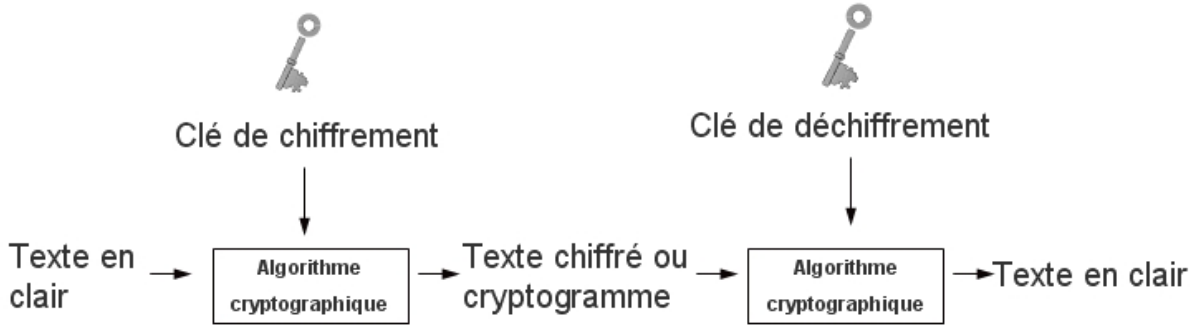
CHAPITRE 3 : Cryptographie moderne

L'idée générale du chiffrement moderne est le chiffrement par blocs. Il est défini par les téapes suivantes:
1. Remplacer les caractères par un code binaire
2. Découper cette chaîne en blocs de longueur donnée
3. Chiffrer un bloc en l'"additionnant" bit par bit à une clef.
4. Déplacer certains bits du bloc.
5. Recommencer éventuellement un certain nombre de fois l'opération 3.
6. Passer au bloc suivant et retourner au point 3 jusqu'à ce que tout le message soit chiffré.

3.1 Cryptosystème à clé symétrique

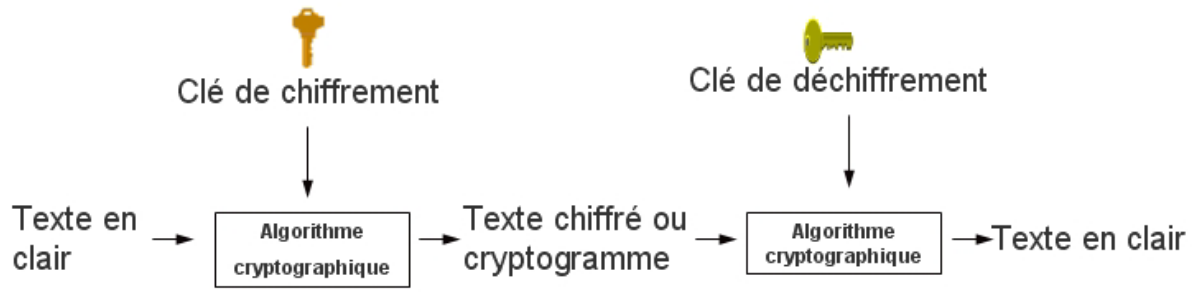


Caractéristiques :
– Les clés sont identiques : KE = KD = K, la clé de chiffrement est égale à la clé de déhiffrement
– La clé doit rester secrète,
– Les algorithmes les plus répandus sont le DES, AES, 3DES, ...

3.1.1 D.E.S. - Data Encryption Standard

Le D.E.S. (Data Encryption Standard, c'est-à-dire Standard de Chiffrement de Données) est un standard mondial depuis la fin des années 1970. Cet algorithme est devenu un standard 1976.

3.2 Cryptosystème à clé publique



Caractéristiques :
– Une clé publique P_K (symbolisée par la clé verticale),
– Une clé privée secrète S_K (symbolisée par la clé horizontale),

– Propriété : La connaissance de P_K ne permet pas de déduire S_K,
– $DS_K(EP_K(M)) = M$,
– L'algorithme de cryptographie asymétrique le plus connu est le RSA,

3.2.1 RSA : Rivest - Shamir - Adleman

Il est basé sur le calcul exponentiel. Sa sécurité repose sur la fonction unidirectionnelle suivante : le calcul du produit de 2 nombres premiers est aisé. La factorisation d'un nombre en ses deux facteurs premiers est beaucoup plus complexe.
Il s'agit du système le plus connu et le plus largement répandu, basé sur l'élévation à une puissance dans un champ fini sur des nombres entiers modulo un nombre premier.
On possède une paire de clés, l'une publique (e,n) et une privée (d,n). La première étape revient à choisir n. Il doit s'agir d'une valeur assez élevée, produit de 2 nombres premiers très grands p et q. En pratique, si p et q ont 100 chiffres décimaux, n possèdera 200 chiffres. Selon le niveau de sécurité souhaité, la taille de n peut varier : 512 bits, 768, 1024 ou 20483.
Dans un second temps, on choisira un très grand entier e, relativement premier à (p-1)*(q-1). La clé publique sera formée par (e,n). On choisira ensuite un d tel que $e * d \equiv 1 \mod (\Phi(n))$.
La clé privée sera donnée par (d,n).

L'algorithme peut etre résumé par les téapes suivantes :
1. Génération de 2 nombres premiers p et q
2. Calcul de n = p*q
3. Déterminer e tel que $3 < e < \_(n)$ et $(e, \Phi(n)) = 1$
4. Calculer d tel que $e * d \equiv 1 \mod (\Phi(n))$
5. Clé publique : (e,n)
6. Clé privée : (d,n)
7. p et q doivent rester secrets, voire supprimés
8. $C = M^e \mod n$ et $M = C^d \mod n$