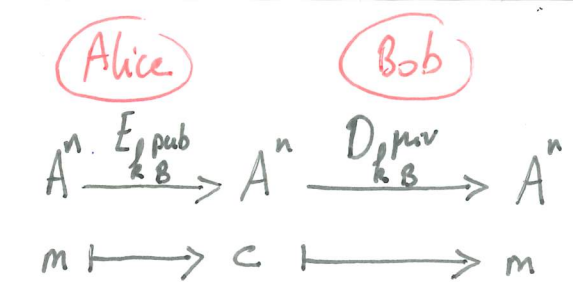
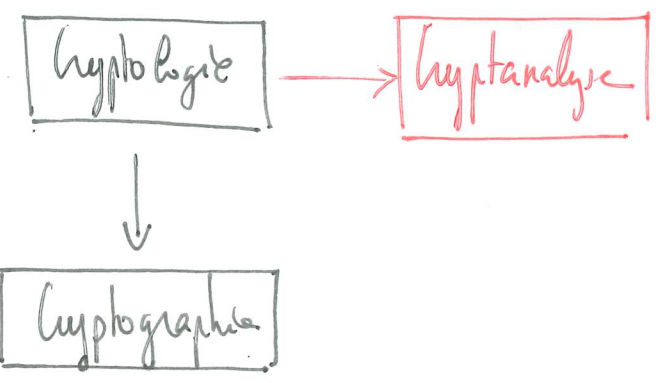


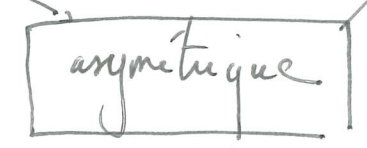
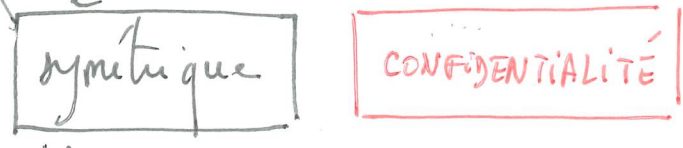
une attaque par force brute (recherche exhaustive) Oscar est toujours possible mais ne doit pas aboutir dans un temps raisonnable (polynomial).



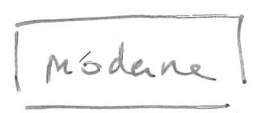
En général, le type de chiffrement est connu et seule la clé privée de (dé)chiffrement est inconnue.

clé privée $k \in K$

clé publique / clé privée (k_{pub}, k_{priv})



(ancien)



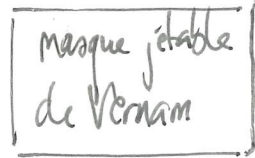
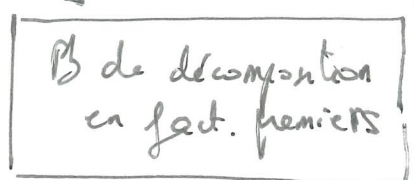
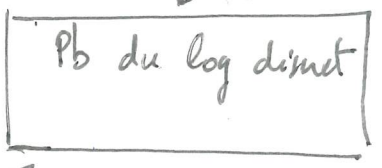
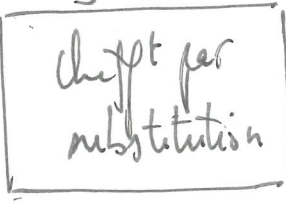
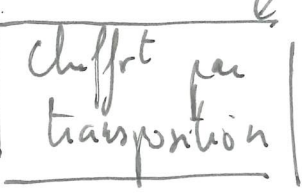
plus long que le chiffrement symétrique donc plus adapté aux messages courts

exponentiation discrète

multiplication d'entiers

Fct à sens unique

(inverse non calculable en un temps poly. les deux pbs se calculent en temps exp voire non exp mais pas mieux.)



utile pour envoyer la clé privée du chiffrement symétrique

Preuve en accord de clé de Diffie-Hellman.

attaque

Scytale par colonnes

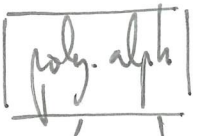
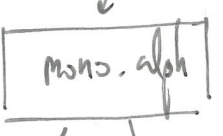
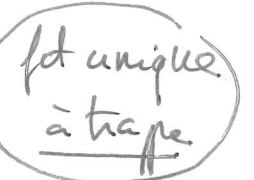
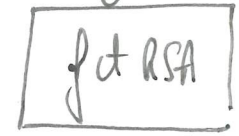


schéma de Feistel DES AES



moins coûteux (tp, mémoire) que le chiffrement par bloc donc plus adapté aux systèmes contraints (mobiles)



César

Chiffrement affine

Vigenère

Hill



attaque à clair (partiellet) connue



attaque

LFSR comb.

LFSR filtré

