R3.09 - Cryptographie et sécurité

L. Naert, T. Godin, S. Bouchelaghem

28 novembre 2025

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 CM de 45 min : apports de cours
- 1 TD en classe entière à partir de la deuxième semaine : 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 chaque semaine.

Évaluation

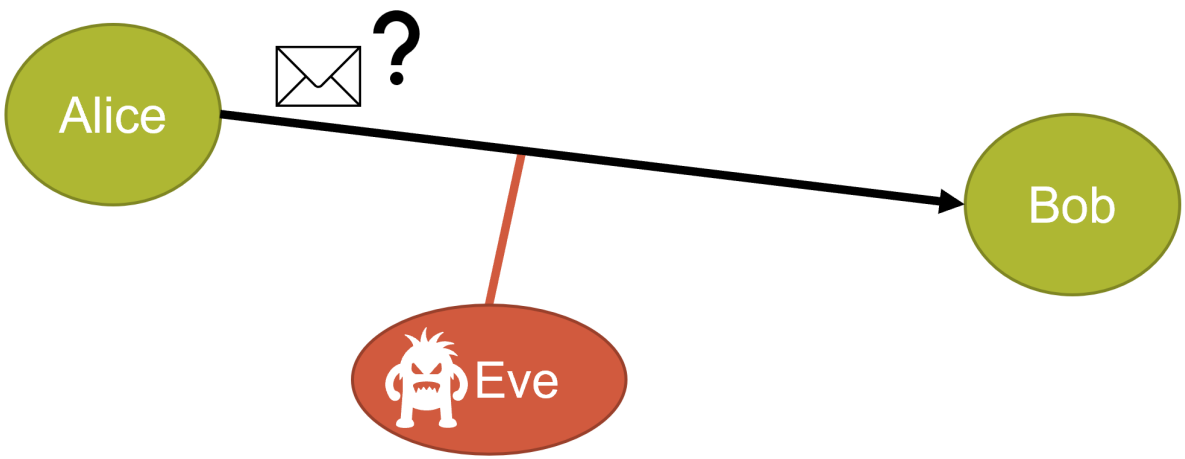
- Contrôle continu avec deux QCM
- Contrôle terminal en semaine 3
- Le retard et/ou l'absence de rendu de TP entraineront des malus qui seront reportés sur la note du contrôle terminal.

Usage de l'IA générative

En R3.09, pour encourager l'apprentissage et la réflexion personnelle, utiliser une intelligence artificielle générative (par exemple : ChatGPT, Copilot...) est **interdit** sauf mention contraire explicite.

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)

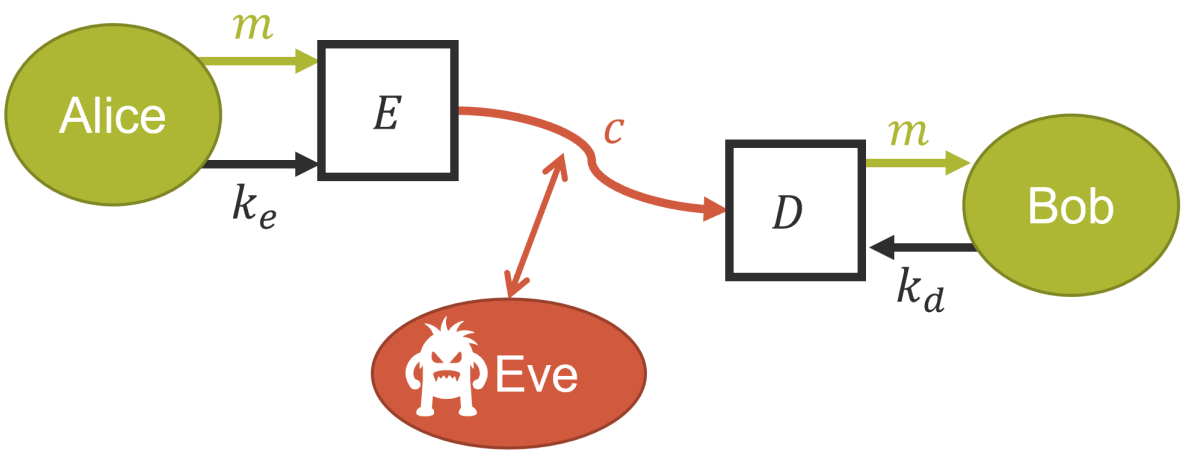
Décrypter un message (chiffré), c'est retrouver le message en clair initial **sans utiliser la clef de déchiffrement**.

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.

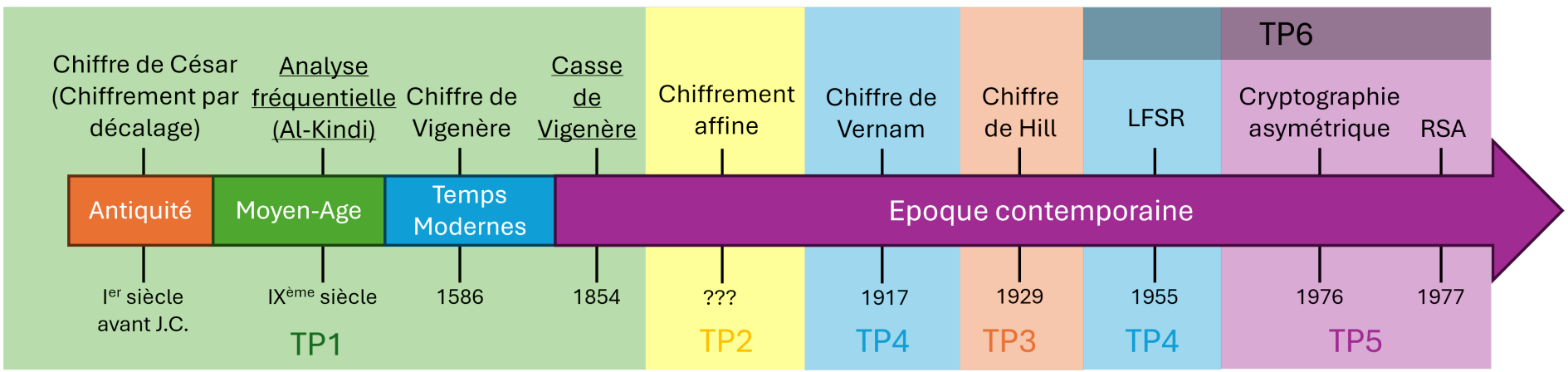
Notations

- 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



Chronologie

Voici un petit historique des différents chiffrements (et techniques de cryptanalyse quand soulignées) que nous allons étudier en cours et en TP. Les techniques de chiffrement plus modernes seront étudiées en R4.B.10 par les chanceux du parcours B.



