RÉSUMÉ VIGENÈRE & RSA

CHIFFREMENT DE VIGENÈRE

Dans les chiffrements **poly-alphabétiques**, une lettre du message initial, peut être remplacée par des symboles différents selon sa position dans le texte.

Dans le **chiffrement de Vigénère,** il s'agit toujours de décaler les lettres du message, comme dans le chiffrement de César, mais le décalage dépend de la position de la lettre dans le message.

Ce décalage peut être donné par une clé pouvant s'exprimer par un **mot**.
Prenons, par exemple, le mot (clé) **'bec'**, dans lequel chaque lettre peut être associée à un rang : 'b' à 1, 'e' à 4, 'c' à 2.

- La 1ère lettre sera décalée de 1 lettre
- *La 2ème de 4 lettres*
- La 3ème de 2 lettres
- La 4ème de 1 lettre
- *La 5ème de 4 lettres*
- …

CRYPTANALYSE

LONGUEUR DE CLÉ CONNUE

Si la longueur $\boldsymbol{l}$ de la clé est connue, il suffit de réaliser une analyse fréquentielle sur les textes correspondants aux lettres de rang $0[l], 1[l], \ldots l-1[l]$.

LONGUEUR DE CLÉ INCONNUE

On peut utiliser l'indice de coïncidence pour déterminer la longueur de la clé. Cet indice correspond à la probabilité que deux lettres consécutives prises au hasard dans un texte soient identiques.

Il se note I :

$$I = \sum_{i=0}^{\mathrm{N}-1} \frac{n_i(n_i-1)}{n \times (n-1)}$$

N : taille de l'alphabet

n : longueur du texte
n_i : nombre de lettre « i » dans le texte

CHIFFREMENT ASYMÉTRIQUE

la cryptographie asymétrique (ou à clé publique) utilise deux clés, une **clé publique** utilisée pour chiffrer le message et une **clé privée (ou secrète)** pour le déchiffrer. Cette dernière n'ayant plus à être envoyée.

Ces méthodes de chiffrement asymétrique n'ont pas supplanté les méthodes de chiffrements symétriques car elles sont en général plus lentes. Elles sont très souvent utilisées, non pas pour le codage du message en entier, mais pour le codage de la clé du chiffrement symétrique utilisé pour ce dernier.

FONCTIONS À SENS UNIQUE

Dans un chiffrement asymétrique, les clés publiques et privées doivent être liées entre elles par un type de fonctions appelées **fonctions à sens unique**

Une fonction f est **à sens unique**, si connaissant x, $f(x)$ est **facile*** à calculer, mais connaissant $f(x)$, il est **pratiquement impossible**** de calculer x, c'est à dure de résoudre l'équation $f(x) = y$ (y connu)

> ***Facile :** un algorithme de complexité **polynomiale** permet de réaliser le calcul (problème P)
> ***Pratiquement impossible :** la complexité n'est pas polynomiale (supérieure). Mais on peut quand même vérifier qu'une solution est correcte en temps polynomial (problème NP)

EXEMPLES DE FONCTIONS À SENS UNIQUE

- Le produit et la décomposition en facteur premier. *Chiffrement RSA*
- L'exponentielle en base a modulo p : $x \longrightarrow a^x$ et sa réciproque, le logarithme en base a modulo p (beaucoup plus difficile à calculer que l'exponentielle). *Chiffrement d'El Gamal*
- Pb du sac dos : il est facile de calculer la valeur totale d'un sac à dos à partir des objets qui le constituent, mais il est beaucoup plus difficile de retrouver les objets d'un sac à partir de sa valeur totale. *Chiffrement de Merkle-Hellman*

OUTILS ARITHMÉTIQUES POUR LE RSA

INDICATEUR D'EULER

L'indicateur d'Euler associé à n est le nombre d'éléments inversibles dans $\mathbb{Z}/n\mathbb{Z}$. On le note $\varphi(n)$.

$$\varphi(n) = \text{card}\{p \in \mathbb{N}^* / \ p \leq n \text{ et } p \text{ premier avec } n\} = \text{card}(\mathbb{Z}/n\mathbb{Z})^*$$

