Cryptographie ?

Crypter = mettre dans un crypte

Histoire naïve du chiffrement

- Chiffre de César
- Chiffre de Viète ? ?
- Enigma
- RSA
- Courbes elliptiques
- Else ...

Chiffre de César

- décalage de caractère
- constant
- facile à chiffrer
- facile à déchiffrer

- A $\rightarrow$ D
- D $\rightarrow$ A

CESAR $\rightarrow$ GIWEV

Chiffre de Viète

- Chiffre multialphabétique ;
-

Enigma

Un message texte = un chiffre

- lettre $\leftrightarrow$ chiffre
- plusieurs codes : ASCII, UTF-8

- A $\rightarrow$ 65
- a $\rightarrow$ 97
- é $\rightarrow$ 195 ou 233

CESAR $\rightarrow$ 6769836582

RSA

- chiffrement asymétrique
- clef publique
- clef privée
- résistance à l'analyse statistique

hQIMAzJEJPrLXcHlARAAutxmrtyxCqbzfRQStvTfpLAoo2hnTLO3Z6J21swH3fPR
xzG9Il2jiigKtevPsDfBHo7dNzJgVLHfh7WbiV5NgVBawKS/NfKErLW+Ovy4QwR2
nfaLguhOseZGFdsF4EYrJuW9Z6NcSXR1BCVvfNWpToLuZuKePKn5k+/H/rIUTxpv
Cftk28du/CNM5qZMf43TOkbmoKiKJYhc0/Qud2+InftmDHyJV8lQWUX5FkMP9Mmo
O9w5Bk7qfClDMin7dG6SxXfzGGc6MiZrIrONDFABqupp7x21KzeAJ2BrJ616whWr
qrMPlRSxXf1yyGHCLtw5Ozv0J24tK3EPMV56sJTzklARONG+OmjHSLowkBywDzBC
pxjklos4J3NU3Kcm9nt35n9Z3ABcnTcuPreu4bHcbPcvLc5kfsNWlAnlHb9RN2te
OxJxOQNPLfIkILE3evCz6Vp00r9w80DfrVD8Yn9X3eGqxaF44Acp7tHc1xk1D4Kd
NgBCvTi4F6Bk7YPDtb0oUZUjhINZnCfP2kyykun7XDmNFKUSRZxGFwK43a/tW/sg
42OatKBgeywwqmIyu2pZRK8t2+IwDjJVK4828mDA3rj/3kOHyuyhk8l2wCp9cJGf
7CIhw2waAZLMKXW/L54o3NXxYrsnGd/fI63TbiMM+odEwJE5AIOFDWoLtpwTfEXS
QAHDsj8uOmlTO+lxoIG/Icj6aDDakn1kZH6GwlIvis4sEOba9CCivaSzgNJiqDSL
kt/m9iz7TXF/pW3GXRwiC3M=
=YxRF

Mécanisme général du chiffrement symétrique

- Alice veut parler à Bob
- Choix d'une clef secrète
- La clef sert à chiffrer et déchiffrer

- facile à mettre en œuvre
- clef faible
- nécessité de renouvellement de la clef via un canal sécurisé

Mécanisme général du chiffrement asymétrique

- Alice veut parler à Bob
- Bob communique publiquement à Alice sa clef publique
- La clef sert uniquement à chiffrer
- Bob déchiffre le message avec sa clef privée

- mise en œuvre plus complexe
- clef forte, mais double
- nécessité de s'assurer de l'identité du destinataire

Effet de bord du chiffrement

- Alice veut s'assurer que Bob reçoit un message qui :
  - provient bien d'Alice
  - n'a pas été altéré
- Alice communique publiquement à Bob sa clef publique
- La clef signe le message avec sa clef privée
- Bob authentifie le message avec la clef publique d'Alice

- mise en œuvre plus complexe
- clef forte, mais double
- nécessité de s'assurer de l'identité de l'expéditeur au préalable

Principes mathématiques

Fonction à sens unique

- Fonction «facile» à calculer
- mais difficile à «inverser»

Brèche «secrète»

- un secret supplémentaire qui permet de retrouver le point de départ
- à ne pas confondre avec une «porte dérobée»

À quoi sert le chiffrement

- Protection des correspondances
- Paiement sécurisé sur un réseau non sécurisé
- Applications militaires

La liberté d'expression privée : un contre-pouvoir

- Avec de la surveillance : pas de liberté d'expression
- Sans garantie d'intégrité : pas de liberté d'expression

La correspondance privée, base du fonctionnement du commerce

- Fixer un prix de prestation dans un contexte concurrentiel

Enjeux de sociétés et commerciaux

- Espionnage industriel
- Espionnage commercial
- Liberté d'expression dans certains pays

Notions mathématiques pour comprendre les méthodes de chiffrements

- ASCII
- Entiers / binaires
- Arithmétiques

Éléments de bases de l'arithmétique

- Nombres premiers
- Division euclidienne
- irréversibilité des opérations

Rappels d'arithmétique I

Définition (Divisibilité)

On dit que a divise b si et seulement s'il existe un nombre c tel que $b = ac$. On note $a \mid b$ si a divise b et $a \not| b$ sinon.

