Chapitre 7

Sécurité des réseaux

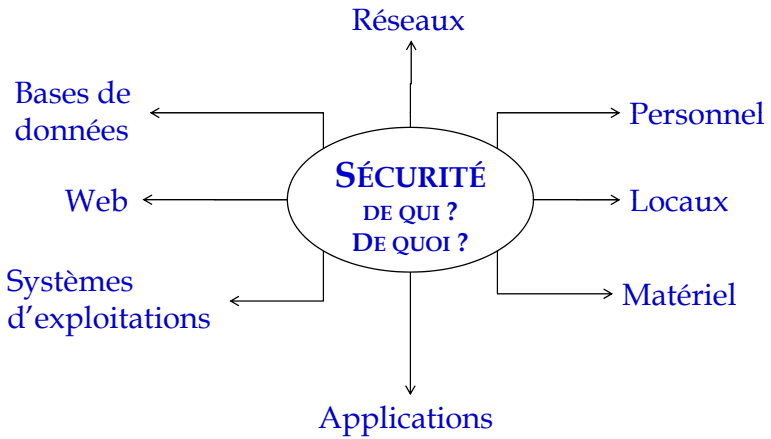
Services,
attaques
et
mécanismes cryptographiques

Partie 1:
Introduction à la sécurité des réseaux

Définitions

- Sécurité:
  - Ensemble des techniques qui assurent que les données et les ressources (matérielles ou logicielles) soient utilisées uniquement dans le cadre où il est prévu qu'elles le soient.
  - ➔Sécurité des systèmes d'informations
- Système d'information:
  - Ensemble d'activités consistant à gérer les informations:
    - acquérir, stocker, transformer, diffuser, exploiter…
  - Fonctionne souvent grâce à un système informatique
  - ➔Sécurité du système d'information = sécurité du système informatique

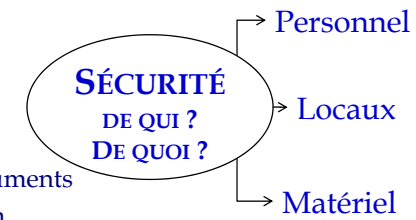
Périmètre de la sécurité (1/3)



Périmètre de la sécurité (1/3)

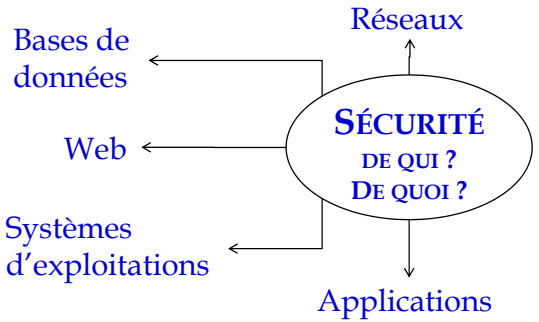
- Périmètre **organisationnel et fonctionnel**:
  - Organisation de la sécurité
    - Répartition des responsabilités
    - Sensibilisations des utilisateurs
    - Contrôle
  - Politique et guides de sécurité
  - Procédure de sécurité

- Sécurité **physique**
  - Lutte anti-incendie, dégâts d'eau
  - Contrôle d'accès physique
  - Sauvegarde et archivage des documents
  - Sécurité du matériel: climatisation…



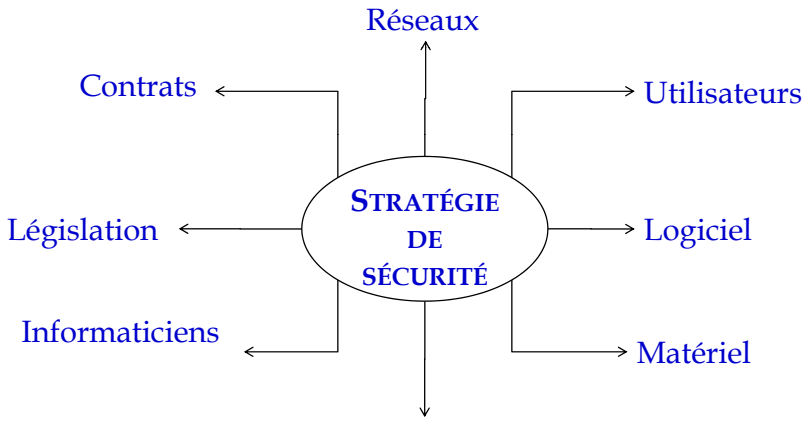
Périmètre de la sécurité (2/2)

- Sécurité **logique**:
  - des données,
  - des applications,
  - des systèmes d'exploitation.
  - Des communications réseaux



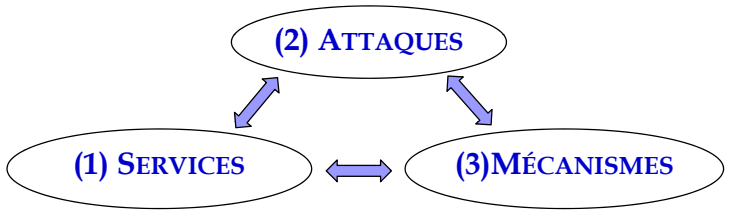
Sécurité: nécessité

- Besoin d'une stratégie de sécurité pour:



Aspects de la sécurité

Méthodes employées pour
casser les services de la sécurité
en détournant les mécanismes



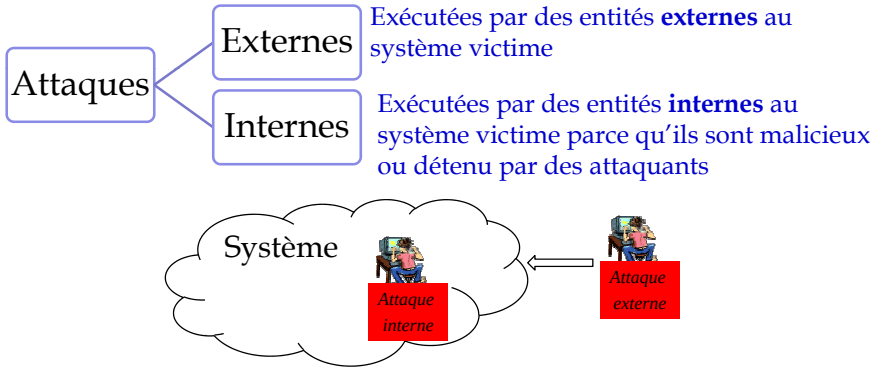
Fonctionnalités requises pour assurer un environnement sécurisé en faisant appel aux mécanismes

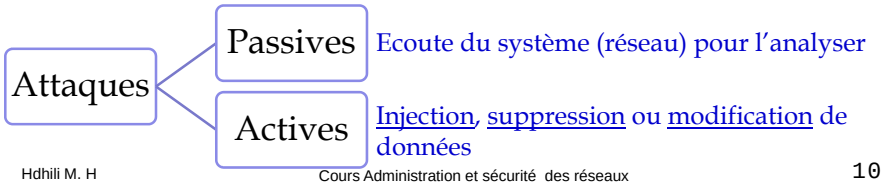
Moyens utilisés pour assurer les services de la sécurité en luttant contre les attaques

Aspects de la sécurité: services

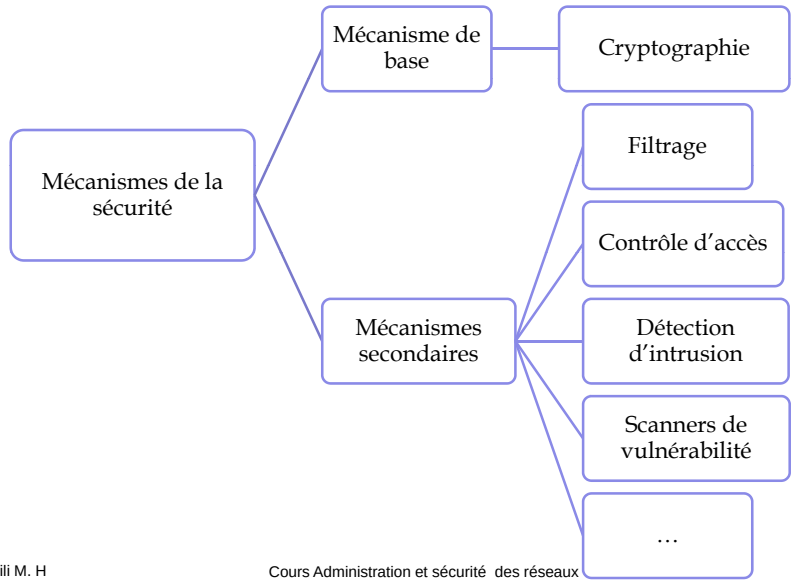
- Authentification
  - Assurance de l'identité d'un objet de tout type qui peut être une personne (identification), un serveur ou une application.
- Intégrité
  - Garantie qu'un objet (document, fichier, message, etc.) ne soit pas modifié par un tiers que son auteur.
- Confidentialité
  - Assurance qu'une information ne soit pas comprise par un tiers qui n'en a pas le droit
- Non répudiation
  - Assurance que l'émetteur d'un message ne puisse pas nier l'avoir envoyé et que son récepteur ne puisse pas nier l'avoir reçu.
- Disponibilité
  - Assurance que les services ou l'information soient utilisable et accessible par les utilisateurs autorisés

Aspects de la sécurité: attaques





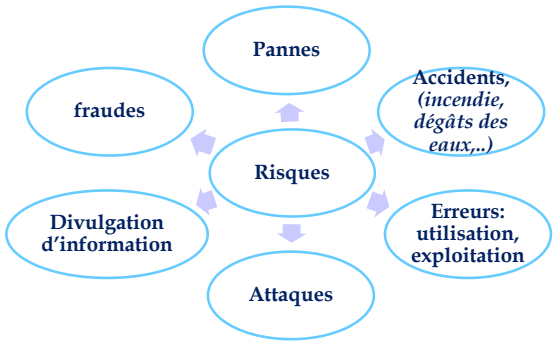
Aspects de la sécurité: Mécanismes



Risques

- Le risque:

  Le fait qu'un événement puisse **empêcher** de
  - Maintenir une situation donnée **et**
  - Maintenir un objectif dans des conditions fixées **et**
  - Satisfaire une finalité programmée



Politique de sécurité

- Objectifs
  - Sécurisation adaptée aux besoins de l'entreprise (après l'analyse des risques)
  - → Compromis sécurité - fonctionnalité.
  - Permet d'analyser un audit de sécurité
- Composantes
  - politique de confidentialité
  - politique d'accès
  - politique d'authentification
  - Politique de responsabilité
  - Politique de maintenance
  - politique de rapport de violations
  - …

Audit de la sécurité

- Audit:
  - Mission d'examen et de vérification de la conformité (aux règles) d'une opération, d'une activitéou de la situation générale d'une entreprise
- Objectifs:
  - Voir si la politique de sécurité est respectée
  - Découvrir les risques
  - Effectuer des tests techniques de vulnérabilité
  - Proposer des recommandations
  - Proposer un plan d'action

Partie 2:
Attaques réseaux et vulnérabilités protocolaires

Les attaques réseaux

- Attaques passives
  - Écoute et analyse du trafic réseau
  - → Exemple d'outils: wireshark, tcpdump
  - → But: trouver des informations susceptibles d'intéresser un attaquant
    - → Adresses IP importantes
    - → Architecture du réseau
    - → Emplacement des nœuds
    - → Informations d'authentification
    - → Information secrète (en cas de guerre par exemple)
    - → …

Les attaques réseaux

- Attaques actives
  - Modification des données stockées ou en transit
  - Injection de données
    - Fabrication (mascarade): injecter des données en spécifiant une adresse source légitime
    - Rejeu: ré-envoyer d'anciens données
  - Suppression de données

Les attaques réseaux

- Les attaques réseaux exploitent les faiblesses (vulnérabilités)
  - Des protocoles:
    - Conception simple, légère et non sécurisé
  - Des mécanismes d'authentification:
    - Exemple: usurpation d'identité
  - Des implémentation:
    - Exemple: mot de passe en clair sur le réseau, bugs
  - Des configuration :
    - Exemple: Firewall mal configuré laissant passer un trafic non autorisé.

