Chiffrement à clef partagée et confidentialité

Chiffrement à clef partagée et confidentialité

- Principes de chiffrement traditionnel
  - Chiffrement symétrique
- Algorithmes de chiffrement
  - DES
  - Le chiffrement chaîné
- Localisation des équipements de chiffrement
- Distribution des clefs

Principes de chiffrement

- Un chiffrement manipule:
  - Le message original
  - L'algorithme de chiffrement
  - La clef secrète (partagée)
  - Le message chiffré
  - L'algorithme de déchiffrement
- La sécurité dépend du secret de la clef, pas du secret des algorithmes
- Association de sécurité (SA):
  - Permet la négociation ou l'échange du contexte de la SA
  - L'ensemble des paramètres nécessaires, notamment au chiffrement ou au déchiffrement, mais aussi à la mise en oeuvre des autres mécanismes de sécurité

Principe du chiffrement
(clef partagée)

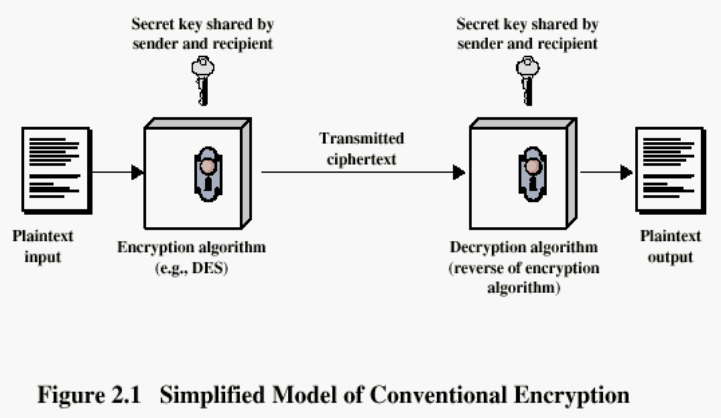


Figure 2.1 Simplified Model of Conventional Encryption

Temps moyen nécessaire pour une recherche exhaustive de clefs

Key Size (bits)	Number of Alternative Keys	Time required at 10^6 Decryption/μs
32	$2^{32} = 4.3 \times 10^9$	2.15 milliseconds
56	$2^{56} = 7.2 \times 10^{16}$	10 hours
128	$2^{128} = 3.4 \times 10^{38}$	5.4×10^{18} years
168	$2^{168} = 3.7 \times 10^{50}$	5.9×10^{30} years

Chiffrement

- Classification suivant 3 dimensions indépendantes :
  - Le type d'opérations utilisées pour chiffrer les éléments du message :
    - Substitution,
    - Transposition.
  - Le nombre de clefs utilisées :
    - Une seule : chiffrement symétrique ou partagée,
    - Deux : chiffrement asymétrique ou à clef publique.
  - L'organisation du traitement du chiffrement :
    - Par bloc,
    - En continu.

Cryptanalyse

- Cryptanalyse : analyse d'un système cryptographique pour en découvrir les secrets, les messages codés (décryptage).

Les niveaux d'attaques contre les messages chiffrés

- On dispose de l'algorithme, toujours.
- Avec le message chiffré seulement ("cyphertext only")
- + le message initial ("known plaintext"")
- + un message choisi et son chiffrement ("chosen plaintext")
- + le message chiffré choisi et son message initial associé ("chosen ciphertext")
- "Chosen text = chosen plaintext + chose ciphertext"

Feistel Cipher Structure

- Principes suivis par tous les algorithmes de chiffrement par bloc (y compris DES) [Horst Feistel of IBM in 1973]
- Un réseau de Feistel Network dépend de nombreux paramètres (voir transparent suivant)
- La valeur des paramètres est un compromis entre :
  - L'accroissement de la sécurité
  - Et celui des performances

Feistel Cipher Structure

- **Block size:** généralement 64 bits,
- **Key Size:** 128 bits est réputé suffisant
- **Number of rounds:** typiquement 16 tours
- **Subkey generation algorithm:** une grande complexité renforce la sécurité
- **Fast software encryption/decryption:** déterminant pour les performances

