

Travaux Dirigés

La cryptographie

Résumé : Il s'agit d'une présentation des différentes approches de la cryptographie – symétrique et asymétrique –, qui débouche sur l'introduction de la cryptographie hybride – à travers *SSL* –, un compromis qui tente de bénéficier des avantages des deux approches, tout en évitant leurs inconvénients.

I – La cryptographie au service de la sécurité informatique

- Définition de la cryptographie.
- Les composantes de la sécurité informatique intéressées par la cryptographie.

Objectifs : Se familiariser avec la cryptographie classique et les attaques usuelles. et les domaines d'application de la cryptographie pour la sécurité informatique.

II – La cryptographie symétrique (dite à clef privée)

- Définition de la cryptographie symétrique.
- Etude d'exemple : *DES*.
- Avantages et inconvénients.

Objectifs : Evaluer l'efficacité de la cryptographie symétrique pour la sécurité informatique.

III – La cryptographie asymétrique (dite à clef publique)

- Définition de la cryptographie asymétrique.
- Etude d'exemple : *RSA*.
- Avantages et inconvénients.

Objectifs : Evaluer l'efficacité de la cryptographie asymétrique pour la sécurité informatique.

IV – La cryptographie hybride : un compromis ?

- Définition de la cryptographie hybride en tant que compromis entre la cryptographie symétrique et celle asymétrique.
- Etude d'exemple : *SSL*.
- Avantages et inconvénients.

Objectifs : Evaluer l'apport de la cryptographie hybride pour la sécurité informatique.

I – La cryptographie au service de la sécurité informatique

I.1 – Définitions¹ :

La cryptographie : Elle a pour objet, l'étude des méthodes permettant de masquer le sens de l'information, en utilisant des transformations inversibles.

Un système cryptographique : C'est un protocole comportant :

- Deux intervenants A et B , désirant établir une communication.
- Une ligne de communication LC .
- Un algorithme de chiffrement AC , dépendant d'une clef de chiffrement K_c .
- Un algorithme de déchiffrement AD , dépendant d'un clef de déchiffrement K_d .

L'interlocuteur A est en possession d'un message M ou texte en clair (ou clair, tout court), qui doit parvenir à l'interlocuteur B , sur la ligne de communication LC .

A utilise AC pour transformer le message M , en un cryptogramme C . A la réception, B utilise AD , pour retrouver le message M .

Un cryptanalyste Cr est à l'écoute sur LC , il tenterait d'intercepter C et de retrouver M , tout en ignorant AD et K_d .

L'algorithme de cryptographie : C'est le couple formé par les deux algorithmes de chiffrement et de déchiffrement. Si les deux clefs K_c et K_d sont identiques, on parle d'*un algorithme à clef secrète* (algorithme symétrique), sinon il est question d'*un algorithme à clef publique* (algorithme asymétrique) et dans ce cas, la clef de déchiffrement peut-être divulguée sans nuire à la sécurité du dispositif.

L'attaque : On parle d'attaque quand le cryptanalyste tente de retrouver le clair ou bien une des clefs du système, à partir d'un cryptogramme.

On peut les classer en trois catégories :

- *L'attaque sur le seul cryptogramme* : Où le cryptanalyste ne dispose que de cryptogrammes pour retrouver les clefs ou le clair.
- *L'attaque à clair connu* : Où le cryptanalyste dispose d'un (ou de plusieurs) clair(s) et du (ou des) cryptogramme(s) correspondant(s).
- *L'attaque à clair choisi* : Où le cryptanalyste dispose d'un (ou de plusieurs) clair(s) de son choix et du (ou des) cryptogramme(s) correspondant(s).

La solidité : On parlera de solidité d'un algorithme de cryptographie en référence à son comportement vis à vis des différents types d'attaques présentés précédemment. On peut dans ce sens faire la remarque suivante : un algorithme résistant à une attaque à clair choisi, l'est aussi à une attaque à clair connu et à fortiori à une attaque sur le seul cryptogramme ...

¹ Cette section a été adaptée du 'Cours d'algorithmique et de cryptographie', de Sami Harari : Webliographie [1].

