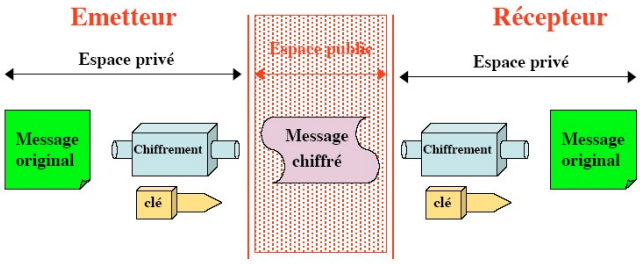
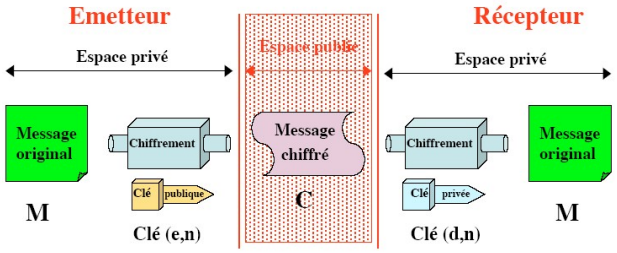
MISTRE : Eléments de CRYPTOGRAPHIE



✓**La même clé est utilisée pour chiffrer et déchiffrer**
✓**Problème : TRANSFERT de la clé**

Figure 1 : Chiffrement : type symétrique (clé privée)



✓**Le chiffrement est effectué avec la clé publique**
✓**Garantie : que « SEUL » le détenteur de la clé privée peut lire le message**

Figure 2 : Chiffrement : type asymétrique (clé publique)

- Soit un alphabet {A, B, C, D}

texte t / clé k	A B C D
A	C D B A
B	D C A B
C	C A B D
D	B D A C

Texte clair : ABCBACCBA ACBB
Clé : DBBCBAACD DBBC

Texte crypté : BCAADBBAB BACA

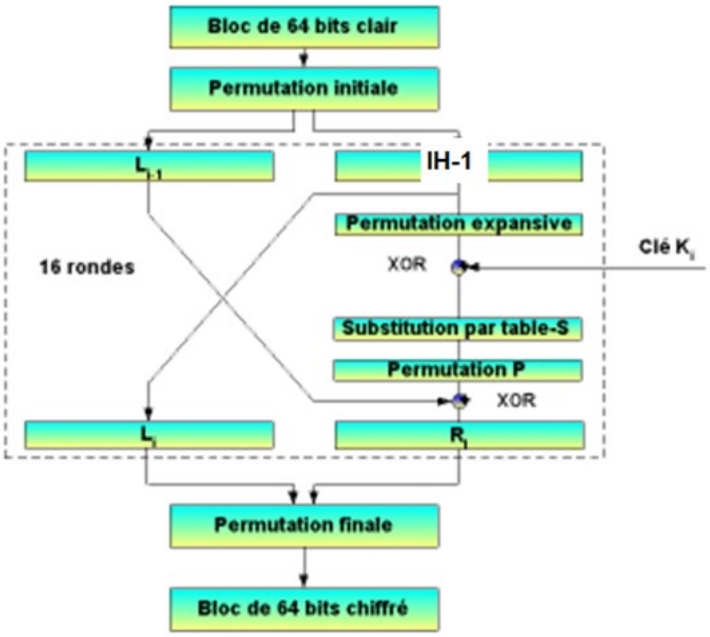
- Nécessite des clés de très grande taille pour être peu vulnérable…

Figure 3 : Exemples de codage : les codes poly-alphabétiques

- (b_n) = (2, 6, 3, 2, 1, 0, 5, 0, 3, 7)
- F= 01001010 10010101 00101001 00010100 11010110 11110001
- Et
- F'= 01**1**010**0**0 10**0**0**0**101 00**0**0**1**001 0**1**010100 **0**1010**0**10 **0**11**0**0000

