Sécurité des systèmes et réseaux

Résumé des cours dispensés par Jean-Marc Muller et Sébastien Schmitt à l'Université de Strasbourg

Session d'automne 2017

L'USAGE DE CE DOCUMENT NE PEUT ÊTRE QU'ACADÉMIQUE

Mise en forme par Marek Felšöci

17 octobre 2017

Crédits

Ce résumé s'appuie sur les notes et les supports du cours de Sécurité des systèmes et réseaux dispensé par Jean-Marc MULLER et Sébastien SCHMITT à l'Université de Strasbourg.

1 Généralités

1.1 Introduction

1.1.1 Origines

En novembre 1988 le ver de Morris a exploité des vulnérabilités connues de *sendmail* et de la commande *finger* sur les systèmes UNIX. Plus de 10% de machines ont été contaminées. Ce ver a provoqué l'interruption de services.

Cet incident a incité à un travail collectif pour le résoudre ainsi qu'une prise de conscience des problèmes de sécurité.

1.1.2 Artisanat

Dans les années 1990 la démocratisation d'Internet a commencé et les premiers hackers ont apparu tout comme les premières exploitations des vulnérabilités par dépassement de tampon ou encore injections SQL et XSS.

En début de 2000 les attaques DDoS, les premiers *Botnets* et vers informatiques ont connu la lumière du jour.

1.1.3 Industrialisation

C'est l'époque de naissance de la cybercriminalité avec l'apparition des gangs de hackers et des organisations criminelles spécialisées notamment dans les domaines des rançonlogiciels et sites de ventes illégaux).

On observe également le phénomène de commerce d'armes d'intrusion

ou de destruction numérique via, par exemple, la location de *Botnets* ou l'achat de *0-day*.

1.1.4 Mondialisation

La guerre de l'information commence lorsque l'influence des gouvernements grandit dans le but d'affecter l'information de l'adversaire, ses processus basés sur l'information, ses systèmes d'information tout en se protégeant simultanément.

1.1.5 Actuellement

De nos jours les plus vulnérables deviennent les objets connectés. La politique de vote en ligne est également menacée ainsi que des smartphones par divers *malwares*. Il faut se méfier notamment des rançonlogiciels et du développement de l'usage de *Darknet*.

La sécurité est malheuresement placée dans un contexte difficile non seulement en termes de poursuite des responsables mais aussi à cause de manque de moyens, la facilité d'action et de nombreuses attaques provenant de tous les niveaux et outils disponibles.

1.1.6 Sécurité des systèmes d'information

Le système d'information est un ensemble d'éléôents participant à la gestion, le stockage, le traitement, le transport et la diffusion de l'information au sein d'une organisation.

La sécurité d'un système d'information est à la fois un challenge technique, à cause de l'immensité du somaine et des évolutions rapides,

et humain, à cause des contraintes imposées en dépit des services, des coûts et de la sensiblisation. De plus les problèmes s'amplifient avec la connectivité globale et le changement des pratiques.

D'autre part de nombreuses problématiques se posent :

- Quelle est la sécurité adaptée à mon entreprise ? Comment l'organiser ?
- Peut-on utiliser le Cloud ? Comment ?
- Comment gérer le nomadisme ? Comment gérer le BYOD ?
- Comment gérer les utilisateurs du SI (authentification, chiffrement des données, ...) ?
- Concurrence avec les services gratuits ?
- Comment respecter le droit des usagers ?
- Les entreprises sont très mal protégées : peu d'informations, de PRA ou de RSSI

1.2 Acteurs

- **ANSSI** : Agence Nationale de la Sécurité des Systèmes d'Information assure notamment la sécurité des systèmes d'information de l'État.
- **DGSI** : Direction Générale de la Sécurité Intérieure est chargée de la protection du potentie économique et scientifique du pays et du contrespionage.
- **CERT** : *Computer Emergency Response Team* a pour mission la centralisation des demandes d'assistance suite aux incidents de sécurité, le traitement des alertes et réactions aux attaques, établissement et

maintenance d'une base de données de vulnérabilités et prévention par diffusion d'informations.