I.2 – La cryptographie classique :

On se propose dans cette section, de présenter deux exemples de la cryptographie classique.

I.2.1 – Le chiffrement par translation (ou l’algorithme de César) :

Le principe est très simple et remonte déjà à l’époque des romains.

- Transcodage : Les 26 lettres de l’alphabet latin sont associés d’une manière bijective aux 26 éléments de l’anneau $A = \mathbb{Z}_{26}$, par exemple : $a \leftrightarrow 0, b \leftrightarrow 1, \dots, z \leftrightarrow 25$.
Pour un clair donné, on obtient donc une séquence de nombres prenant leurs valeurs dans A : le clair transcodé.
- Chiffrement : On se donne une clef $k \in A$, et pour tout nombre du clair transcodé, on associe :
$$C_k(x) = x + k \pmod{26}$$

Enfin, chaque nombre est ‘dé-transcodé’ pour obtenir la lettre à laquelle il correspond, selon la bijection introduite plus haut.

Activité I.2.1 :

A. Retrouver le processus de déchiffrement pour l’algorithme de César ?

- Déchiffrement : On dispose d’une séquence de lettres, composant le cryptogramme.
On transcode cette séquence et pour chaque nombre y , du cryptogramme transcodé on associe :
$$D_k(y) = y - k \pmod{26}$$

Enfin il ne reste plus qu’à ‘dé-transcoder’ le résultat pour obtenir le clair.

B. Retrouver le clair M, correspondant au cryptogramme C = FHVDU, pour la clef 3 ?

C	=	FHVDU
Transcodé (C)	=	5-7-21-3-20
Transcodé (M)	=	2-4-18-0-17
M	=	CESAR

C. Discuter la solidité de l’algorithme de chiffrement par translation ?

Tout d’abord une attaque à clair connu (et à fortiori à clair choisi), est inévitablement fatale pour ce système cryptographique. Il suffira alors de transcoder clair et cryptogramme associé pour obtenir la clef, en soustrayant les deux premiers nombres !

Une attaque sur le seul cryptogramme semble moins évidente, sauf que l’ensemble des clefs étant réduit à un ensemble à 26 éléments, rien n’empêche un essai systématique de toutes les clefs, d’aboutir à temps (et surtout à l’époque de César !).

I.2.2 – Le chiffrement par permutation :

Il existe $26!$ permutations possibles des éléments de A et ce nombre est de l'ordre de : 10^{26} .
En choisissant une permutation π , il est possible de définir un algorithme de chiffrement :

- Chiffrement : On se donne une permutation π de A , et pour tout nombre du clair transcodé, on associe :

$$C_k(x) = \pi(x)$$

- Déchiffrement : Pour tout nombre du cryptogramme transcodé, on associe :

$$D_k(y) = \pi^{-1}(y)$$

Activité I.2.2 :

A. Expliquer le gain de solidité qu'apporte cet algorithme par rapport à celui de César ?

Il est évident que l'attaque sur le seul cryptogramme, par essai systématique des clefs est sensiblement moins efficace, que dans le cas de l'algorithme de César, dans la mesure où l'espace des clefs a une cardinalité de l'ordre de 10^{26} . De ce point de vue le chiffrement par permutation est plus solide que celui de César.

Par contre, une attaque à clair donné (à fortiori à clair choisi), permet de retrouver – certainement pas au bout de la première lettre – la définition (ou une partie suffisante de cette définition) de la permutation utilisée. La solidité de cet algorithme reste sensiblement équivalente à celle de l'algorithme de César, lors d'une attaque à clair donné (à fortiori à clair choisi).

B.1 Voici un tableau dans lequel sont consignées les fréquences d'apparition de toutes les lettres de l'alphabet, dans ce propre document.

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
16				16																					

En supposant que ce document représente un échantillon significatif des documents écrits dans la langue française, décrire le principe d'une attaque sur un éventuel cryptogramme associé à ce document ?