Cryptographie symétrique et asymétrique

Il existe deux grands types de cryptographies :

- **La cryptographie symétrique** : la plus ancienne et souvent la plus rapide mais qui nécessite la transmission préalable d'une clef secrète.
- **La cryptographie asymétrique** : plus récente, plus sûre mais plus lente.

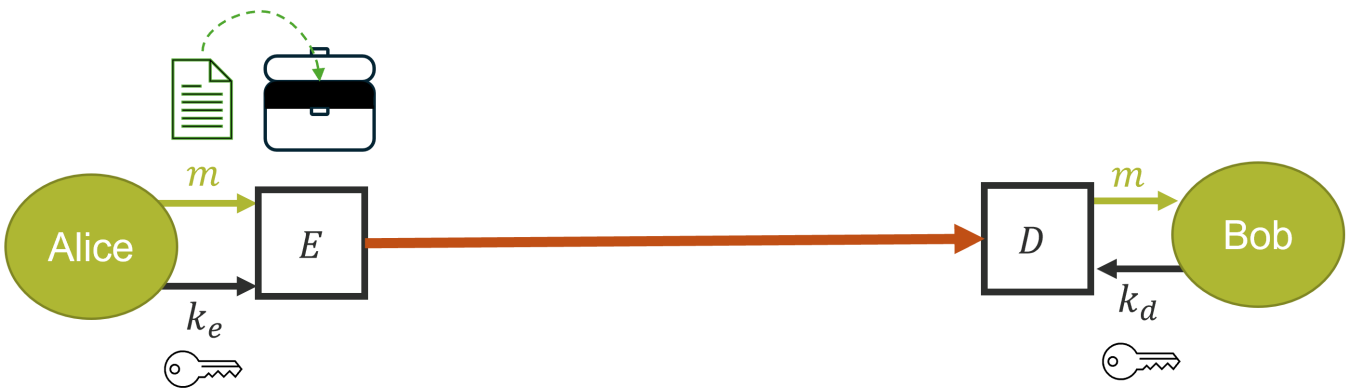
En travaux pratiques, nous étudierons d'abord diverses techniques de cryptographie symétrique (TP1, TP2, TP3, TP4) puis nous aborderons un exemple de cryptographie asymétrique avec le chiffrement RSA dans le TP5.

Cryptographie symétrique

Définition (Cryptographie symétrique)

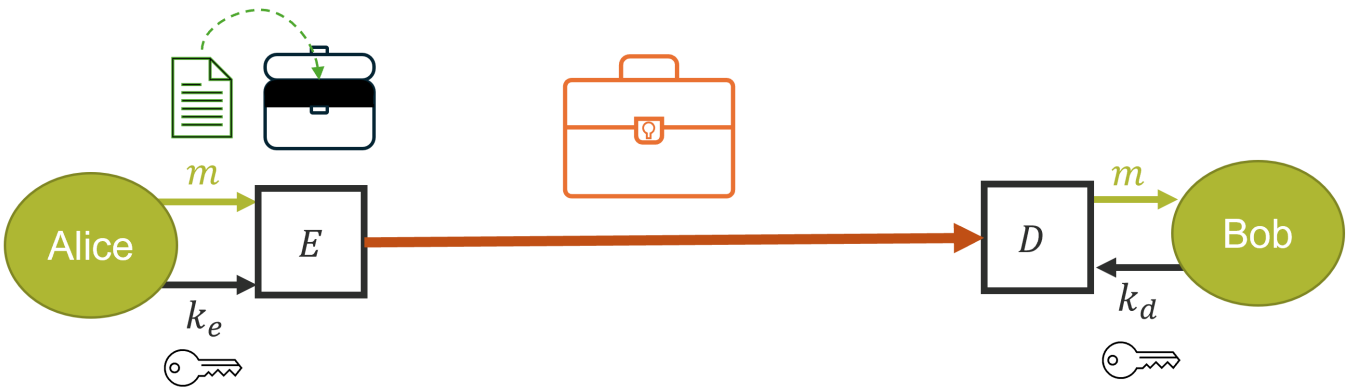
La cryptographie symétrique, aussi appelée "cryptographie à clef secrète" consiste à chiffrer et déchiffrer le message avec **la même clef de chiffrement**. Cette clef doit donc rester secrète.

Cryptographie symétrique



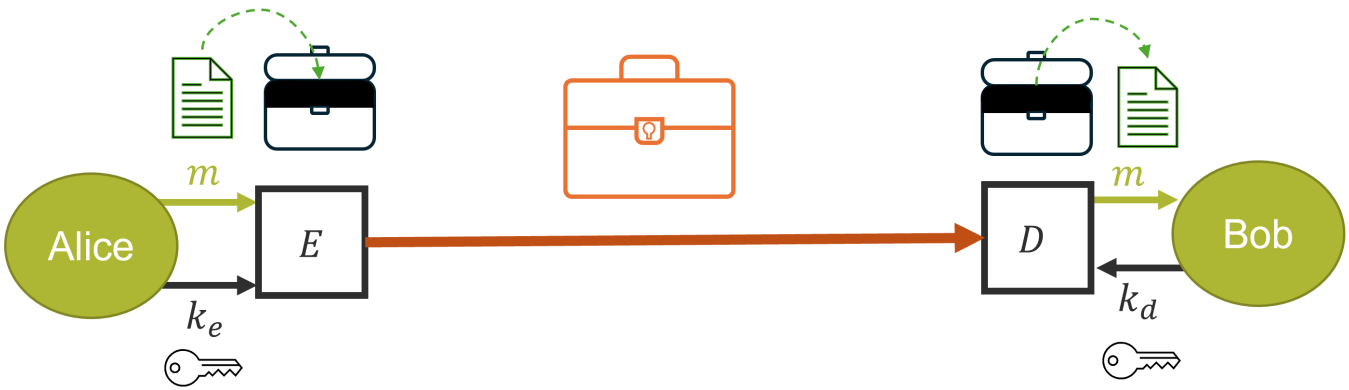
Chiffrement du message en clair avec une clef

