IUT Villetaneuse
Université Sorbonne Paris Nord

But Passerelle Technologie de l'information
Informatique - Science des données

Introduction à la cryptographie

Année 2023-2024

Table des matières

1.1 Généralités

On peut définir **la cryptographie** comme l'ensemble des techniques permettant de rendre un message incompréhensible pour ceux qui n'en sont pas les destinataires légitimes.

Le **principe de Kerchoffs** (1883) est aujourd'hui universellement adopté : il stipule que la sécurité d'un système de cryptographie (cryptosystème) ne doit pas reposer sur la confidentialité de l'algorithme de chiffrement ; elle doit uniquement reposer sur « la clef » du système, qui est un paramètre que l'on peut changer facilement. On distingue deux types de cryptosystèmes. Les **systèmes symétriques** pour lesquels la clef de l'expéditeur du message et celle du destinataire se déduisent facilement l'une de l'autre, et doivent donc être maintenues toutes deux secrètes. Les **systèmes asymétriques** où une partie des clefs est rendue publique. Traditionnellement, l'expéditeur du message est appelé Alice et le destinataire Bob. On fait aussi intervenir d'autres personnages (Eve, Mallory, ...) dont le but est d'intercepter le message transmis.

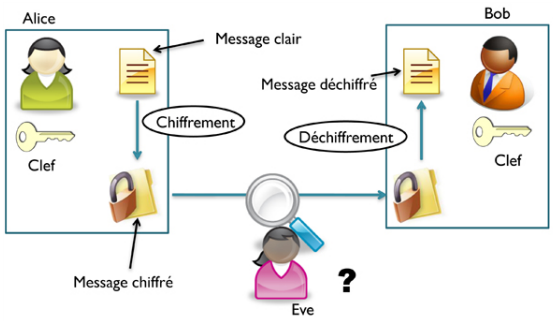

FIGURE 1.1 – Communication entre Alice et Bob espionnée par Eve

1.2 Rappels et compléments d'arithmétique

1.2.1 Division euclidienne

Théorème 1.1

Étant donné $(a, b) \in \mathbb{Z}^2$ avec $b \neq 0$, il existe un unique couple $(q, r) \in \mathbb{Z}^2$ tel que

$$a = qb + r \quad \text{et} \quad 0 \leq r \leq |b| - 1.$$

On dit que q est ***le quotient*** *de la division euclidienne de a par b et r* ***le reste*** *de cette division.*

Définition 1.1

On dit que l'entier $b \neq 0$ est un diviseur de l'entier a si le reste de la division euclidienne de a par b est nul, autrement dit s'il existe $q \in \mathbb{Z}$ tel que $a = qb$; on note alors $b|a$.

1.2.2 Pgcd, théorèmes de Bézout et de Gauss

Définition 1.2

- Soit $(a, b) \in \mathbb{Z}^2$ avec $(a, b) \neq (0, 0)$. Le plus grand commun diviseur de a et b est le plus grand entier divisant à la fois a et b ; on le note $pgcd(a, b)$ ou $a \wedge b$.
- on dit que les entiers a, b sont premiers entre eux si $a \wedge b = 1$.

Théorème 1.2 (*Théorème de Bézout*)

Soit $(a, b) \in \mathbb{Z}^2 \setminus \{(0, 0)\}$. Un entier $d \in \mathbb{Z}$ est multiple de $a \wedge b$ si et seulement si il existe $(u, v) \in \mathbb{Z}^2$ tel que $au + bv = d$. En particulier a et b sont premiers entre eux si et seulement si il existe des entiers u, v tels que $au + bv = 1$.

Théorème 1.3 (*Théorème de Gauss*)

Soit $(a, b, c) \in \mathbb{Z}^3$. Si $a|bc$ et $a \wedge b = 1$ alors $a|c$.

1.2.3 L'algorithme d'Euclide

Soit $(a, b) \in \mathbb{Z}^2$, avec $(a, b) \neq (0, 0)$.

1. On effectue la division euclidienne de a par b : $a = q_0 b + r_0$ où $0 \leq r_0 \leq |b| - 1$. Si $r_0 = 0$ on s'arrête à cette première étape ; sinon :
2. On effectue la division euclidienne de b par r_0 : $b = q_1 r_0 + r_1$ où $0 \leq r_1 \leq r_0 - 1$. Si $r_1 = 0$ on s'arrête à cette deuxième étape ; sinon :
3. On effectue la division euclidienne de r_0 par r_1 : $r_0 = q_2 r_1 + r_2$ où $0 \leq r_2 \leq r_1 - 1$. Si $r_2 = 0$ on s'arrête à cette troisième étape ; sinon :
4. On effectue la division euclidienne de r_1 par r_2 : $r_1 = q_3 r_2 + r_3$ où $0 \leq r_3 \leq r_2 - 1$.

   Et ainsi de suite jusqu'à obtenir un reste nul.

Cet algorithme finit par s'arrêter car la suite $r_0, r_1, r_2, \cdots$ est une suite d'entiers strictement décroissante et minorée par 0.

Propriété 1.1

Si $r_0 = 0$ alors b est un diviseur de a et donc $a \wedge b = b$. Si $r_0 \geq 1$, alors le dernier reste non nul dans la suite $r_0, r_1, \cdots$ est égal à $a \wedge b$.