Bit 2 Bit 6 Bit 3 Bit 2 …

Figure 4 : Inversion de bits suivant une suite aléatoire : exemple



L'algorithme DES

Application des Algorithmes asymétriques

- https://www.cs.drexel.edu/~jpopyack/IntroCS/HW/RSAWorksheet.html
- On va encrypter le message '**HELLO**'. On va prendre le code ASCII (en décimal) de chaque caractère et on les met bout à bout:
  - **m = 72-69-76-76-79 (en base 10)**
- Ensuite, il faut découper le message en blocs qui comportent moins de chiffres que **n**.
- **n** comporte 4 chiffres, on va donc découper notre message en blocs de 3 chiffres:
  - 726 976 767 900
    (on complète avec des zéros)
- Ensuite on encrypte chacun de ces blocs:
  - 726^13 mod **21209** = 11600
    976^13 mod **21209** = 5705
    767^13 mod **21209** = 16590
    900^13 mod **21209** = 3565
    Le message encrypté est **11600.5705.16590.3565**. On peut le décrypter avec d:
  - 11600^1609 mod **21209** = 726 (si 1 bit est corrompu 11601^1609 mod 21209 = 6051)
    5705^1609 mod **21209** = 976
    16590^1609 mod **21209** = 767
    3565^1609 mod **21209** = 900
- C'est à dire la suite de chiffre **726976767900**.
  On retrouve notre message en clair **72 69 76 76 79** : '**HELLO**'.

Exemple : cryptographie hybride : génération d'une clé de partage

- Deux utilisateurs vont concevoir une clé commune qui ne servira qu'à eux seuls

ASPECT ASSYMETRIQUE

- Ils choisissent n un nombre produit de deux nombres premier p et q et un entier a (a et n n'étant pas forcément confidentiels)
- Ensuite chacun choisit un entier X appartenant à [1, n-1] et calcule l'entier $Y=a^X \bmod n$
- On obtient deux couples (X_1,Y_1) et (X_2, Y_2) où les valeurs Y_1 et Y_2 vont être publiées

ASPECT HYBRIDE

- Chacun d'eux peut alors calculer la clé $c=a^{X1.X2} \bmod n$ car $c=(Y1^{X2} \bmod n)=(Y2^{X1} \bmod n)$
- R : Chacun ignore le X de l'autre
- La sécurité vient du fait qu'il est impossible en un temps raisonnable de découvrir la clé c par le calcul d'un logarithme discret (infaisable en un temps raisonnable compte tenu de la taille de n)

ASPECT SYMETRIQUE

- Les utilisateurs peuvent maintenant échanger leurs données de manière cryptée en utilisant un système

symétrique grâce à la clé commune c

- Le hash consiste à crypter 25 fois une chaîne de caractère vide, en utilisant le mot de passe comme clé
- Par exemple : DES utilise une clé de 56 bits, donc 7 bits sont pris sur le mot de passe et les caractères après le 8ème sont ignorés
- Un « gain de sel » est ajouté afin d'éviter que le même mot de passe utilisé par deux utilisateurs différents ne génère la même somme de contrôle

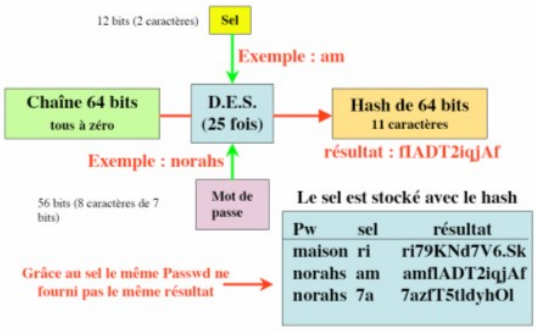
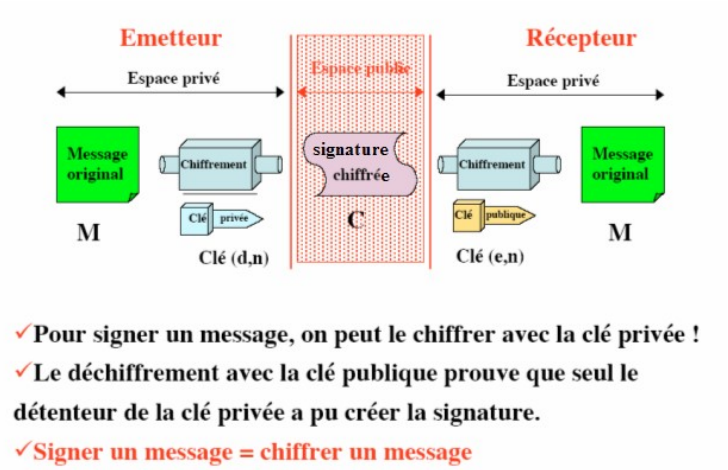