- **CNIL** : Commission Nationale de l'Informatique et des Libertés protège la vie privée et les libertés individuelles et publiques et veille au respect de la loi informatique.
- **Organismes de normalisation** : ISO, Organisation de coopération et de développement économique, *British Standard Institute*, SSI
- **Acteurs privés** : Club de la Sécurité de l'Information Français (sécurité de l'information, sensibilisation), *Herve Schauer Consultants* (expertise), Alain Bensoussan Avocats (droit)

1.3 Concepts de base

1.3.1 Risque

Le risque se détermine en fonction de la menace, la vulnérabilité et de l'impact.

La menace représente l'attaquant possible d'un élément du système d'information.

La vulnérabilité est la faiblesse, la faille au regard de la sécurité d'un élément du système d'information.

L'impact est la conséquence de l'occurrence du risque et peut être quantifié par un niveau de sévérité.

Le risque peut être également défini enm fonction de la probabilité d'occurrence et du préjudice.

1.3.2 Objectifs

- **Confidentialité** : L'information doit être disponibles uniquement aux ayant droits.
- **Intégrité** : L'information doit être exacte, non-altérée ou modifiée.
- **Disponibilité** : La ressource doit être accessible et utilisable.
- **Authenticité, autorisation, traçabilité** : Nécessaire de prouver l'identité, gérér les droits d'accès aux ressources et tenir un historique des actions effectuées sur les données.

1.3.3 Impacts

- **Financier** : perte d'argent
- **Image** : dégradation de la réputation
- **Organisationnel** : soucis de continuité d'activité
- **Réglementaire** : poursuites juridiques

1.3.4 Menaces et vulnérabilités

Crime organisé, les services d'États, *Script kiddies* et les hacktivistes sont les menaces extérieures. Cependant la menace peut provenir aussi de l'intérieur qu ce soit de la part d'un utilisateur novice (maladresse, curiosité) ou averti (fraude, revanche).

D'autre part les vulnérabilités peuvent être humaines, réseautiques ou logicielles.

1.4 Attaques et vulnérabilités

1.4.1 Vulnérabilités humaines

- **Incompréhension des enjeux** : La sécurité est perçue comme une contrainte car les enjeux sont souvent mal expliqués.
- **Manque de pédagogie** : Adapter la sécurité aux utilisateurs pour améliorer leur niveau de compréhension.
- **Contournement de la politique de sécurité** : mot de passe sur un bout de papier, logiciels à la mode, P2P, etc.
- **Nature humaine** : influençabilité, corruptibilité
- **Ressorts psychologiques** : approche physique, déresponsabilité
- **Attaques ciblés**

1.4.2 Collecte d'information passive

Grandes quantité de nos données personnelles se retrouve sur Internet par l'intermédiaire les réseaux sociaux (comptes compromis, *pishing* des adresses de courriel), les services gratuits en ligne, les moteurs de recherche. Des informations techniques telles que les cartographies de réseaux, les identifications de systèmes sont aussi menacées via les accès aux réseaux et l'écoute du traffic ou *sniffing*.

1.4.3 Vulnérabilités systèmes et logicielles

Elles résident notamment dans la faiblesse d'authentification et sont représentées soit par un mot de passe trivial, des noms de comptes classiques, des mots de passe de constructeurs ou encore des protocoles bavards. D'autre

part la conception souffre des failles systèmes et protocolaires. La vulnérabilité est renforcée également à cause de la publication des failles, la faiblesse des langages et des mauvaises techniques de programmation.