Cette suite de divisions euclidiennes donne aussi un moyen pratique de trouver des entiers u, v apparaissant dans le théorème de Bézout, c'est à dire vérifiant $au + bv = a \wedge b$. En effet, la dernière division euclidienne ayant un reste non nul est de la forme $r_n = q_{n+2} r_{n+1} + a \wedge b$, donc

$$(*) \qquad a \wedge b = r_n - q_{n+2} r_{n+1}.$$

La division précédente $r_{n-1} = q_{n+1} r_n + r_{n+1}$ s'écrit aussi $r_{n+1} = r_{n-1} - q_{n+1} r_n$; en reportant cette expression dans l'équation $(*)$ on obtient une équation de la forme

$$(**) \quad a \wedge b = \alpha r_{n-1} + \beta r_n$$

pour certains entiers α, β. On continue ainsi en remontant jusqu'à la première division, ce qui donne une relation du type $a \wedge b = au + bv$.

1.2.4 Congruences ; anneaux $\mathbb{Z}/n\mathbb{Z}$

Définition 1.3

Soient $(a, a') \in \mathbb{Z}^2$ et $n \in \mathbb{N}^*$. On dit que a et a' sont congrus modulo n si n divise $a - a'$, ce qui est équivalent à dire que a et a' ont le même reste dans la division euclidienne par n. On écrit alors $a \equiv a' \ mod \ n$.

Proposition 1.1

*La relation $\equiv$ est une relation d'équivalence sur $\mathbb{Z}$; il y a exactement n classes d'équivalence différentes pour cette relation, appelées **classes de congruence modulo** n, qui sont : la classe de 0, la classe de 1, $\cdots$, la classe de $n - 1$.*

Notation 1.1 *La classe de congruence modulo n d'un entier $a \in \mathbb{Z}$ est notée $[a \mod n]$; ainsi*

$$[a \mod n] = \{a + kn \,|\, k \in \mathbb{Z}\} = \{\cdots, a - 3n, a - 2n, a - n, a, a + n, a + 2n, a + 3n, \cdots\}.$$

S'il n'y a pas d'ambiguïté sur l'entier n considéré, on écrit plus rapidement $\overline{a}$ au lieu de $[a \mod n]$. On dit aussi que $a+kn$ (où $k \in \mathbb{Z}$) est ***un représentant*** *de la classe de congruence $[a \mod n]$. L'ensemble de ces n classes est noté $\mathbb{Z}/n\mathbb{Z}$; autrement dit*

$$\mathbb{Z}/n\mathbb{Z} = \big\{[0 \mod n], [1 \mod n], \cdots, [n-1 \mod n]\big\}.$$

Exemple 1.1 *Prenons $n = 4$. On a quatre classes de congruence modulo 4, qui sont*

$[0 \mod 4] = \{\cdots, -12, -8, -4, 0, 4, 8, 12, \cdots\}$,
$[1 \mod 4] = \{\cdots, -11, -7, -3, 1, 5, 9, 13, \cdots\}$,
$[2 \mod 4] = \{\cdots, -10, -6, -2, 2, 6, 10, 14, \cdots\}$,
$[3 \mod 4] = \{\cdots, -9, -5, -1, 3, 7, 11, 15, \cdots\}$.

On les note simplement $\overline{0}, \overline{1}, \overline{2}, \overline{3}$ s'il n'y a pas d'ambiguïté sur le fait que l'on considère des classes de congruence modulo ; ainsi

$$\mathbb{Z}/4\mathbb{Z} = \Big\{[0 \mod 4], [1 \mod 4], [2 \mod 4], [3 \mod 4]\Big\} = \big\{\overline{0}, \overline{1}, \overline{2}, \overline{3}\big\}.$$

Proposition 1.2

Soit $n \in \mathbb{N}^*$.

- *La relation de congruence modulo n est compatible avec l'addition des entiers, c'est à dire : si $a \equiv a' \mod n$ et si $b \equiv b' \mod n$ alors $a+b \equiv a'+b' \mod n$.*
  La relation de congruence modulo n est compatible avec la multiplication des entiers, c'est à dire : si $a \equiv a' \mod n$ et si $b \equiv b' \mod n$ alors $ab \equiv a'b' \mod n$.
- *Le point précédent permet de définir une addition et une multiplication des classes de congruence modulo n en posant*

$$\overline{a} + \overline{b} = \overline{a+b} \quad \text{et} \quad \overline{a} \times \overline{b} = \overline{ab}.$$

Proposition 1.3 (*Propriétés de l'addition et de la multiplication dans $\mathbb{Z}/n\mathbb{Z}$*)

Soit $n \in \mathbb{N}^*$. Pour toutes classes de congruence $\overline{a}, \overline{b}, \overline{c}$ dans $\mathbb{Z}/n\mathbb{Z}$ on a :

1. $(\overline{a}+\overline{b})+\overline{c} = \overline{a}+(\overline{b}+\overline{c})$ *[associativité de $+$]* ;
2. $\overline{a}+\overline{b} = \overline{b}+\overline{a}$ *[commutativité de $+$]* ;
3. $\overline{a}+\overline{0} = \overline{0}+\overline{a} = \overline{a}$ *[$\overline{0}$ est élément neutre pour $+$]* ;
4. $\overline{a}+\overline{-a} = \overline{-a}+\overline{a} = \overline{0}$ *[$\overline{-a}$ est le symétrique de $\overline{a}$ pour $+$]* ;
5. $(\overline{a}\times\overline{b})\times\overline{c} = \overline{a}\times(\overline{b}\times\overline{c})$ *[associativité de $\times$]* ;
6. $\overline{a}\times\overline{b} = \overline{b}\times\overline{a}$ *[commutativité de $\times$]* ;
7. $\overline{a}\times\overline{1} = \overline{1}\times\overline{a} = \overline{a}$ *[$\overline{1}$ est élément neutre pour $\times$]* ;
8. $\overline{a}\times(\overline{b}+\overline{c}) = \overline{a}\times\overline{b}+\overline{a}\times\overline{c}$ *[distributivité de $\times$ par rapport à $+$]*.

