Alice Bob

$A^n \xrightarrow{E_k} A^n \xrightarrow{D_k} A^n$

$m \longmapsto c \longmapsto m$

Oscar : une attaque par force brute (recherche exhaustive) est toujours possible mais ne doit pas aboutir dans un temps raisonnable (polynomial).

En général, le type de chiffrt est connu et seule la clé privée de (dé)chiffrt est inconnue.

Cryptologie → Cryptanalyse

Cryptologie

Cryptographie

clé privée $k \in K$

symétrique

CONFIDENTIALITÉ

(ancien)

classique

chiffrt par transposition

Scytale

par colonnes

chiffrt par substitution

mono. alph

César

Chiffrt affine

poly. alph

Vigenère

Hill

analyse fréquentielle

ECB CBC CTR CFB

modes opératoires

moderne

chiffrt par bloc

schéma de Feistel

DES

AES

chiffrt par flot

masque jetable de Vernam

GNA

attaque

GCL

GMR

GMR comb.

LFSR

LFSR à tps irreg

attaque

LFSR comb.

LFSR filtré

plus long que le chiffrt symétrique donc plus adapté aux messages courts

Chiffrement parfait

utile pour envoyer la clé privée du chiffrt symétrique

moins coûteux (tps, mémoire) que le chiffrt par bloc donc plus adapté aux systèmes contraignants (mobile)

asymétrique

clé publique / clé privée (k^{pub}, k^{priv})

exponentiation discrète

multiplication d'entiers

Pb du log discret

Mise en accord de clé de Diffie-Hellman.

Chiffrt d'ElGamal

Pb de décomposition en fact. premiers

Fct à sens unique

(inverse non calculable en un tps polyn. ces deux pbs se calculent en tps exp voire sous exp mais pas mieux.)

fct RSA

fct unique à trappe

Chiffrt RSA

attaque

Signature RSA

INTÉGRITÉ

AUTHENTIFICATION

NON-RÉPUDIATION

Fct de hachage