CRY-Résumé

Définitions
Adversaire passif : peut espionner une comm. mais pas modifier le contenu
Adversaire actif : peut espionner une comm., la modifier et se faire passer pour un des communiquants
Authenticité : On peut prouver l'origine avec certitude
Intégrité : On peut prouver la non-modification d'un message
Adversaire black-box : Considère les algo comme des boîtes noires et les utilise comme oracle (*attaque texte chiffré connu, clair connu, chiffré connu/choisi*)
Adversaire gray-box : Peut obtenir de l'info de l'implémentation
Chance nbr à 100 chiffres soit premier ?
$\frac{10^{100}}{\frac{10^{100}}{\ln(10^{100})}} = \frac{1}{\ln(10^{100})} = \frac{1}{10 \ln(2)}$

Théorème Fermat-Euler
$a^{\varphi(n)} \equiv 1 \pmod{n}$ si **a premier avec n**
$7^{123456} \pmod{13} = 7^{10288 \cdot 12} \pmod{13}$
$= (7^{12})^{10288} \pmod{13} = (1)^{10288} \pmod{13} \equiv 1$

Calculer un inverse mutliplicatif
Après algo Euclide étendu :
$(3, -1, 1) \quad (1, -2, -7)$
Inverse de $13 \pmod{23} \rightarrow -7$

Calculer $\log_3$ de 4 mod 17
On cherche x tel que $3^x = 4 \pmod{17}$
$\rightarrow$ On s'amuse à toutes les calculer...

Factorisation d'un polynôme p
$2 \leq Deg(p) \leq 3$: on regarde si racine
$Deg(p) > 3$ test si div. par polynôme Deg $\leq k/2$

Anneau
$\mathbb{F}[x]/m(x)$
Corps
$\mathbb{F}[x]/m(x)$ pour $m(x)$ irréductible sur $\mathbb{F}$
$GF(p)$: Corps de Galois premier
$GF(p^m)$: Corps de Galois non-premier
$\rightarrow$ Si on demande si $GF(36)$ existe, non car il n'existe pas de paire (p,m) tel que $p^m = 36$
$\rightarrow$ Un corps de Galois à 81 éléments existe : $\mathbb{Z}_3$ avec un polynôme de **irréductible** de degré 4

Montrer que f est une permutation
Il suffit de montrer que f est inversible

Chiffrement symétrique
Modèles de sécurité : pas trouver la clé décrypter le message, obtenir le moindre bit
Chiffrement par blocs : *input :* plaintext + key *output :* ciphertext
Chiffrement par flot :*input :* init. vector + key *output :* flot de bits (pour XOR avec plaintext)

Casser Vigenère
Pour $(m, c = m + k) \rightarrow k = c - m$

Casser Hill (avec n paires textes clairs)
$K = YX^{-1} \pmod{m}$ si $\det(X)$ premier avec m

Opérations sur GF(2^8)
Addition : XOR
Multiplication par 0x02 : Shift vers la gauche (avec en plus un XOR avec 0x1b si carry)
Multiplication par 0x03 : Xor entre les multiplications par 0x02 et 0x01
CBC $\leftarrow$ **Pas parallélisable**
Si le nonce se répète :
On peut distinguer des messages qui commencent par les mêmes blocs car les textes chiffrés correspondants seront les mêmes
CTR $\leftarrow$ **Parallélisable**
Si le nonce se répète :
$C_{11} = M_{11} \oplus AES(NC_1)$
$C_{12} = M_{12} \oplus AES(NC_1)$
$\rightarrow C_{11} \oplus C_{12} = M_{11} \oplus M_{12}$
GCM
Pareil que CTR mais propose l'authenticité.
L'AD permet d'authentifier sans les chiffré. Utile pour l'authentification de certaines valeurs dans les paquets réseau au moment du routage

---

Taille des blocs
AES : 128 bits
DES : 64 bits
Triple-DES : 64 bits

Paradoxe des anniversaires
Pour une empreinte de l bits, trouver une collision demande au plus $2^{\frac{l}{2}}$
$\rightarrow$ Taille moyenne du plaintext pour une répétition de blocs (AES, DES, Triple-DES) : $k \cdot 2^{\frac{k}{2}}$

Courbes elliptiques
Inverse d'un point P :
Pour un point $P = (x; y) \rightarrow P^{-1} = (x; -y)$
Addition de points $P + Q$:
$\mathcal{O}$ si $P = -Q$
P si $Q = \mathcal{O}$
$2P$ si $P = Q$ (Doublement de point)
sinon : Addition de points
Formules pour $P(x_P; y_P)Q(x_Q; y_Q)$:
Addition $x_P \neq x_Q$:
$x_R = (\frac{y_Q - y_P}{x_Q - x_P})^2 - x_P - x_Q$
$y_R = -y_P + (\frac{y_Q - y_P}{x_Q - x_P})(x_P - x_R)$
Doublement de point :
$x_R = (\frac{3x_P^2 + a}{2y_P})^2 - 2x_P$
$y_R = (\frac{3x_P^2 + a}{2y_P})(x_P - x_R) - y_P$
Courbes elliptiques sur $GF(2^r)$
Il vaut mieux ne pas les utiliser, des attaques rendent leur utilisation douteuse

---

Théorème de Hasse
Si N est le nombre de points sur une courbe elliptique définie sur un corps à q éléments, alors N est borné par :
$(q+1) - 2\sqrt{q} \leqslant N \leqslant (q+1) + 2\sqrt{q}$

Problème du logarithme discret
<u>Groupe multiplicatif :</u> g^r
Trouver r sachant g, g^r est difficile
<u>Groupe additif :</u> rG
Trouver r sachant G, rG est difficile

ECDH

Théorème des restes chinois

$\boldsymbol{x \in \mathbb{Z}_{pq} \rightarrow (a;b) \in \mathbb{Z}_p \times \mathbb{Z}_q}$
$a = x \mod p$ et $b = x \mod q$

$\boldsymbol{(a;b) \in \mathbb{Z}_p \times \mathbb{Z}_q \rightarrow x \in \mathbb{Z}_{pq}}$
$x \equiv (a(q^{-1} \mod p)q + b(p^{-1} \mod q)p \mod pq$