1.4.4 Vulnérabilités web

- client
- serveur web
- serveur d'applications
- serveur de données
- communications

Organismes concernés :

- *Web Application Security Consortium* (WASC)
- *Open Web Application Security Project*

1.4.5 Attaques réseaux

Plusieurs types existent :

- Usurpation d'identité : ARP ou IP *spoofing*, *Man in the middle* (relais applicatifs - SSL, *hijacking* - vol de session TCP)
- Falsification du routage : par OSPF, DNS *poisoning*, par BGP
- Déni de service : *Smurf attack*, SYN *flooding*, DDoS, Courriel indésirable

- Botnets : machines esclaves
- Attaques ciblées : Kali Linux (distribution de *pentest*), scanneur de vulnérabilités système, *Metasploit*
- Attaques combinées : *malwares*, boîtes à outils complexes (*Stuxnet*, *Flame*, ...)

1.5 Outils et techniques de protection

1.5.1 Authentification

Il s'agit de la vérification de l'identité d'une personne pour autoriser l'accès à des ressources. Pour ce faire il faut passer par l'identification (pseudo), l'authentification pour prouver que l'identificateur nous appartient (mot de passe) et l'autorisation qui est ce à quoi l'authentification nous donne accès (droits).

Parmi les mécanismes plus ou moins élaborés sont *Single Sign-On*, CAS, *Shibboleth*.

1.5.2 VPN

VPN est une technique d'utilisation d'une infrastructure publique pour raccorder deux sites distants qui ne demande pas de coûts d'infrastructures supplémentaires et dont le coût ne dépande pas non plus de la distance. Cependant des difficultés peuvent être rencontrées pour garantir la bande passante.

1.5.3 Pare-feu

C'est une protection qui contrôle l'ensemble des paquets et permet d'appliquer une politique de sécurité (acceptation, rejet, destruction) ainsi qu'une journalisation des actions.

1.5.4 DMZ

C'est ce que l'on appelle une zone démilitarisée qui sert à isoler les réseaux sensibles des machines vulnérables pour mieux protéger les machines faibles. Elle permet d'exposer des services sur Internet.

1.5.5 Serveur mandataire

- Proxy
- Pare-feu de niveau applicatif
- Relai d'information selon divers critères (authentification, contrôle de contenu, contrôle de la source et de la destination)
- Filtre en fonction du contenu et/ou du protocole (mots interdits dans les URL)

1.5.6 IDS & IPS

C'est un système de détection d'intrusion qui capture le traffic ou analyse des logs. Il effectue une analyse sur des séquences d'octets, du contenu des champs et du comportement. Il détient une base de données de signatures.

Malheureusement il y a le risque des alertes faussement positives.

Cet outil est qualifié selon la taille de la base de connaissance, la validité de la base et la proportion des alarmes justifiées et injustifiées.

En principe IPS est un IDS plus un pare-feu.

1.5.7 Pot de miel *Honeypot*

Pot de miel est une machine qui simule un serveur ou un réseau pour attirer toutes les attaques. Elle est couplée à un IDS ou un IPS. C'est un système cloisonné pour éviter les rebonds qui permet d'qnticiper et de comprendre les stratégies d'attaques.

1.5.8 Chiffrement

Le chiffrement est utilisé dans :

- **l'identification** pour garantir l'identité de l'utilisateur,
- **l'authentification** pour garantir l'origine de l'information,
- **la confidentialité** pour garantir le secret de l'information transmise,
- **l'intégrité** pour garantir la validité des informations et
- **la non-répudiation** qui est l'impossibilité d'un auteur de nier avoir transmis ou écrit une information.

Le chiffrement **symétrique** utilise une clé secrète partagée entre l'expéditeur et le destinataire.

Le chiffrement **asymétrique** utilise une clé publique et une clé privée et potentiellement une clé de session secrète. Ce type de chiffrement est également exploité par des certificats. Cependant il y a des menaces d'attaques

car on ne peut pas s'assurer de la provenance de la clé publique. De plus celle-ci est transmises aux correspodants via des canaux potentiellement vulnérables. La clé publique peut alors être interceptée et remplacée. C'est ce que l'on appelle une attaque de l'homme du milieu.

1.5.9 PKI

Public Key Infrastructure est une infrastructure de gestion de certificats permettant de mettre à disposition les clés publiques. Chaque demande de certificats fait l'objet d'une demande de validation auprès d'une autorité.