Proposition

La relation $\mid$ est une relation d'ordre partiel

Proposition (Division euclidienne)

Soient a et b deux nombres relatifs, $b \neq 0$, $((a, b) \in \mathbb{Z} \times \mathbb{Z}^*)$; il existe un entier relatif et un entier naturel tels que $a = bq + r$. Si on impose que $0 < r < b$, alors q et r sont uniques.

Démonstration.

Rappels d'arithmétique II

Soient $a \in \mathbb{Z}$ et $b \in \mathbb{Z}^*$. Supposons qu'il existe deux couples (q, r) et (q', r') tels que $0 < r < b$ et $0 < r' < b$ et $a = bq + r = bq' + r'$.

$$\implies b(q - q') = r' - r$$

or $r' - r \not| b$, donc $r' - r = 0$ et $q - q' = 0$, car $b \neq 0$. $\square$

Définition (classes de congrucence)

On note $n\mathbb{Z} = \{kn, n \in \mathbb{Z}\}$; on dit que x est congru à y modulo n et on note $x \equiv y \mod n \iff x - y \in n\mathbb{Z}$.
On note $\overline{x}$ les éléments congrus à x modulo n ; l'ensemble des classes de congruences $\left\{\overline{1}, \overline{2}, \ldots, \overline{n-1}\right\} = \mathbb{Z}/n\mathbb{Z}$.

Sous groupe additifs de $\mathbb{Z}$

Proposition

Soient $a_1, a_2, \ldots, a_n$ des entiers non nuls ; il existe un unique entier d tel que $a_1\mathbb{Z} + a_2\mathbb{Z} + \cdots + a_n\mathbb{Z} = d\mathbb{Z}$

Démonstration.

- *Les sous groupes additifs de $\mathbb{Z}$ sont de le forme $a\mathbb{Z}$*
- *Si G_1 et G_2 sont des sous groupes d'un groupe «additif», alors $G_1 + G_2$ est un sous groupe.*

$\square$

PGCD

Définition

- Le nombre d de la proposition précédente est le *pgcd*. On note $a_1 \wedge a_2 \wedge \ldots \wedge a_n = d$.
- Si $d = 1$, on dit que les nombres sont premiers dans leur ensemble.

Démonstration.

$d = a \wedge b \neq 0 \implies d \mid a$ et $d \mid b$ et c'est bien le plus grand. $\square$

Bezout et Gauss

Théorème (Bezout)

$a \wedge b = 1 \iff \exists (u, v) \in \mathbb{Z}^2,\ au + bv = 1$

Démonstration.

- $a \wedge b = 1 \implies a\mathbb{Z} + b\mathbb{Z} = \mathbb{Z}$
- Soient
  $(u, v) \in \mathbb{Z}^2,\ au+bv = 1 \implies 1 \in a\mathbb{Z}+b\mathbb{Z} \implies \mathbb{Z} \subset a\mathbb{Z}+b\mathbb{Z}$,
  d'où l'égalité d'ensemble et donc l'égalité.

$\square$

Théorème (Gauss)

Si $a \mid (bc)$ *et* $a \wedge b = 1$, *alors* $a \mid c$.

Démonstration.

Bezout $\implies au + bv = 1 \implies acu + bcv = c$.
Or $a \mid acu$ et $a \mid bcv$ donc $a \mid c$. $\square$

Théorème (Infinité des nombres premiers)

Il y'a une infinitié de nombres premiers

Démonstration.

Supposons que l'ensemble des nombres premiers soit fini. Prenons le produit de tous les nombres premiers augmenté de 1. Ce nombre n'est divisible par aucun des nombres premiers précédents. Ce nombre est donc plus grand, ce qui contredit l'hypothèse initiale $\square$

Décomposition des nombres

Théorème (Décomposition)

Soit n un nombre entier. Il existe une unique décomposition, à l'ordre près, de n en produit de nombres premiers $p_1, \ldots, p_r$ et $n = p_1^{\nu_1} \times \cdots \times p_k^{\nu_k}$.

Démonstration.

- Tout entier $n \geq 2$ admet un facteur premier p tel que $n = pn_1$, $n_1 < n$
- si n_1 n'est pas premier, alors il est composé. En un nombre fini d'étape, on aboutit à la décomposition
- S'il existe deux décompositions, $p_1^{\nu_1} \times \cdots \times p_k^{\nu_k}$ et $p_1^{\nu'_1} \times \cdots \times p_k^{\nu'_k}$, alors $p_1^{\nu_1} \mid p_1^{\nu'_1}$, car étranger à tous les autres, d'où $\nu_1 \leq \nu'_1$ et par symétrie $\nu_1 \geq \nu'_1$ et donc l'égalité.