- Au vu des propriétés 1 à 4 on dit que $\big(\mathbb{Z}/n\mathbb{Z}, +\big)$ est **groupe commutatif**. Au vu des propriétés 1 à 8, on dit que $\big(\mathbb{Z}/n\mathbb{Z}, +, \times\big)$ est **un anneau commutatif**.
- Par analogie avec les nombres réels, $\overline{-a}$ est appelé **l'opposé** de $\bar{a}$ et se note $-\bar{a}$. Ceci permet

de définir une soustraction dans $\mathbb{Z}/n\mathbb{Z}$ en disant que « soustraire $\bar{a}$, c'est ajouter l'opposé de $\bar{a}$ » ; précisément on pose, pour toutes classes de congruence $\bar{a}, \bar{b}$:

$$\bar{b} - \bar{a} = \bar{b} + (-\bar{a}) = \bar{b} + \overline{-a}.$$

- Si une classe de congruence $\bar{a}$ admet un symétrique $\bar{b}$ pour la loi $\times$ (c'est à dire s'il existe $\bar{b}$ tel que $\bar{a} \times \bar{b} = \bar{1}$) on dit que $\bar{a}$ est **inversible**. Remarquons qu'un tel symétrique $\bar{b}$, s'il existe, est unique : en effet les égalités $\bar{a} \times \bar{b} = \bar{1}$ et $\bar{a} \times \bar{c} = \bar{1}$ impliquent

$$\bar{b} = \bar{b} \times \bar{1} = \bar{b} \times (\bar{a} \times \bar{c}) = (\bar{b} \times \bar{a}) \times \bar{c} = (\bar{a} \times \bar{b}) = \bar{1} \times \bar{c} = \bar{c}.$$

On dit alors que $\bar{b}$ est **l'inverse** de $\bar{a}$ et on le note $\bar{a}^{-1}$. Le résultat suivant explique quels sont les élements inversibles dans $\mathbb{Z}/n\mathbb{Z}$.

Théorème 1.4

*Soient $n \in \mathbb{N}^*$ et $a \in \mathbb{Z}$. Alors la classe de congruence $\bar{a}$ admet un inverse dans $\mathbb{Z}/n\mathbb{Z}$ si et seulement si $a \wedge n = 1$. Le nombre d'éléments inversibles dans $\mathbb{Z}/n\mathbb{Z}$ est noté $\varphi(n)$; on l'appelle **l'indicateur d'Euler** de n. En particulier, si n est un nombre premier alors tout élément $\bar{a} \neq \bar{0}$ de $\mathbb{Z}/n\mathbb{Z}$ admet un inverse et on a $\varphi(n) = n - 1$.*

On termine ce paragraphe par deux énoncés qui seront utiles pour les cryptosystèmes asymétriques RSA et El Gamal.

Théorème 1.5 (*petit théorème de Fermat*)

Soit p un nombre premier. Pour tout $a \in \mathbb{Z}$ on a $a^p \equiv a \mod p$; de plus, si $a \wedge p = 1$ alors on a aussi $a^{p-1} \equiv 1 \mod p$.

Théorème 1.6

Soit p un nombre premier. Alors il existe $\overline{g} \in \mathbb{Z}/p\mathbb{Z}$ tel que

$$\left\{\bar{1}, \bar{2}, \cdots, \overline{p-1}\right\} = \left\{\bar{g}^k \,|\, 0 \leq k \leq p-2\right\}.$$

1.3 Exemples de cryptosystèmes symétriques

Ce sont les systèmes pour lesquels la clef de l'expéditeur (Alice) et celle du destinataire (Bob) se déduisent facilement l'une de l'autre (et sont même éventuellement égales). Il est donc impératif de les conserver confidentielles toutes les deux.

Inconvénients :

- grand nombre de clefs nécessaires : 1 clef (au moins) pour 2 utilisateurs, 3 pour 3 utilisateurs, 6 pour 4 utilisateurs, de façon générale $\binom{n}{2} = n(n-1)/2$ clefs pour n utilisateurs.
- problème du transport des clefs.

Avantages : Les calculs sont en général rapides.

Dans toute la suite, on représentera chaque lettre de l'alphabet latin par un élément de $\mathbb{Z}/26\mathbb{Z}$: A par $\bar{0}$, B par $\bar{1}, \cdots$, Z par $\overline{25}$. On ignore les accents et tous les symboles qui ne sont pas des lettres. On pourrait bien sûr utiliser d'autres façons de représenter les lettres (et divers symboles) par des nombres, par exemple le code ASCII.

