R3.09 - Cryptographie et sécurité
Cours 1 - Arithmétique pour la cryptographie classique

L. Naert, T. Godin, T. Ferragut

Merci à A. Ridard pour ce cours !

A propos de ce document

- Pour naviguer dans le document, vous pouvez utiliser :
  - le menu (en haut à gauche)
  - l'icône en dessous du logo IUT
  - les différents liens
- Pour signaler une erreur, vous pouvez envoyer un message à l'adresse suivante : lucie.naert@univ-ubs.fr

Plan du cours

Introduction

La cryptologie signifie "science du secret". Elle est composée de deux branches :

- la **cryptographie** qui étudie les techniques pour rendre un message secret et
- la **cryptanalyse**, qui s'attache aux techniques permettant l'opération inverse : retrouver le message initial à partir d'un "message secret".

En travaux pratiques, nous ferons à la fois de la cryptographie et de la cryptanalyse.

Organisation de la ressource

Par semaine :

- 1 TD en classe entière : apports de cours et exercices sur feuille
- 1 TP en demi-groupe : Mise en pratique de techniques de cryptographie et cryptanalyse en Python sur des jupyter Notebook

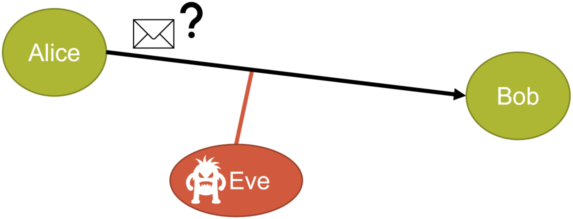
Les TP sont à rendre régulièrement.

Évaluation

- Contrôle terminal en semaine 3
- Un TP sera évalué et donnera lieu à un bonus/malus allant de -2 à +2 point sur la note du contrôle terminal.

Pourquoi la cryptographie ?

Un expéditeur (souvent appelé "Alice" dans la littérature) souhaite envoyer un message à un destinataire ("Bob") via un canal peu sûr sans qu'un étranger ("Eve" ou "Oscar") puisse lire et/ou modifier le message. Comment Alice doit-elle s'y prendre ?



Terminologie

Définition (message chiffré)

Le **chiffrement** est l'opération visant à protéger un message de manière à ce qu'il ne puisse être lu et/ou modifié que par les personnes disposant de la clef de déchiffrement. Le message résultant d'un chiffrement est appelé **message chiffré**.

Définition (message en clair)

Un **message en clair** est un message non chiffré.

Terminologie (suite)

Définition (Déchiffrer)

Déchiffrer un message (chiffré), c'est retrouver le message en clair initial **en utilisant la clef de déchiffrement**.

Définition (Décrypter)

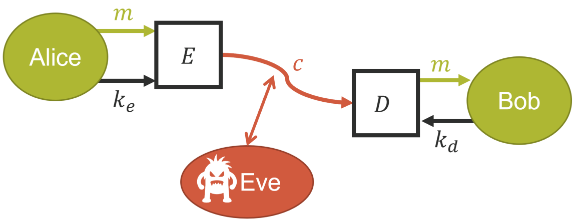
Décrypter un message (chiffré), c'est retrouver le message en clair initial **sans utiliser la clef de déchiffrement**.

Crypter VS chiffrer

Si l'on suit cette logique, "crypter" reviendrait à rendre un message secret **sans clef de chiffrement** ce qui n'est pas raisonnable puisque cela empêcherait le déchiffrement. Utiliser "crypter" à la placer de "chiffrer" est donc un abus de langage.

Notations

- Message en clair, m
- Message chiffré, c
- Fonction de chiffrement (*encryption*),E
- Fonction de déchiffrement (*decryption*), D
- Clef de chiffrement, k_e
- Clef de déchiffrement, k_d



Et les maths ?

Pour définir nos fonctions de chiffrement/déchiffrement, nous allons avoir besoin de quelques connaissances mathématiques !