Cryptographie symétrique



Transmission du message chiffré

Cryptographie symétrique



Déchiffrement du message chiffré avec la même clef : $k_d = k_e$

Un exemple ancien : le chiffrement par décalage

Une des méthodes de cryptographie les plus connues est celle utilisée par César dans ses correspondances secrètes. Celui-ci remplaçait chaque lettre de son message en clair par la lettre située trois places après dans l'alphabet.

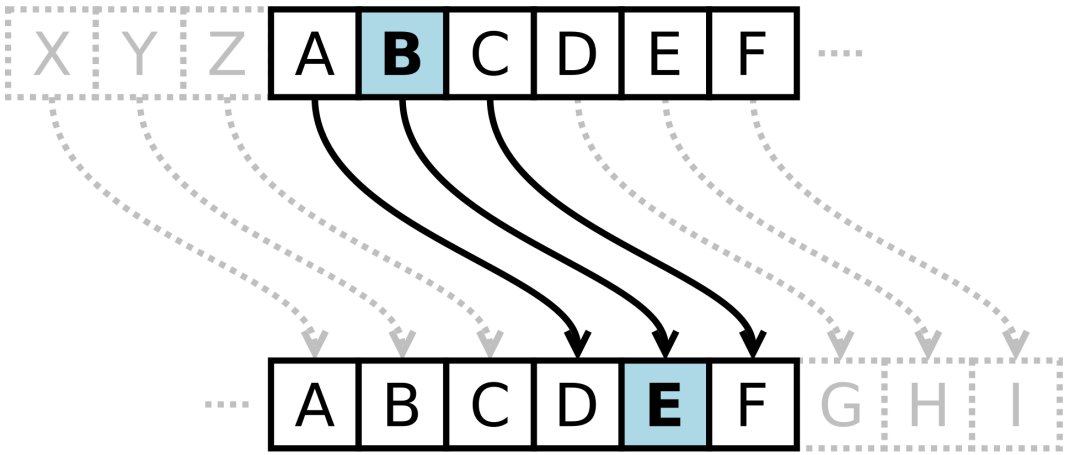


Figure – Décalage circulaire de 3 places dans le chiffre de César (source : Wikipedia, chiffrement par décalage)

Il s'agit d'un cas particulier de **chiffrement par décalage** qui consiste à décaler, dans un sens ou dans l'autre, les lettres de l'alphabet d'un nombre constant de position. **Ce nombre constitue la clef du chiffrement par décalage.**

Fonction de chiffrement par décalage

Soient k la clef de chiffrement, m_i la lettre de rang i du message en clair, et c_i la lettre de rang i du message chiffré. Dans le cas du chiffrement par décalage on peut écrire la fonction de chiffrement E_k de la façon suivante :

$$\begin{aligned} E_k : E &\to E \\ m_i &\mapsto c_i = m_i + k \end{aligned}$$

Fonction de chiffrement par décalage

Soient k la clef de chiffrement, m_i la lettre de rang i du message en clair, et c_i la lettre de rang i du message chiffré. Dans le cas du chiffrement par décalage on peut écrire la fonction de chiffrement E_k de la façon suivante :

$$E_k : E \to E$$
$$m_i \mapsto c_i = m_i + k$$

Mais à quel ensemble E doivent appartenir m_i et c_i pour que le décalage circulaire fonctionne ?

Fonction de chiffrement par décalage

Tout d'abord, coder chaque lettre par son rang dans l'alphabet permet de faciliter les calculs (a devient 0, b devient 1, ..., et z devient 25).
Supposons donc que $E = \{0, 1, 2, \ldots, 25\}$.

Fonction de chiffrement par décalage

Tout d'abord, coder chaque lettre par son rang dans l'alphabet permet de faciliter les calculs (a devient 0, b devient 1, ..., et z devient 25).
Supposons donc que $E = \{0, 1, 2, \ldots, 25\}$.

Cela n'est pas satisfaisant car, dans le chiffrement par décalage, on effectue un décalage circulaire, c'est à dire que z (donc 25) devrait être chiffré par un c (donc 2) si $k = 3$. Or, ce E n'est pas stable pour l'addition ($25 + 3 = 28 \notin E$). De plus $28 \neq 3$. Il nous faut un ensemble dans lequel $25 + 3 = 2$!

Fonction de chiffrement par décalage

Tout d'abord, coder chaque lettre par son rang dans l'alphabet permet de faciliter les calculs (a devient 0, b devient 1, ..., et z devient 25).
Supposons donc que $E = \{0, 1, 2, \ldots, 25\}$.

Cela n'est pas satisfaisant car, dans le chiffrement par décalage, on effectue un décalage circulaire, c'est à dire que z (donc 25) devrait être chiffré par un c (donc 2) si $k = 3$. Or, ce E n'est pas stable pour l'addition ($25 + 3 = 28 \notin E$). De plus $28 \neq 3$. Il nous faut un ensemble dans lequel $25 + 3 = 2$!

Cet ensemble se note $\mathbb{Z}/26\mathbb{Z}$.

Les maths pointent leur nez !

De façon plus générale, en cryptographie, nous travaillerons quasi exclusivement dans des ensembles du type $\mathbb{Z}/n\mathbb{Z}$ avec $n \in \mathbb{N}$.

Pour comprendre ce que signifie exactement cette notation, nous avons besoin de mathématiques et, plus précisément, de notions d'arithmétique modulaire.