Les attaques réseaux (plan)

- Les attaques sur les protocoles
  - Niveau Application
    - DNS, DHCP
  - Niveau transport
    - TCP
  - Niveau réseau
    - IP, ICMP
  - Niveau liaison
    - Ethernet

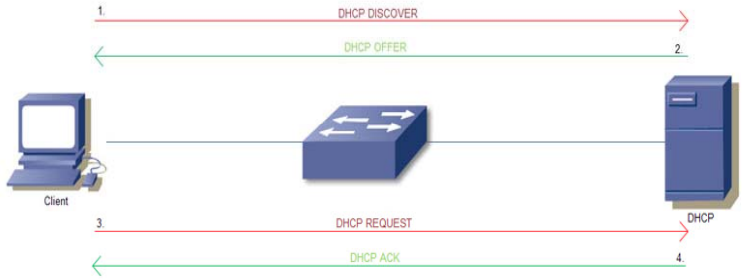
Les attaques réseaux

Les attaques niveau application

DNS, DHCP

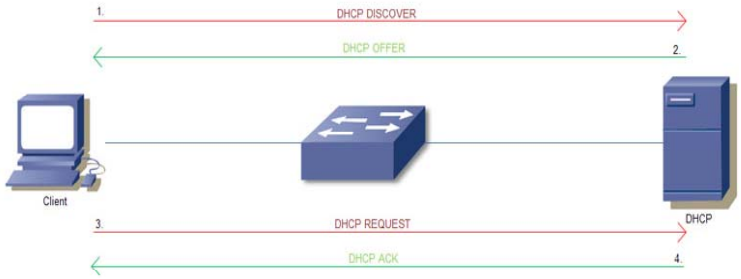
DHCP- rappel

- Le client **diffuse** une demande de bail IP (DHCPDISCOVER) contenant l'adresse IP source 0.0.0.0, l'adresse IP destination 255.255.255.255 et son adresse MAC.
- Les serveurs DHCP répondent **en unicast** par un (DHCOFFER) en proposant une adresse IP avec une durée de bail et l'adresse IP du serveur DHCP



DHCP- rappel

- Le client sélectionne la première offre (adresse IP) reçue et **diffuse** un message (DHCPREQUEST) d'utilisation de cette adresse au serveur DHCP. Son message envoyé par diffusion comporte l'identification du serveur sélectionné qui est informé que son offre a été retenue ; tous les autres serveurs DHCP retirent leur offre et les adresses proposées redeviennent disponibles.
- Le serveur DHCP accuse réception de la demande **(en unicast)** et accorde l'adresse en bail (DHCPACK).



DHCP- attaques

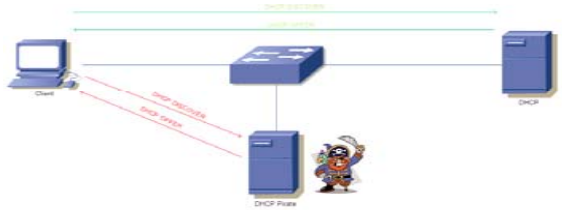
- Épuisement des adresses IP – DCHP Starvation
- Faux serveur DHCP

Attaque DHCP starvation

- Vulnérabilité:
  - Les requêtes DHCP ne sont pas authentifiées.
- Attaque:
  - L'attaquant inonde le serveur avec des messages **DHCPREQUEST** afin de réserver toutes les adresses IP disponibles.
    - L'attaquant doit utiliser une nouvelle adresses MAC pour chaque requête.
- Risque:
  - Dénis de service.
- Contre mesures:
  - Limiter le nombre d'adresses MAC permises sur un port donné.
  - Authentification

Faux serveurs DHCP

- Vulnérabilité: Les requêtes DHCP ne sont pas authentifiées.
- Attaque: L'attaquant prend le rôle d'un serveur DCHP.
  - L'attaquant répond avec un DHCPOFFER en donnant de fausses paramètres IP à l'utilisateur
    - Fausses adresses IP et réseau
    - Faux routeur par défaut
      - L'adresse de l'attaquant si celui veut voir tout le trafic de la victime.
  - L'attaquant peut effectuer un déni de service sur le serveur légitime afin qu'il n'interfère pas avec cette attaque.



Faux serveurs DHCP

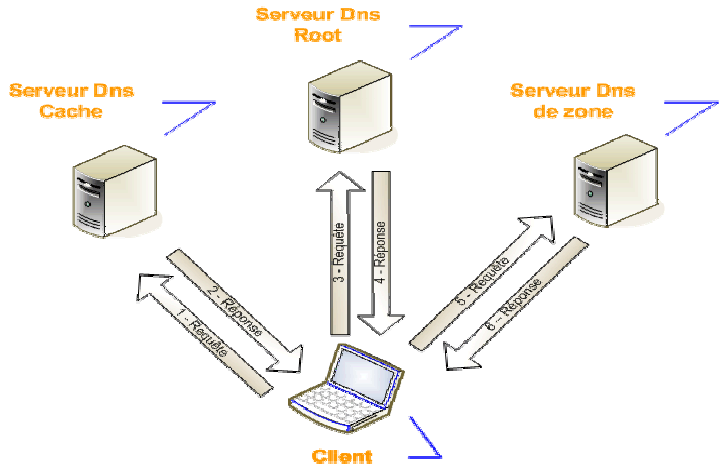
- Risque:
  - Dénis de service.
  - Divulgation d'informations sensibles (p.ex. mots de passe) qui ne devraient pas être envoyées sur un port.
- Contre mesures:
  - DHCP snooping : Défense contre le DHCP spoofing
    - Implémenté dans certains commutateurs CISCO
    - Mettre en place une liste de ports sur le commutateur sur lequel se trouvent les "trusted dhcp server".
    - ➔ Limite l'impact de l'attaque

DNS- Rappel

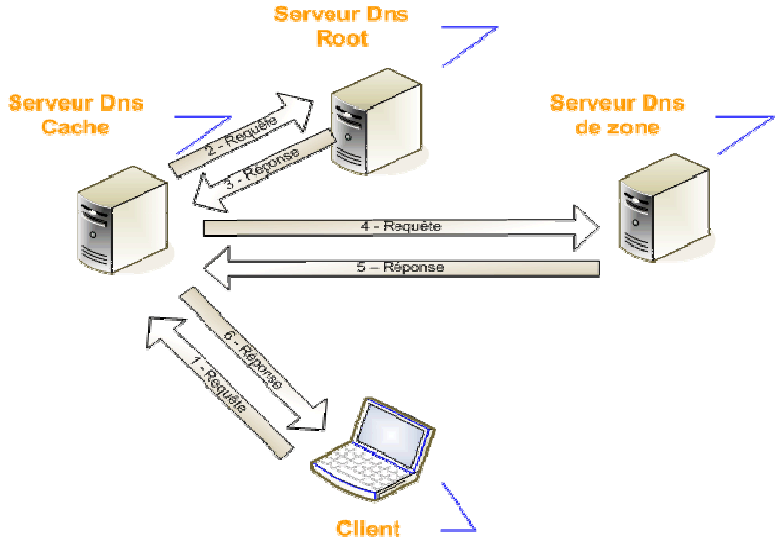
- Assurer la conversion noms d'hôtes - adresses IP

  Machine.domaine.xyz <==> 193.95.66.15
- Un serveur DNS reçoit des requêtes du type:
  - *DNS Query (Quel est l'adresse de www.abc.tn)*
- Il a deux choix:
  - Répondre à la requête (Mode Itératif)
    - DNS Answer: www.abc.tn ➔ 195.93.66.41
      - Tout en disant si l'information provient de la mémoire cache ou si le serveur est l'autorité responsable de ce domaine.
    - DNS Answer: www.abc.tn ➔ inconnu ?
      - Voici une liste de serveurs DNS qui pourraient répondre: …..
  - Effectuer une autre requête (Mode récursif)
    - DNS Query (Quelle est l'adresse de www.abc.tn?)
      - Cette nouvelle requête est envoyée vers d'autres serveurs DNS.