1.6 Organisation de la sécurité

Il existe plusieurs référentiels selon le domaine d'activité comme par exemple ISO27001 (environ 130 mesures de sécurité détaillées) pour les systèmes d'information, critères communs et catalogues de sécurité.

D'autre part l'approche organisationnelle via un Système de management de la Sécurité de l'Information permettant de mettre en place, faire évoluer et maintenir dans le temps des mesures de sécurité techniques et organisationnelles et d'atteindre les objectifs de sécurité fixés.

L'appréciation des risques se fait en constituant une liste pondérée de ceux-ci et en faisant le choix.

1.7 Sécurité au quotidien

1.7.1 Concepts de base

- Moindre privilège

- Défense en profondeur
- Simplicité
- Placement de l'utilisateur au centre de la démarche
- Points d'accès uniques
- Interdiction par défaut
- Maillon faible
- Pas d'obscurité

1.7.2 Sécurité physique

Il est nécessaire de tenir les serveurs sous clés et sous alarme et les postes dans des boîtiers fermés avec un mot de passe BIOS et le démarrage à partir des médias amovibles désactivé. Les sécurités climatique et électrique sont également importantes.

1.7.3 Sensibilisqtion des utilisateurs

Il faut dispenser des conseils aux utilisateurs comme :

- Ne pas donner son mot de passe
- Ne pas tenter de contourner les barrières
- Connaître les applications douteuses
- Mettre en place des solutions sûres

1.7.4 Choix des applications

Il faut éviter les logiciels connus pour leurs défauts comme *telnet*, *ftp*, RPC. De plus, il existe souvent un équivalent sécurisé comme grâce à SSL.

1.7.5 Mises à jour

Les mises à jour sont indispensables. Elles peuvent se faire par *patches*, *apt-get upgrade/update* ou la compilation. Sans mises à jour il n'y a pas de sécurité valable.

1.7.6 Gestion des comptes utilisateurs

- Éviter des comptes sans mot de passe
- Changer de mot de passe régulièrement
- Gestion des droits
- Authentification (PAM, *Kerberos*, LDAP)
- *Single Sign-On* : propagation d'identité (CAS, *Shibboleth*)

1.7.7 Sauvegardes

La sauvegarde permet la recupération des données détruites et assure la continuité d'activité. Il existe différents types de sauvegarde :

- Complète
- Incrémentale

Il faut bien distinguer le stockage, la sauvegarde et l'archivage !

1.7.8 Sécurisation des communications

Au niveau système on y procède par chiffrement des communications par SSH ou VPN et par chiffrement des données. Au niveau réseau via un pare-feu ou un IDS.

1.7.9 Traitement des logs

Les fichiers de log permet de détecter les tentatives d'intrusion. Cependant il faut bien les configurer pour ne pas saturer le système mais pour avoir des informations suffisamment précises. Leur stockage devrait se faire sur un serveur dédié et pour une durée limitée (CNIL).

2 Mot de passe

Le mot de passe est souvent utilisé pour s'authentifier et donc **prouver son identité** par un élément que l'on connaît.

2.1 Recommendations

- au minimum 10 caractères
- différents types de caractères
- pas de lien personnel
- ne pas confondre avec un identificateur
- changement régulier
- ne pas mémoriser dans les applications

- ne pas stocker dans un fichier ou lieu proche de l'ordinateur
- limiter le nombre de tentatives d'accès si possible

2.2 Stockage

Les mots de passe sont généralement stockés dans des bases de données. Cependant pour limiter les danger ils ne doivent pas être stockés sous la forme lisible mais sous celle d'une empreinte non-réversible.

Même une empreinte peut être menacée soit par une attaque par dictionnaire, par force brute ou par « table arc-en-ciel » qui est une base de données en ligne disposant de toutes les paires mot de passe-empreinte possibles selon les algorithmes.

2.3 Protection des fonctions générant des empreintes

Le problème est qu'un même mot de passe génère une empreinte identique. Il peut aussi exister une collision mathématique provoquant une empreinte identique pour deux mots de passe différents.