Par la suite, sauf mention contraire, n désigne un entier naturel, et a, b 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 $a\mathbb{Z}$

Cas particuliers

- 1 et -1 divisent tous les entiers : $\forall m \in \mathbb{Z}, \{-1,1\} \subset \mathscr{D}(m)$
  mais ne sont divisibles que par 1 et -1 : $\mathscr{D}(1) = \mathscr{D}(-1) = \{-1,1\}$
- 0 est multiple de tous les entiers : $\forall m \in \mathbb{Z}, 0 \in m\mathbb{Z}$
  mais n'est diviseur que de lui-même : $\forall m \in \mathbb{Z}, 0 \in \mathscr{D}(m) \Rightarrow m = 0$

Par exemple :

- $\mathscr{D}(12) = \{-12, -6, -4, -3, -2, -1, 1, 2, 3, 4, 6, 12\}$
- $\mathscr{D}(1) = \{-1, 1\}$
- $\mathscr{D}(0) = \mathbb{Z}$
- $\{-10, 0, 10, 20\} \subset 10\mathbb{Z}$
- $0\mathbb{Z} = \{0\}$
- $1\mathbb{Z} = \mathbb{Z} = -1\mathbb{Z}$

Propriété (division euclidienne)

La division euclidienne de a (appelé **dividende**) par b (appelé **diviseur**) est définie de la manière suivante :
Il existe un unique $q \in \mathbb{Z}$ (appelé **quotient**) et un unique $r \in \mathbb{N}$ (appelé **reste**) tels que :

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

Remarque

On "approche" a par un nombre inférieur ou égal car **le reste r est toujours positif**.

Exemples

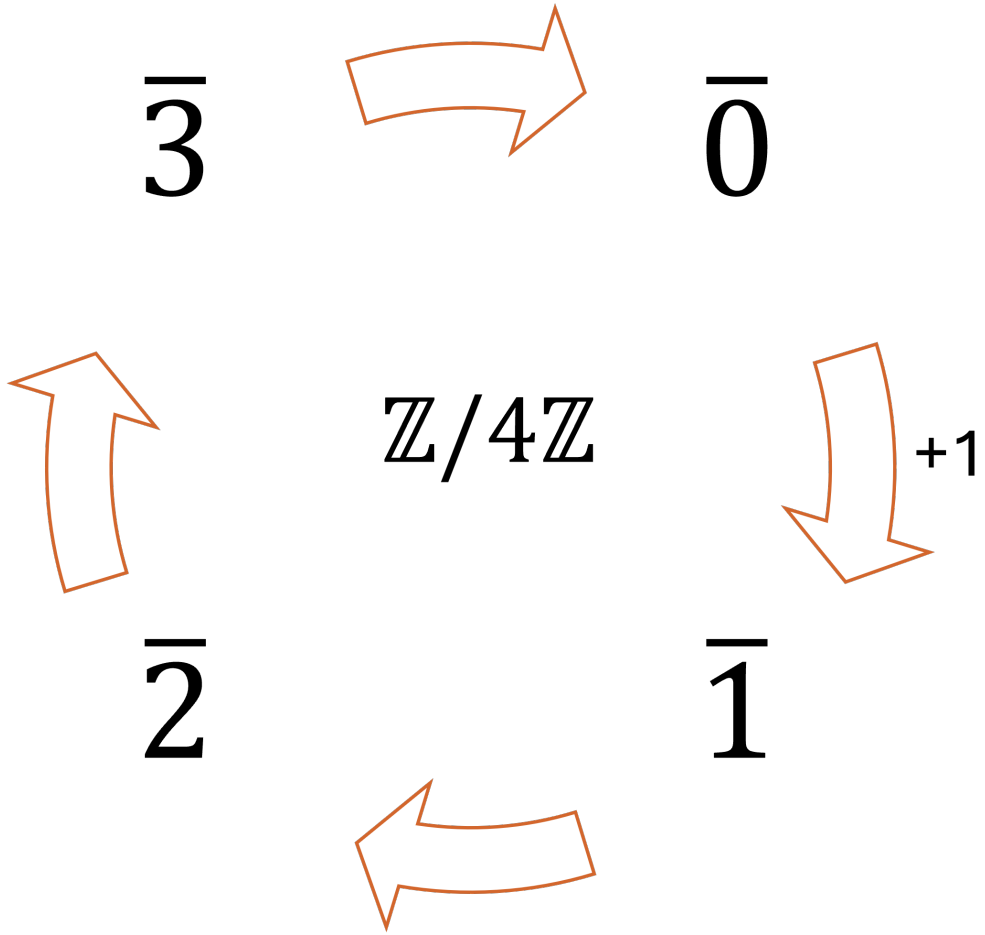
1. Effectuer la division euclidienne de 32 par 7
2. Effectuer la division euclidienne de -32 par 7

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 $a = b + kn$.
On note $a \equiv b \mod n$

- On peut comprendre a et b sont congrus modulo n comme a et b sont à une distance multiple de n.
- La congruence modulo n est une relation d'équivalence sur $\mathbb{Z}$ où les éléments d'une même classe d'équivalence ont le même reste dans la division euclidienne par n
- L'ensemble des classes d'équivalence est notée $\mathbb{Z}/n\mathbb{Z}$
- $\mathbb{Z}/n\mathbb{Z} = \left\{\overline{0}, \overline{1}, \ldots, \overline{n-1}\right\}$
- $\overline{a} = \overline{b} \iff a \equiv b \mod n$