Sauf mention contraire, a et b désignent des entiers relatifs.

Définition

On dit que a *divise* b ou que a est un *diviseur* de b ou que b est un *multiple* de a si :

$$\exists k \in \mathbb{Z}, b = ka$$

Notations

- Si a divise b, on note : $a|b$
- L'ensemble des diviseurs de b est noté $\mathscr{D}(b)$
- L'ensemble des multiples de a est noté $a\mathbb{Z}$

Exemples

1. Déterminer $\mathscr{D}(12)$, $\mathscr{D}(10)$, $\mathscr{D}(1)$ et $\mathscr{D}(0)$
2. Donner quelques éléments de $10\mathbb{Z}$, $1\mathbb{Z}$, $0\mathbb{Z}$

Cas particuliers

- 1 et -1 divisent tous les entiers mais ne sont divisibles que par 1 et -1
- 0 est multiple de tous les entiers mais n'est diviseur que de lui-même

Relation d'ordre

La relation de divisibilité dans $\mathbb{Z}$ est réflexive et transitive mais n'est pas une relation d'ordre car elle n'est pas antisymétrique, contrairement à la divisibilité dans $\mathbb{N}$. D'ailleurs, pour cet ordre (partiel), le plus petit élément est 1 et le plus grand est 0. Enfin, la divisibilité dans $\mathbb{N}^*$ est liée à l'ordre (total) naturel de $\mathbb{N}^*$: $a|b \Rightarrow a \leq b$ (la réciproque est fausse !)

Propriété (division euclidienne)

Si b est non nul, alors il existe un unique couple $(q,r) \in \mathbb{Z}^2$ tel que :

$$a = bq + r \qquad \text{avec} \quad 0 \leq r < |b|$$

Vocabulaire

Déterminer les entiers q et r, c'est effectuer la division euclidienne de a par b.
a est le *dividende*, b le *diviseur*, q le *quotient* et r le *reste*.

Exemples

1. Effectuer la division euclidienne de 56 par 17
2. Effectuer la division euclidienne de -56 par 17
3. Effectuer la division euclidienne de 32 par -7

Définition (pgcd)

Soit $(a,b) \neq (0,0)$.
Le Plus Grand Commun Diviseur de a et b, noté $pgcd(a,b)$, est le plus grand entier positif qui divise à la fois a et b.

Propriété (théorème de Bézout)

Si $(a,b) \neq (0,0)$, alors il existe un couple $(u,v) \in \mathbb{Z}^2$ tel que :

$$ua + vb = pgcd(a,b)$$

⚠ Le couple (u,v) dans l'identité de Bézout n'est pas unique.

Exemple

1. Déterminer $pgcd(12{,}10)$.
2. Trouver une identité de Bézout entre 12 et 10.
3. En déduire une autre identité.

Algorithme d'Euclide étendu

Il permet de calculer simultanément $pgcd(a,b)$ et deux entiers u et v tels que :

$$au + bv = pgcd(a,b)$$

On peut supposer $a \geq b > 0$ sans perdre en généralité [a].

On calcule une suite $(r_k)_{k\in\mathbb{N}}$ de restes obtenus par divisions euclidiennes successives à partir de $r_0 = a$ et $r_1 = b$:

- $r_0 = r_1 q_1 + r_2$ avec $0 \leq r_2 < r_1$
- $r_1 = r_2 q_2 + r_3$ avec $0 \leq r_3 < r_2$
- ...
- $r_{k-2} = r_{k-1} q_{k-1} + r_k$ avec $0 \leq r_k < r_{k-1}$
- $r_{k-1} = r_k q_k + r_{k+1}$ avec $0 \leq r_{k+1} < r_k$

Ainsi que deux suites $(u_k)_{k\in\mathbb{N}}$ et $(v_k)_{k\in\mathbb{N}}$ définies par une récurrence d'ordre 2 :

