# EPITA

# FMSI

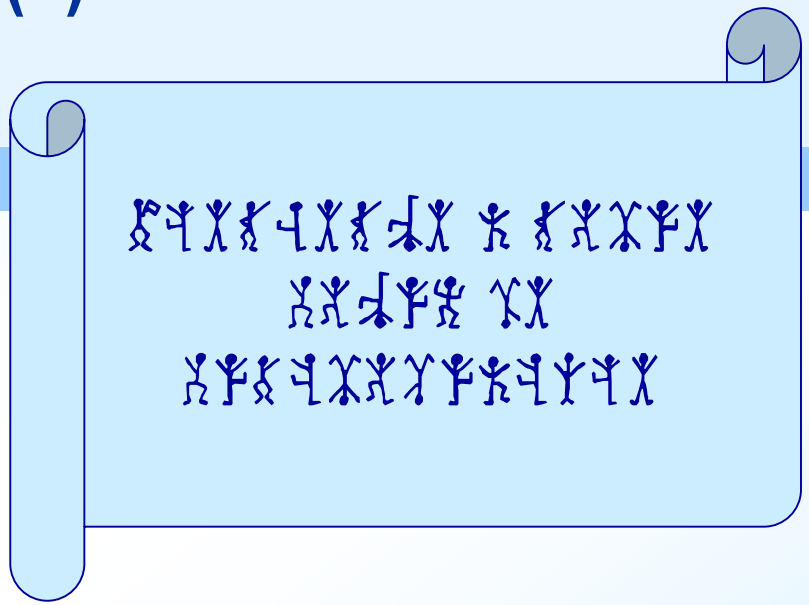
Herbert GROSCOT

Mail 2018

# Plan du cours

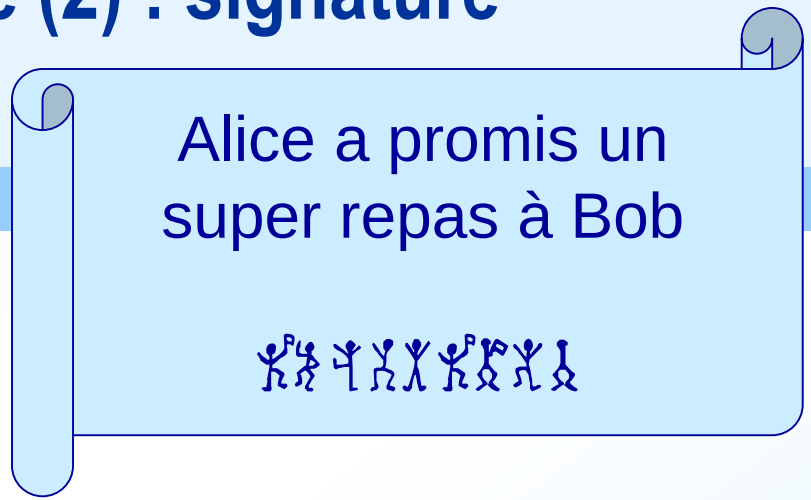
- Courte introduction à la cryptographie
- Eléments d'arithmétique modulaire
- Principe du RSA
- Introduction aux tests de primalité

# Utilisation de la cryptographie (1)



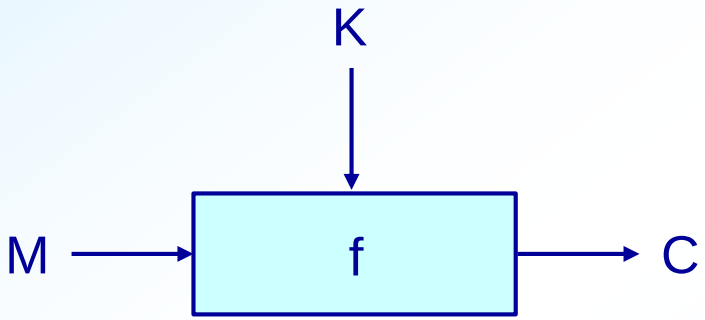
- Chiffrement de messages
- C’est le contenu du message qui est secret
- Il doit être impossible pour un cryptanalyste (*i.e. un adversaire*) de retrouver le moyen de passer d’un message chiffré vers un message en clair, même si le message initial (en clair) est connu.