1.3.1 Chiffrements affines

Principe : La fonction de chiffrement est de la forme

$$\Phi : \begin{array}{ccc} \mathbb{Z}/26\mathbb{Z} & \to & \mathbb{Z}/26\mathbb{Z} \\ \bar{x} & \mapsto & \bar{a} \times \bar{x} + \bar{b} \end{array}$$

où $\bar{a}, \bar{b}$ sont choisis de telle façon que Φ soit bijective. La fonction de déchiffrement est alors la bijection réciproque de Φ.

Proposition 1.4

La fonction Φ ci-dessus est bijective si et seulement si $a \wedge 26 = 1$, c'est à dire si et seulement si $\bar{a}$ admet un inverse dans $\mathbb{Z}/26\mathbb{Z}$. Dans ce cas, la bijection réciproque de Φ est $\Phi^{-1}(\bar{x}) = \bar{a}^{-1} \times \bar{x} - \bar{a}^{-1} \times \bar{b}$.

La clef de chiffrement est le couple $(\bar{a}, \bar{b})$, celle de déchiffrement est $(\bar{a}^{-1}, -\bar{a}^{-1} \times \bar{b})$.

Remarque 1.1
- *Dans le cas particulier où $\bar{a} = \bar{1}$, on parle de **chiffrement de César**. Il consiste simplement à décaler toutes les lettres du message d'une même quantité.*
- *On peut construire de façon similaire des cryptosystèmes où le message est découpé en blocs de m lettres ($m \geq 2$). Par exemple, avec $m = 2$ il y a $26^2 = 676$ blocs possibles ; on fait correspondre à chaque bloc un élément de $\mathbb{Z}/676\mathbb{Z}$ et on procède au chiffrement avec une fonction affine bijective $\Phi : \mathbb{Z}/676\mathbb{Z} \to \mathbb{Z}/676\mathbb{Z}$.*

1.3.2 Chiffrement de Vigenère

Principe : Il s'agit d'une variante du code de César où le décalage varie d'une lettre à l'autre, en fonction de la clef de chiffrement.

- On choisit une clef de chiffrement K qui est mot dont le nombre de lettres est noté n : $\mathrm{K} = \bar{c}_1\bar{c}_2\cdots\bar{c}_n$ (où $n \geq 2$)

- On découpe le message clair en blocs de n lettres consécutives. Si nécessaire, on ajoute à la fin un certain nombre de X (ou toute autre lettre peu utilisée) pour que sa longueur devienne un multiple de n :

$$\underbrace{\bar{x}_1\bar{x}_2\cdots\bar{x}_n}_{\text{n lettres}}\underbrace{\bar{x}_{n+1}\bar{x}_{n+2}\cdots\bar{x}_{2n}}_{\text{n lettres}}\underbrace{\bar{x}_{2n+1}\bar{x}_{2n+2}\cdots\bar{x}_{3n}}_{\text{n lettres}}\cdots\cdots\underbrace{\bar{x}_{(k-1)n+1}\cdots\bar{x}_{kn}}_{\text{n lettres}}.$$

Le cryptogramme est alors $\bar{y}_1\bar{y}_2\cdots\cdots\bar{y}_{kn}$ où

$$\bar{y}_1 = \bar{x}_1 + \bar{c}_1, \bar{y}_2 = \bar{x}_2 + \bar{c}_2, \cdots, \bar{y}_{n+1} = \bar{x}_{n+1} + \bar{c}_1, \cdots, \bar{y}_{kn} = \bar{x}_{kn} + \bar{c}_n.$$

La clef de déchiffrement est simplement le mot K' constitué des opposés des lettres du mot K, c'est à dire $K' = -\bar{c}_1\ -\bar{c}_2\cdots-\bar{c}_n$.

1.3.3 Chiffrement de Hill

Principe : Il s'agit d'une méthode utilisant le calcul matriciel. Le message clair est découpé en blocs de deux lettres consécutives (si nécessaire, on ajoute à la fin une lettre peu utilisée, par exemple X, pour avoir un nombre pair de lettres). La fonction de chiffrement est de la forme

$$\Phi : \begin{array}{ccc} (\mathbb{Z}/26\mathbb{Z})^2 & \to & (\mathbb{Z}/26\mathbb{Z})^2 \\ \begin{pmatrix}\bar{x}\\ \bar{y}\end{pmatrix} & \mapsto & \begin{pmatrix}\bar{a} & \bar{b}\\ \bar{c} & \bar{d}\end{pmatrix}\begin{pmatrix}\bar{x}\\ \bar{y}\end{pmatrix} \end{array}$$

où $\bar{a}, \bar{b}, \bar{c}, \bar{d}$ sont choisis dans $\mathbb{Z}/26\mathbb{Z}$ de telle façon que Φ soit bijective ; la fonction de déchiffrement est alors la bijection réciproque Φ^{-1}.

Proposition 1.5

La fonction Φ ci-dessus est bijective si et seulement si $(ad - bc) \wedge 26 = 1$, c'est à dire si et seulement si $\overline{ad - bc}$ admet un inverse dans $\mathbb{Z}/26\mathbb{Z}$. Dans ce cas, en notant $\bar{\Delta} = \overline{ad - bc}$, la bijection réciproque de Φ est

$$\Phi^{-1}\begin{pmatrix}\bar{x}\\ \bar{y}\end{pmatrix} = \bar{\Delta}^{-1}\begin{pmatrix}\bar{d} & -\bar{b}\\ -\bar{c} & \bar{a}\end{pmatrix}\begin{pmatrix}\bar{x}\\ \bar{y}\end{pmatrix}.$$

Clef de chiffrement : $\left(\bar{a}, \bar{b}, \bar{c}, \bar{d}\right)$;
Clef de de déchiffrement $\left(\bar{\Delta}^{-1} \times \bar{d}, \bar{\Delta}^{-1} \times (-\bar{b}), \bar{\Delta}^{-1} \times (-\bar{c}), \bar{\Delta}^{-1} \times \bar{a}\right)$.