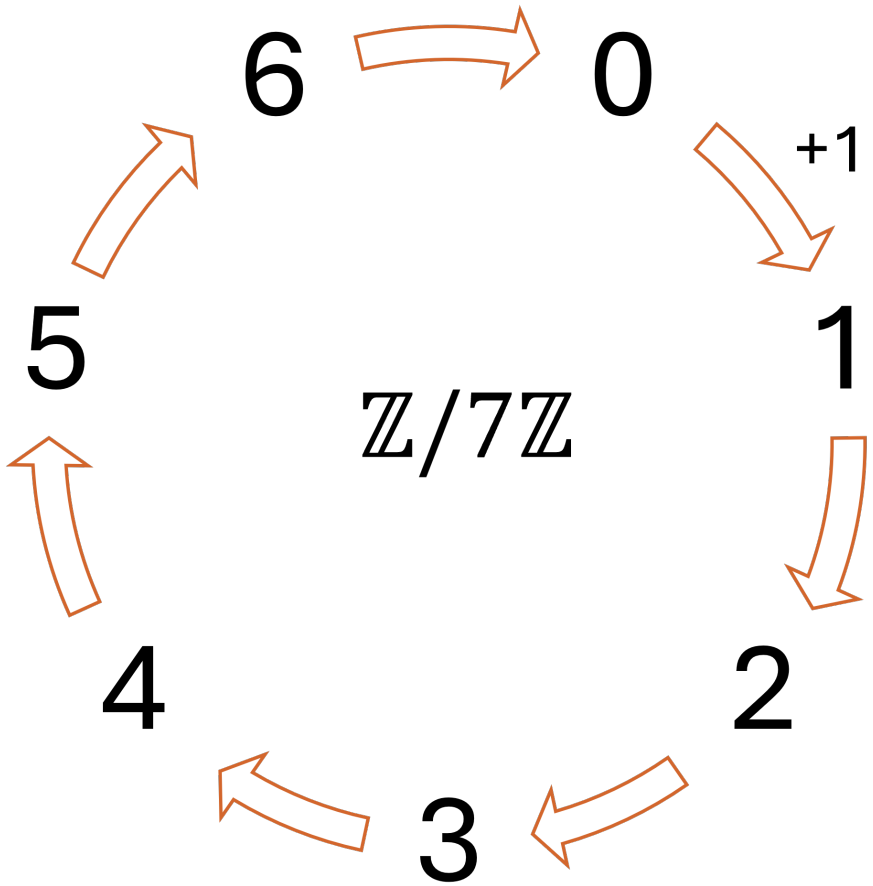
Représentation graphique circulaire



Donner quelques éléments positifs et négatifs de chacune des classes d'équivalence de $\mathbb{Z}/4\mathbb{Z}$

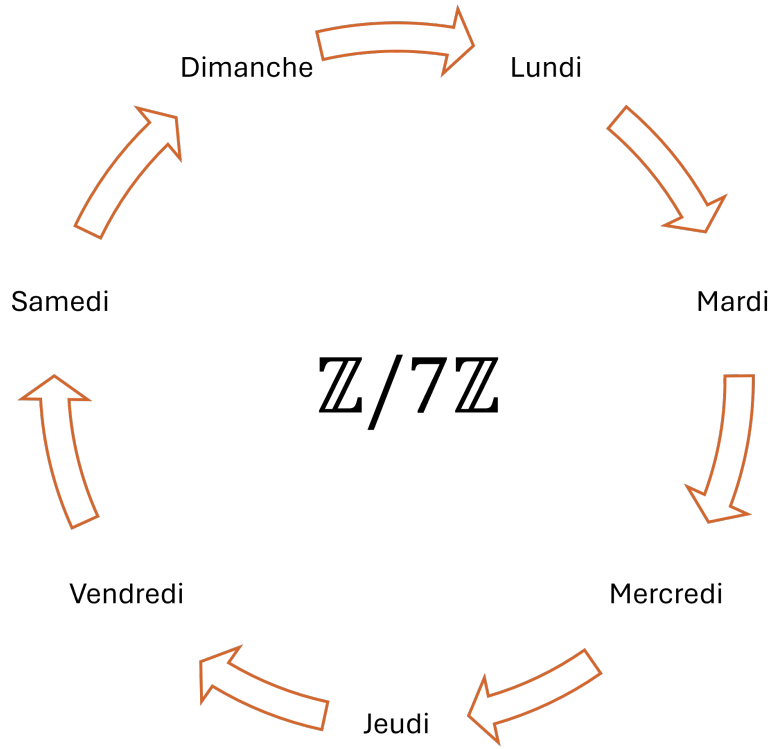
Représentation graphique circulaire

En pratique, on va rapidement omettre les barres horizontales...



Représentation graphique circulaire

Et dans la vie de tous les jours...



Si l'on est mardi, quel jour sera t'on dans 23 jours ? Quel jour était-il 10 jours avant ?

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

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

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

- 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 $\overline{a} \in \mathbb{Z}/4\mathbb{Z}$, déterminer son opposé (pour rappel : l'opposé de $\overline{a}$ est le nombre $\overline{b}$ tel que $\overline{a}+\overline{b}=\overline{0}$).
2. Dans $\mathbb{Z}/4\mathbb{Z}$, quel est le résultat de $\overline{3}\times\overline{2}$? de $\overline{3}\times\overline{3}$?

Retour au chiffrement par décalage

Maintenant que la terminologie est plus claire. Nous pouvons formaliser les fonctions de chiffrement E et déchiffrement D :

$$E_k : \mathbb{Z}/26\mathbb{Z} \to \mathbb{Z}/26\mathbb{Z}$$
$$m_i \mapsto c_i = m_i + k$$

$$D_k : \mathbb{Z}/26\mathbb{Z} \to \mathbb{Z}/26\mathbb{Z}$$
$$c_i \mapsto m_i = c_i - k$$

Nous pouvons remarquer que la même clef k est utilisée dans le chiffrement et le déchiffrement. Le chiffrement par décalage est donc bien un **chiffrement symétrique**.

Chiffrement affine

Étudions un autre type de chiffrement symétrique : **le chiffrement affine**.

La clef de chiffrement k est maintenant composée d'un couple d'entiers (a, b) avec $a \in (\mathbb{Z}/n\mathbb{Z})^*$ (l'ensemble des éléments inversibles de $\mathbb{Z}/n\mathbb{Z}$) et $b \in \mathbb{Z}/n\mathbb{Z}$.