- L'analyse fréquentielle : Si on fait l'hypothèse que certaines lettres gardent à peu près les mêmes fréquences d'apparition, dans un texte en clair. Alors forcément les lettres correspondantes dans le cryptogramme (supposé être assez long) doivent aussi présenter les mêmes fréquences d'apparition (en effet une lettre est toujours chiffrée de la même manière ...). En reliant les lettres les plus fréquentes, selon le tableau du dessus à celles plus fréquentes dans le cryptogramme, on peut déjà caractériser la permutation sur cette partie de l'alphabet A .

La définition de la permutation sur l'ensemble restant des lettres peut se déduire à travers le sens des mots partiellement déchiffrés.

B.2 Reproduire cette attaque sur le cryptogramme suivant (dont le clair est issu du même document) ?

«*xw yuppyozwt qux cx documxwt rxprxyxwtx uw xchzwtillow yigwificztif dxy documxwty xcrtiy dzwy lz lzwgux fizwczix, dxcrirx lx priwcipx d'uwz zttzqux yur uw vxwxtuxl cryptogrmmx zyyocix z cx documxwt ?*»

- Analyse fréquentielle du cryptogramme :

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
16				16																					

On observe une concordance dans les fréquences d'apparition des couples (lettre de clair, lettre de crypto) suivants :

(A,Z) ; (E,X) ; (S,Y)

En effectuant les substitutions nécessaires dans le cryptogramme on obtient le clair partiellement déchiffré suivant :

«*Ew supposawt que ce documewt représewte uw échawtillow sigwificatif des documewts écrits daws la lawgue frawçaise, décrire le priwcipe d'uwe attaque sur uw éwewtuel cryptogramme associé à ce documewt ?*»

Intuitivement il nous vient tout de suite à l'esprit que la lettre W, représente le cryptogramme de la lettre N et que le cryptogramme de la question est en fait le résultat du chiffrement du clair :

«*En supposant que ce document représente un échantillon significatif des documents écrits dans la langue française, décrire le principe d'une attaque sur un éventuel cryptogramme associé à ce document ?*»

En utilisant comme clef la permutation définie par la composée de ces substitutions :

(A,Z) o (E,X) o (S,Y) o (N,W)

I.3 – La cryptographie et la sécurité informatique:

La cryptographie est traditionnellement utilisée pour dissimuler des messages aux yeux de certains utilisateurs. Cette utilisation a aujourd'hui un intérêt d'autant plus grand, pour l'informatique, que les communications via Internet circulent dans des infrastructures dont on ne peut garantir la fiabilité et la confidentialité. Désormais, la cryptographie devrait non seulement préserver la *confidentialité* des données mais aussi garantir leur *intégrité* et leur *authenticité* et instaurer le principe de *non répudiation*.

I.3.1 – La cryptographie au service de la confidentialité :

La confidentialité :

C'est la garantie du secret d'une information, un secret partagé uniquement par une certaine classe d'interlocuteurs.

Les techniques cryptographiques au service de la confidentialité :

Ceci est sans doute le domaine de prédilection de l'application directe des techniques cryptographiques, au service de la sécurité informatique.

En effet, le chiffrement garantit une certaine confidentialité des données échangées, dans la mesure où, seuls les détenteurs de la clef de déchiffrement, peuvent y accéder.

I.3.2 – La cryptographie au service de l'authentification, l'intégrité et la non répudiation :

La signature électronique :

On appelle un système (ou schéma) de signature, un couple d'algorithmes :

- La fonction de création : $\sigma()$, qui dépend d'une quantité secrète K et du message à signer M , ayant pour résultat : $\sigma(M,K)$ et telle que seul le détenteur de K , peut créer la signature en un temps raisonnable.
- La fonction de vérification : $v()$, qui appliquée à la signature aurait pour résultat le message initial M : $v(\sigma(M,K)) = M$.

On pourrait dériver autant de systèmes de signature, que de systèmes cryptographiques. Cependant les systèmes basés sur la cryptographie asymétrique, s'y prête mieux que d'autres. (cf. III – Cryptographie asymétrique)

L'authentification : C'est une assurance de l'authenticité, notamment de l'identité d'un interlocuteur ou de l'origine d'une information.