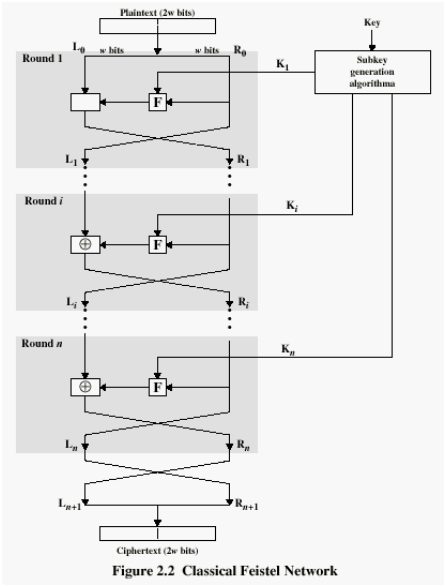


Figure 2.2 Classical Feistel Network

Algorithmes de chiffrement traditionnels

- Data Encryption Standard (DES)
  - Très utilisé
  - Son algorithme est appellé ''Data Encryption Algorithm (DEA)''
  - Chiffrement par bloc basé sur Feistel
  - En bloc de 64 bits
  - Une clef de 56 bits

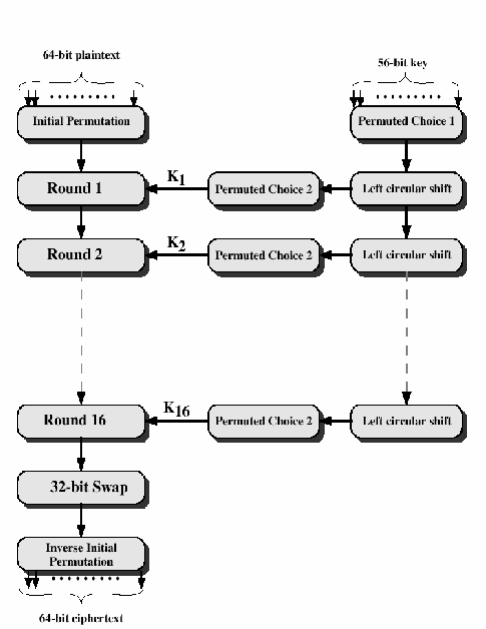


Figure 2.3 General Depiction of DES Encryption Algorithm

13

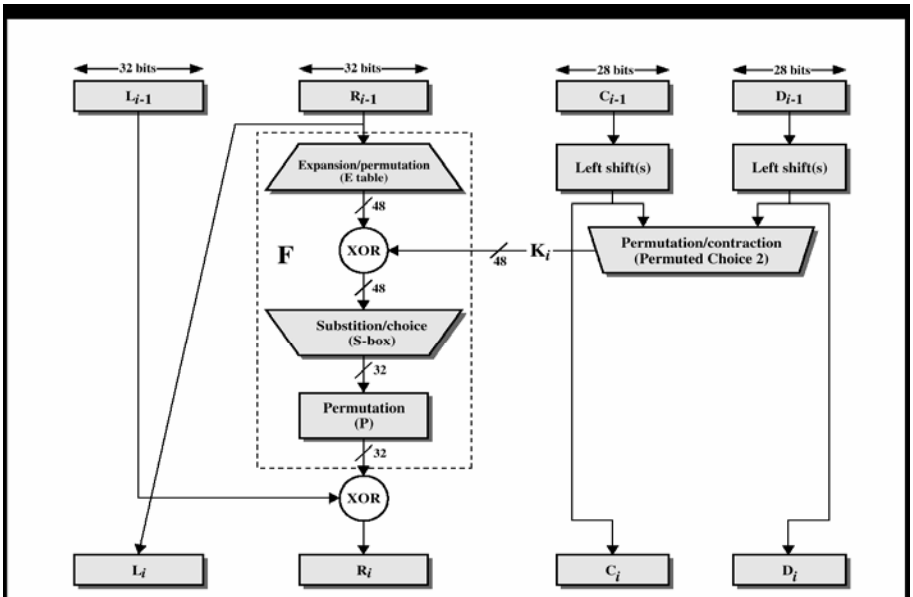


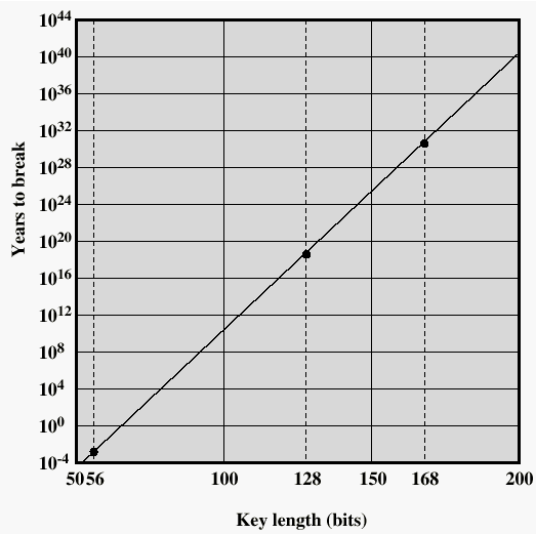
Figure 2.4 Single Round of DES Algorithm

DES

- **Traitement à chaque itération:**
  - $L_i = R_{i-1}$
  - $R_i = L_{i-1} \otimes F(R_{i-1}, K_i)$
- Préoccupation au niveau de la sécurité :
  - En juillet 1998, Electronic Frontier Foundation a construit une machine spéciale pour $250.000 et réussi une attaque qui pris seulement 3 jours.

Durée de la cryptanalyse

(10^6 déchiffrement/μs)



3DES

- Utilisation d'une clef de 128 bits
- Réutiliser l'algorithme du DES
- 3 clefs et 3 exécutions du DES (encrypt-decrypt-encrypt) :

$$C = E_{K3}[D_{K2}[E_{K1}[P]]]$$

  - C = ciphertext
  - P = plaintext
  - $E_K[X]$ = encryption of X using key K
  - $D_K[Y]$ = decryption of Y using key K

Compatibilité entre DES et 3DES

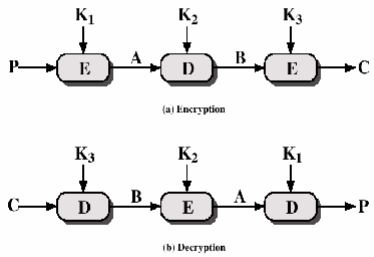


Figure 2.6 Triple DEA

Les modes opératoires de DES