- $\begin{cases} u_0 = 1,\ u_1 = 0 \\ \forall k \in \mathbb{N}^*,\ u_{k+1} = u_{k-1} - u_k q_k \end{cases}$
- $\begin{cases} v_0 = 0,\ v_1 = 1 \\ \forall k \in \mathbb{N}^*,\ v_{k+1} = v_{k-1} - v_k q_k \end{cases}$

a. Cela vient du fait que $pgcd(a,b) = pgcd(|a|,|b|)$ et $pgcd(a,0) = a$

Algorithme d'Euclide étendu (fin)

En notant r_n le dernier reste non nul [a], on a [b] :

$$pgcd(a,b) = pgcd(r_n, r_{n+1}) = pgcd(r_n, 0) = r_n = au_n + bv_n$$

Dans la pratique, on pourra utiliser un tableau pour effectuer les calculs :

k	r_k	u_k	v_k	q_k	
0	366	1	0		
1	56	0	1	6	$(366 = 6 \times 56 + 30)$
2	30	1	-6	1	$(56 = 1 \times 30 + 26)$
3	26	-1	7	1	$(30 = 1 \times 26 + 4)$
4	4	2	-13	6	$(26 = 6 \times 4 + 2)$
5	2	-13	85	2	$(4 = 2 \times 2 = 0)$
6	0				

On en tire :

$$pgcd(366, 56) = 2 \quad \text{et} \quad 2 = 366 \times (-13) + 56 \times 85$$

a. La suite des restes étant une suite strictement décroissante d'entiers positifs, on obtient nécessairement un reste nul au bout d'un nombre fini de divisions.

b. Cela repose sur les deux résultats suivants :

- Si r est le reste de la division euclidienne de a par b, alors $pgcd(a,b) = pgcd(b,r)$
- Pour tout $k \in \mathbb{N}$, $r_k = au_k + bv_k$

Exemples

- Déterminer une identité de Bézout entre 17 et 9
- Déterminer une identité de Bézout entre -48 et 27

Définition (entiers premiers entre eux)

On dit que a et b sont *premiers entre eux* si $pgcd(a,b) = 1$.

Propriété (caractérisation)

a et b sont *premiers entre eux* si et seulement s'il existe un couple $(u,v) \in \mathbb{Z}^2$ tel que :

$$ua + vb = 1$$

Preuve

Démontrer la propriété.

Lemme de Gauss

Montrer que si a divise bc tout en étant premier avec b, alors a divise c.

Définition (entier premier)

On dit qu'un entier $n \geq 2$ est *premier* si ses seuls diviseurs positifs sont 1 et lui même.

Propriété (décomposition en facteurs premiers)

Tout entier $n \geq 2$ admet une unique décomposition de la forme :

$$n = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_r^{\alpha_r}$$

où les p_k sont des nombres premiers vérifiant $p_1 < p_2 < \cdots < p_r$
et les α_k des entiers naturels non nuls.

Cette décomposition peut aussi s'écrire :

$$n = \prod_{p \in \mathscr{P}} p^{\alpha_p}$$

avec $\alpha_p = 0$ si $p \notin \{p_1, \dots, p_r\}$

Définition (ppcm)

Le Plus Petit Commun Multiple de a et b, noté $ppcm(a, b)$, est le plus petit entier strictement positif qui soit multiple de a et b.

Donner $ppcm(30,18)$ et $ppcm(-3,13)$

1. Décomposer en facteurs premiers 60 et 50.
2. Calculer puis décomposer en facteurs premiers :
   - $pgcd(50,60)$
   - $ppcm(50,60)$
3. Que remarquez-vous ?

Sauf mention contraire, n désigne un entier naturel, et a, b des entiers relatifs.

Définition (congruence modulo n)

On dit que a et b sont *congrus modulo* n s'ils ont le même reste dans la division euclidienne par n, autrement dit si $a-b$ est multiple de n ou encore s'il existe $k \in \mathbb{Z}$ tel que $a = b + kn$.