PROPRIÉTÉS

- $\boldsymbol{\varphi(n) \geq 2}$ **si** $\boldsymbol{n \geq 3}$
- $\boldsymbol{\forall n \geq 3, \varphi(n)}$ **pair**
- **Si** $\boldsymbol{n = p^r}$ **:** $\boldsymbol{\varphi(p^r) = p^r - p^{r-1}}$
- **Si** $\boldsymbol{p}$ **et** $\boldsymbol{q}$ **sont premiers entre eux :** $\boldsymbol{\varphi(p \times q) = \varphi(p) \times \varphi(q)}$

Ces deux dernières propriétés permettent de calculer l'indicateur d'Euler d'un entier dont on connait la décomposition en facteurs premiers

THÉORÈME D'EULER

Si $\boldsymbol{m}$ et $\boldsymbol{p}$ sont premiers entre eux alors : $\boldsymbol{m^{\varphi(p)} = 1[p]}$

Variante utile pour le RSA, si $\boldsymbol{p}$ et $\boldsymbol{q}$ sont premiers entre eux alors et si $\boldsymbol{m} \in \mathbb{Z}/\boldsymbol{n}\mathbb{Z}$, alors :

$$\boldsymbol{m^{\varphi(p)\varphi(q)} = 1[pq]}$$

C'est-à-dire $m^{\varphi(n)} = 1[n]$ avec $n = pq$

Attention, il n'est pas nécessaire que m soit premier avec p ou q (ce qui rend la démonstration un peu délicate

CHIFFREMENT À CLÉ PUBLIQUE RSA

Pour le codage RSA nous avons besoin des données suivantes :

- Deux grands entiers premiers $\boldsymbol{p}$ et $\boldsymbol{q}$ à partir desquels nous calculons $\boldsymbol{n = pq}$
- Un grand entier $\boldsymbol{d}$ premier avec $\boldsymbol{\varphi(n) = (p-1)(q-1)}$ à partir duquel nous calculons :

$$\boldsymbol{e = d^{-1}[\varphi(n)]}$$

SYSTÈME RSA

La clé publique est le couple (e, n)
La clé privée est d

Les calculs se faisant $modulo\ n$, il est important que M soit plus petit que n

- Chiffrement d'un message M avec la clé publique : $C \equiv M^e[n]$
- Déchiffrement d'un cryptogramme C avec la clé privée : $M \equiv C^d[n]$

POURQUOI RETOMBE-T-ON SUR M ?

$$M \equiv C^d[n] \equiv (M^e)^d[n] \equiv M^{ed}[n]$$

Or $e \equiv d^{-1}[\varphi(n)]$ donc $\boldsymbol{ed \equiv 1[\varphi(n)]}$

Ce qui signifie aussi que $\boldsymbol{ed = 1 + k\varphi(n)}$: $M^{ed}[n] \equiv M^{+k\varphi(n)}[n] \equiv M \times \left(M^{\varphi(n)}\right)^k[n] \equiv M[n]$

car $M^{\varphi(n)} \equiv 1[n]$

EXEMPLE DE CHIFFREMENT RSA

$p = 53, q = 67 \Longrightarrow \begin{cases} n = pq = 3551 \\ (p-1)(q-1) = 3432 \end{cases}$

Nous choisissons d premier avec 3551 : $d = 809 \Longrightarrow e \equiv d^{-1}[(p-1)(q-1)] \Longrightarrow e = 2609$

Prenons le message : **mesmeilleursvoeux**

Chaque lettre est remplacée par deux chiffres (sinon ambigüité possible) : 'a' $\longrightarrow$ '01' ;' b' $\longrightarrow$ '02' … 'z' $\longrightarrow$ '26' . On obtient pour le message « **mesmeilleursvoeux** », la suite de chiffres :

$$\boldsymbol{M = 13051913050912120521181922150521 24}$$

On découpe la suite en blocs de même longueur en partant par la droite.
Dans chaque bloc, le nombre le plus grand possible doit être inférieur à $\boldsymbol{n = 3551}$:

$$\boldsymbol{13\ 0519\ 1305\ 0912\ 1205\ 2118\ 1922\ 1505\ 2124}$$

$$\boldsymbol{M_1 = 13\ ;\ M_2 = 519\ ;\ M_3 = 1305\ ;\ M_4 = 0912\ ;M_5 = 1205}$$
$$\boldsymbol{M_6 = 2118;\ M_7 = 2622\ ;\ M_8 = 1505\ ;\ M_9 = 2124}$$