# Utilisation de la cryptographie (2) : signature




- **Si Alice signe un message M envoyé à Bob :**
  - Bob doit être capable de valider la signature de A dans M – pouvoir avoir confiance dans le fait que c'est bien Alice qui a signé le message,
  - Il doit être impossible pour quiconque, y compris Bob de contrefaire la signature d'Alice,
  - Dans le cas où Alice renierait avoir envoyé le mesage, une tierce partie (Jean) doit pouvoir résoudre le conflit entre Alice et Bob.

# Algorithme de chiffrement




- **Principe**
  - M : le « message », en clair
  - K : la clé
  - C : le message « chiffré » : C = f(M,K)

- **Il doit être impossible de retrouver la clé K, même si la fonction f est connue et si l'adversaire dispose d'une infinité de couples (M,C).**

# Signature avec un algorithme de chiffrement à clé publique

- **Principe**
  - M : le message en clair
  - D : une clé privée (i.e. secrète)
  - S : la signature de M : S = f(M,D)
  - E : un clé, « publique » permettant da calculer : $M=f^{-1}(S,E)$
- **Procédure**
  - Alice signe le message M en calculant : S = f(M,D)
  - Bob valide la signature d'Alice en vérifiant que : $f^{-1}(S,E)$ redonne bien M.
  - Jean règle un conflit éventuel entre Alice et Bob en vérifiant de manière indépendante que $f^{-1}(S,E)$ redonne bien M.

# Décrypter / déchiffrer ?

- **On déchiffre un message dont on connaît la clé**
- **On décrypte un message pour lequel on ne connaît pas la clé (las anglo-saxons disent, quant à eux, qu'ils « cassent » les codes secrets)**

# Motivation de l'arithmétique modulaire

- Les messages M et la clé K sont, informatiquement, implémentés de manière à contenir un nombre fini de « bits » (ou d'octets)

- => Emploi de $\mathbb{Z} / n\mathbb{Z}$ comme ensemble sur lequel on effectue les opérations élémentaires (addition, soustraction, multiplication, éventuellement division, élévation à la puissance).

# Addition et multiplication dans $\mathbb{Z}/n\mathbb{Z}$ (rappel)

- **Concruence :**

$$a \equiv b \,(\mathrm{mod}\, n) \quad si\ (b-a)\ divisible\ par\ n$$

- **Classe d'un nombre**

$$\overline{a} \equiv \{kn + a\ ;\ k \in \mathbb{Z}\}$$

- **Si r est le reste de la division euclidienne de a par n :**

$$\overline{a} = \overline{r}$$

$$\mathbb{Z}/n\mathbb{Z} = \{\overline{0}, \overline{1}, \ldots, \overline{n-1}\}$$

- **Addition**

$$\overline{a} + \overline{b} = \overline{a+b}$$

- **Multiplication**

$$\overline{a}.\overline{b} = \overline{ab}$$

# Addition et multiplication dans $\mathbb{Z}/n\mathbb{Z}$ (rappel)

- **Quand il n'y a pas d'ambigüité**

$$\mathbb{Z}/n\mathbb{Z} = \{0,1,\ldots,n-1\}$$

- **Opérations existant en standard dans tous les outils de programmation, disponibles sous forme de librairies travaillant sur de très grands nombres :**

$$a \in \{0,1,\ldots,n-1\}$$

$$b \in \{0,1,\ldots,n-1\}$$

$$x\,\%\,n : reste\ de\ la\ division\ de\ x\ par\ n$$

$$a+b = (a+b)\,\%\,n$$

$$ab = (ab)\,\%\,n$$

# Propriétés de $\mathbb{Z}/n\mathbb{Z}$ muni de l'addition

- **C'est un groupe commutatif :**
  - Possibilité d'additionner des nombres sans se préoccuper de l'ordre dans lequel on additionne et des priorités avec lesquelles on effectue les additions :