Remarque 1.2 *On peut démontrer qu'il y a* 157248 *clefs de chiffrement pour le codage de Hill (*$157248 = (2^2 - 1)(2^2 - 2)(13^2 - 1)(13^2 - 13)$*).*

1.4 Exemples de cryptosystèmes asymétriques

Avec ce type de systèmes, chaque utilisateur dispose de deux clefs ; l'une est publique et l'autre est privée (c'est à dire secrète). Si Alice veut chiffrer un message clair m à destination de Bob, elle utilise la clef publique de Bob (que l'on désignera par $pu(B)$) et lui envoie $\Phi_{pu(B)}(m)$ où $\Phi_{pu(B)}$ est la fonction de chiffrement paramétrée par la clef publique de Bob. Ce dernier retrouve le message clair à l'aide de la fonction de déchiffrement $\Psi_{pr(B)}$ paramétrée par sa clef privée $pr(B)$: $\Psi_{pr(B)}\big(\Phi_{pu(B)}(m)\big) = m$.

Avantages :
- seulement $2n$ clefs sont nécessaires pour n utilisateurs du système ;
- pas de problème de transport de clef.

Inconvénients : calculs plus coûteux que pour les systèmes symétriques.

1.4.1 Le système RSA

Du nom des inventeurs Rivest, Shamir, Adleman (1977).

Principe : Il repose sur les faits suivants :

- d'une part, dans $\mathbb{Z}/n\mathbb{Z}$, la fonction « élévation à la puissance k » (où $k \in \mathbb{N}^*$) est « une fonction à sens unique ». Cela signifie qu'il est facile et rapide de calculer $\bar{x}^k$ pour tout $\bar{x} \in \mathbb{Z}/n\mathbb{Z}$ mais qu'il est difficile de retrouver $\bar{x}$ à partir de $\bar{x}^k$ et de k (sauf si l'on dispose d'une information supplémentaire, la clef secrète).

- d'autre part, la factorisation d'un entier en produit de facteurs premiers est aussi un problème difficile, coûteux en temps de calcul.

Alice veut chiffrer un message à destination de Bob. Ce dernier choisit deux (très grands) nombres premiers p et q, ainsi qu'un entier $e \geq 2$ premier avec $(p-1)(q-1)$. À l'aide de l'algorithme d'Euclide, il calcule un entier $d \geq 1$ vérifiant $de \equiv 1 \mod (p-1)(q-1)$.

Clef publique de Bob : $pu(B) = (n, e)$ où l'on a posé $n = pq$.
Clef privée de Bob : $pr(B) = d$.

L'ensemble des messages clairs ainsi que celui des messages chiffrés est $\mathbb{Z}/n\mathbb{Z}$. Alice chiffre $\bar{x} \in \mathbb{Z}/n\mathbb{Z}$ à l'aide de la fonction de chiffrement

$$\Phi_{pu(B)} : \begin{array}{ccc} \mathbb{Z}/n\mathbb{Z} & \to & \mathbb{Z}/n\mathbb{Z} \\ \bar{x} & \mapsto & \bar{x}^e \end{array}.$$

Elle envoie donc le cryptogramme $\bar{y} = \Phi_{pu(B)}(\bar{x})$ à Bob. Celui-ci calcule alors $\Psi_{pr(B)}(\bar{y})$, où

$$\Psi_{pr(B)} : \begin{array}{ccc} \mathbb{Z}/n\mathbb{Z} & \to & \mathbb{Z}/n\mathbb{Z} \\ \bar{y} & \mapsto & \bar{y}^d. \end{array}$$

La proposition suivante dit que Bob retrouve bien ainsi le message clair :

Proposition 1.6

Avec les notations précédentes, on a

$$\forall \bar{x} \in \mathbb{Z}/n\mathbb{Z} \qquad \Psi_{pr(B)}\big(\Phi_{pu(B)}(\bar{x})\big) = \bar{x} \quad \textit{et} \quad \Phi_{pu(B)}\big(\Psi_{pr(B)}(\bar{x})\big) = \bar{x}.$$

Autrement dit, $\Phi_{pu(B)}$ et $\Psi_{pr(B)}$ sont des bijections réciproques l'une de l'autre.

Si une tierce personne (Eve) intercepte le message chiffré $\bar{y} = \Phi_{pu(B)}(\bar{x})$, elle ne pourra pas calculer $\bar{x}$ à partir de $\bar{y}$ ni retrouver la clef privée d car le calcul de cette dernière nécessite la connaissance de p et q.

Le protocole RSA avec signature.

Il permet à Bob qui reçoit le message de s'assurer de l'identité de l'expéditeur Alice. Pour cela, chacun des deux individus dispose d'un jeu de clefs RSA comme vu ci-dessus :

clef publique d'Alice : $pu(A) = (n_A, e_A)$; clef privée d'Alice : $pr(A) = d_A$;
clef publique de Bob : $pu(B) = (n_B, e_B)$; clef privée de Bob : $pr(B) = d_B$.