La fonction de chiffrement correspondante est :

$$E_k : \mathbb{Z}/26\mathbb{Z} \to \mathbb{Z}/26\mathbb{Z}$$
$$m_i \mapsto c_i = am_i + b$$

Ainsi, si k = (3,4), la lettre codée 6 (donc g) sera chiffrée avec la lettre codée $(3 * 6 + 4) \mod 26 \equiv 22$ (donc w).

Déchiffrement affine

Partant du message chiffré et connaissant la clef $k = (a, b)$, il est possible de déchiffrer le message.

La fonction de déchiffrement s'écrit :

$$D_k : \mathbb{Z}/26\mathbb{Z} \to \mathbb{Z}/26\mathbb{Z}$$
$$c_i \mapsto m_i = \alpha c_i + \beta$$

avec $\alpha \equiv a^{-1} \mod n$ et $\beta \equiv (-a^{-1} b) \mod n$
où a^{-1} désigne l'**inverse modulaire** de a.

Mais qu'est-ce que l'inverse modulaire et comment le calcule-t-on ?

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 $\overline{a}$ est inversible dans $\mathbb{Z}/n\mathbb{Z}$ s'il existe $\overline{b} \in \mathbb{Z}/n\mathbb{Z}$ tel que $\overline{a}\overline{b} = \overline{1}$
- On note $(\mathbb{Z}/n\mathbb{Z})^*$ l'ensemble des inversibles de $\mathbb{Z}/n\mathbb{Z}$

- Contrairement à ce qui se passe dans $\mathbb{R}$, 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 $(\mathbb{Z}/n\mathbb{Z}) \setminus \{\overline{0}\}$ en général

Déterminer les éléments inversibles et leurs inverses dans $\mathbb{Z}/4\mathbb{Z}$.

Comment déterminer des inverses dans des cas plus complexes ?

Pour cela, nous avons besoin de quelques concepts arithmétiques supplémentaires...

PGCD

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.

Déterminer $pgcd(12,10)$.

Calcul du pgcd en pratique

Propriétés

- $pgcd(a,b) = pgcd(|a|,|b|)$
- Si r est le reste de la division euclidienne de a par b et $a \geq b > 0$, alors $pgcd(a,b) = pgcd(b,r)$
- $pgcd(a,0) = a$

En pratique, on effectue le calcul du pgcd sur la valeur absolue de a et b. Ce pgcd peut être calculé à l'aide d'un tableau récapitulant les quotients et restes successifs en posant $r_0 = max(|a|,|b|)$ et $r_1 = min(|a|,|b|)$

Exemple avec la recherche de $pgcd(366,56)$:

k	q_k	r_k	
0		366	
1	6	56	$(366 = 6 \times 56 + 30)$
2	1	30	$(56 = 1 \times 30 + 26)$
3	1	26	$(30 = 1 \times 26 + 4)$
4	6	4	$(26 = 6 \times 4 + 2)$
5	2	2	$(4 = 2 \times 2 + 0)$
6		0	

On en tire :

$$pgcd(366,56) = 2$$

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.

Algorithme d'Euclide étendu

L'algorithme d'Euclide étendu permet de trouver un couple (u, v) de coefficients de Bézout.

Pour cela, on ajoute deux suites $(u_k)_{k\in\mathbb{N}}$ et $(v_k)_{k\in\mathbb{N}}$ définies par une récurrence d'ordre 2 :

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

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

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

Ces deux suites peuvent être ajoutées à notre tableau pour déterminer le pgcd de la façon ci-dessous [1] :

Pour rappel : $\begin{cases} u_0 = 1,\ u_1 = 0 \\ \forall k \in \mathbb{N}^*,\ u_{k+1} = u_{k-1} - u_k q_k \end{cases}$

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

On en tire :

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

1. La dernière colonne du tableau détaille les calculs pour déterminer les $(u_k)_{k\in\mathbb{N}}$, un calcul similaire est fait pour les $(v_k)_{k\in\mathbb{N}}$

Déterminer une identité de Bézout entre 17 et 9

Entiers premiers entre eux

Définition (entiers premiers entre eux)

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

Propriété (caractérisation)

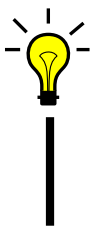
a et b sont *premiers entre eux* si et seulement s'il existe un couple $(u,v) \in \mathbb{Z}^2$ tel que :

$$ua + vb = 1$$

Entiers premiers

Définition (entier premier)

On dit qu'un entier $n \geq 2$ est *premier* s'il admet exactement deux diviseurs positifs distincts : 1 et n.



Remarque

- 0 n'est pas premier car il admet une infinité de diviseurs positifs.
- 1 n'est pas premier car il n'admet qu'un seul diviseur positif, lui-même.

Propriété (décomposition en facteurs premiers)

Tout entier $n \geq 2$ admet une unique décomposition en un produit de facteurs premiers :

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

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.

Exemples de décompositions en facteurs premiers :

- $50 = 2^1 \times 5^2$
- $60 = 2^2 \times 3^1 \times 5^1$

pgcd avec la décomposition en facteurs premiers

$pgcd(a,b)$ est le produit du plus petit nombre d'occurrences de chaque facteurs premiers en commun entre a et b.
Exemple : $pgcd(50,60) = 2^1 \times 5^1 = 10$

En utilisant la décomposition en facteurs premiers, donner $pgcd(30,18)$ et $pgcd(-3,13)$.

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

Retour sur le chiffrement affine

Rappel : dans le cas d'un chiffrement affine, la clef de chiffrement k est composée d'un couple d'entiers (a, b) avec $a \in (\mathbb{Z}/26\mathbb{Z})^*$ et $b \in \mathbb{Z}/26\mathbb{Z}$.

1. La clef (22,5) est-elle valide ? Si oui, quelle est la fonction de déchiffrement ?
2. Mêmes questions pour la clef (15,10)

Chiffrement de Hill

Le chiffrement de Hill est un dernier exemple de chiffrement symétrique dans lequel les lettres du messages en clair sont chiffrées et déchiffrées par paquets et non les unes à la suite des autres.