Pour résoudre ce problème on augmente le délai après tentatives ainsi que la compléxité de l'algorithme et on ajoute un élément aléatoire dans la fonction (un grain de sel) comme par exemple le pseudo, la position de la souris ou un NONET avec un fragement de la mémoire.

3 Chiffrement symétrique

Le principe de ce type de chiffrement est une clé secrète que partagent l'émetteur et le récepteur de l'information chiffrée.

Exemples de techniques

- **Code de César** : substitution d'une lettre par une autre en utilisant un décalage **fixe** qui constitue la clé
- **Code de Vigenère** : amélioration du Code de César, introduction du décalage **variable**, la clé est un mot définissant le décalage successif de chaque lettre, vulnérable si la clé est trop courte (motifs répétitifs)
- **Chiffre de Vernam (masque jetable)** : la clé doit être une suite de caractères aléatoires et de longueur identique au texte à chiffrer, pas de motif réproductible, simple opération de subtitution, transmission doit être absolument sûre, difficulté de produire des clés aléatoires, clés valables uniquement pour un seul échange

3.1 Cryptographie

C'est l'ensemble des solutions de chiffrement permettant d'assurer la sécurité des données en garantissant la **confidentialité**, l'**intégrité** et l'**authenticité** (non-répudiation).

3.2 Chiffrement par flux

Le principe de base repose dans l'utilisation de la fonction logique OUEX avec sa propriété involutive et d'un générateur binaire Gx pseudo-aléatoire.

Le chiffrement utilise les formules suivantes pour chiffrer respectivement déchiffrer un message :

$$Mc = Md \oplus K(Gx)$$

$$Md = Mc \oplus K(Gx)$$

3.2.1 Générateur pseudo-aléatoire

Le générateur utilise un registre à décalage à rétroaction linéaire (*Linear Feedback Shift Register*). C'est un système électronique ou logiciel qui produit une suite de bits sous forme de registre à *n*-bits avec un coût faible.

La faiblesse de ce générateur repose dans le fait que les aléas sont générés par une solution prédictible et reproductible vulnérable aux attaques mathématiques. C'est pourquoi il ne doit pas être utilisé seul. Le

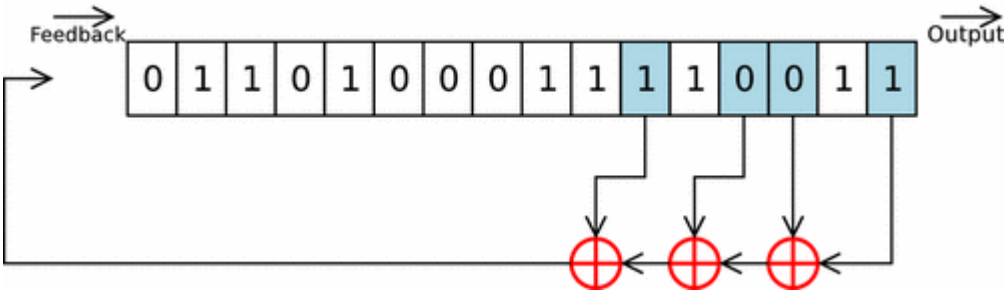

Figure 1: Exemple d'un registre à décalage à rétroaction linéaire (LFSR)

bit calculé est réinjecté dans le registre.

3.2.2 Chiffrement par flux A5/1

Le chiffrement A5/1 a été utilisé dans la communication GSM depuis 1994. Il a été cassé en 2009.

La communication utlise deux flux (montant et descendant). Chaque flux transmet 114 *bits* chiffrés dans un bloc de 4,6 *ms*. Un générateur aléatoire produit 228 *bits*. Ensuite l'algorithme utilise trois LFSR et une clé de session K entre le portable et l'antenne. Chacun des trois LFSR utilise un *clocking bit* lui indiquant s'il peut se décaler ou pas. Cet horodotage irrégulier permet d'introduire une confusion. Un LFSR est autorisé à se décaler si la valeur de son bit d'horloge est majoritaire parmi celles des trois LFSR.