- Le texte initial est formé de plusieurs blocs
  - Comment sont enchaînés les blocs du texte
- 4 modes :
  - Electronic CodeBook :
    - chiffrement par blocs individuels
    - (Une même entrée fournie toujours une même sortie)
  - Cipher Block Chaining :
    - Le bloc chiffré est obtenu en chiffrant le résultat du ou-exclusif entre le bloc non-chiffré initial et bloc chiffré précédent
  - Cipher FeedBack
    - Le bloc chiffré est obtenu en chiffrant le bloc chiffré précédent puis en effectuant un ou-exclusif du résultat avec le bloc non-chiffré initial
  - Output FeedBack
    - Le bloc chiffré est obtenu en chiffrant la sortie du chiffrement (avant le ou-exclusif) précédent puis en effectuant un ou-exclusif avec le bloc non-chiffré initial
    - Ils utilisent tous un "Initialization vector"
      - Connu du codeur et du décodeur pour amorcer le processus de chiffrement
      - N'a pas besoin d'être secret mais doit ne pas être réemployé

Chiffrement chainé

- La technique de chiffrement par bloc souffre d'une faiblesse:
  - 2 blocs d'un même flux sont codés de manière identique ("birthday attack")
- Le mode "Cipher Block Chaining" (CBC)
  - L'entrée fournie à l'algo. est produit par le XOR du bloc à chiffrer et le bloc chiffré précédent.
  - Initialization Vector (IV) : pour le premier bloc, doit être connu de tous les partenaires