$$a+b=b+a$$

$$a+(b+c)=(a+b)+c$$

  - 0 élément neutre :

$$a+0=0+a=a$$

  - Existence d'un opposé pour tout nombre :

$$a+(-a)=(-a)+a=0$$

# … et muni de l'addition et de la multiplication

- **Anneau commutatif unitaire,**
- **Propriété de la multiplication :**

$$ab = ba$$

$$a(bc) = (ab)c$$

$$1.a = a.1 = a$$

- **Distributivité de la multiplication / l'addition:**

$$a(b+c) = ab + ac$$

$$(b+c)a = ba + ca$$

- **0 est absorbant :**

$$a0 = a.0 = 0$$

# Comparaison avec $\mathbb{Z}$

- **Les opérations dans $\mathbb{Z}$ et dans $\mathbb{Z}/n\mathbb{Z}$ ont le même comportement,**
- **Ce qui permet d'obtenir une famille d'opérations élémentaires travaillant sur des blocs de taille finie :**
  - Sans perte d'informations – pour les opérations réversibles
  - Sans répercutions d'erreurs d'arrondis

- **MAIS : il n'est pas toujours possible d'effectuer des divisions**
  - Dans $\mathbb{Z}/10\mathbb{Z}$
  - 2 et 5 ne sont pas inversibles
  - 2 x 5 = 0 !!!

# Division : Emploi du théorème de Bezout

- Il n'est pas tours possible d'effectuer une division dans $\mathbb{Z} / n\mathbb{Z}$.

- Théorème de Bezout : Pour que a et n soient premiers entre eux, il est nécessaire et suffisant qu'il existe des entiers s et t tels que :

$$sa + tn = 1.$$

# Algorithme

- Plusieurs versions existent (optimisées, inspirées de la théorie des fractions continues, …), appelées : « algorithme d'Euclide étendu »
- Nous nous contentons d'un exemple :

- Problème : calculer l'inverse de 3 modulo 41 ?
- 3 et 41 sont bien premiers entre eux

- $41 = 13 \times 3 + 2$ ; $3 = 2 + 1$
- $1 = 3 - 2$ ; $2 = 41 - 13 \times 3$ : $1 = 3 - (41 - 13 \times 3) = -41 + 14 \times 3$

- (Bezout) : $-41 + 14 \times 3 = 1$
- (Inversion) : $3^{-1} \equiv 14 \pmod{41}$

# Conséquence dans $\mathbb{Z} / n\mathbb{Z}$

- On ne peut inverser a que s'il est premier avec n
- Dans ce cas, avec les notations des slides précédent :

$$a^{-1} \equiv s \pmod{n}.$$

- Autre conséquence : $\mathbb{Z} / n\mathbb{Z}$ est un corps ssi n est premier - i.e. tout élément non nul est alors inversible.

- Pour inverser un nombre a, on emploie alors l'algorithme d'Euclide étendu présenté plus haut.

# Exponentiation modulaire

- **Elévation à de grandes puissance, un algorithme (présenté dans un autre cours EPITA) dit d'exponentiation rapide, utilise l'astuce suivante :**

$$a^{2q} = (a^2)^q$$

$$a^{2q+1} = a.(a^2)^q$$

- **Et permet de réduire considérablement le nombre de multiplications pour élever un nombre à une puissance élevée.**

- **Nous disposons des bases pour calculer dans $\mathbb{Z} / n\mathbb{Z}$.**

# Lemme chinois

- **Soient $n_1,\ldots,n_k$ des nombres premiers entre eux deux à deux et $a_1,\ldots,a_k$ des entiers quelconques.**
- **Soit $n = n_1 \ldots n_k = \prod_{i=1}^{k} n_i$.**
- **Il existe un entier $a$ tel que (*en fait il y en a une infinité*) :**

$$\forall i \in \{1,\ldots,k\} \quad a \equiv a_i \pmod{n_i}.$$

# Fonction indicatrice d'Euler

- Le nombre d'éléments inversibles de $\mathbb{Z}/n\mathbb{Z}$ est égal au nombre d'entier entre 1 et n-1 premiers avec n.
- Ce nombre est noté $\phi(n)$ et $\phi$ est la fonction indicatrice d'Euler.