DNS- Rappel (mode itératif)



DNS- Rappel (mode récursif)



DNS- Rappel

- Serveurs DNS envoient régulièrement des requêtes du type :
  - DNS Query (Quelle est l'adresse de www.abc.tn?)
- Serveurs DNS reçoivent alors des réponses du type
  - DNS Answer (www.abc.tn → → 195.93.66.41)
- Ces réponses ne sont pas authentifiées (pas de cryptographie)
- Bien que:
  - L'entête DNS contient un numéro permettant d'associer une réponse à une question (16 bits). **Mais**, ce numéro peut être deviné!
  - Port UDP du client DNS (16 bits) **Mais**, le client peut être amené à toujours utiliser le même port pour faciliter la configuration du pare-feu.
- **→ Il est simple de forger une réponse malicieuse à une question légitime.**

Attaque DNS cache poisoning

- Vulnérabilité:
  - Les messages DNS ne sont pas authentifiés.
- Attaque:
  - L'attaquant envoie de faux messages à un serveur DNS local.
    - Réponse qui spécifie un nom de domaine différent que celui demandé → à ignorer
    - Réponse qui spécifie un serveur DNS appartenant à un domaine différent de celui demandé → douteux
    - Réponse contenant une adresse suspecte (frauduleuse)
- Risque:
  - Redirection du trafic légitime

Email - attaques

- Email Bombing/Spamming
  - Données
    - Falsification de l 'adresse d 'origine
  - Attaque:
    - **Bombing**: envoi d 'un message répété à une même adresse
    - **Spamming**:le message est envoyé à des milliers d 'adresses
  - Objectif:
    - congestion du réseau
    - crash du serveur de messagerie
  - Parade
    - Supervision, filtrage…

Les attaques réseaux

Les attaques niveau transport

TCP, UDP

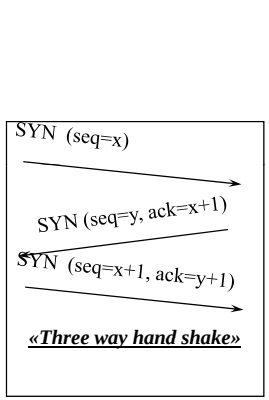
TCP- Rappel

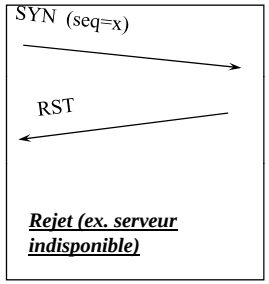
- Ordonnancement des paquets:
  - numéro de séquence par octet
- fenêtre d'anticipation ajustable par le destinataire
- Accusés de réception

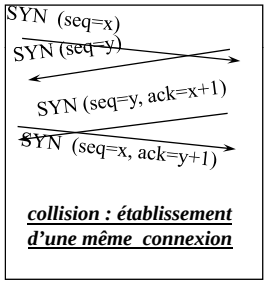
Port source								Port destination
Numéro de séquence								
Numéro d'ACK								
Long. En-tête		URG	ACK	PSH	RST	SYN	FIN	Fenêtre
Checksum								Pointeur urgent
Options (exemples : négociation du MSS Max segment size (non inclus l'entête TCP, par defaut 536 bytes), « Window scale factor », No-Op, utilisation d'un protocole de retransmission sélective RFC 1106 …)								

TCP- Rappel

- Etablissement d'une connexion

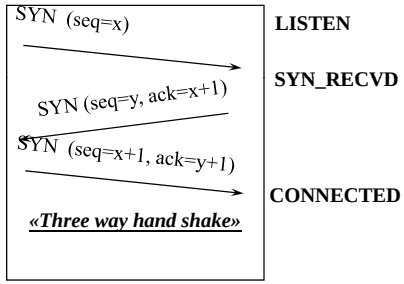






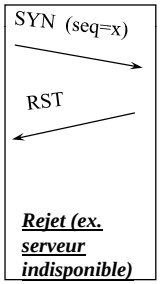
TCP-attaques

- TCP syn flooding
  - Données:
    - Attente dans l'état *SYN_RECVD (75s)*
    - Nombre limité de connexions dans cet état
  - Attaque:
    - Etablir plusieurs connexion successives semi-ouverte (avec adresse IP fausse) afin de saturer la pile TCP de la victime
  - Risque:
    - DoS, Perte de connectivité
  - Parade
    - *SYN cache, SYN cookies dans les OS modernes*
    - *Filtrage en analysant les communication TCP*



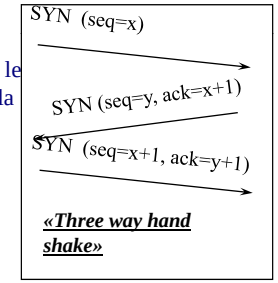
TCP-attaques

- TCP Reset Flooding
  - Données:
    - TCP réordonne les paquets selon leur numéro de séquence.
    - Les paquets sont acceptés seulement si leur numéro correspond à un intervalle.
  - Vulnérabilité:
    - Les paquets TCP ne sont authentifiés que par leur numéro de séquence et leurs paramètres de session.
  - Attaque:
    - inonder la victime avec des paquets TCP RST afin d'interrompre une connexion.
  - Risque: DoS
  - Parade
    - *Numéros de séquence imprévisibles ➔ RFC 1948 – Defending Against Sequence Number Attacks*
    - *Petits intervalles de validité ➔ Perte de robustesse.*



TCP-attaques

- TCP Hijacking (Man in the middle)
  - Vulnérabilité:
    - Les applications authentifient généralement les participants seulement lors des ouvertures de session.
  - Attaque:
    - L'attaquant écoute une communication. Puis, après que le participant s'est authentifié, il injecte des paquets dans la connexion.
      - Interrompt la connexion du point de vue du client.
      - Personnifie le client face au serveur.
  - Risque:
    - Dénis de service
    - Divulgation d'informations sensibles qui ne peuvent être obtenues qu'après authentification.
  - Parade
    - Utilisation de protocoles cryptographiques (SSL…).



UDP-Attaques

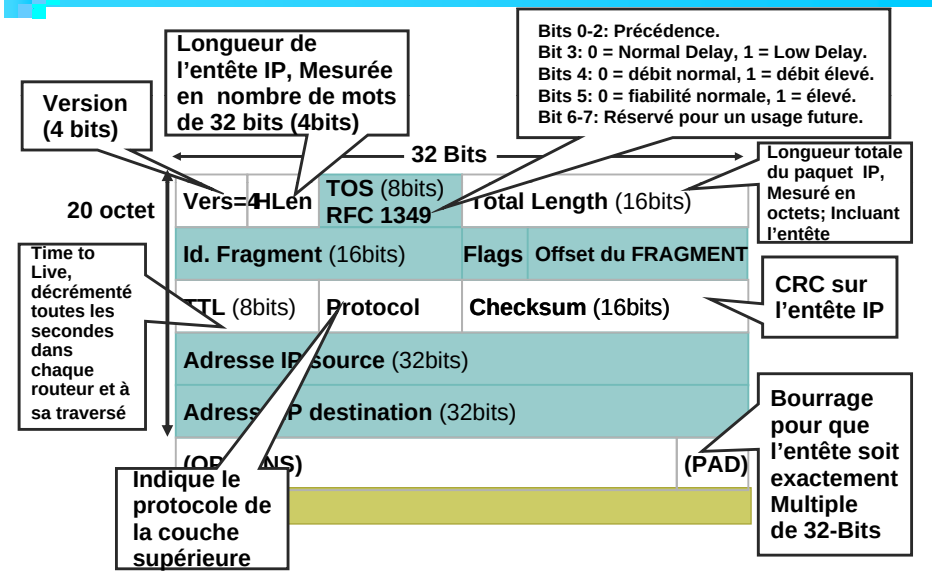
- UDP bombing
  - Données:
    - Deux services utilisés dans le passé pour le test du réseau et sont activés par défaut
      - Service **echo**: echo des caractères reçus
      - Service **chargen**: générateur de caractères
  - Attaque:
    - Établir une connexion entre ces deux services (dans deux machines différentes ou dans la même machine)
  - Objectifs
    - Congestion du réseau et dégradation des performances des machines victimes
  - Parade:
    - désactiver les ports correspondants

Les attaques réseaux

Les attaques niveau réseau

IP, ICMP, ARP

IP- Rappel



IP- attaques sur la fragmentation IP

- Ping of death attack
  - Données:
    - Taille maximum d 'un paquet IP = 65535 octets
    - ICMP est encapsulé par IP
  - Vulnérabilité:
    - IP ne teste pas la longueur totale des fragments avant de les réassembler
  - Attaque:
    - Générer des fragments appartenant à des paquets ICMP de taille > 65535
  - Risque:
    - Le réassemblage des fragments provoque le crash du buffer ou le reboot du système
  - Contres mesures:
    - Patches (déjà existants dans les nouveaux OS)

  ➔ les systèmes récents ne sont plus vulnérable à cette attaque

IP- attaques sur la fragmentation IP

- Tiny Fragment attack
  - Données:
    - TCP est encapsulé dans IP
  - Vulnérabilité
    - Les filtres testent généralement le premier fragment
  - Attaque:
    - Utiliser de petit fragments pour forcer la division de l'entête TCP sur deux fragments
    - Exemple: les flags TCP sont placés dans le second fragment, ce qui ne permet pas au filtres de supprimer les connexions indésirable
  - Risque
    - Établissement de connexions indésirables: intrusions
  - Contres mesures
    - Fixer, au niveau des filtres, une taille minimale du premier fragment

IP- attaques sur la fragmentation IP

- Teardrop attack
  - Donnée
    - L'entête IP contient un champs offset qui indique l'emplacement du fragment dans le paquet initial
  - Attaque:
    - Insertion de faux offsets résultant en des
      - **Chevauchement** de fragments
      - **Gaps** (vide) entre fragments
  - Risque:
    - Instabilité du système, DoS
  - Contre mesure
    - Patches

  ➔ les systèmes récents ne sont plus vulnérable à cette attaque

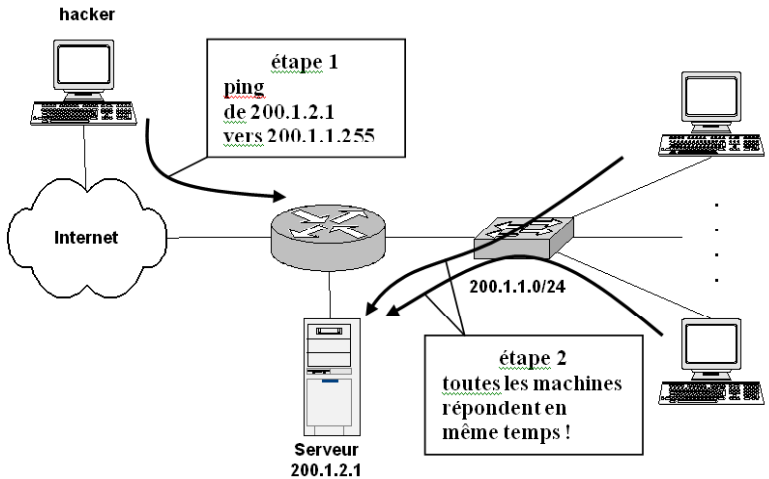
IP-attaque sur l'adressage IP

- IP spoofing (usurpation d'identité)
  - Vulnérabilité:
    - L'adresse IP source est contrôlé par l'envoyeur
  - Attaque
    - L'attaquant peut envoyer des attaques tout en personnifiant n'importe quelle source pour ne pas être retracé.
  - Risque:
    - Utiliser les privilèges de l'adresse usurpée.
  - Contre mesure:
    - Authentification (Ipsec, SSL…)

IP-attaque sur l'adressage IP

- Smurf:
  - Données
    - IP permet la diffusion !
  - Attaque:
    - Inondation du réseau avec des ping ayant des adresses de diffusion et une adresse source fausse ou d'une victime
  - Risques:
    - Rendre indisponible un service, un système ou un réseau
  - Parade
    - Ne pas répondre pour les adresses broadcast, filtrage

IP-attaque sur l'adressage IP

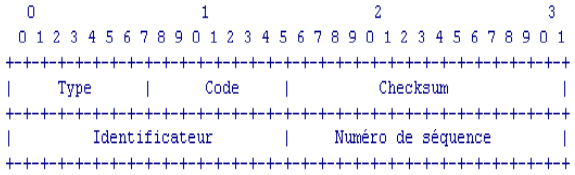


IP-attaque sur l'adressage IP

- LAND (Local Area Network Denial of service):
  - Vulnérabilité:
    - Les champs @IP source et @IP destination peuvent être similaire
  - Attaque:
    - Forger plusieurs segments *TCP syn* @IP source et @IP destination identiques et égales à l 'adresse de la machine victime
  - Risques:
    - La victime répond à elle-même continuellement
    - DoS: congestion de la victime
  - Parades:
    - Filtrage, patch sur les systèmes

ICMP- Rappel

- Deux types de paquet ICMP :
  - Les messages d'indication d'erreur;
  - Les messages de demande d'information.



