes de chiffrement à clef publique, l'étape la plus longue est le calcul de $b^n mod\ m$. les étapes de cet algorithme sont :

Considérons $(n_0, n_1, \ldots, n_{k-1})$ les éléments binaires de n tel que : $n = n_0 + 2n_1 + ... + 2^{k-1}n_{k-1}$, avec $\{n_j = 0 \rightarrow 1; 0 \leq j \leq k-1\}$.

- Etape 1 : posant $a = 1$.
- Etape 2 : calculer $b_1 = b^2 \ mod \ m$.
  Si $n_0 = 1 : (a \leq b)$;
  Sinon : a reste inchangé.
- Etape 3 : calculer $b_2 = b_1^2 \ mod \ m$.
  Si $n_1 = 1 : a = (a \times b_1) \ mod \ m$
  Sinon : a reste inchangé.
- Etape 4 : calculer $b_3 = b_2^2 \ mod \ m$.
  Si $n_2 = 1 : a = (a \times b_2) \ mod \ m$
  Sinon : a reste inchangé
- Etape n : à la $j^{ième}$ étape on va calculer
Si $n_j = 1 : a = (a.b_j) \ mod \ m$
Sinon : a reste inchangé
Donc : $b^n mod \ m = a$

Logarithme discret de y en base g

Donnée g et y éléments d'un groupefini G d'ordre n. Trouver x tel que $g^x = y \bmod n$. Ou, pour p un entier premier, g un élément élément générateur de G, $y = g^x \bmod p$ *et* $x = log_g(y) \bmod p - 1$.

2.7.3 Protocole d'échange de clef Diffie-Hellman

Inventé en 1976 par WHITFIELD DIFFIE et MARTIN HELLMAN c'est le plus ancien cryptosystème à clef publique, et il est encore largement en usage. Il autorise « simplement » deux correspondants à convenir d'une clef de chiffrement sans avoir à se préoccuper de la confidentialité de cet échange. Il repose sur des fonctions à sens unique. Le principe est le suivant :

D'après cette figure, les deux interlocuteurs (Alice et Bob) choisissent, ensemble et publiquement, un nombre premier p, et un entier a tel que $1 < a < p$.

1. *Alice* choisit secrètement m, et *Bob* choisit secrètement n ;
2. *Alice* envoie à *Bob* : $A = a^m \bmod p$, et *Bob* calcule $K = A^n \bmod p = a^{m.n} \bmod p$;
3. *Bob* envoie à *Alice* :$B = a^n \bmod p$, et *Alice* calcule $K = B^m \bmod p = a^{n.m} \bmod p$.

Example 6 *Supposons à titre d'exemple, qu'Alice et Bob partagent* $p = 233$ *et* $a = 45$.
1. Si Alice choisit $m = 11$ *et Bob* $n = 20$, *alors* $A = 45^{11} \bmod 233 = 147$, $B = 45^{20} \bmod 233 = 195$, *donc :*
2. Chez Alice :$K = 147^{20} \bmod 233 = 169$.
3. Chez BOB : $K = 195^{11} \bmod 233 = 169$.
Alice et Bob disposent d'une clef privée, $K = 169$.

2.7.4 Algorithme RSA

Le RSA a été inventé par Rivest, Shamir et Adleman en 1978. C'est l'exemple le plus courant de cryptographie asymétrique, toujours considéré comme sûr, avec la technologie actuelle, pour des clefs suffisamment grosses (1024, 2048 voire 4096 bits). D'ailleurs le RSA128 (clés de 128 bits), proposé en 1978, n'a été "cassé" qu'en 1996, en faisant travailler en parallèle de nombreux ordinateurs sur internet.

Tout le principe de RSA repose sur le fait qu'il est très facile de multiplier deux grands nombres premiers, mais très difficile et très long de factoriser le très grand nombre ainsi obtenu en deux facteurs premiers.

Description du protocole RSA Si on appelle *Alice* la destinatrice du message, et *Bob* l'émetteur.

- *Alice* génère deux gros nombres premiers p et q, (plus de cent chiffres en pratique), elle calcule $n = p \times q$, et aussi l'indicateur d'Euler de n, c'est-à-dire $\varphi(n) = (p-1) \times (q-1) = w$, puis elle génère un gros nombre e premier avec le produit w.

- Alice utilise l'algorithme d'Euclide pour calculer la clef de déchiffrement d tel que :$e \times d = 1 \, (\mathrm{mod}\, w)$. En d'autre terme :$d = e^{-1} \bmod (w)$, d et n sont aussi premiers entre eux.

- Alice diffuse n et e, garde d secret et oublie w.

- Bob converti le texte en nombre, donc il sera nécessaire de le découper en blocs de taille égale et inférieurs à n. Il pourra utiliser le standard ASCII, qui code chaque caractère de 000 à 255, pour transformer partie par partie

l'information à crypter en nombres. Ensuite il crypte chaque message M par $M \to M^e\,[n]$ et envoie le résultat à Alice.

- Alice décode alors le message crypté par $C \to C^d\,[n]$.

