Crypto cours 4

Crypto à clé secrète :

➔ Produit et itérés

Produit : substitution + transposition
Iterés : repete l'action d'un chiffre produit

Crypto à clé secrete ? ça va vite ! 1000 fois plis rapide qu'une PKC
En + utilisation des modes de chainage CBC

La crypto, c'est la crypto à clé secrete (pr des raisons de taille et de rapidité)
Mais la crypto à clé secrete) besoin de crypto à clé pub (pour transmettre la clé partagée)

Chiffrer : Calculer le produit scalaire entre n-uplet et le codage binaire de m lettre
(1, 3, 5, 10, 21) <- 21
m > $\sum a_i = 40$
module m > 40
on choisi t inversible mod 50

Transporter le chiffrement : resoudre SSP (B,C) -> SSP (A,C)
c = (B,p)
$t^{-1}C = t^{-1}$ <t A mod m, p> = <A,p>
c = 42 = <B, 10001>
$t^{-1} = 41$
t = 11 mod 50

Dechiffrer = c'est resoudre SSP(A, t^{-1}) -> C mod m = 22

Post quantum crypto : revient sur des problème combinatoire

3 problèmes difficiles :
SSP (comme sous ensemble) -> MH
Factorisation -> RSA
Logarithme discret -> El gamal

➔ cryptographie egyptien
- inventeur de SSL