Pour chiffrer, on commence par choisir une matrice carrée inversible dans $\mathbb{Z}/26\mathbb{Z}$ de taille $p \times p$. **Cette matrice constitue la clef de chiffrement.**

Le message en clair est ensuite divisé en blocs/vecteurs de longueur p. Le dernier bloc est éventuellement complété avec une lettre choisie arbitrairement si sa longueur est différente de p. Chaque vecteur est chiffré en le multipliant avec la matrice carré.

La fonction de chiffrement correspondante pour un bloc de p lettres est donc :

$$E_K : (\mathbb{Z}/26\mathbb{Z})^p \to (\mathbb{Z}/26\mathbb{Z})^p$$

$$\begin{pmatrix} m_i \\ m_{i+1} \\ \dots \\ m_{i+p-1} \end{pmatrix} \mapsto \begin{pmatrix} c_i \\ c_{i+1} \\ \dots \\ c_{i+p-1} \end{pmatrix} = K \times \begin{pmatrix} m_i \\ m_{i+1} \\ \dots \\ m_{i+p-1} \end{pmatrix}$$

où K est une matrice carrée inversible dans $\mathbb{Z}/26\mathbb{Z}$ de taille $p \times p$.

Exemple

Chiffrons le message "TEXTE" avec une matrice $K \in \mathcal{M}_{2,2}$: $\begin{pmatrix} 3 & 5 \\ 6 & 17 \end{pmatrix}$.

1. Commençons par faire des blocs de 2 lettres : "TE","XT","EW" (ici, on rajoute un W en fin de message pour avoir un dernier bloc de deux lettres car le message initial n'a pas un nombre pair de lettres).
2. "TE" est codé (19,4), on a donc : $\begin{pmatrix} 3 & 5 \\ 6 & 17 \end{pmatrix} \times \begin{pmatrix} 19 \\ 4 \end{pmatrix} = \begin{pmatrix} 77 \\ 182 \end{pmatrix}$
3. Il faut ensuite convertir le résultat $\begin{pmatrix} 77 \\ 182 \end{pmatrix}$ en nombre de $\mathbb{Z}/26\mathbb{Z}$: $\begin{pmatrix} 25 \\ 0 \end{pmatrix}$ puis en lettre : $\begin{pmatrix} Z \\ A \end{pmatrix}$. "TE" sera donc chiffré "ZA".
4. Le processus est répété pour les autres couples de lettres.

Ainsi, le clair "TEXTE" devient le chiffré "ZAITSI".

Déchiffrement

Partant du message chiffré c et connaissant la matrice de chiffrement $K \in \mathcal{M}_{p,p}$, il est possible de déchiffrer le message pour obtenir le clair m.

Pour cela, il faut diviser le message chiffré en vecteurs de p lettres et multiplier chacun de ces vecteurs par l'**inverse de la matrice de chiffrement**.

La fonction de déchiffrement d'un bloc de p lettres est ainsi :

$$D_K : (\mathbb{Z}/26\mathbb{Z})^p \to (\mathbb{Z}/26\mathbb{Z})^p$$

$$\begin{pmatrix} c_i \\ c_{i+1} \\ \dots \\ c_{i+p-1} \end{pmatrix} \mapsto \begin{pmatrix} m_i \\ m_{i+1} \\ \dots \\ m_{i+p-1} \end{pmatrix} = K^{-1} \times \begin{pmatrix} c_i \\ c_{i+1} \\ \dots \\ c_{i+p-1} \end{pmatrix}$$

où K^{-1} est l'inverse de la matrice de chiffrement K dans $\mathbb{Z}/26\mathbb{Z}$.

Mais comment savoir qu'une matrice est inversible dans $\mathbb{Z}/26\mathbb{Z}$ et comment calculer son inverse ?

Inverse de matrice dans $\mathbb{Z}/n\mathbb{Z}$

Propriété (Inversibilité d'une matrice)

Soit A une matrice à coefficients dans $\mathbb{Z}/n\mathbb{Z}$.
A est inversible si et seulement si $\det(A)$ est inversible dans $\mathbb{Z}/n\mathbb{Z}$, c'est à dire si $\det(A)$ est premier avec n.

Inversibilité d'une matrice

La matrice $\begin{pmatrix} 3 & 2 \\ 4 & 6 \end{pmatrix}$ est-elle inversible dans $\mathbb{Z}/21\mathbb{Z}$?

Inverse de matrice dans $\mathbb{Z}/n\mathbb{Z}$

Définition (Inverse modulaire d'une matrice)

L'inverse modulaire d'une matrice carré A modulo n est une matrice A^{-1} telle que :

$$AA^{-1} \equiv I \mod n$$

avec I la matrice identité de même dimension que A.

Propriété (Inversion d'une matrice)

Soit A une matrice à coefficients dans $\mathbb{Z}/n\mathbb{Z}$.
Si A est inversible alors, on a :

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

Inverse de matrice dans $\mathbb{Z}/n\mathbb{Z}$

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 $\mathbb{Z}/n\mathbb{Z}$.

- On appelle comatrice de A ou $com(A)$ la matrice des cofacteurs de A.

$$com(A) = \left(c_{ij}\right)_{1\leq i,j\leq n}$$

- c_{ij} est ainsi le cofacteur d'indice i,j de A. Il est défini par

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

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 :

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

Calcul de la comatrice

1. Calculer $com(A)$ avec $A = \begin{pmatrix} 3 & 2 \\ 4 & 6 \end{pmatrix}$
2. Vérifier $A\Big(com(A)\Big)^t = \Big(com(A)\Big)^t A = \det(A) I_n$
3. Calculer $\begin{pmatrix} 3 & 2 \\ 4 & 6 \end{pmatrix}^{-1} \mod 21$