Example 7 *Si Alice prend pour les deux nombres p et q les valeurs 11 et 17. Elle a alors : $n = 187$ et $w = (11-1).(17-1) = 160$.*

Si elle prend $e = 7$, elle utilise l'algorithme d'Euclide pour déterminer d : $160 = 22 \times 7 + 6 \to\ 7 = 1 \times 6 + 1 \to 6 = 6 \times 1 + 0$

Le calcul inverse donne : $1 = 7 - 6 \times 1 = 7 - 1 \times (160 - 22 \times 7) = 23 \times 7 - 1 \times 160 = d \times e - 1 \times 160$.

Donc elle peut prendre $d = 23$ la clef secrète.

Alice va rendre public le couple$(n = 187, e = 7)$ et oublie p, q et w.

Bob veut transmettre à Alice un message codé plus petit que $n = 187$. Par exemple $(M = 13)$, ce message qui ne doit pas être intercepté (déchiffré) par Eave, bien sûr. Bob va donc calculer $M_{chiffré} = M^e\,[n] = 13^7 mod(187) = 106$, et envoyer le résultat (le message chiffré) $M_{chiffré} = 106$ à Alice.

Alice va calculer le reste de la division euclidienne de 106^{23} par 187 c-à-d $106^{23} mod\ (187)$. (remarquer ici, la manière de calc

- Elle calcule d'abord $106^2 = 11236 = 60 \times 187 + 16, donc\ 106^2 = 16[187]$.

- Ensuite, $16^2 = 256 = 1 \times 187 + 69,\ donc\ 106^4 = 69[187]$.

- Puis, $69^2 = 4761 = 25 \times 187 + 86, donc\ 106^8 = 86[187]$.

- Et $86^2 = 7396 = 39 \times 187 + 103\ donc\ 106^{16} = 103[187]$.

- Enfin, $106^{23} = 106^{16} \times 106^4 \times 106^2 \times 106\ donc : 106^{23} = 103 \times 69 \times 16 \times 106[187]$

Or $103 \times 69 \times 16 \times 106 = 12053472 = 64457 \times 187 + 13$.

Alice retrouve donc bien le message envoyé par Bob (13).

2.7.5 Cryptosystème d'ELGAMAL

L'algorithme ELGAMAL est un algorithme de cryptographie asymétrique basé sur les logarithmes discrets. Il a été créé par TAHER ELGAMAL en 1985. Sa sécurité repose, comme le protocole de Diffie et Hellman, sur la difficulté de calculer le logarithme discret. Le destinataire (Bob) possède deux clefs :

- Une clef publique, qui consiste en un entier premier p, un entier a premier avec p (a doit être inférieur $a \times p$), et l'entier $P = a^s \bmod p$.

- Une clef secrète, un entier s inférieur à p.

Si Alice veut envoyer le message M à Bob, elle procède de la façon suivante :

1. Génère un nombre k aléatoirement, tel que k et $p-1$ soient premiers entre eux ;
2. Calcule $C_1 = a^k \bmod p$ et et $C_2 = \beta^k \bmod p$.

Le message chiffré est : $y = M \times C_2 \bmod p$.

Alice envie à Bob $(y,\ C_1)$;

Le message chiffré est le couple (y, C_1), qu'elle transmet à Bob. A la réception, celui-ci (Bob) calcule $C_2 = C_1^s \bmod p$.Puis ; il déchiffre le message par $M = \frac{y}{C_2} \bmod p$.

1. Bob commence par la création des clefs : $s = 8, p = 89, a = 5 \to \beta = a^s \bmod p = 5^8 \bmod 89 = 4$, donc :

   La clef secrète chez Bob est $s = 8$.

   La clef publique envoyée à Alice $(p, a, \beta) = (89, 5, 4)$.

2. Ensuite Alice veut envoyer le message $(M = 35)$. Elle prend pour k la valeur 13, donc : $C_1 = a^k \bmod p = 5^{13} \bmod 89 = 40$ et $C_2 = \beta^k \bmod p = 4^{13} \bmod 89 = 16$.

Le message chiffré est : $y = M \times C_2 \bmod p = 35 \times 16 \bmod 89 = 26$

Alice envie à Bob $(y,\ C_1) = (26,\ 40)$.

3. Enfin, le destinataire (Bob) calcule M à partir de $(y,\ C_1)$:

Il calcule à son tour $C_2 = C_e^s \bmod p = 40^8 \bmod 89 = 16$ (identique à celle de Alice).

Le message déchiffré est : $M = \frac{y}{C_1} \bmod p = \frac{26}{16} \bmod 89 = 26 \times 16^{-1} \bmod 89 = 26 \times 39 \bmod 39 = 35$.

$M = 35$.