On dispose donc des fonctions $\Phi_{pu(A)}, \Psi_{pu(A)} : \mathbb{Z}/n_A\mathbb{Z} \to \mathbb{Z}/n_A\mathbb{Z}$ qui sont des bijections réciproques l'une de l'autre et de même pour les fonctions $\Phi_{pu(B)}, \Psi_{pu(B)} : \mathbb{Z}/n_B\mathbb{Z} \to \mathbb{Z}/n_B\mathbb{Z}$.

Le message clair est un élément $\bar{x}$ de $\mathbb{Z}/n_B\mathbb{Z}$; la « signature » d'Alice est un élément $\tilde{s}$ de $\mathbb{Z}/n_A\mathbb{Z}$ propre à cet individu. Alice envoye à Bob le cryptogramme

$$(\bar{y}, \tilde{z}) = \big(\Phi_{pu(B)}(\bar{x}), \Psi_{pr(A)}(\tilde{s})\big).$$

À la réception de ce cryptogramme, Bob calcule $\big(\Psi_{pr(B)}(\bar{y}), \Phi_{pu(A)}(\tilde{z})\big)$. Comme dans le cadre du protocole RSA simple, on a $\Psi_{pr(B)}(\bar{y}) = \Psi_{pr(B)}(\Phi_{pu(B)}(\bar{x})) = \bar{x}$ donc Bob retrouve le message clair $\bar{x}$; de plus $\Phi_{pu(A)}(\tilde{z}) = \Phi_{pu(A)}(\Psi_{pr(A)}(\tilde{s})) = \tilde{s}$ donc Bob voit la signature d'Alice, et seulement Alice a pu expédier ce message car le chiffrement de $\tilde{s}$ en $\tilde{z}$ nécessite la clef privée $pr(A)$.

1.4.2 Le système El Gamal

Principe : Il repose sur le fait que, si p est un (grand) nombre premier et $\bar{x}$ est un élément non nul de $\mathbb{Z}/p\mathbb{Z}$, la fonction

$$\begin{array}{ccc} \mathbb{N}^* & \to & \mathbb{Z}/p\mathbb{Z} \\ n & \mapsto & \bar{x}^n \end{array}$$

est « une fonction à sens unique » : il est facile et rapide de calculer $\bar{x}^n$ pour tout $n \in \mathbb{N}^*$ mais il est long et difficile de retrouver n à partir de $\bar{x}^n$ (c'est ce qu'on appelle le problème du logarithme discret). On note par la suite

$$\big(\mathbb{Z}/p\mathbb{Z}\big)^* = \mathbb{Z}/p\mathbb{Z} \setminus \{\bar{0}\} = \big\{\bar{1}, \bar{2}, \cdots, \overline{p-1}\big\}.$$

Alice veut chiffrer et envoyer un message à Bob. Ce dernier choisit un (très grand) nombre premier p et détermine un élément $\bar{g} \in \big(\mathbb{Z}/p\mathbb{Z}\big)^*$ donné par le théorème 1.6, c'est à dire tel que

$$\big(\mathbb{Z}/p\mathbb{Z}\big)^* = \big\{\bar{g}^k \,|\, 0 \leq k \leq p-2\big\}.$$

Il choisit aussi un entier $s \in \{1, \cdots, p-2\}$. De son coté, Alice choisit au hasard un nombre entier $k \in \{1, \cdots, p-2\}$.

Clef publique de Bob : $pu(B) = (\bar{g}, \bar{g}^s)$;
Clef privée de Bob : $pr(B) = s$.

L'ensemble de messages clairs est $\big(\mathbb{Z}/p\mathbb{Z}\big)^*$, celui des cryptogrammes est $\Big(\big(\mathbb{Z}/p\mathbb{Z}\big)^*\Big)^2$. Alice chiffre $\bar{x} \in \big(\mathbb{Z}/p\mathbb{Z}\big)^*$ à l'aide de la fonction de chiffrement

$$\Phi_{pu(B)} : \begin{array}{ccc} \big(\mathbb{Z}/p\mathbb{Z}\big)^* & \to & \Big(\big(\mathbb{Z}/p\mathbb{Z}\big)^*\Big)^2 \\ \bar{x} & \mapsto & \big(\bar{g}^k, \bar{x} \times \big(\bar{g}^s\big)^k\big) \end{array}.$$

Elle fait donc parvenir le couple $(\bar{y}, \bar{z}) = \big(\bar{g}^k, \bar{x} \times \big(\bar{g}^s\big)^k\big)$ à Bob ; ce dernier calcule alors

$$\Psi_{pr(B)}\big(\bar{g}^k, \bar{x} \times \big(\bar{g}^s\big)^k\big)$$

avec la fonction de déchiffrement

$$\Psi_{pr(B)} : \begin{array}{ccc} \big(\mathbb{Z}/p\mathbb{Z}\big)^* \times \big(\mathbb{Z}/p\mathbb{Z}\big)^* & \to & \big(\mathbb{Z}/p\mathbb{Z}\big)^* \\ (\bar{y}, \bar{z}) & \mapsto & \big(\bar{y}^s\big)^{-1} \times \bar{z} \end{array}.$$

La proposition suivante dit que Bob retrouve bien ainsi le message clair $\bar{x}$ d'origine :

Proposition 1.7

Avec les notations précédentes, on a

$$\forall \bar{x} \in \left(\mathbb{Z}/p\mathbb{Z}\right)^* \qquad \Psi_{pr(B)}\big(\Phi_{pu(B)}(\bar{x})\big) = \bar{x}.$$

1.5 Feuilles d'exercices

IUT de Villetaneuse **Année 2023-2024**
But Passerelle Informatique - Science des données

Introduction à la cryptographie (TD 1)

Exercice 1. Effectuer les divisions euclidiennes de
a) 78 par 21 ; b) 1693 par 214 ; c) -151 par -30 ; d) 77 par -16.