- Si a et b sont congrus modulo n, on note : $a \equiv b \mod n$
- La congruence modulo n est une relation d'équivalence sur $\mathbb{Z}$
- L'ensemble des classes d'équivalence est notée $\mathbb{Z}/n\mathbb{Z}$
- $\mathbb{Z}/n\mathbb{Z} = \left\{\overline{0}, \overline{1}, \ldots, \overline{n-1}\right\}$
- $\overline{a} = \overline{b} \Longleftrightarrow a \equiv b \mod n$
- Si r est le reste de la division euclidienne de a par n, alors $\overline{a} = \overline{r}$

1. Proposer un b tel que $12 \equiv b \mod 5$ et b positif
2. Proposer un b tel que $12 \equiv b \mod 5$ et b négatif
3. Donner quelques éléments positifs et négatifs de chacune des classes d'équivalence de $\mathbb{Z}/3\mathbb{Z}$

Propriété (la congruence respecte l'addition et la multiplication)

Si $a \equiv a' \mod n$ et si $b \equiv b' \mod n$, alors

$$\begin{array}{rcll} a+b & \equiv & a'+b' & \mod n \\ ab & \equiv & a'b' & \mod n \end{array}$$

- La congruence respecte aussi la puissance [a] :
  Si $a \equiv b \mod n$, alors $a^k \equiv b^k \mod n$
- On peut définir sur l'ensemble $\mathbb{Z}/n\mathbb{Z}$ une addition et une multiplication :

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

a. Les formules $a^{k+l} = a^k a^l$ et $a^{kl} = \left(a^k\right)^l$ sont encore valables modulo n

1. Pour tout $\overline{a} \in \mathbb{Z}/5\mathbb{Z}$, déterminer son opposé $-\overline{a}$.
2. Dresser la table de multiplication de $\mathbb{Z}/5\mathbb{Z}$.
3. Reprenez les questions précédentes avec $\mathbb{Z}/6\mathbb{Z}$.

Définition (inversible modulo n)

On dit que a est *inversible modulo* n s'il existe $b \in \mathbb{Z}$ tel que :

$$ab \equiv 1 \mod n$$

Dans ce cas, b est unique modulo n, appelé inverse de a modulo n et noté $a^{-1} \mod n$.

- 0 n'est jamais inversible modulo n, 1 l'est toujours
- On dit aussi que $\bar{a}$ est inversible dans $\mathbb{Z}/n\mathbb{Z}$ s'il existe $b \in \mathbb{Z}$ tel que $\bar{a}\bar{b} = \bar{1}$
- On note $(\mathbb{Z}/n\mathbb{Z})^*$ l'ensemble des inversibles de $\mathbb{Z}/n\mathbb{Z}$

- Contrairement à ce qui se passe dans $\mathbb{R}$, dans $\mathbb{Q}$, dans $\mathbb{C}$ ou tout autre « corps », un élément non nul de $\mathbb{Z}/n\mathbb{Z}$ n'est pas toujours inversible
- $\mathbb{R}^* = \mathbb{R} \setminus \{0\}$ mais $(\mathbb{Z}/n\mathbb{Z})^*$ n'est pas égal à $(\mathbb{Z}/n\mathbb{Z}) \setminus \{\bar{0}\}$ en général

1. A l'aide des tables de multiplication précédentes, déterminer les éléments inversibles et leurs inverses dans $\mathbb{Z}/5\mathbb{Z}$ et $\mathbb{Z}/6\mathbb{Z}$.
2. Comment peut-on expliquer cette différence ?

Propriété (CNS pour être inversible modulo n)

a est inversible modulo n si et seulement si $pgcd(a,n)=1$.

Dans ce cas, $a^{-1} \mod n$ est fourni par une identité de Bézout entre a et n :
si $au+nv=1$, alors $au \equiv 1 \mod n$ et donc $a^{-1} \equiv u \mod n$.