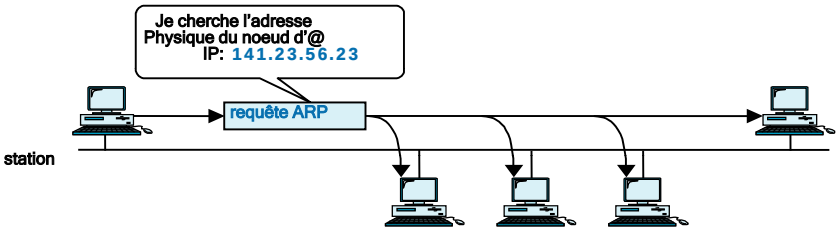
- Types et codes :
  - Exemples:

Type	Code	Description
0	3	Réponse à une demande d'écho
3	0	Réseau inaccessible
3	1	Hôte inaccessible
3	2	Protocole inaccessible
3	3	Port inaccessible
3	4	Fragmentation nécessaire mais interdite
3	5	Echec de routage par la source

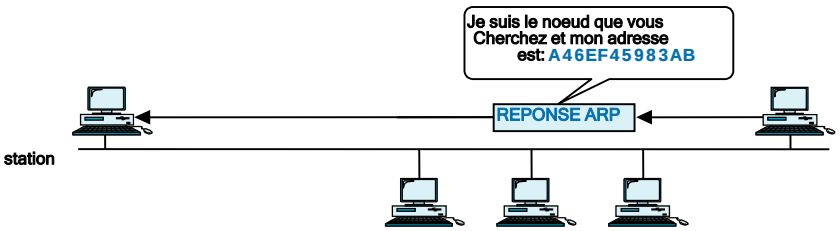
ICMP- Attaques

- Vulnérabilités logicielles
  - Ping-of-death
    - Paquet IP de plus de 65,535 octets.
- Inondation
  - Smurf Attack
    - Ping echo request à un réseau en personnifiant la victime. Cette victime reçoit une multitude de Ping echo reply.
- ICMP Destination Unreachable ou Time Exceeded malicious
  - La victime peut alors interrompre sa communication.
- ICMP Redirection
  - Un attaquant envoie à une machine un message ICMP-redirect pour lui indiquer un autre chemin à suivre (qui passe par lui)
  - Parade
    - Les paquets ICMP-redirect ne devraient pas être accepté par les serveurs, routeurs et poste utilisateurs

ARP-Rappel



(a) requête ARP



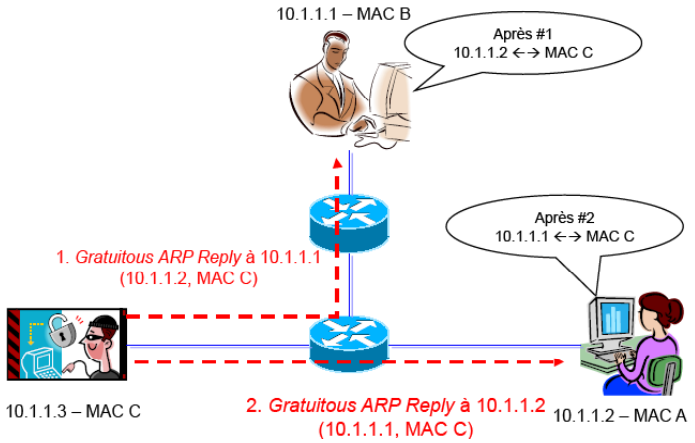
(b) Réponse ARP

ARP-Attaques

- ARP spoofing
  - Vulnérabilité:
    - Toute personne peut clamer être le propriétaire d'une adresse IP donnée (Gratuitous ARP Reply).
    - Selon le protocole, il est possible d'envoyer un ARP Reply sans sollicitation au préalable. ➔**Gratuitous ARP Reply**.
  - Attaque:
    - L'attaquant s'insère entre deux intervenants IP au niveau Ethernet ➔ Man-in-the-middle.
    - Pour l'intervenant A, l'attaquant possède l'adresse IP de B.
    - ➔ Gratuitous ARP Reply avec l'adresse MAC de l'attaquant et l'adresse IP de B.
    - Pour l'intervenant B, l'attaquant possède l'adresse IP de A.
    - ➔ Gratuitous ARP Reply avec l'adresse MAC de l'attaquant et l'adresse IP de A.
  - Risques:
    - Divulgation d'informations sensibles (p.ex. mots de passe)
  - Parade: Éviter de considérer les Gratuitous ARP Reply.

ARP-Attaques

- ARP spoofing



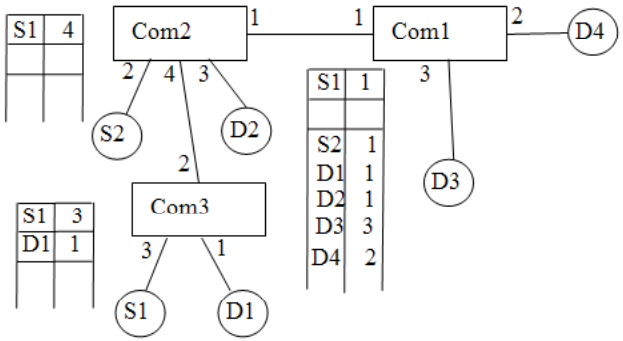
Les attaques réseaux

Les attaques niveau Liaison

Ethernet

Ethernet - Rappel

- Réseau composé de répéteurs (hubs) et de commutateurs (switches) liés en point à point
- Les hubs diffuse les trames.
- Les commutateur utilisent leurs tables de commutation pour diriger une trame vers un port spécifique s'il peut déterminer à quel sous réseau appartient le destinataire de la trame. Sinon, la trame est diffusé de façon générale.



Ethernet - Attaques

- Inondation de la table de commutation TC
- Mystification de l'adresse MAC (MAC spoofing)
- Manipulation de l'arbre sous-tendant (spanning tree)
- Manipulation du VLAN (VLAN hopping)

Inondation de la TC

- Vulnérabilité:
  - Lorsqu'une adresse MAC ne se retrouve pas dans la table TC, le commutateur diffuse la trame sur tous les ports.
- Attaque:
  - L'attaquant inonde le commutateur avec de fausses trames.
    - Le commutateur ajoute les pairs (MAC (source de la trame), Port) dans sa table TC. Lorsque cette table est pleine, il enlève des entrées.
    - Lorsqu'une entrée valide est enlevée, tout le trafic y étant associé est maintenant diffusé sur tous les ports.
    - Logiciel **macof** permet de créer des paquets avec des adresses MAC et IP aléatoires.
- Risque:
  - Divulgation d'informations sensibles (p.ex. mots de passe) qui ne devraient pas être envoyées sur un port.
    - Logiciel d'analyse de trafic Ethereal / Wireshark.

Inondation de la TC

- Parades:
  - Limiter le nombre d'adresses MAC permises sur un port donné.
  - Limiter la durée qu'une adresse sera assignée à un port.
    - Une fois pleine de fausses entrées, la table se videra d'elle-même.
  - Assigner des adresses MAC statiques à des ports.
    - Ces adresses ne seraient jamais enlevées si la table devenait pleine.
    - Les adresses des serveurs ou des équipements importants sont ainsi configurées dans le commutateur.
  - Authentification 802.1X
    - L'accès à un port n'est permis qu'après une authentification.

Mystification d'une adresse MAC

- Vulnérabilité:
  - Lorsqu'une adresse MAC (source) apparaît sur un autre port, le commutateur met à jour sa table TC.
- Attaque:
  - Inonder le commutateur avec de fausses trames ayant l'adresse MAC ciblée
    - Le commutateur ajoute cette nouvelle paire (MAC, Port) dans sa table TC et enlève celle qui était déjà là.
    - Concurrence critique avec l'ordinateur légitime.
  - Logiciel **macof** permet de créer de telles trames (paquets).
- Risque:
  - Dénis de service
  - Divulgation d'informations sensibles (p.ex. mots de passe) qui ne devraient pas être envoyées sur un port.

Mystification d'une adresse MAC

- Parades:
  - Assigner des adresses MAC statiques à des ports.
    - Ces adresses ne seront jamais enlevées.
    - Les adresses des serveurs ou des équipements importants sont ainsi configurées dans le commutateur.
  - Les adresses MAC sont obtenues lors de la requête DHCP.
    - Éviter d'utiliser une adresse IP avec une autre adresse MAC.
    - Fonctionnalité CISCO/Nortel.
  - Authentification 802.1X
    - L'accès à un port n'est permis qu'après une authentification.

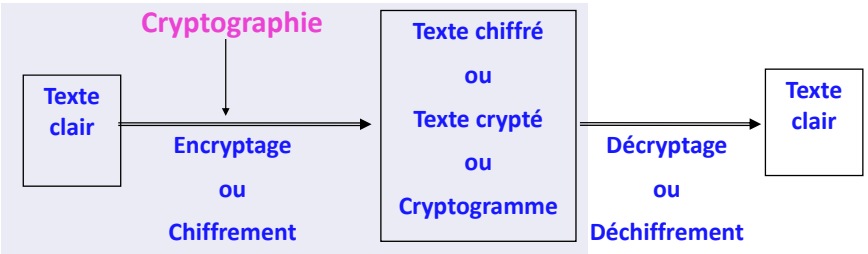
Partie 3:
Mécanismes cryptographique de la sécurité

Définitions

- Cryptologie (Cryptology) :
  - Science (branche des mathématiques) des communications secrètes.
  - Composée de deux domaines d'études complémentaires :
    - Cryptographie
    - Cryptanalyse.