Exercice 2. Traduire en termes de congruences les propriétés « être un entier pair » et « être un entier impair ».

Exercice 3. 1) En utilisant la compatibilité des relations de congruence avec l'addition et la multiplication des entiers, vérifier que $13 + 7 \times 22 \equiv 3 \mod 4$.
2) Calculer le reste de $13 + 7 \times 22 + (8 \times 42 + 25)^3$ dans la division euclidienne par 4.

Exercice 4. 1) Déterminer, en fonction de $n \in \mathbb{N}$, le reste de la division euclidienne de 2^n par 10. En déduire le chiffre des unités de 12^{2023}.

Exercice 5. Étant donné un entier $n \in \mathbb{N}^*$, calculer le reste de la division euclidienne de $\sum_{k=1}^{n} k$ par n.

Exercice 6. 1) Calculer $\bar{1} + \bar{2} + \cdots + \bar{8}$ dans $\mathbb{Z}/8\mathbb{Z}$.
2) Calculer $\bar{1} + \bar{2} + \cdots + \bar{9}$ dans $\mathbb{Z}/9\mathbb{Z}$.
3) En vous inspirant des questions précédentes, calculer de façon générale $\bar{1} + \bar{2} + \cdots + \bar{n}$ dans $\mathbb{Z}/n\mathbb{Z}$.

Exercice 7. 1)
a) Écrire les tables de l'addition et de la multiplication dans $\mathbb{Z}/4\mathbb{Z}$, en choisissant pour chaque classe de congruence $\bar{x}$ le représentant x entre 0 et 3.
b) Quels sont les éléments inversibles dans $\mathbb{Z}/4\mathbb{Z}$?
c) Dans $\mathbb{Z}/4\mathbb{Z}$, a-t-on : $(\bar{x} \times \bar{y} = \bar{0}) \Rightarrow (\bar{x} = \bar{0}$ ou $\bar{y} = \bar{0})$?
c) Résoudre dans $\mathbb{Z}/4\mathbb{Z}$ l'équation $\bar{x}^2 = \bar{3}$.
2) Mêmes questions dans $\mathbb{Z}/5\mathbb{Z}$ et dans $\mathbb{Z}/6\mathbb{Z}$.

Exercice 8.
1) Montrer que si n est un entier impair alors $n^2 \equiv 1 \mod 8$.
2) Montrer que si n est un entier pair alors $n^2 \equiv 0 \mod 8$ ou $n^2 \equiv 4 \mod 8$.
3) Quels couples d'entiers $(x, y) \in \mathbb{Z}^2$ vérifient $x^2 + y^2 \equiv 2 \mod 8$?

Exercice 9. Soit $n \in \mathbb{N}$ dont l'écriture en base 10 est $n = \overline{a_k a_{k-1} \cdots a_1 a_0}$.
1) Vérifier que $10 \equiv 1 \mod 9$ et que $10 \equiv -1 \mod 11$.
2) a) Montrer à l'aide du 1) que $n \equiv \sum_{i=0}^{k} a_i \mod 9$ et que $n \equiv \sum_{i=0}^{k} (-1)^i a_i \mod 11$. b) En déduire un critère de divisibilité par 9 et un critère de divisibilité par 11.
3) Les entiers 2768, 64669, 9655569 sont-ils divisibles par 9 ? par 11 ?

Exercice 10. 1) a) Appliquer l'algorithme d'Euclide aux entiers $a = 71$ et $b = 19$. Combien vaut $71 \wedge 19$? Pouvait-on trouver ce pgcd par un autre argument ?
b) En déduire deux entiers u, v satisfaisant l'égalité de Bézout $71u + 19v = 1$.
2) Appliquer l'algorithme d'Euclide aux entiers $a = 240$ et $b = -36$. En déduire $240 \wedge (-36)$ ainsi que deux entiers u, v satisfaisant $240u - 36v = 240 \wedge (-36)$.

Introduction à la cryptographie (TD 2)

Exercice 1. 1) Combien a-t-on de clefs de chiffrement pour un chiffrement affine comme dans le paragraphe 1.3.1 du cours ?
2) Convenez d'une clef avec votre voisin, envoyez-vous mutuellement un (court) message chiffré et déchiffrez le message que vous avez reçu.
3) Vous avez intercepté le cryptogramme suivant :

KNDPTKVMIVDPPXTOVHNOVIHVZVPPTJV

Retrouvez le message clair sachant qu'il a été chiffré avec un chiffrement affine et en utilisant le document sur la fréquence d'apparition des lettres et des bigrammes dans la langue française.