Activité I.3.2 :

A. Expliquer comment un système de signature peut garantir l'authentification du signataire auprès du vérificateur ?

C'est dans la première partie de la définition d'un système de signature que tient la réponse. En effet : « ... *seul le détenteur de K , peut créer la signature en un temps raisonnable* ... ». Cette certitude pourrait être interprété comme un authentification.

L'intégrité : C'est la garantie de la non-altération, intentionnelle ou fortuite, d'une information durant sa transmission.

La signature électronique au service de la garantie de l'intégrité des données :

On a vu dans la définition d'un système de signature, que la signature dépendait étroitement du message à signer. On peut donc très bien considérer cette signature comme un gage de l'intégrité du document signé.

En effet une modification sur le message, entraînerait un échec lors de la vérification de sa signature ...

La non répudiation : C'est la garantie qu'un interlocuteur ne puisse nier ultérieurement l'émission d'une certaine information.

La signature électronique au service de la garantie de la non répudiation :

Si la signature électronique peut garantir l'authentification et l'intégrité d'un message, aucun interlocuteur ne pourrait venir contester, la valeur d'un document qu'il a lui-même signé auparavant ...

II – La cryptographie symétrique (dite à clef privée)

II.1 – Définitions :

Un système cryptographique symétrique : C'est un système cryptographique où les clefs de chiffrement et de déchiffrement sont déductibles, l'une de l'autre en un temps raisonnable.

Dans la majeure partie des cas les clefs sont même identiques ; c'est le cas du système cryptographique de César, et la sécurité dépend étroitement du degré de protection de cette clef unique.

II. 2 – Data Encryption Standard (DES) :

Développé par IBM et adopté comme standard, en 1977, ce système cryptographique reprend des concepts déjà utilisés dans la cryptographie classique, à savoir la permutation des données. Cependant il fait intervenir des notions mathématiques nouvelles, comme les structures de Feistel et suppose un transcodage préalable en binaire.

Il utilise un algorithme de chiffrement, bit par bit, sur des blocs de 64 bits, à l'aide d'une clef de même longueur (le dernier bit de chaque octet étant un bit de parité ...).

II.2.1 – Les structures de Feistel :

On considère une fonction φ quelconque $\varphi : \{0,1\}^{32} \rightarrow \{0,1\}^{32}$

Et on définit une structure de Feistel par la fonction f_φ :

$$\begin{aligned} f_\varphi : \{0,1\}^{32} \times \{0,1\}^{32} &\rightarrow \{0,1\}^{32} \times \{0,1\}^{32} \\ (L,R) &\rightarrow (R, L \oplus \varphi(R)) \end{aligned}$$

Activité II.2.1 :

A. Montrer le théorème de Feistel: Quelque soit la fonction j , la structure de Feistel correspondante f_j , est toujours inversible ?

Il suffit de voir que :

$$\begin{aligned} f_\varphi^{-1} : \{0,1\}^{32} \times \{0,1\}^{32} &\rightarrow \{0,1\}^{32} \times \{0,1\}^{32} \\ (L,R) &\rightarrow (R \oplus \varphi(L), L) \end{aligned}$$

est l'inverse de f_φ , en effet :

$$\begin{aligned} f_\varphi^{-1} \circ f_\varphi (L,R) &= f_\varphi^{-1}(R, L \oplus \varphi(R)) \\ &= (L \oplus \varphi(R) \oplus \varphi(R), R) \quad \{\text{Remarque : } \varphi(R) \oplus \varphi(R) = 0 \text{ et } L \oplus 0 = L\} \\ &= (L,R) \end{aligned}$$

Les structures de Feistel représente une mine inépuisable de fonctions inversibles – et donc utilisables pour les algorithmes de chiffrement – construites à partir de fonctions quelconques.

II.2.2 – L’algorithme de chiffrement du DES :

II.2.2.1 – Description informelle de l’algorithme de chiffrement :

L’algorithme de chiffrement du DES, repose sur 16 itérations d’une structure de Feistel, qui expliquent réellement sa solidité. Les deux permutations effectuées ne le consolident pas vraiment, d’un point de vue cryptographique.