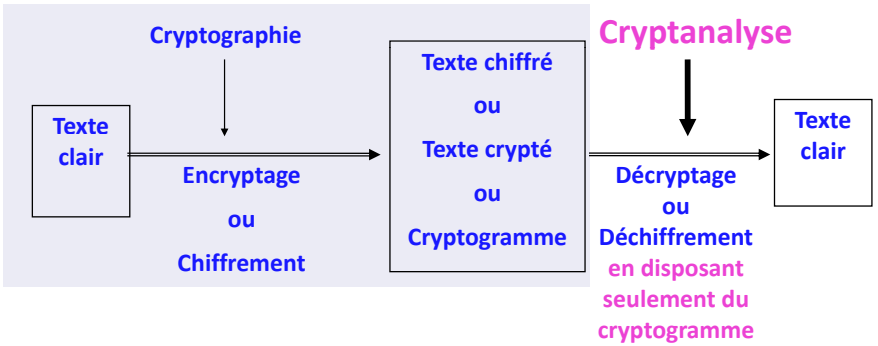
Définitions

- Cryptographie (cryptography) = Chiffrement=Encryptage
  - Ensemble des méthodes et techniques qui permettent de transformer un message afin de le rendre incompréhensible pour quiconque n'est pas doté du moyen de le déchiffrer.
    - On parle d'***encrypter*** (***chiffrer***) un message,
    - Le code résultant s'appelle ***cryptogramme***.
    - L'action inverse s'appelle ***décryptage*** (***déchiffrement***).



Définitions

- Cryptanalyse (cryptanalysis)
  - **Art de révéler les messages** qui ont fait l'objet d'un encryptage.
  - Lorsqu'on réussie, au moins une fois, à **déchiffrer un cryptogramme**, on dit que l'**algorithme** qui a servi à l'encrypter a été **cassé**.



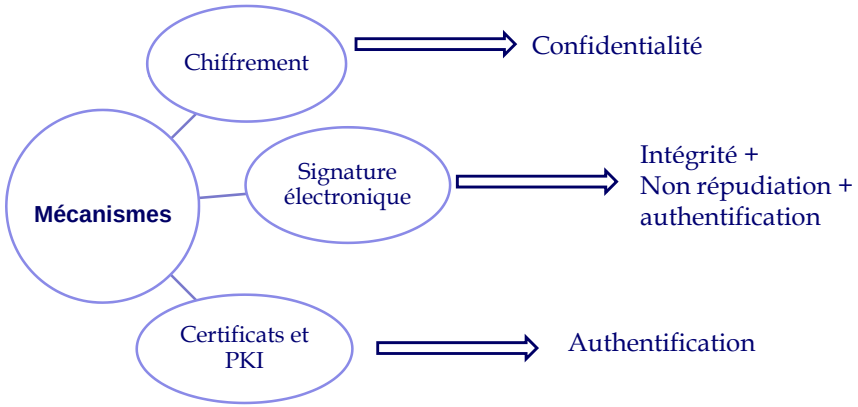
Définitions

- Clé :
  - Information qui sera utilisée pour encrypter et / ou décrypter un message.

  *On peut cependant concevoir un algorithme **qui n'utilise pas de clé**, dans ce cas c'est lui-même qui constitue le secret et son principe représente la clé*

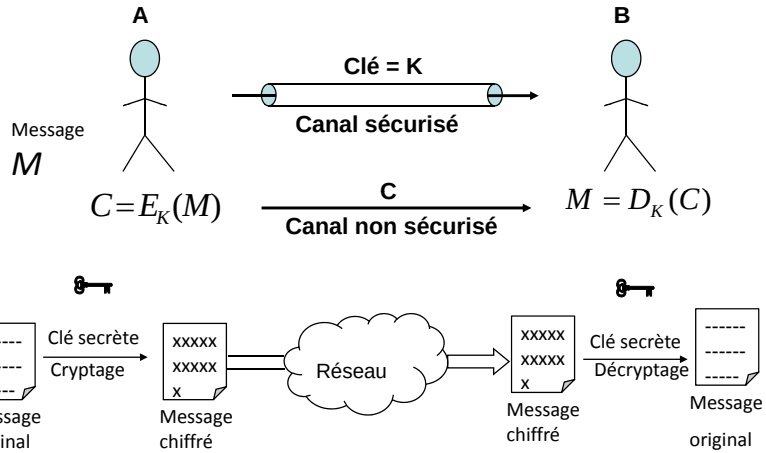
- Crypto système:
  - Ensemble composé d'un algorithme, de tous les textes en clair, de tous textes chiffrés et de toutes clés possibles.

Mécanismes cryptographiques de la sécurité



Chiffrement

- Chiffrement symétrique



- Exemples: ECB, CBC, DES, AES, IDEA…

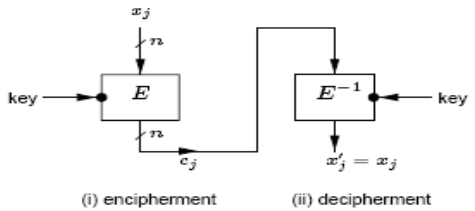
Chiffrement

- Cryptosystèmes symetriques modernes
  - Deux modes de chiffrement
    - En Stream
    - Par bloc
      - Segmentation du message M à chiffrer
        - M est scindé en un nombre de bloc de taille fixe
      - Cryptage des blocs
      - C est obtenu en concaténant les cryptogrammes des bloc
  - Modes de chiffrement par bloc
    - ECB (Electronic CodeBook)
    - CBC(Cipher bloc Chaining)
    - CBF (Cipher FeedBack)
    - OFB (Output FeedBack)

Chiffrement

- Mode ECB (Electronic CodeBook)
  - Un bloc de texte se chiffre indépendamment de tout en un bloc de texte chiffré

a) Electronic Codebook (ECB)



7.11 Algorithm ECB mode of operation

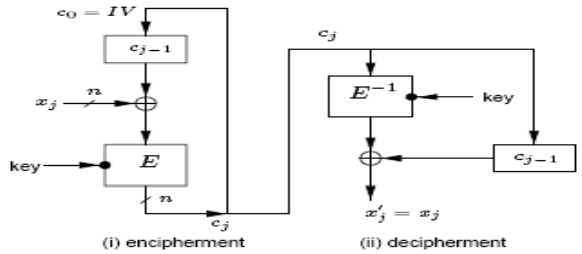
INPUT: k-bit key K; n-bit plaintext blocks $x_1, \ldots, x_t$.
SUMMARY: produce ciphertext blocks $c_1, \ldots, c_t$; decrypt to recover plaintext.

1. Encryption: for $1 \le j \le t$, $c_j \leftarrow E_K(x_j)$.
2. Decryption: for $1 \le j \le t$, $x_j \leftarrow E_K^{-1}(c_j)$.

Chiffrement

- Mode CBC (Cipher Block Chaining)
  - Chaque bloc du cryptogramme dépend du bloc de texte en clair et de tous les blocs précédents

b) Cipher-block Chaining (CBC)



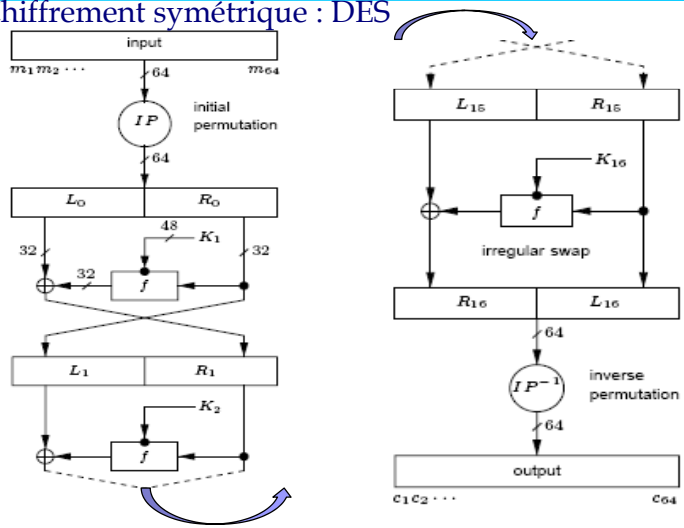
7.13 Algorithm CBC mode of operation

INPUT: k-bit key K; n-bit IV; n-bit plaintext blocks $x_1, \ldots, x_t$.
SUMMARY: produce ciphertext blocks $c_1, \ldots, c_t$; decrypt to recover plaintext.

1. Encryption: $c_0 \leftarrow IV$. For $1 \le j \le t$, $c_j \leftarrow E_K(c_{j-1} \oplus x_j)$.
2. Decryption: $c_0 \leftarrow IV$. For $1 \le j \le t$, $x_j \leftarrow c_{j-1} \oplus E_K^{-1}(c_j)$.

Chiffrement

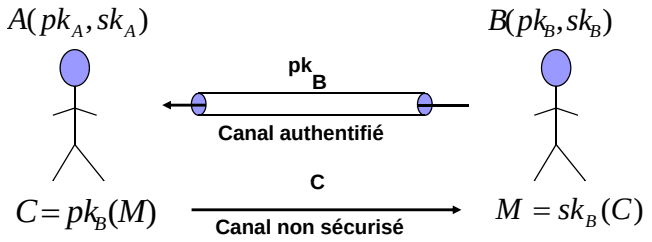
- Chiffrement symétrique : DES

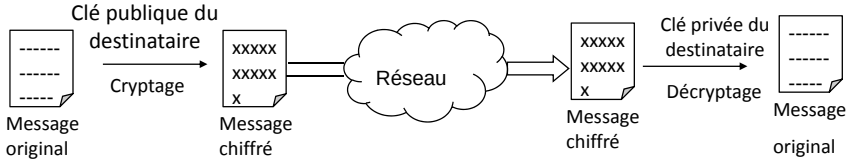


$L_i = R_{i-1}$;
$R_i = L_{i-1} \oplus f(R_{i-1}, K_i)$, where $f(R_{i-1}, K_i) = P(S(E(R_{i-1}) \oplus K_i))$

Chiffrement

- Chiffrement asymétrique





- Exemples: RSA, Rabin, Elgamal…

Cryptosystèmes asymétriques

public-key encryption scheme	computational problem
RSA	integer factorization problem (§3.2) RSA problem (§3.3)
Rabin	integer factorization problem (§3.2) square roots modulo composite n (§3.5.2)
ElGamal	discrete logarithm problem (§3.6) Diffie-Hellman problem (§3.7)
generalized ElGamal	generalized discrete logarithm problem (§3.6) generalized Diffie-Hellman problem (§3.7)
McEliece	linear code decoding problem
Merkle-Hellman knapsack	subset sum problem (§3.10)
Chor-Rivest knapsack	subset sum problem (§3.10)
Goldwasser-Micali probabilistic	quadratic residuosity problem (§3.4)
Blum-Goldwasser probabilistic	integer factorization problem (§3.2) Rabin problem (§3.9.3)

Chiffrement

- Chiffrement asymétrique: RSA

8.1 Algorithm Key generation for RSA public-key encryption

SUMMARY: each entity creates an RSA public key and a corresponding private key. Each entity A should do the following:

1. Generate two large random (and distinct) primes p and q, each roughly the same size.
2. Compute $n = pq$ and $\phi = (p-1)(q-1)$. (See Note 8.5.)
3. Select a random integer e, $1 < e < \phi$, such that $\gcd(e, \phi) = 1$.
4. Use the extended Euclidean algorithm (Algorithm 2.107) to compute the unique integer d, $1 < d < \phi$, such that $ed \equiv 1 \pmod{\phi}$.
5. A's public key is (n, e); A's private key is d.