Exercice 2. Chiffrez le message clair « rendez-vous la semaine prochaine » avec le chiffrement de Vigenère et en utilisant la clef « iut ».

Exercice 3. Le but de cet exercice est de retrouver le message clair correspondant au cryptogramme

QXMYSU TLKWXA WLUXAK HLUOGB FUVXYK QLELVQ SWYGUT LKWXHH
TEQTHB KXELLL DELOMY ABUKZA BZKQNM SANRXZ WFEZHM JEGKAS NBAWQT
XUVDOB AKFONA AZDBCA PUTKJA IMHDMV BLSXAE PTQRML WFAEHK
GRXAWP ELHHQR LVFZEM VMFIGK AHIWBS PRHPLM UGLFMT BVFMLB AWFONA
WBEKZG ZNXHME SBIAQN LLMXEJ BWZCHS DQCMPN UTXHVD OBASXA IYGBRB
LLQTHB LQPXYK ANGLSP RHPLML TSANEK AWPEKL MZIHUW FDTZKA CBHLUO
GWSOIY PIGEL

sachant que ce dernier a été obtenu par un chiffrement de Vigenère.
1) Peut-on utiliser directement l'analyse des fréquences des lettres dans la langue française pour déchiffrer ce texte ?
2) **Première étape : recherche de la longueur de la clef.** La méthode décrite ici est appelée *test de Kasiski*. On note n le nombre de lettres de la clef de chiffrement.

a) Justifier que si un mot se trouve au moins $n+1$ fois dans le texte clair, alors il sera chiffré au moins deux fois par la même suite de symboles. Que peut-on dire de l'écart entre deux répétitions d'une même suite de symboles dans le cryptogramme si elles proviennent du chiffrement d'un même mot du texte clair ?

b) Repérez dans le texte chiffré des groupes de lettres consécutives se répétant au moins deux fois ; en déduire la longueur (probable) de la clef ayant servi pour obtenir ce cryptogramme.
3) **Deuxième étape : analyse des fréquences des lettres.** Supposons connue la longueur n de la clef de chiffrement. On découpe le cryptogramme en n parties de la façon suivante :

- la première partie contient les lettres numéro $1, n+1, 2n+1, \cdots$;
- la seconde partie contient les lettres numéro $2, n+2, 2n+2, \cdots$;
- la troisième partie contient les lettres numéro $3, n+3, 2n+3, \cdots$;

  etc

a) Pourquoi peut-on analyser la fréquence des lettres dans chacune des parties ainsi définies ?
b) En déduire les clefs de chiffrement et de déchiffrement.
c) Déchiffrez le cryptogramme ci-dessus.

Exercice 4.
1) Vérifier que la fonction Φ définie pour le chiffrement de Hill est bijective si l'on prend $a = 9, b = 2, c = 6, d = 3$.
2) Calculer alors la clef de déchiffrement.
3) Envoyez un (court) message chiffré à votre voisin et déchiffrez celui qu'il vous a envoyé.
4) Déchiffrez le cryptogramme DAEOMFTCEUFICAUAIUZFFMHNMEUMFIDAAV

Exercice 5. Le cryptosystème RSA est notamment utilisé pour l'échange de données confidentielles sur internet, par exemple des informations bancaires pour le commerce électronique. Pour simplifier, nous supposerons par la suite qu'un numéro de compte bancaire est un nombre entier entre 0 et 99.

1) Un individu A effectue un achat en ligne auprès d'une société B ; il lui transmet pour cela son numéro de compte bancaire qui sera crypté avec le système RSA. La clef publique de la société B est $pu(B) = (n, e)$ avec $n = 119$ et $e = 25$. Dans toute la suite, $\bar{x}$ désigne la classe de congruence d'un entier x modulo 119.

a) Trouvez les nombres premiers p, q tels que $p \times q = 119$, vérifier que 25 est bien premier avec $(p-1) \times (q-1)$ puis calculer la clef privée de B.

b) Si le numéro de compte bancaire de A est 58, quel cryptogramme reçoit B ?

c) Si B reçoit le cryptogramme $\overline{48} \in \mathbb{Z}/119\mathbb{Z}$, quel est le numéro de compte de A ?

2) On suppose dans cette question que A et B communiquent avec le protocole de signature RSA. Le client A a pour clef publique $(n_A, e_A) = (143, 77)$, son numéro de compte est 58 et sa signature est le nombre 10. Pour faire la distinction avec les classes modulo 119, on notera $\tilde{x}$ la classe d'un entier x module 143.

a) Trouver la clef privée de A

b) L'entreprise B reçoit une commande au nom de A et accompagnée du cryptogramme $(\overline{44}, \widetilde{27})$. Est-ce vraiment A qui a passé cette commande ?

Exercice 6. Trois personnes A, B, C échangent des informations cryptées à l'aide du système RSA. On note $pu(A) = (n_A, e_A)$, $pu(B) = (n_B, e_B)$ les clefs publiques de A et B, et $pr(A) = d_A$, $pr(B) = d_B$ leurs clefs privées. On suppose que $n_A = n_B = n$ et de plus que $e_A \wedge e_B = 1$. L'individu C envoie le même message à A et à B. En utilisant le théorème de Bézout, montrer que si une quatrième personne intercepte les cryptogrammes destinés à A et B, alors elle pourra retrouver le message clair de C. Quelle précaution cela suggère pour l'utilisation du cryptosystème RSA ?