Il faut donc calculer $\boldsymbol{M_i^e[n] = M_i^{2609}[3551]}$ pour $\boldsymbol{i \in \{1, \dots, 9\}}$
$M_1^{2609}[3551] \equiv 13^{2609}[3551] \equiv 1104\ [3551]$
$M_2^{2609}[3551] \equiv 519^{2609}[3551] \equiv 314[3551]$
$M_3^{2609}[3551] \equiv 1305^{2609}[3551] \equiv 1723[3551]$
$M_4^{2609}[3551] \equiv 912^{2609}[3551] \equiv 2071[3551]$
$M_5^{2609}[3551] \equiv 1205^{2609}[3551] \equiv 2947[3551]$
$M_6^{2609}[3551] \equiv 2118^{2609}[3551] \equiv 2138[3551]$
$M_7^{2609}[3551] \equiv 2622^{2609}[3551] \equiv 1756[3551]$
$M_8^{2609}[3551] \equiv 1505^{2609}[3551] \equiv 1920[3551]$
$M_9^{2609}[3551] \equiv 2124^{2609}[3551] \equiv 3080\ [3551]$

Cryptogramme : C='1104031417232071294721381756192030 80 '

Déchiffrement :

- **Séparation en blocs $\boldsymbol{C_1, \dots, C_9}$: 1104 0314 1723 2071 2947 2138 1756 1920 3080**
- Puis calculs $\boldsymbol{M_i \equiv C_i^d[n] \equiv C_i^{809}[3551]}$

EXERCICES

Exercice 1 – Système RSA

Bob choisit comme nombre premier $p = 17$ et $q = 23$, comme exposant e = 7.
Alice et Bob se fixent un protocole RSA dans lequel les messages sont des nombres en base 10 que l'on code par bloc de 2 chiffres. Alice veut envoyer le message "442838".

1. Donner la clé publique de Bob :
2. Donner la clé secrète d de Bob.
3. Écrire le message chiffré que Alice envoie à Bob.
4. Déchiffrer le message reçu par Bob et vérifier que c'est bien celui envoyé par Alice.

Exercice 2 – Système RSA

Un professeur envoie ses notes au secrétariat par mail. La clef publique du professeur est $(3{,}55)$, celle du secrétariat est $(3{,}33)$.

1. Calculer les clés privées du professeur et du secrétariat
2. Authentification : comment l'enseignant peut-il faire pour « signer » son message, de sorte que le secrétariat soit sûr de son origine ?
3. Le professeur « signe » ses messages pour le secrétariat après les avoir chiffrés. Le secrétariat reçoit le message 23.
   Quelle est la note correspondante ?

Exercice 3 – Système RSA

$p = 47$ et $q = 59$

1. On prendra $e = 17$. Justifier la possibilité de ce choix
2. Déterminer la clé publique et la clé privée
3. Le code binaire ASCII de la lettre B est 1000010. Chiffrer la lettre B avec la clé publique et vérifier que la clé privée permet bien de retrouver le message initial.

Exercice 4 – Système RSA

On considère un système RSA de clé publique $(e, n) = (11{,}319)$

1. Quel est le chiffrement du message $M = 100$?
2. Calculer la clé privée du système
3. Déchiffrer le message $C = 133$. On pourra se servir du résultat $133^{25} \equiv 133[319]$
4. Le message 612 peut-il résulter d'un codage avec la clé publique $(e, n) = (11{,}319)$

Exercice 5 – Système RSA

Bob1 et Bob2 ont pour clé publique RSA respectivement (e_1, n) et (e_2, n) avec e_1 et e_2 premiers entre eux.
Alice envoie le même message m crypté par les clés publiques RSA de Bob1 et Bob2.
Expliquer comment Eve, qui intercepte les deux cryptogrammes et qui connait les clés publiques de Bob1 et Bob2, peut retrouver le message m.
Exemple

- $(e_1, n) = (111{,}5627)$
- $(e_2, n) = (89{,}5627)$
- $m_1 = 4837$ *et* $m_2 = 4626$

Exercice 5. Connaître n et $\varphi(n)$, c'est connaître p et q

On suppose que n est un entier naturel non nul dont la décomposition en facteurs premiers est : $n = pq$.