Chiffrement

- Chiffrement asymétrique: RSA

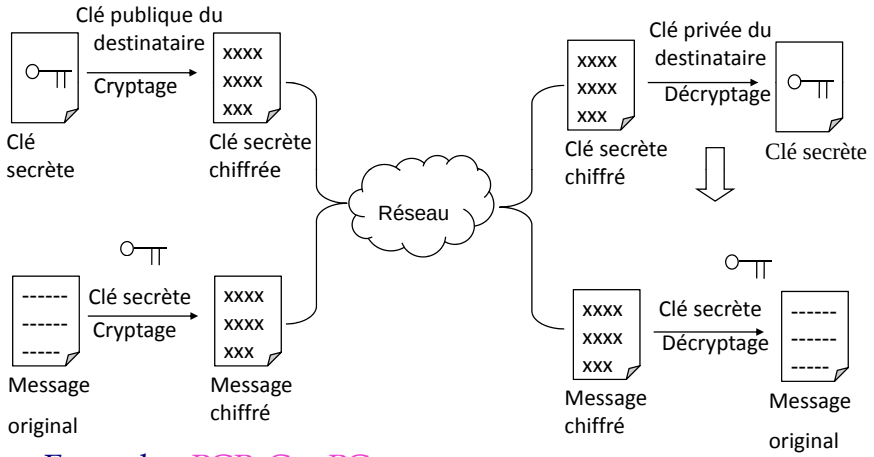
8.3 Algorithm RSA public-key encryption

SUMMARY: B encrypts a message m for A, which A decrypts.

1. *Encryption.* B should do the following:
   (a) Obtain A's authentic public key (n, e).
   (b) Represent the message as an integer m in the interval $[0, n-1]$.
   (c) Compute $c = m^e \bmod n$ (e.g., using Algorithm 2.143).
   (d) Send the ciphertext c to A.
2. *Decryption.* To recover plaintext m from c, A should do the following:
   (a) Use the private key d to recover $m = c^d \bmod n$.

Chiffrement

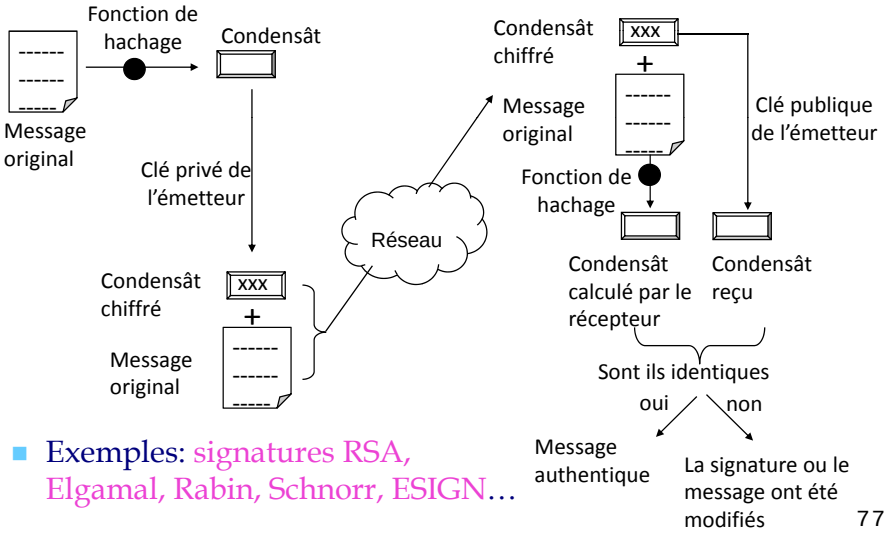
- Chiffrement hybride



- Exemples: PGP, GnuPG

Signature électronique

- Permet l'authentification, l'intégrité et la non répudiation



- Exemples: signatures RSA, Elgamal, Rabin, Schnorr, ESIGN…

Signature électronique

- Signature RSA

11.19 Algorithm RSA signature generation and verification

SUMMARY: entity A signs a message $m \in \mathcal{M}$. Any entity B can verify A's signature and recover the message m from the signature.

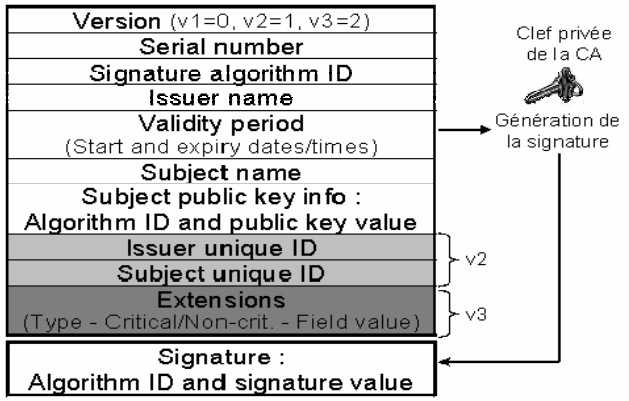
1. *Signature generation.* Entity A should do the following:
   (a) Compute $\bar{m} = R(m)$, an integer in the range $[0, n-1]$.
   (b) Compute $s = \bar{m}^d \bmod n$.
   (c) A's signature for m is s.
2. *Verification.* To verify A's signature s and recover the message m, B should:
   (a) Obtain A's authentic public key (n, e).
   (b) Compute $\bar{m} = s^e \bmod n$.
   (c) Verify that $\bar{m} \in \mathcal{M}_R$; if not, reject the signature.
   (d) Recover $m = R^{-1}(\bar{m})$.

Fonctions de hashage

- Fonction de hashage
  - H (M) = C
    - M est de taille quelconque
    - C est de taille fixe (16 ou 20 octets)
      - appelé condensât, ou empreinte, ou fingerprint, ou message digest
  - Fonction à sens unique
  - Si H (M_1) = C_1 ,
    - il est très difficile de trouver :
      M_2 différent de M_1 tel que H (M_2) = C_1
  - Usage : checksums, « intégrité »
- Exemples
  - MD5, SHA-1

Certificat numérique

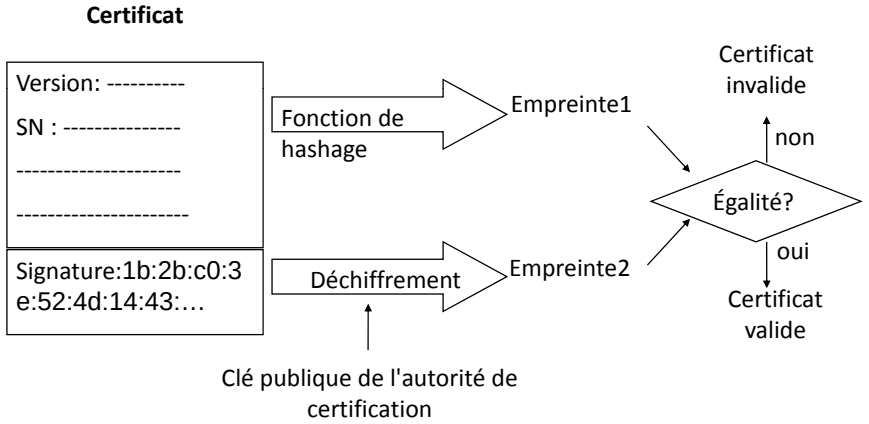
- Permet l'authentification
  - Garantit l'appartenance d'une clé publique à une entité
- Principal format: **certificats X.509**



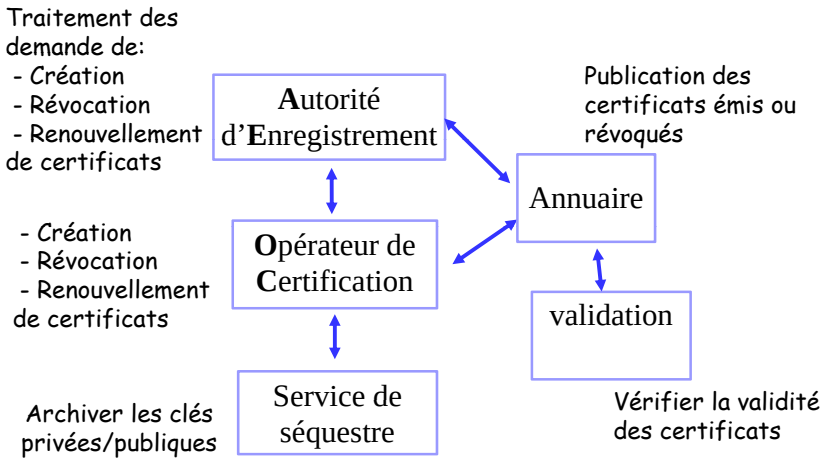
Certificat numérique

- *Serial number* :
  - Numéro de série du certificat (propre à chaque CA).
- *Signature Algorithm ID :*
  - Identifiant du type de signature utilisée.
- *Issuer Name :*
  - *Distinguished Name (DN)* de CA qui a émis ce certificat.
- *Subject Name :*
  - *Distinguished Name (DN)* du détenteur de la clé publique.
- *Subject public key info :*
  - Informations sur la clé publique du certificat.
- *Signature :*
  - Signature numérique du CA sur l'ensemble des champs