- Si la décomposition en nombres premiers de $n$ est la suivante :

$$n = \prod_{i=1}^{k} p_i^{v_i}$$

- Alors :

$$\phi(n) = \prod_{i=1}^{k} (p_i - 1) p_i^{v_i - 1} = n \prod_{i=1}^{k} (1 - \frac{1}{p_i})$$

# Caractère cyclique du groupe additif $(\mathbb{Z}/n\mathbb{Z},+)$

- Dans ce groupe, lorsque l'on prend les multiples de 1 les uns après les autres, on « tourne en rond »
- Pout tout $\overline{a}$ (cette fois on laisse la barre pour lever les ambiguïtés) :

$$\overline{a} = a.\overline{1}$$

- On dit que $\overline{1}$ est un générateur du groupe.
- Le nombre de générateurs de $(\mathbb{Z}/n\mathbb{Z},+)$ vaut $\phi(n)$.
- Les générateurs sont en effet les « nombres » premiers avec n.

# Caractère cyclique du groupe multiplicatif $(\mathbb{Z}/p\mathbb{Z}^*,\times)$ où p est premier.

- On admet sans démonstration :

- Si p est premier, le groupe $(\mathbb{Z}/p\mathbb{Z}^*,\times)$ est cyclique.
- Son nombre de générateurs est égal à $\phi(p-1)$.

- Si g est un générateur :

$$\mathbb{Z}/p\mathbb{Z}^* = \left\{1, g, g^2, ..., g^{p-2}\right\}$$

- Par ailleurs :

$$\forall a \in \mathbb{Z}/p\mathbb{Z}^*, \quad a^{p-1} = 1$$

- Petit théorème de Fermat :

$$\forall a \in \mathbb{Z}, a \, non \, divisible \, par \, p, \quad a^{p-1} \equiv 1 \, (\mathrm{mod}\, p)$$

# « Inversion » de l'exponentiation modulaire dans $\mathbb{Z}/p\mathbb{Z}$

- **Soit $e$ un nombre entier (plus petit que p-2) et premier avec p-1**

- **Soit $d$ tel que $ed \equiv 1 \pmod{p-1}$ alors :**

$$\forall a \in \mathbb{Z}/p\mathbb{Z}, \quad a^{ed} = a$$

- **Soit cette fois avec des entiers m et c :**

$$m \to c = m^e \to c^d = m$$

# Propriété analogue pour $\mathbb{Z}/n\mathbb{Z}$ où $n = pq$

- On suppose $e$ premier avec $\phi(n) = (p-1)(q-1)$
- Soit $d$ tel que $ed \equiv 1 \pmod{\phi(n)}$
- Pour tout $m \in \mathbb{Z}/n\mathbb{Z}$
- Si $m \in \mathbb{Z}/n\mathbb{Z}$ est quelconque (même non premier avec n)
- Si $c = m^e$
- Alors $c^d = m$
- Cette propriété est employée pour la construction d'un algorithme de chiffrement asymétrique.