Figure 5 : Hash sur un système Unix



- Il n'est pas nécessaire de chiffrer un message complet pour le signer, il suffit de chiffrer son « hash »
- La résistance aux collisions de la fonction de « hashage » garantit que c'est bien ce document qui a été signé

Principaux paramètres d'un certificat numérique selon norme X509v3

1. Version du certificat
2. Numéro de série
3. Algorithme utilisé pour signer le certificat
4. Nom de l'organisme qui a géré le certificat
   - Le couple numéro de série-nom de l'organisme doit être unique
5. Période de validité
6. Nom du propriétaire du certificat
7. Clé publique du propriétaire
8. Informations additionnelles concernant le propriétaire ou les mécanismes de chiffrement
9. Signature du certificat
   - Algorithme et paramètres utilisés pour la signature ainsi que la signature

TD Sécurité : Cryptage

Ex 1 : Cryptage de CRYPTO en utilisant la technique de l'inversion de bits suivant une suite aléatoire sur des paquets de 8 bits

- Avec la suite a_n = (11,20,3,19,24,33,4,145,69,15)

Ex 2 : Principe de Kerckhoffs

En 1883, Auguste Kerckhoffs a établi un principe fondamental de la cryptographie : "il faut qu'un système cryptographique n'exige pas le secret, et qu'il puisse sans inconvénient tomber entre les mains de l'ennemi". Expliquer ce principe.

Ex 3 : Recherche exhaustive (attaque par force brute) de clefs symétriques

Sachant qu'une certaine machine peut tester en moyenne 400 000 combinaisons par seconde, de combien de temps a besoin cette machine pour retrouver par une recherche exhaustive une clé de 56 bits, combien de temps mettrait-elle pour trouver une clé de 40 bits ? une clé de 112 bits ?

Ex 4 : Chiffrement symétrique et asymétrique

Un groupe de n personnes souhaite utiliser un système cryptographique pour s'échanger deux à deux des informations confidentielles. Les informations échangées entre deux membres du groupe ne devront pas pouvoir être lues par un autre membre. Le groupe décide d'utiliser un système de chiffrement symétrique.

1. Quel est le nombre minimal de clés symétriques nécessaires ?
2. Donner le nom d'un algorithme de chiffrement symétrique reconnu.

Le groupe décide ensuite de remplacer ce système par un système asymétrique.

3. Quel est le nombre minimal de couples de clés asymétriques nécessaires pour que chaque membre puisse envoyer et recevoir des informations chiffrées et/ou signées ? Si l'on considère que chacun peut communiquer avec tout le monde, combien de clés privées et publiques chaque utilisateur devra-t-il détenir
4. Bob souhaite envoyer des informations chiffrées et signées à Alice (Bob et Alice appartiennent tous les deux au groupe). Quelle(s) clé(s) Bob doit-il utiliser ?
5. Donner le nom d'un algorithme de chiffrement asymétrique reconnu.

Le groupe décide finalement d'utiliser un système hybride pour le chiffrement (c'est-à-dire qui utilise la cryptographie symétrique et asymétrique).

6. Donner les raisons qui ont poussé ce groupe à utiliser un tel système.

Ex 5 : Perte d'une clé privée

Un utilisateur, qui utilise souvent la messagerie sécurisée de son entreprise, vient de perdre sa clé privée, mais dispose encore de la clé publique correspondante.

1. Peut-il encore envoyer des courriers électroniques chiffrés ? Décrypter les messages reçus ?
2. Peut-il encore signer les courriers électroniques qu'il envoie ? Vérifier les signatures des courriers électroniques qu'il reçoit ?
3. A quoi peut encore servir la clé publique de notre utilisateur ?
4. Que doit-il faire pour être à nouveau capable d'effectuer toutes les opérations mentionnées ci-dessus ?

Ex 6 : Limitations des certificats numériques

Quelles sont les limites des certificats numériques utilises pour le contrôle d'accès ?