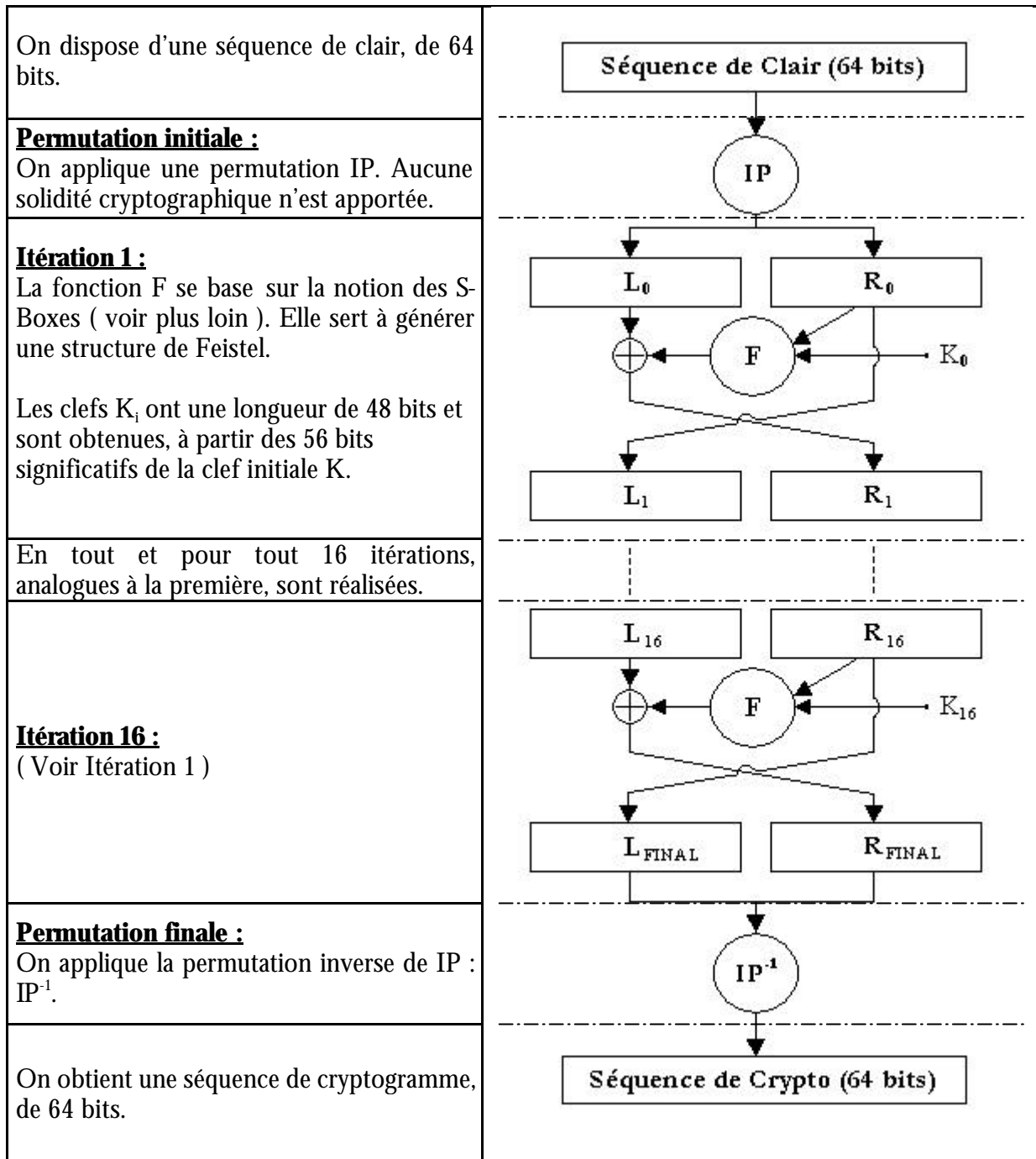


Figure 1 : Description informelle de l’algorithme de chiffrement du DES

II.2.2.1 – Description de la structure de Feistel :

Comme le montre la figure 2, la fonction F récupère deux arguments :

- R_i : C'est le bloc de 32 bits correspondant aux poids les plus forts, du bloc $i-1$.
- K_i : C'est une clef obtenue à partir de la clef K , en effectuant des décalages et des permutations, soigneusement choisies pour mettre à contributions tous ses bits significatifs.