1. Exprimer $\varphi(n)$, en fonction de p et q.
2. Exprimer $x = pq$ et $y = p + q$ en fonction de n et $\varphi(n)$.
3. En déduire une méthode pour obtenir p et q lorsque l'on connait n et $\varphi(n)$.
4. Si $n = 17063$ et $\varphi(n) = 16800$, calculer p et q

PYTHON

Exercice 1

Comment programmer une fonction de puissance modulaire en Python ?

- Programmation itérative
- Programmation récursive
- **Algorithme récursif d'exponentiation rapide (*square-and-multiply :* « mettre au carré et multiplier »).**
  L'idée : $a^{11} = a \times (a^5)^2 = a \times (a \times (a^2)^2)^2$

Exercice 2

Mettre en place un système de chiffrement-déchiffrement de textes basé sur le système RSA.

CORRIGÉS EXOS 1 ET 2

Exercice 1

Bob choisit comme nombre premier $p = 17$ et $q = 23$, comme exposant $e = 7$.
Alice et Bob se fixent un protocole RSA dans lequel les messages sont des nombres en base 10 que l'on code par bloc de 2 chiffres. Alice veut envoyer le message "442838".

1. Donner la clé publique de Bob.
   $$\boldsymbol{n = pq = 391}$$
   clé publique : $\boldsymbol{(n, e) = (391, 7)}$
2. Donner la clé secrète d de Bob.
   $$\boldsymbol{d \equiv e^{-1}[\varphi(n)]}$$
   Or $\boldsymbol{\varphi(n) = (p-1)(q-1) = 16 \times 22 = 352}$
   $$\boldsymbol{d \equiv 7^{-1}[352]}$$
   L'inverse modulaire s'obtient assez rapidement en appliquant l'algorithme d'Euclide étendu :
   $\boldsymbol{352 = 50 \times 7 + 2 \Rightarrow 2 = 352 - 50 \times 7}$
   $\boldsymbol{7 = 3 \times 2 + 1 \Rightarrow 1 = 7 - 3 \times 2 = 7 - 3 \times 352 + 150 \times 7 = 151 \times 7 - 352 \times 3}$
   $\boldsymbol{1 = 151 \times 7 - 352 \times 3}$ $\boldsymbol{donc}$ $\boldsymbol{151 \times 7 = 1 + 352 \times 3 \Rightarrow 151 \times 7 \equiv 1[391]}$
   $\boldsymbol{151 \equiv 7^{-1}[391]}$
   $\boldsymbol{d = 151}$
3. Écrire le message chiffré que Alice envoie à Bob.
   $\boldsymbol{M = 442838 = M_1M_2M_3}$ **avec** $\boldsymbol{M_1 = 44, M_2 = 28, M_3 = 38}$
   $$\boldsymbol{C_1 \equiv M_1^e[391] \equiv 44^7\ [391] \Rightarrow C_1 = 56}$$
   $$\boldsymbol{C_2 \equiv M_2^e[391] \equiv 28^7\ [391] \Rightarrow C_2 = 224}$$
   $$\boldsymbol{C_3 \equiv M_3^e[391] \equiv 38^7\ [391] \Rightarrow C_3 = 149}$$
   Message chiffré : 056224149
4. Déchiffrer le message reçu par Bob et vérifier que c'est bien celui envoyé par Alice.
   $\boldsymbol{C =}$ **056224149** $\boldsymbol{= C_1C_2C_3}$ **avec** $\boldsymbol{C_1 = 56, C_2 = 224, C_3 = 149}$
   $$\boldsymbol{M_1 \equiv C_1^d[391] \equiv 56^{151}\ [391] \Rightarrow M_1 = 44}$$

$$M_2 \equiv C_2^d[391] \equiv 224^{151}\ [391] \Rightarrow M_2 = 28$$
$$M_3 \equiv C_3^d[391] \equiv 149^{151}\ [391] \Rightarrow M_3 = 38$$

Exercice 2

Un professeur envoie ses notes au secrétariat par mail. La clef publique du professeur est (3,55), celle du secrétariat est (3,33).