Vérification d'un certificat

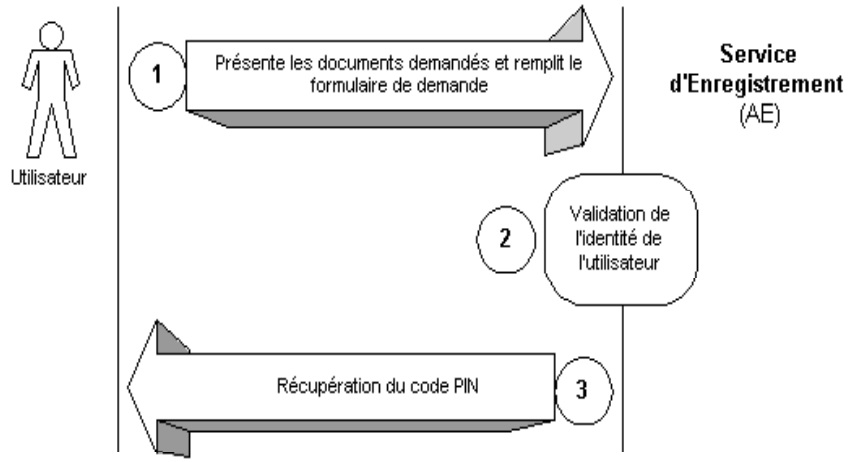


PKI: Public Key Infrastructure



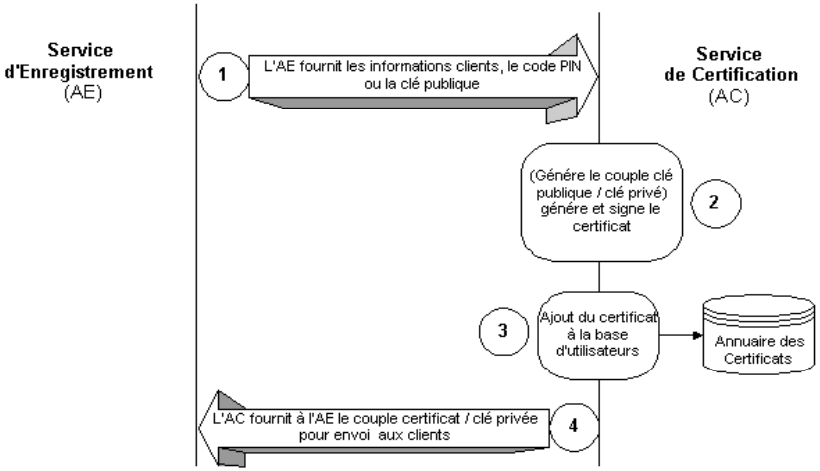
PKI: Exemple de fonctionnement

- Enregistrement

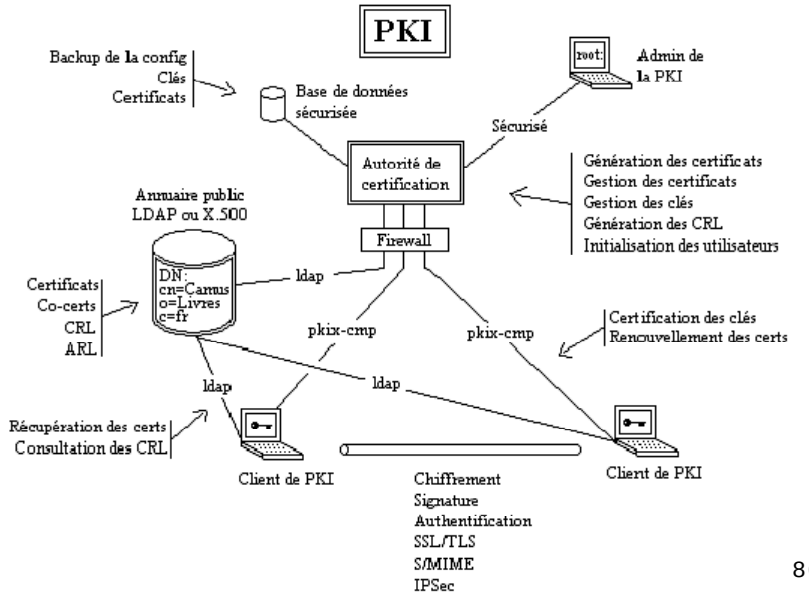


PKI: Exemple de fonctionnement

- Création de certificats



PKI: Fonctionnement



Annexe

Détail du DES

Data Encryption Standard (DES)

- Généralités:
  - Chiffrement **par bloc** : 64bits
  - Clé de taille variable:
    - Entre 56 et 128 bits selon le niveau de sécurité désiré
    - Version initiale du DES utilise une clé de taille 64 bits dont 56 sont réellement utilisés
  - Utilise un **chiffrement produit**
    - Combine des algorithmes de **substitution** et des algorithmes de **transposition** → maximiser la complexité de l'algorithme

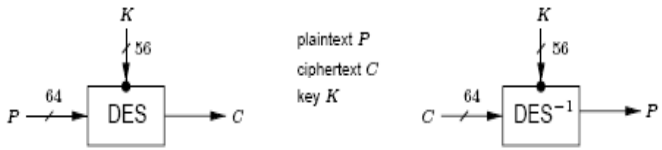
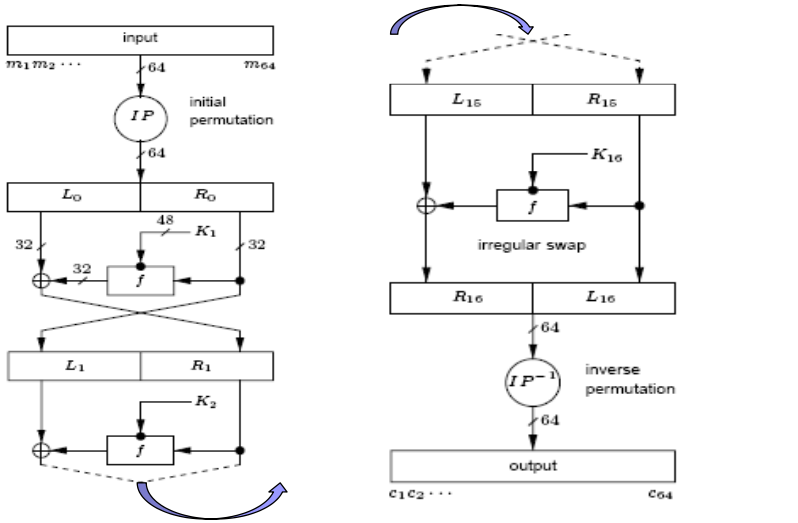


Figure 7.8: DES input-output.

Etapes du chiffrement DES



$$L_i = R_{i-1};$$
$$R_i = L_{i-1} \oplus f(R_{i-1}, K_i), \text{ where } f(R_{i-1}, K_i) = P(S(E(R_{i-1}) \oplus K_i))$$

DES: IP et IP-1 (inverse de IP)

IP							
58	50	42	34	26	18	10	2
60	52	44	36	28	20	12	4
62	54	46	38	30	22	14	6
64	56	48	40	32	24	16	8
57	49	41	33	25	17	9	1
59	51	43	35	27	19	11	3
61	53	45	37	29	21	13	5
63	55	47	39	31	23	15	7

IP^{-1}							
40	8	48	16	56	24	64	32
39	7	47	15	55	23	63	31
38	6	46	14	54	22	62	30
37	5	45	13	53	21	61	29
36	4	44	12	52	20	60	28
35	3	43	11	51	19	59	27
34	2	42	10	50	18	58	26
33	1	41	9	49	17	57	25

Table 7.2: DES initial permutation and inverse (IP and IP^{-1}).

Etapes du chiffrement DES

- E: Expansion
  - Permutation avec expansion: entrée 32bits ➔ sortie 48 bits
- S: substitution
  - 8 substitutions (S_1, S_2,S_3,S_4,S_5,S_6) 6to4 bits
- P: permutation fixe de 32 bits

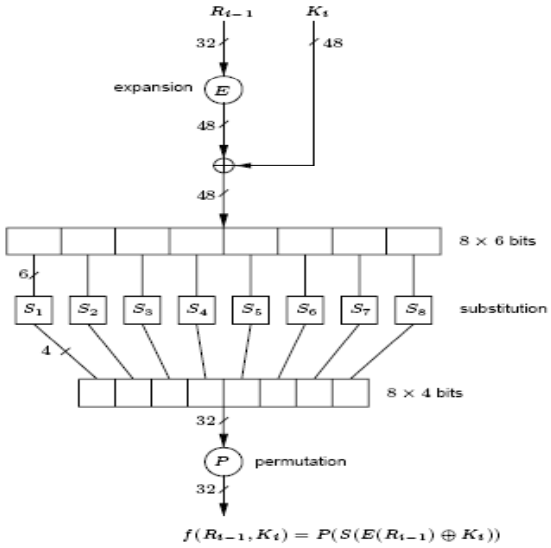


Figure 7.10: DES inner function f.

DES: Expansion (E), Permutation (P)

Expand $R_{i-1} = r_1 r_2 \ldots r_{32}$ from 32 to 48 bits using E per Table 7.3: $T \leftarrow E(R_{i-1})$. (Thus $T = r_{32} r_1 r_2 \ldots r_{32} r_1$.)