La fonction E : Cette fonction récupère R_i et « l'explode » en une séquence de 48 bits : R'_i . La duplication de bits qui en résulte, augmente la diffusion de l'information.

Les S-Boxes ou les boîtes de substitution (S) : Ce sont des fonctions qui compriment une séquence de 6 bits en une séquence de 4 bits. Le rôle des S-Boxes est primordial. Elles détruisent la structure et immunisent le système contre des attaques par permutations circulaires ... Parmi les 2^{256} choix possibles, pour les S-Boxes, seules les 8 retenues par IBM, donne lieu à un système solide : les critères qui ont motivé ce choix, restent inconnus.

La permutation P : C'est une permutation fixe (pour toutes les itérations).

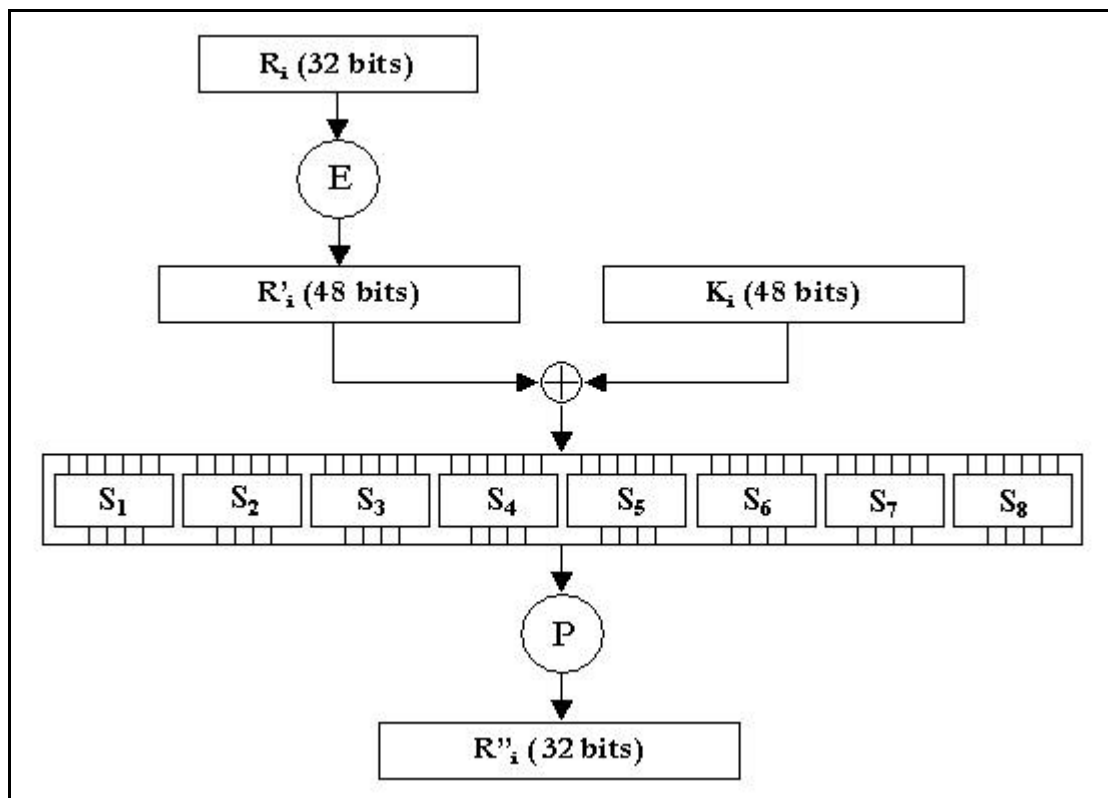


Figure 2 : Description de la fonction F

II.2.3 – Le DES en pratique :

On a traité dans la section précédente, la manière de chiffrer un unique bloc de 64 bits. Comment le chiffrement se généralise-t-il à une séquence de données plus grandes.