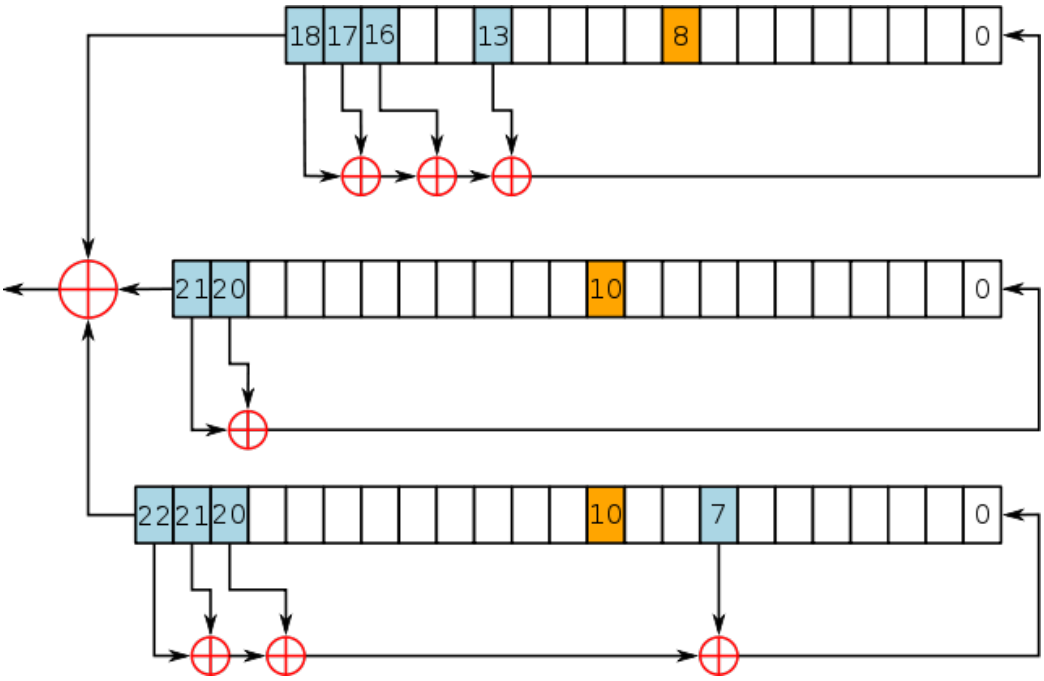

Figure 2: Utilisation de LFSR par l'algorithme de chiffrement A5/1 (bit d'horloge est en orange)

3.3 Chiffrement par bloc

Le principe est de découper le texte claire en **blocs de taille identique** et d'effectuer un chiffrement itératif sur chaque bloc. La longueur des clés

doit être supérieure à 128 *bits*. Cet algorithme utilise une fonction interne *F* appliquée à chaque tour de chiffrement qui utilise une combinaison de « boîtes » et de OUEX pour effectuer une permutation linéaire (*P-Box*) et une substitution non-linéaire (*S-Box*).

P-Box utilise une matrice pour permuter les bits. Par contre *S-Box* effectue une substitution de bits d'entrée en fonction d'un tableau. Cette substituion peut également servir pour compresser des données car la sortie de la substitution peut être d'une longueur inférieure à l'entrée (*S-Box 6/4* du chiffrement DES).

3.3.1 Réseau de Feistel

Lors du chiffrement on découpe le bloc en deux parties (L_0, R_0) et à chaque tour $i = 0...n$ on effectue :

$$L_{i+1} = R_i$$

$$R_{i+1} = L_i \oplus F(R_i, K_i)$$

Le message chiffré obtenu est (R_{n+1}, L_{n+1}).

3.3.2 Chiffrement DES

C'est un chiffrement symétrique par blocs de 64 *bits*. Les clés sont de 58 *bits*. Les 6 *bits* restant sont pour le contrôle de parité. L'algorithme effectue 16 itérations de chiffrement.