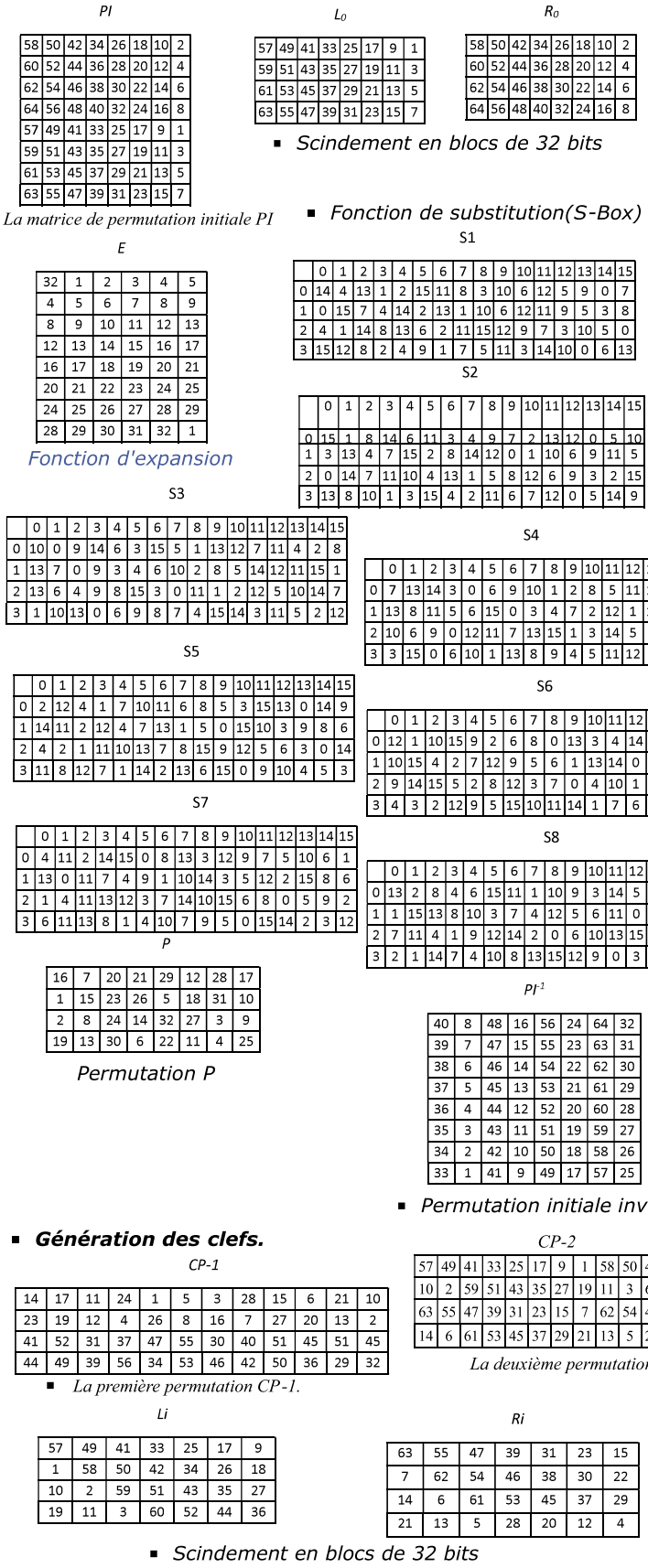

FIGURE 2.12 – Les matrices de DES.

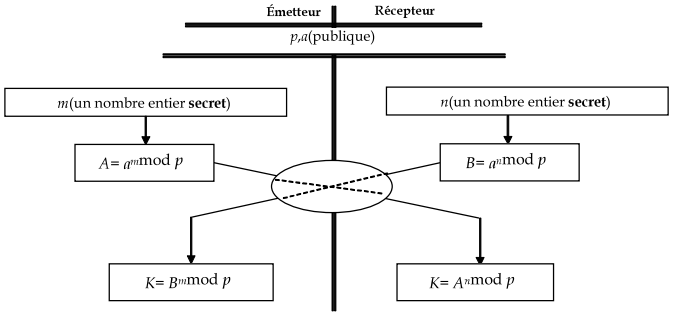

FIGURE 2.13 – Schéma du protocole DIFFIE-HELLMAN.

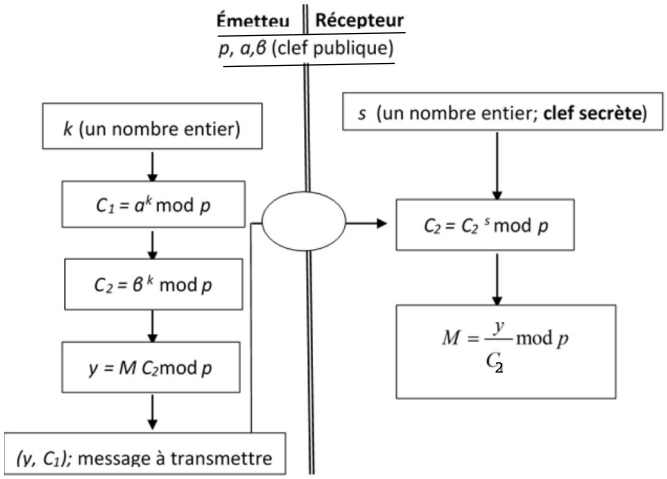

FIGURE 2.14 – Schéma du cryptosystème ELGAMAL.