$$C_i = E_k[C_{i-1} \oplus P_i]$$

$$D_K[C_i] = D_K[E_K(C_{i-1} \oplus P_i)]$$

$$D_K[C_i] = (C_{i-1} \oplus P_i)$$

$$C_{i-1} \oplus D_K[C_i] = C_{i-1} \oplus C_{i-1} \oplus P_i = P_i$$

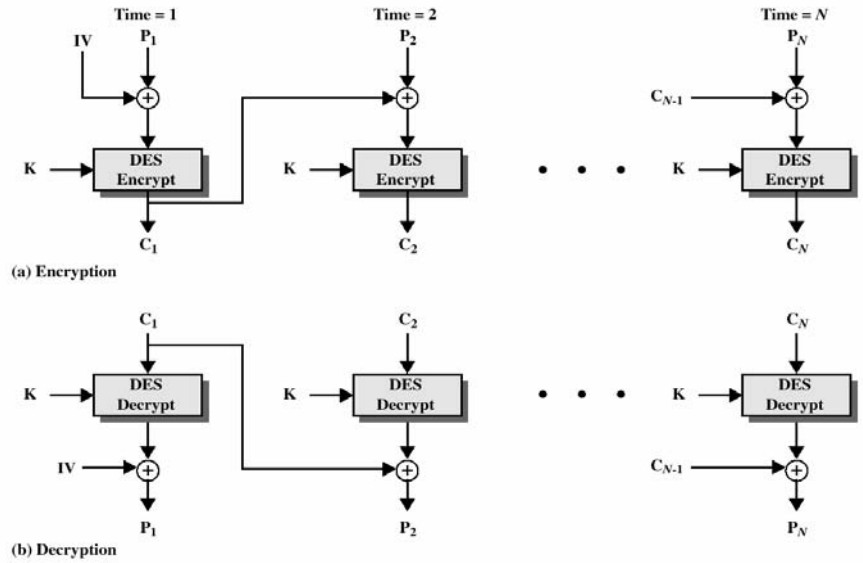


Figure 2.7 Cipher Block Chaining (CBC) Mode

Autres algorithmes de chiffrement traditionnels

- **International Data Encryption Algorithm (IDEA)**
  - Clef de 128 bits, bloc de 64 bits, 8 tours
  - Utilisé par PGP
- **Blowfish**
  - Clef de longueur variable jusqu'à 448 bits, bloc de 64 bits, 16 tours
  - Facile à implémenter, algorithme simple et efficace, code de taille réduite (5 Ko)
- **Advanced Encryption Standard (EAS)**
  - Clef de 128 bits; Bloc de 128, 192 ou 256 bits; Nombre de tours 10, 12 ou 14
  - Remplacant de DES et 3DES

Autres algorithmes de chiffrement traditionnel

- **RC5**
  - Proposé par Ronald Rivest en 1995
  - Clef de longueur variable jusqu'à 2048 bits, bloc de 64 bits, nombre de tours variable jusqu'à 255
  - Paramètres adaptables à l'application
  - Proposé par l'IETF
- **Cast-128**
  - Clef de 40 à 128 bits
  - La fonction de calcul diffère à chaque tour

Localisation des équipements de chiffrement

- **Chiffrement du lien:**
  - Nécessite beaucoup d'équipements de chiffrement
  - À la charge du réseau
  - Déchiffremnent/Chiffrement à chaque routeur
- **Chiffrement d'extrémité**
  - Le chiffrement peut être délégué à un serveur de chiffremment (serveur de sécurité) ou aux équipements terminaux
    - Seule la charge utile est chiffrée, l'entête (information de routage) est visible
    - Chiffrement au niveau Réseau : IPsec
    - Chiffrement au niveau Transport : TLS/SSL
    - Chiffrement applicatif
- Tous les types d'équipements sont nécessaires