3.3.3 Chiffrement AES

L'algorithme AES utilise des blocs et des clés de 128 à 256 *bits* et effectue respectivement 10, 12 et 14 itérations. *A contrario* de DES il n'est pas basé

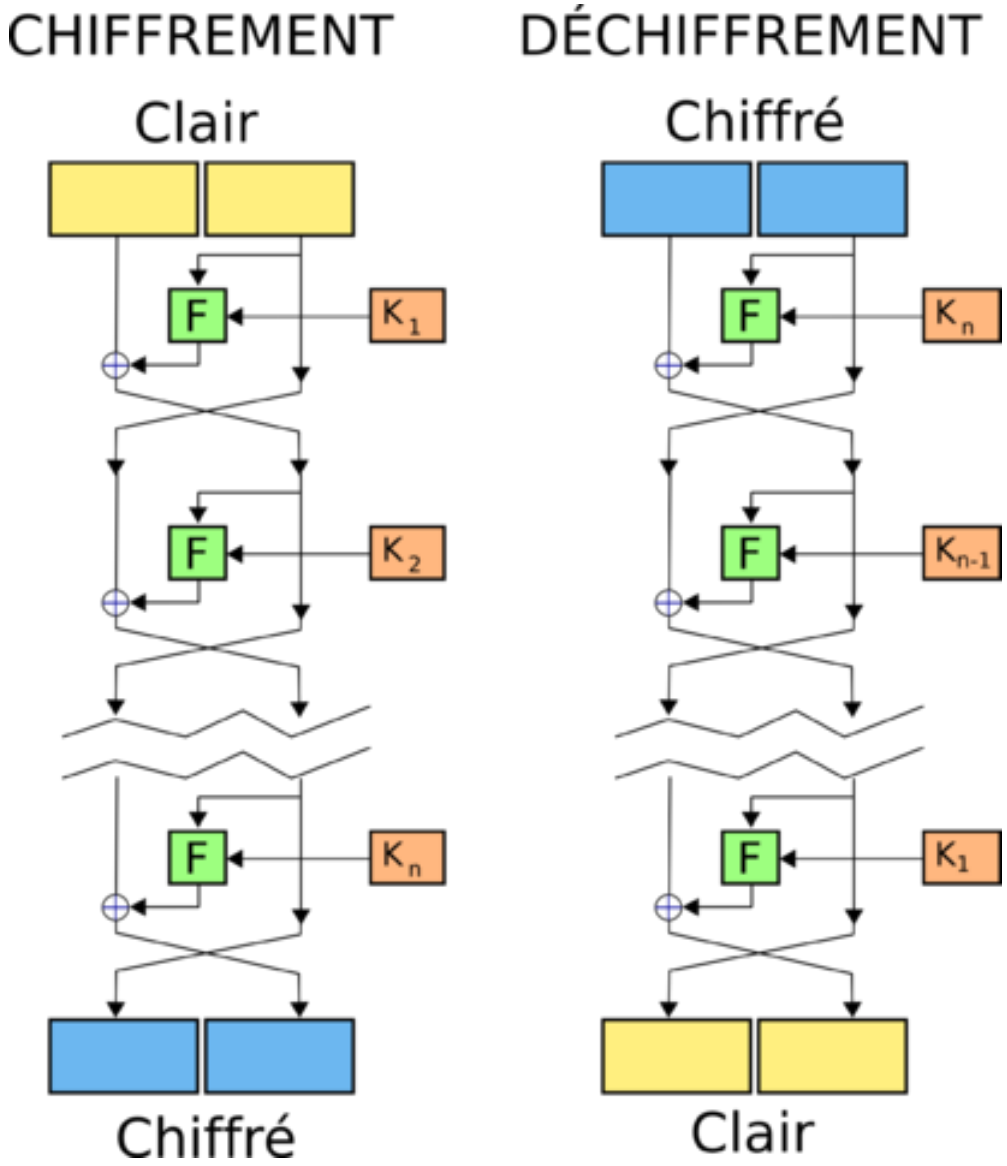

Figure 3: Déroulement de chiffrement respectivement de déchiffrement de Feistel

sur un réseau de Feistel. AES est encore considéré sûr de nos jours. La seule attaque possible est par force brute.