Le mode Electronic Code Book (ECB) : Le chiffrement des blocs est indépendant et se fait avec la même clef.

Le mode MAC : Chaque cryptogramme i est la clef de chiffrement pour le bloc $i+1$. Le dernier cryptogramme obtenu est une signature du document.

II.2.4 – La solidité du DES :

Cryptanalyse différentielle du DES : Les structures de Feistel ont été très critiquées pour leur faible diffusion². Elles favorisent une cryptanalyse différentielle. Shamir a réussi à cryptanalyser un DES à 8 itérations, en exploitant cette faiblesse.

Cryptanalyse par attaque de la linéarité du DES : Pour certaines S-Boxes, la non linéarité n'est assurée que par un petit nombre de variables. Si celles-ci sont figées, les S-Boxes sont linéaires sur les variables restées libres. Matsui a réussi une cryptanalyse partielle du DES, exploitant cette faiblesse.

Cryptanalyse par essai systématique des clefs : La longueur de la clef (réellement 56 bits), a donné lieu à plusieurs tentatives de cryptanalyse par essai systématique des clefs. En 1997 une telle expérience, sur un campus universitaire a abouti en quelques mois sans pour autant utiliser des circuits spécialisés (auquel cas, une cryptanalyse aurait abouti en une semaine).

Activité II.2.4 :

Effectuer une critique de la cryptographie symétrique, en en dégagant les avantages et les inconvénients, à la lumière de l'étude du cas DES ?

Avantages :

- La rapidité des algorithmes de chiffrement et de déchiffrement, due à l'utilisation d'opérations déjà disponibles sur les machines (permutations, décalages, opérations booléennes).
- L'aptitude des solutions proposées à un câblage sur circuits intégrés, pour obtenir des performances meilleurs.

Inconvénients :

- La vulnérabilité du chiffrement (essentiellement basé sur les permutations ou les décalages de bits), qui prend de l'ampleur avec les performances croissantes des calculateurs (même ceux communément commercialisés).
- La nécessité de prévoir autant de clefs secrètes que de couples d'interlocuteurs ($N \times (N-1) / 2$ pour N interlocuteurs) et de pouvoir en gérer l'échange.

² L'attaque différentielle se base sur l'analyse de l'impact d'un changement de quelques bits du clair, sur le cryptogramme correspondant.

III – La cryptographie asymétrique (dite à clef publique)

III.1 – Définitions :

Un système cryptographique asymétrique : Dans un tel système, on essaie de rendre impossible de retrouver la clef de déchiffrement à partir de celle de chiffrement. Il est donc possible de rendre publique (d'où le nom) la clef de chiffrement, sans pour autant donner des informations sur la clef de déchiffrement.

Il s'agit donc de trouver des fonctions (qui correspondraient au chiffrement), très difficilement inversibles (dont les inverses correspondraient au déchiffrement). C'est dans le domaine de l'arithmétique des grands nombres, que l'on est allé s'approvisionner en de telles fonctions.

La factorisation d'un entier : On se fixe un entier N , et on considère :

- $P(N)$: l'ensemble des nombres premiers, inférieurs à N .
- E : l'ensemble des entiers se décomposant en un produit de deux éléments de $P(N)$.

On définit alors l'application FACTORISATION, comme l'inverse de l'application PRODUIT, définie, comme suit :

$$\begin{array}{lcl} \text{PRODUIT} & : & P^2(N) \text{ \textcircled{R}} \quad E \\ & & (p,q) \text{ \textcircled{R}} \quad p \cdot q \end{array}$$

La complexité d'un algorithme : On définit la complexité d'un algorithme comme étant le nombre d'opérations nécessaires à sa réalisation.

On parle alors de deux sortes de problèmes :

- **Problèmes NP Complets :** La théorie écarte toute possibilité d'amélioration de la complexité de l'algorithme. La solidité d'un tel algorithme ne dépendra pas du temps.
- **Problèmes non NP Complets :** La théorie n'exclut pas une éventuelle amélioration de la complexité de l'algorithme. La solidité risque d'être compromise par la découverte de méthodes de complexité inférieure.