$\square$

Arithmétique modulaire

Définition

$a \equiv b[n] \iff a = q \times n + b,\ q \in \mathbb{Z}$

Proposition

$a \equiv b[n] \iff a - b \equiv 0[n]$

Proposition

$(\mathbb{Z}/nZ, +, \times)$ *est un coprs si et seulement si* n *est premier.*

Démonstration.

- $\bar{k}$ est inversible dans $\mathbb{Z}/n\mathbb{Z} \iff k \wedge n = 1$. Si k est premier, $\forall p < k, k \wedge p = 1$, d'où $\bar{p}$ est inversible.
- Si $\mathbb{Z}/n\mathbb{Z}$ est un corps, il possède $n - 1$ éléments inversibles. $\implies$ n est premier avec tous les éléments de 1 à $n - 1$. N'ayant pas d'autres diviseurs que 1 ou lui-même, il est premier.

$\square$

Théorème chinois

Théorème (des chinois)

$\mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$ et $\mathbb{Z}/mn\mathbb{Z}$ sont isomorphes.

Démonstration.

On considère l'application $f : \mathbb{Z} \to \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z},\ x \mapsto (\dot{x}, \bar{x})$
$\ker f = \{x \in \mathbb{Z} \mid m \mid x \text{ et } n \mid x\}$ et comme
$m \wedge n = 1 \implies \ker f = \{x \in \mathbb{Z} \mid mn \mid x\}$. On a donc
$f(\mathbb{Z}) \cong \mathbb{Z}/mn\mathbb{Z}$.
$Card\, f(\mathbb{Z}) = Card\, f(\mathbb{Z}/mn\mathbb{Z}) = mn$ qui est le cardinal de
$\mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$, ce qui achève la démonstration. $\square$

Quelques théorèmes utiles I

Théorème (Fermat)

Soit $p \geq 2$ un nombre premier.

$$\forall a \in \mathbb{Z} \; a^p \equiv a \mod p$$

et

$$\forall a \in \mathbb{Z}, \; a \nmid p \; a^{p-1} \equiv 1 \mod p$$

Démonstration.

$\binom{n}{p} \equiv 0 \mod n$ si n est premier
$a^p = ((a-1)+1)^p \equiv (a-1)^p + 1 \mod p$ $\square$

Indicatrice d'Euler

Définition (Indicatrice d'Euler)

Soit $n > 1$ un entier naturel. On note G_n le groupe des inversibles de $\mathbb{Z}/n\mathbb{Z}$. On note $\varphi(n) = Card\ G_n$ le cardinal de ce groupe.

Théorème (Euler)

Soit $n > 1$ un entier naturel. Si $k \wedge n = 1$, alors $k^{\varphi(n)} \equiv 1 \mod n$

Démonstration.

$k \wedge n = 1 \implies \bar{k} \in G_n$ qui est cyclique, d'ordre $\varphi(n)$. Donc $\bar{k}^{\varphi(n)} = \dot{1}$ $\square$

Factorisation de $\varphi(n)$

Proposition

Soit $n \geq 1$ un nombre entier, dont la décomposition est $n = p_1^{\nu_1} \times \cdots \times p_n^{\nu_n}$.

$$\varphi(n) = p_1^{\nu_1 - 1} \times \cdots \times p_k^{\nu_k - 1}(p_1 - 1) \cdots (p_k - 1)$$

Démonstration.

- Soit p un nombre premier et $\alpha > 1$. k n'est pas premier avec $p^\alpha \iff p \mid k$. L'ensemble des nombres premiers de $\{1, \ldots, p^\alpha\}$ est $\{p, 2p, \ldots, p^{\alpha-1}p\}$, de cardinal $p^{\alpha-1}$. On en tire que $\varphi(p^\alpha) = p^\alpha - p^{\alpha-1}$.
- Si m et n sont deux nombres premiers entre eux, alors, en utilisant l'isomorphisme du théorème chinois $\mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z} \cong \mathbb{Z}/mn\mathbb{Z}$ et donc $\varphi(mn) = \varphi(n)\varphi(m)$
- En combinant ces deux résultats, on a le résultat.

RSA en pratique

- On se donne deux nombres premiers distincts p et q et on calcule $n = pq$.
- On se donne deux autres nombres c et d, tels que $cd \equiv 1 \mod \varphi(n)$ où $\varphi(n)$ est l'indicatrice d'Euler.
- L'application $g : \mathbb{Z}/n\mathbb{Z} \to \mathbb{Z}/n\mathbb{Z}, \dot{t} \mapsto \dot{t}^c$ est une fonction de chiffrement.
- L'application $f : \mathbb{Z}/n\mathbb{Z} \to \mathbb{Z}/n\mathbb{Z}, \dot{t} \mapsto \dot{t}^d$ est une fonction de déchiffrement.
- $f \circ g = g \circ f = Id$

Preuve de RSA