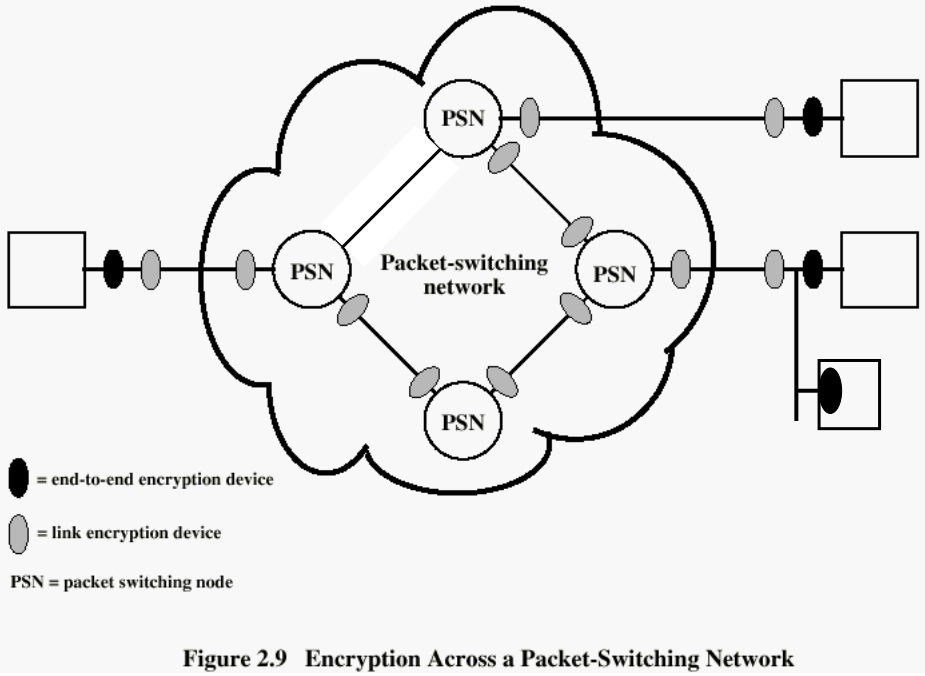


Figure 2.9 Encryption Across a Packet-Switching Network

La distribution des clefs

La même clef (chiffrement symétrique) doit être utilisée par les partenaires.

La sécurité du système repose sur le secret entourant la clef.

Donc il faut échanger de manière secrète les clefs :

1. Une clef peut être choisie par un partenaire et transmis physiquement et confidentiellement à l'autre.
2. Un tiers peut choisir la clef et la transmettre aux partenaires
   - les partenaires doivent avoir une connexion sécurisée avec le tiers.
   - (Voir transparent suivant)
3. S'ils partagent une clef, la nouvelle clef peut être transmises de l'un à l'autre de manière sécurisée en utilisant la première clef.
4. Utilisation du système de chiffrement Diffie-Hellman ou un dérivée

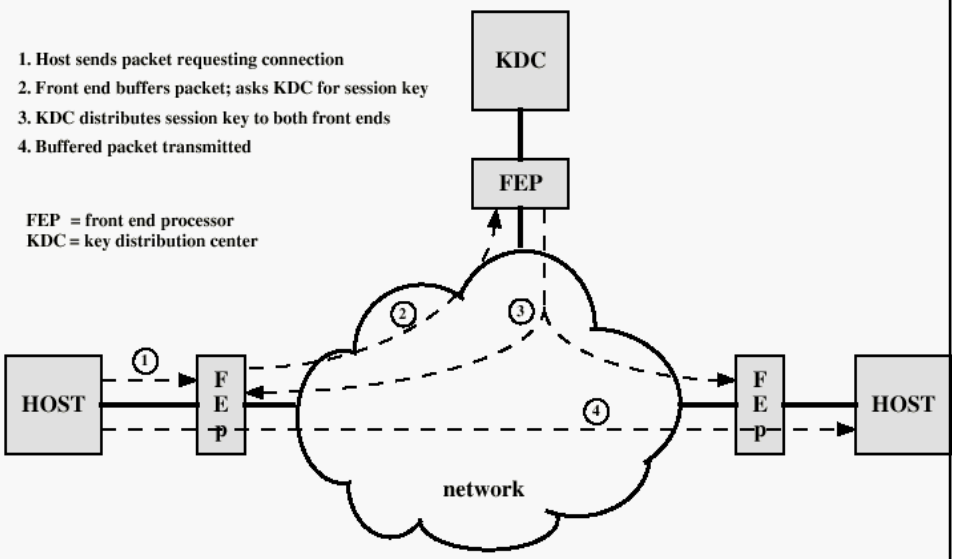


Figure 2.10 Automatic Key Distribution for Connection-Oriented Protocol

La résistance au facteur d'échelle de la distribution

- **Clef de Session :**
  - Les données sont chiffrées avec la clef de session. À la fin de la session la clef de session est détruite.
- **Clef permanente:**
  - Clef utilisée entre un couple de partenaires dans le but de distribuer des clefs de session.
- Principe repris par exemple dans Kerberos pour les certificats ("ticket"):
  - Authentication Server, <ticket-granting ticket> Ticket-granting Server,<service-granting ticket>, Server