On se rend vite compte que PRODUIT est une bijection au sens mathématique, mais pas au sens algorithmique. En effet en terme de complexité, autant le produit d'entier à une complexité d'une seule multiplication : $O(1)$, autant la complexité de la factorisation d'entiers est de l'ordre d'un $O(N^{\lceil \log(\log(N)) \rceil})$!

III.2 – Le système cryptographique de Rivest Shamir et Adelman (RSA) :

Cet algorithme se base sur la complexité de la factorisation d'un grand entier. On suppose que deux agents A et B interviennent et que A désire communiquer avec B.

III.2.1 – L’algorithme de RSA :

L’établissement des clefs :

- B choisit p et q deux nombres premiers de l’ordre de (10^{150}) et calcule
 - $n = p \times q$
 - $\varphi(n) = (p-1) \times (q-1)$
- B trouve k, k' tels que $k \times k' = 1 \pmod{\varphi(n)}$ ($k \times k' = 1 + \lambda \times \varphi(n)$)

Quantités publiques : n, k .

Quantités privées : $\varphi(n), k'$.

Le chiffrement :

- A dispose du clair, un entier $m < n$. Il calcule $C(m) = m^k$ et l’envoie à B.

Le déchiffrement :

- B calcule $(C(m))^{k'} = m^{k \times k'} \pmod{n}$
 $= m^{1 + \lambda \times \varphi(n)} \pmod{n}$
 $= m \times (m^{\varphi(n)})^\lambda \pmod{n}$
 $= m \pmod{n}$

III.2.2 – Solidité de RSA :

Théorème : Cryptanalyser RSA équivaut à la factorisation de n .

Activité III.2.2 :

A. Prouver le théorème précédant ?

D’une part cryptanalyser RSA équivaut à retrouver k' , la clef de déchiffrement.

D’autre part retrouver k' , équivaut à retrouver $\varphi(n)$.

Et enfin retrouver $\varphi(n)$ équivaut à factoriser n . En effet, on s’en rend compte en considérant l’équation : $X^2 - S \times X + P$, où $S = p + q$ et $P = p \times q$, et en remarquant que $\varphi(n) = n - S + 1$.

B.1 Lors de l’établissement des clefs, il est demandé à B, de choisir deux entiers k et k' tels que : $k \times k' = 1 \pmod{\varphi(n)}$?

$$k \times k' = 1 + \lambda \times \varphi(n) \quad \Leftrightarrow \quad 1 + \lambda \times \varphi(n) = 0 \pmod{k}$$

On fixe $k = k_0 = 257$ et on cherche λ_0 (au plus 256 itérations) et alors $k_0' = (1 + \lambda_0 \times \varphi(n)) / 257$.

B.2 Proposer une méthode pour trouver de tels entiers qui soient de l'ordre de 10^{150} ?

$$k \times k' = 1 \pmod{\varphi(n)} \quad \Rightarrow \quad k^i \times k'^i = 1 \pmod{\varphi(n)}$$

Ainsi pour i de l'ordre de 50, on pourra trouver des k, k' de l'ordre de 10^{150} .

III.2.3 – Avantages et inconvénients de la cryptographie asymétrique :

Voici une critique de la cryptographie asymétrique, basée sur l'étude du cas RSA :

Avantages :

- Une solidité parfaite dans le cas des problèmes NP complets.
- La notion de clefs publiques facilite les communications multi-interlocuteurs.
- La possibilité de dériver des schémas de signature, pour des besoins d'authentification ou de garantie de la non répudiation.

Inconvénients :

- L'utilisation d'algorithmes très coûteux en temps de réponse. En effet pour le cas de RSA : chiffrement et déchiffrement nécessitent chacun, le calcul d'une exponentielle d'entier, sans oublier les calculs intermédiaires.
- Le problème de la génération de nombres premiers, très grands : d'ailleurs en pratique on n'utilise que des nombres « très probablement » premiers.

WEBLIOGRAPHIE

- [1] Sami Harari, Université de Toulon et du Var
http://sis.univ-tln.fr/sis/info_harari.html