# Le RSA (Rivest – Shamir – Adleman)

- **On part de :**

$$n = pq, \quad p \text{ et } q \text{ premiers}$$

$$e : \text{premier avec } \phi(n)$$

$$d : \text{inverse de } e \pmod{\phi(n)}$$

- **Secret :** $d$
- **Public :** $n, e$

- **Chiffrement (public) :** $m \rightarrow c = m^e \pmod{n}$
- **Déchiffrement (secret) :** $c \rightarrow m = c^d \pmod{n}$

- **Tous les algorithmes permettant les calculs ont été présentés dans ce cour.**

# Signature d'un message

- Alice envoie à Bob un message M (éventuellement très long)
- Alice dispose d'une clé secrète et publique : n, e,d
- Bob connaît la clé publique de Alice n, e
- A partir de M, construction d'un hash : m inférieur à n, méthode connue de Alice et Bob
- Alice construit $c = m^d \pmod{n}$

- Elle envoie à Bob : M, c
- c est la signature de M

- Bob peut reconstruire m à partir de M
- Bob peut ensuite vérifier : $m = c^e \pmod{n}$

# Sélection des paramètres :

- p et q : grands nombres premiers (de $2^{512}$ à $2^{3072}$ …)
- p-q : doit être très grand
- p-1 doit avoir un grand facteur premier r
- r-1 : un grand facteur premier,
- q-1 : un grand facteur premier

# Difficulté du RSA

- Factorisation de n (très grand nombre)
- Extraction de racines e-ièmes
- Calcul du logarithme discret
- Pas d'algorithmes connus à ce jour.
- Toutefois, les performances des algorithmes de factorisation s'améliorent en permanence

# A propose de la factorisation

- La connaissance de $n, \phi(n)$
- La connaissance de $n, e, d$

☝ Permettent dans chacun des cas de retrouver les facteurs de n.

# Une recommandation

- **Deux personnes différentes doivent employer des modules n différents,**
- **Sinon des attaques sont possibles !**

# Tests de primalité

- **Pour construire une clé, il est nécessaire de savoir générer des très grands nombres premiers**

$\Rightarrow$ **Tests de primalité**

- **Le test naïf (essai des diviseurs jusqu'à $\sqrt{n}$) n'est pas praticable.**

- **Autres tests :**
  - Test de Fermat (*probabiliste*)
  - Test de Miller-Rabin (*probabiliste*)
  - Test de Solovay et Strassen (*probabiliste* - hors programme)
  - Test de Lucas (*probabiliste* - hors programme)
  - Test s'appuyant sur des courbes elliptiques (*déterministe* - hors programme)
  - Test AKS (*déterministe, polynomial* - hors programme)

# Test de Fermat

- **Si :** $a^{n-1} \not\equiv 1 \pmod{n}$ **, ou alors** $a$ **et** $n$ **non premiers entre eux, alors,** $n$ **est composé (non premier), dans ce cas** $a$ **est un « témoin de Fermat », du fait que** $n$ **est composé**
- **Dans le cas contraire :** $a^{n-1} \equiv 1 \pmod{n}$ **nous restons indécis quant à la nature de** $n$ **!**
- **Si un nombre a beaucoup de « non témoins » de Fermat, il y a de grandes chances pour qu'il soit premier**

- **Malheureusement, il existe des nombres (nombres de Carmichael),** $n$**, dont tous les nombre** $a$ **inférieurs et premiers avec** $n$ **sont des « non témoins » de Fermat (ex : 561).**

$\rightarrow$**Test non employé en pratique**

# Test de Miller-Rabin

- On cherche à tester la primalité de n.
- On écrit : $n-1=2^s d$ où d est impair.

- Si $\exists a,\ a^d \not\equiv 1 \pmod{n}\ et\ (\forall r \leq s) a^{2^r d} \not\equiv -1 \pmod{n}$
- Alors n est composé.
- Dans ce cas, a est un témoin de Miller pout le fait que n est composé.

- On montre qu'un nombre composé n a au moins une proportion de ¾ de témoins de Miller-Rabin

⇒Permet des tests probabilistes.

- Exemple : si on trouve 40 non-témoins de Miller-Rabin pour n, choisis au hasard, n est premier avec une probabilité d'erreur < $4^{-40}$ < $10^{-24}$.
- Test employé en pratique.

# Document NIST (National Institute of Standards and Technology)

- **FIPS PUB 186-4**
- **Digital Signature Standard (DSS)**
- **Version de juillet 2013**