E					
32	1	2	3	4	5
4	5	6	7	8	9
8	9	10	11	12	13
12	13	14	15	16	17
16	17	18	19	20	21
20	21	22	23	24	25
24	25	26	27	28	29
28	29	30	31	32	1

P			
16	7	20	21
29	12	28	17
1	15	23	26
5	18	31	10
2	8	24	14
32	27	3	9
19	13	30	6
22	11	4	25

Table 7.3: DES per-round functions: expansion E and permutation P.

$$L_i = R_{i-1};$$
$$R_i = L_{i-1} \oplus f(R_{i-1}, K_i), \text{ where } f(R_{i-1}, K_i) = P(S(E(R_{i-1}) \oplus K_i))$$

DES: Substitutions (S)

(c) $T'' \leftarrow (S_1(B_1), S_2(B_2), \ldots S_8(B_8))$. (Here $S_i(B_i)$ maps $B_i = b_1 b_2 \ldots b_6$ to the 4-bit entry in row r and column c of S_i in Table 7.8, page 260 where $r = 2 \cdot b_1 + b_6$, and $b_2 b_3 b_4 b_5$ is the radix-2 representation of $0 \leq c \leq 15$. Thus $S_1(011011)$ yields $r = 1, c = 13$, and output 5, i.e., binary 0101.)

$$L_i = R_{i-1};$$
$$R_i = L_{i-1} \oplus f(R_{i-1}, K_i), \text{ where } f(R_{i-1}, K_i) = P(S(E(R_{i-1}) \oplus K_i))$$

DES: S-boxes (substitutions)

row	column number															
	[0]	[1]	[2]	[3]	[4]	[5]	[6]	[7]	[8]	[9]	[10]	[11]	[12]	[13]	[14]	[15]
S_1																
[0]	14	4	13	1	2	15	11	8	3	10	6	12	5	9	0	7
[1]	0	15	7	4	14	2	13	1	10	6	12	11	9	5	3	8
[2]	4	1	14	8	13	6	2	11	15	12	9	7	3	10	5	0
[3]	15	12	8	2	4	9	1	7	5	11	3	14	10	0	6	13
S_2																
[0]	15	1	8	14	6	11	3	4	9	7	2	13	12	0	5	10
[1]	3	13	4	7	15	2	8	14	12	0	1	10	6	9	11	5
[2]	0	14	7	11	10	4	13	1	5	8	12	6	9	3	2	15
[3]	13	8	10	1	3	15	4	2	11	6	7	12	0	5	14	9
S_3																
[0]	10	0	9	14	6	3	15	5	1	13	12	7	11	4	2	8
[1]	13	7	0	9	3	4	6	10	2	8	5	14	12	11	15	1
[2]	13	6	4	9	8	15	3	0	11	1	2	12	5	10	14	7
[3]	1	10	13	0	6	9	8	7	4	15	14	3	11	5	2	12
S_4																
[0]	7	13	14	3	0	6	9	10	1	2	8	5	11	12	4	15
[1]	13	8	11	5	6	15	0	3	4	7	2	12	1	10	14	9
[2]	10	6	9	0	12	11	7	13	15	1	3	14	5	2	8	4
[3]	3	15	0	6	10	1	13	8	9	4	5	11	12	7	2	14

DES: S-boxes (substitutions)

S_5																
[0]	2	12	4	1	7	10	11	6	8	5	3	15	13	0	14	9
[1]	14	11	2	12	4	7	13	1	5	0	15	10	3	9	8	6
[2]	4	2	1	11	10	13	7	8	15	9	12	5	6	3	0	14
[3]	11	8	12	7	1	14	2	13	6	15	0	9	10	4	5	3
S_6																
[0]	12	1	10	15	9	2	6	8	0	13	3	4	14	7	5	11
[1]	10	15	4	2	7	12	9	5	6	1	13	14	0	11	3	8
[2]	9	14	15	5	2	8	12	3	7	0	4	10	1	13	11	6
[3]	4	3	2	12	9	5	15	10	11	14	1	7	6	0	8	13
S_7																
[0]	4	11	2	14	15	0	8	13	3	12	9	7	5	10	6	1
[1]	13	0	11	7	4	9	1	10	14	3	5	12	2	15	8	6
[2]	1	4	11	13	12	3	7	14	10	15	6	8	0	5	9	2
[3]	6	11	13	8	1	4	10	7	9	5	0	15	14	2	3	12
S_8																
[0]	13	2	8	4	6	15	11	1	10	9	3	14	5	0	12	7
[1]	1	15	13	8	10	3	7	4	12	5	6	11	0	14	9	2
[2]	7	11	4	1	9	12	14	2	0	6	10	13	15	3	5	8
[3]	2	1	14	7	4	10	8	13	15	12	9	0	3	5	6	11

Table 7.8: DES S-boxes.

DES: calcul des sous clés

7.83 Algorithm DES key schedule

INPUT: 64-bit key $K = k_1 \ldots k_{64}$ (including 8 odd-parity bits).
OUTPUT: sixteen 48-bit keys K_i, $1 \leq i \leq 16$.

1. Define v_i, $1 \leq i \leq 16$ as follows: $v_i = 1$ for $i \in \{1, 2, 9, 16\}$; $v_i = 2$ otherwise. (These are left-shift values for 28-bit circular rotations below.)
2. $T \leftarrow \text{PC1}(K)$; represent T as 28-bit halves (C_0, D_0). (Use PC1 in Table 7.4 to select bits from K: $C_0 = k_{57} k_{49} \ldots k_{36}$, $D_0 = k_{63} k_{55} \ldots k_4$.)
3. For i from 1 to 16, compute K_i as follows: $C_i \leftarrow (C_{i-1} \hookleftarrow v_i)$, $D_i \leftarrow (D_{i-1} \hookleftarrow v_i)$, $K_i \leftarrow \text{PC2}(C_i, D_i)$. (Use PC2 in Table 7.4 to select 48 bits from the concatenation $b_1 b_2 \ldots b_{56}$ of C_i and D_i: $K_i = b_{14} b_{17} \ldots b_{32}$. '$\hookleftarrow$' denotes left circular shift.)

PC1						
57	49	41	33	25	17	9
1	58	50	42	34	26	18
10	2	59	51	43	35	27
19	11	3	60	52	44	36
above for C_i; below for D_i						
63	55	47	39	31	23	15
7	62	54	46	38	30	22
14	6	61	53	45	37	29
21	13	5	28	20	12	4

PC2					
14	17	11	24	1	5
3	28	15	6	21	10
23	19	12	4	26	8
16	7	27	20	13	2
41	52	31	37	47	55
30	40	51	45	33	48
44	49	39	56	34	53
46	42	50	36	29	32

Table 7.4: DES key schedule bit selections (PC1 and PC2).

DES: Algorithme

Algorithm Data Encryption Standard (DES)

INPUT: plaintext $m_1 \dots m_{64}$; 64-bit key $K = k_1 \dots k_{64}$ (includes 8 parity bits).
OUTPUT: 64-bit ciphertext block $C = c_1 \dots c_{64}$. (For decryption, see Note 7.84.)

1. (key schedule) Compute sixteen 48-bit round keys K_i from K using Algorithm 7.83.
2. $(L_0, R_0) \leftarrow \text{IP}(m_1 m_2 \dots m_{64})$. (Use IP from Table 7.2 to permute bits; split the result into left and right 32-bit halves $L_0 = m_{58} m_{50} \dots m_8$, $R_0 = m_{57} m_{49} \dots m_7$.)
3. (16 rounds) for i from 1 to 16, compute L_i and R_i using Equations (7.4) and (7.5) above, computing $f(R_{i-1}, K_i) = P(S(E(R_{i-1}) \oplus K_i))$ as follows:
   (a) Expand $R_{i-1} = r_1 r_2 \dots r_{32}$ from 32 to 48 bits using E per Table 7.3: $T \leftarrow E(R_{i-1})$. (Thus $T = r_{32} r_1 r_2 \dots r_{32} r_1$.)
   (b) $T' \leftarrow T \oplus K_i$. Represent T' as eight 6-bit character strings: $(B_1, \dots, B_8) = T'$.
   (c) $T'' \leftarrow (S_1(B_1), S_2(B_2), \dots S_8(B_8))$. (Here $S_i(B_i)$ maps $B_i = b_1 b_2 \dots b_6$ to the 4-bit entry in row r and column c of S_i in Table 7.8, page 260 where $r = 2 \cdot b_1 + b_6$, and $b_2 b_3 b_4 b_5$ is the radix-2 representation of $0 \le c \le 15$. Thus $S_1(011011)$ yields $r = 1$, $c = 13$, and output 5, i.e., binary 0101.)
   (d) $T''' \leftarrow P(T'')$. (Use P per Table 7.3 to permute the 32 bits of $T'' = t_1 t_2 \dots t_{32}$, yielding $t_{16} t_7 \dots t_{25}$.)
4. $b_1 b_2 \dots b_{64} \leftarrow (R_{16}, L_{16})$. (Exchange final blocks L_{16}, R_{16}.)
5. $C \leftarrow \text{IP}^{-1}(b_1 b_2 \dots b_{64})$. (Transpose using IP^{-1} from Table 7.2; $C = b_{40} b_8 \dots b_{25}$.)

DES: calcul des sous clés

- Exemple:
  - Pour mieux voir les permutations, considérons des chaines de caractères au lieu des bits. Les bits de parité sont représenté par des 0.

abcdefg0hijklmn0opqrstu0vwxyzAB0CDEFGHI0JKLMNOP0QRSTUVW0 XYZ12340

  - Après la permutation PC1, on obtient C_0 et D_0 suivants

C_0							D_0						
X	Q	J	C	v	o	h	4	W	P	I	B	u	n
a	Y	R	K	D	w	p	G	3	V	O	H	A	t
i	b	Z	S	L	E	x	m	f	2	U	N	G	z
q	j	e	1	T	M	F	s	l	e	y	r	k	d

DES: calcul des sous clés

- Après la permutation CP1, on obtient C_0 et D_0 suivants

C_0							D_0						
X	Q	J	C	v	o	h	4	W	P	I	B	u	n
a	Y	R	K	D	w	p	G	3	V	O	H	A	t
i	b	Z	S	L	E	x	m	f	2	U	N	G	z
q	j	e	1	T	M	F	s	l	e	y	r	k	d

- La première clé K1 =PC2(C_1 , D_1)= iSDlQoCXbhqKcEwvMYZaFxpJtyIVGdPAeUuz2sH4nrNml3Wb

i	S	D	l	Q	o
C	X	b	h	q	K
c	E	w	v	M	Y
Z	a	F	x	p	J
t	y	I	V	G	d
P	A	e	U	u	z
2	s	H	4	n	r
N	m	l	3	W	b

PC2					
14	17	11	24	1	5
3	28	15	6	21	10
23	19	12	4	26	8
16	7	27	20	13	2
41	52	31	37	47	55
30	40	51	45	33	48
44	49	39	56	34	53
46	42	50	36	29	32

DES: calcul des sous clés

- La première clé K1 =PC2(C_1 , D_1)= iSDlQoCXbhqKcEwvMYZaFxpJtyIVGdPAeUuz2sH4nrNml3Wb

➔ Les caractères R, L, j, T, g, O, f et k n'apparaissent pas dans K1

- La deuxième clés K2 sera:

K2 = bLwTJhvQZajD1xpoFRSYXqiCmrBOz4ItyNnsUIAWgkGfePu

➔ Les caractères absents dans K1 sont maintenant présents dans K2

Particularités du DES:

- Souplesse d'implémentation:
  - ECB ou CBC (en modifiant la phase de pré traitement des blocs de données)
  - Différentes implémentation en modifiants les fonction d'expansion ou de sélection

- Faiblesses
  - Conservation de la taille ➔ sensible aux attaques d'analyse de flux: on peut connaitre la taille exacte de chaque message
  - La clé est réduite à 56 bits ➔ réduit la sécurité de l'algorithme
  - Avec une clé de taille 128 bits ➔ algorithme couteux en temps
  - Peut être cassé par les processeurs actuels (exhaustive key search)
  - ➔ Triple DES (trois clés différentes)
  - ➔ AES : remplaçant du DES