1. Calculer les clés privées du professeur et du secrétariat

La clé privée se calcule à partir de e, p et q. Les clés n étant petites, leur décomposition est facile.
Clé privée du professeur

$$n = 55 \Rightarrow n = 5 \times 11 \Rightarrow p = 5\ et\ q = 11$$
$$\Rightarrow \varphi(n) = (p-1)(q-1) = 4 \times 10 = 40$$
$$d \equiv e^{-1}[\varphi(n)] \equiv 3^{-1}[40]$$

Algorithme d'Euclide étendu pour calculer $3^{-1}[40]$

$$40 = 3 \times 13 + 1 \Rightarrow 1 = 40 - 3 \times 13 \Rightarrow -3 \times 13 \equiv 1[40] \Rightarrow 3^{-1} \equiv -13[40] \equiv 27[40] \Rightarrow d = 27$$

Clé privée du secrétariat

$$n = 33 \Rightarrow n = 3 \times 11 \Rightarrow p = 3\ et\ q = 11$$
$$\Rightarrow \varphi(n) = (p-1)(q-1) = 2 \times 10 = 20$$
$$d \equiv e^{-1}[\varphi(n)] \equiv 3^{-1}[20]$$

Algorithme d'Euclide étendu pour calculer $3^{-1}[20]$

$$20 = 3 \times 6 + 2 \Rightarrow 2 = 20 - 3 \times 63 = 2 + 1 \Rightarrow 1 = 3 - 2 = 3 - 20 + 3 \times 6 = 3 \times 7 - 20$$
$$\Rightarrow 3 \times 7 \equiv 1[20] \Rightarrow 3^{-1} \equiv 7[20] \Rightarrow d = 7$$

2. Authentification : comment l'enseignant peut-il faire pour « signer » son message, de sorte que le secrétariat soit sûr de son origine ?

Il peut envoyer un message codé avec sa clé privée. Le secrétariat pourra le décoder avec la clé publique.
Par exemple : s'il code la clé publique 3 du secrétariat en utilisant sa clé privée (27,55) : $3^{27}[55] \equiv 42$
Le professeur peut envoyer le message au secrétariat : « Votre clé publique est 42 »
Le secrétariat décode 42 en utilisant la clé publique du professeur (3,55) : $42^3[55] \equiv 3$
3 est la bonne clé, ce qui prouve que l'interlocuteur est bien le professeur.

Ce procédé d'authentification fonctionne car le produit ed est commutatif, $ed = de$, on peut donc changer l'ordre des puissances.

3. Le professeur « signe » ses messages pour le secrétariat après les avoir chiffrés avec la clé publique du secrétariat. Le secrétariat reçoit le message 23.
   Quelle est la note correspondante ?

Notations préliminaires :
Clés du professeur : $n_p = 55$; $e_p = 3$; $d_p = 27$
Clés du professeur : $n_s = 33$; $e_s = 3$; $d_s = 7$
Le professeur a codé le message M (note) en utilisant la clé publique du secrétariat : $M^{e_s}[n_s]$
Il signe ensuite son message en utilisant sa clé privée : $(M^{e_s}[n_s])^{d_p}[n_p] = 23$
Il faut d'abord décoder la signature en utilisant la clé publique du professeur : $23^{e_P}[n_P]$
Puis déchiffrer en utilisant la clé privée du secrétariat : $(23^{e_P}[n_P])^{d_s}[n_s]$
$(23^{e_P}[n_P])^{d_s}[n_s] \equiv (23^3[55])^7[33] = 12$
La note correspondante est 12
Remarque : la signature n'est pas très utile ici, puisqu'elle ne permet pas d'authentifier l'expéditeur (le professeur)