4 blocs de fonctions sont utilisés (*SubBytes*, *ShiftRows*, *MixColumns*, *AddRoundKey*) ainsi que 10 itérations. La clé de chaque itération est dérivée

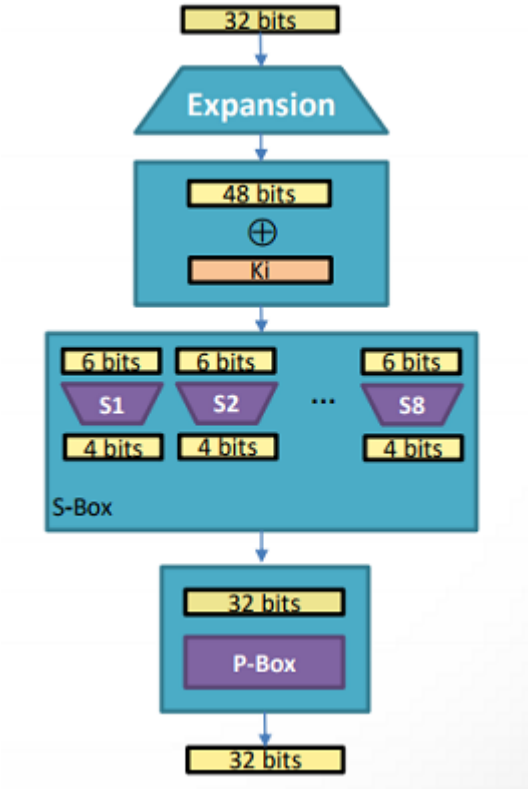

Figure 4: Fonction F utilisé par le chiffrement DES

par fonction successive (*X, S-Box, OUEX*).

SubBytes substitue 16 *octets* correspondant à 128 *bits* selon une table prédéfinie.

ShiftRows effectue un décalage variable des octets selon la ligne.

MixColumns multiple chaque colonne par une matrice prédéfinie.

AddRoundKey calcule un OUEX avec la clé.

3.3.4 Contraintes des algorithmes de chiffrement par bloc

- taille de blocs limitée

- taille de clés limitée
- impossible pour de grandes quantités de données

Plusieurs solutions existent :

- chaînage de blocs
- utiliser un vecteur d'initialisation
- dictionnaire de codes (*Electronic CodeBook*, ECB, $Mc_i = F(Md_i, K)$) : séparation de données par morceau qui sont chiffrés séparément avec la même clé, possibilité de comparer les textes chiffrés et faire une analyse statistique
- enchaînement de blocs (*Cipher Block Chaining*, CBC, $Mc_1 = F(Md_1 \oplus IV, K), Mc_i = F(Mc_{i-1} \oplus Md_i, K)$) : effectue un OUEX avec le bloc qui précède avant le chiffremenr par bloc, utilise un vecteur d'initialisation *IV* aléatoire et unique
- chiffrement à rétroaction (*Cipher Feedback*, CFB, $Mc_1 = F(IV, K) \oplus Md_1, Mc_i = F(Mc_{i-1}, K) \oplus Md_i$) : vecteur d'initialisation est chiffré avec la clé, le texte clair n'est pas directement chiffré par un bloc, en disposant de la clé il est possible de déchiffrer jusqu'à l'avant dernier bloc
- chiffrement à rétroaction de sortie (*Output Feedback*, OFB, $Mc_1 = F(IV, K) \oplus Md_1, Mc_i = F(IV, K)_{i-1} \oplus Md_i$) : vecteur d'initialisation est chiffré avec la clé, la clé précédente est utlisée pour chiffrer la clé suivante

3.4 Partage de secret

Le problème du chiffrement symétrique à grande échelle est l'échange de la clé qui doit être absolument sûre. De plus entre chaque paire de correspondant il faut une clé.