- L'algorithme d'Euclide étendu entre a et n permet de décider si a est inversible modulo n, mais aussi de calculer son inverse le cas échéant
- Si $n=p$ est premier, tout élément non nul de $\mathbb{Z}/p\mathbb{Z}$ est inversible et $(\mathbb{Z}/p\mathbb{Z})^* = (\mathbb{Z}/p\mathbb{Z}) \setminus \{\overline{0}\} = \left\{\overline{1},\overline{2},\ldots,\overline{p-1}\right\}$

En utilisant la propriété précédente, donner les éléments inversibles de $\mathbb{Z}/8\mathbb{Z}$.

1. Résoudre $x+2=0$ dans $\mathbb{Z}/5\mathbb{Z}$ puis dans $\mathbb{Z}/6\mathbb{Z}$.
2. Résoudre $3x+2=0$ dans $\mathbb{Z}/5\mathbb{Z}$ puis dans $\mathbb{Z}/6\mathbb{Z}$.
3. Résoudre $5x+4=1$ dans $\mathbb{Z}/6\mathbb{Z}$.
4. Résoudre $4x^2+2=0$ dans $\mathbb{Z}/5\mathbb{Z}$ puis dans $\mathbb{Z}/6\mathbb{Z}$.

1. 1 est toujours un carré mais combien possède-t-il de racines carrées dans $\mathbb{Z}/5\mathbb{Z}$? dans $\mathbb{Z}/6\mathbb{Z}$? dans $\mathbb{Z}/8\mathbb{Z}$?
2. Tous les éléments de $\mathbb{Z}/5\mathbb{Z}$ sont-ils des carrés ?

Inverser une matrice à l'aide de sa comatrice

Soit $A = \left(a_{ij}\right)_{1 \leq i,j \leq n}$ une matrice à coefficients dans un anneau commutatif K.

- Le cofacteur d'indice i,j de A est défini par :

$$(-1)^{i+j} \det\left(A_{i,j}\right)$$

  où $A_{i,j}$ est déduite de A en supprimant la i-ème ligne et la j-ème colonne.
- La matrice des cofacteurs, appelée comatrice, vérifie :

$$A\left(com(A)\right)^t = \left(com(A)\right)^t A = \det(A) I_n$$

Propriété (Inversion d'une matrice)

A est donc inversible si et seulement si $\det(A)$ est inversible dans K.
Dans ce cas, on a :

$$A^{-1} = \det(A)^{-1}\left(com(A)\right)^t$$

- $\mathbb{Z}/n\mathbb{Z}$ est un anneau commutatif
- Le deuxième point se démontre à l'aide des formules de Laplace [a] :
  - par rapport à la colonne j :

$$\det(A) = \sum_{i=1}^{n} (-1)^{i+j} \det\left(A_{i,j}\right)$$

  - par rapport à la ligne i :

$$\det(A) = \sum_{j=1}^{n} (-1)^{i+j} \det\left(A_{i,j}\right)$$

- Si K est un corps [b], $\det(A)$ est inversible si et seulement s'il est non nul.

---

a. Ces formules sont utilisées pour développer un déterminant selon une colonne ou une ligne
b. Par exemple, $\mathbb{R}$ ou $\mathbb{Z}/p\mathbb{Z}$ avec p premier

Propriété (Inversion du déterminant)

Si $K = \mathbb{Z}/n\mathbb{Z}$, $\det(A)$ est inversible si et seulement s'il est premier avec n

Inversion modulaire d'une matrice

1. Calculer $\begin{pmatrix} 3 & 2 \\ 4 & 6 \end{pmatrix}^{-1} \mod 21$
2. Calculer $\begin{pmatrix} 1 & 2 & 3 \\ 0 & 1 & 2 \\ -1 & -4 & -1 \end{pmatrix}^{-1} \mod 35$