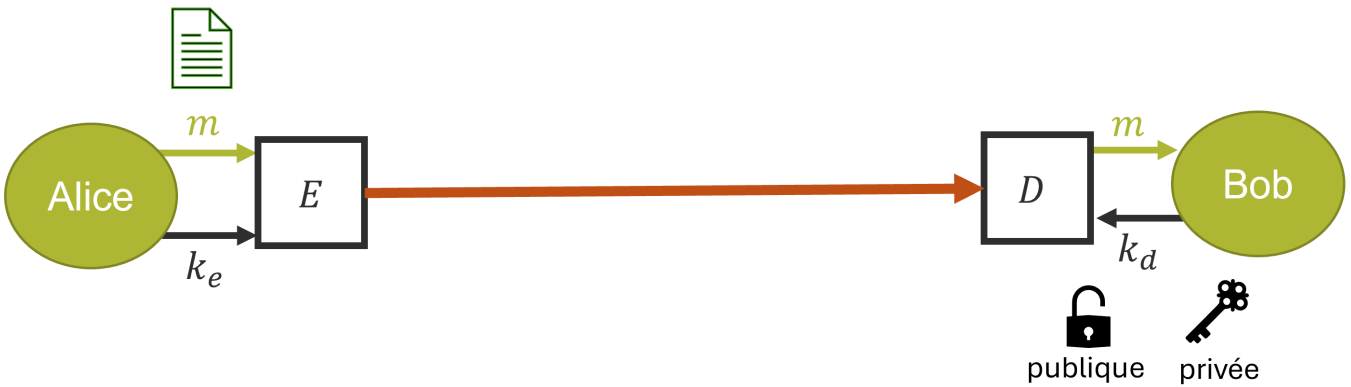
Sauf mention contraire, n désigne un entier supérieur ou égal à 1.

Cryptographie asymétrique

Définition (Cryptographie asymétrique)

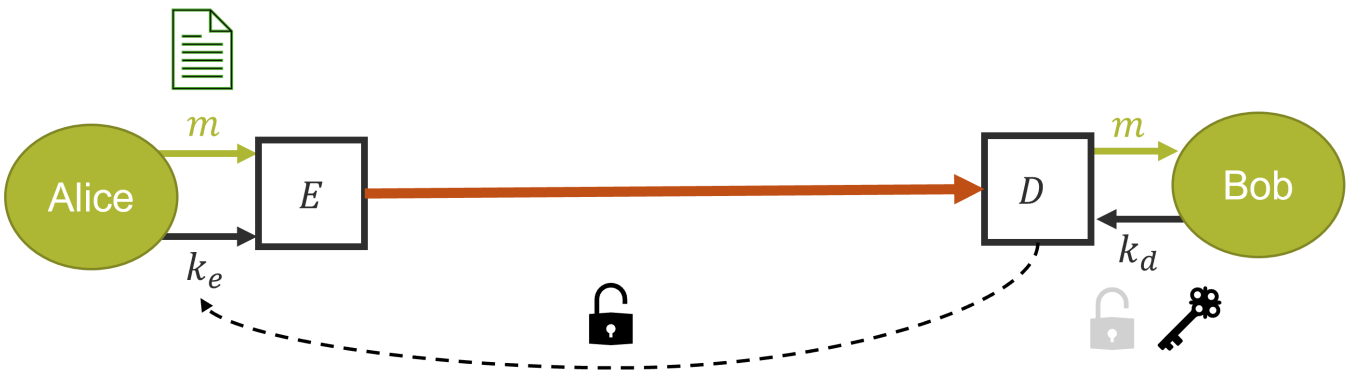
Dans la cryptographie asymétrique, aussi appelée "cryptographie à clef publique", le destinataire du message possède une clef composée de deux parties différentes : l'une publique, connue de tous, et la deuxième privée, connue de lui seul. Le chiffrement du message se fait grâce à la clef publique du destinataire. Celui-ci utilise ensuite sa clef privée pour déchiffrer le message.

Cryptographie asymétrique



Alice cherche à transmettre un message. Bob est en possession d'une clef composée de deux parties : l'une publique, l'autre privée

Cryptographie asymétrique



Bob transmet la partie publique de sa clef à Alice

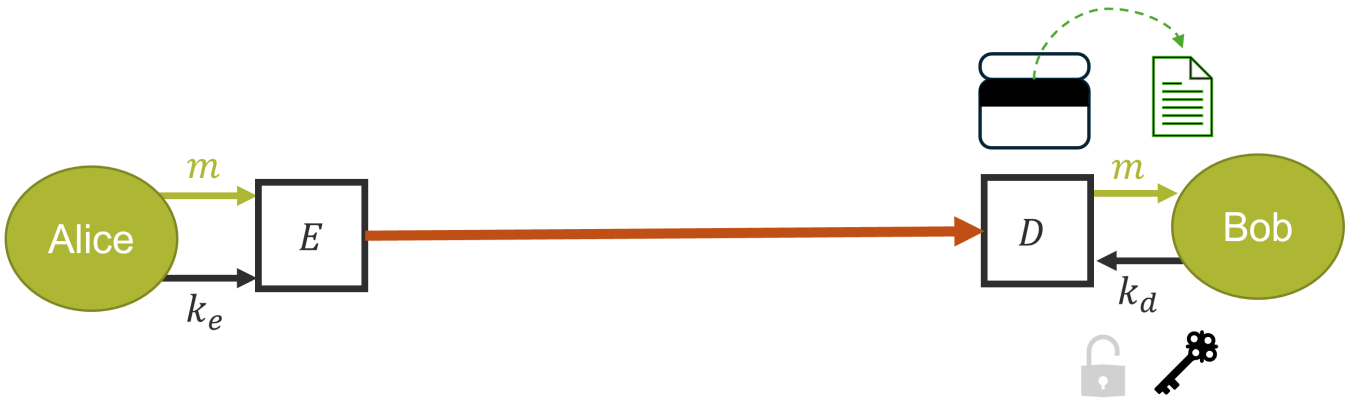
Cryptographie asymétrique

Alice chiffre son message à l'aide de la partie publique de la clef de Bob

Cryptographie asymétrique

Transmission du message chiffré

Cryptographie asymétrique



Bob déchiffre le message grâce à la partie privée de sa clef

Formalisation

Les interlocuteurs possèdent chacun une clef composée d'une partie publique connue de tous et d'une partie privée connue uniquement du propriétaire de la clef :

- clef d'Alice : $k_A = (k_A^{pub}, k_A^{priv})$
- clef de Bob : $k_B = (k_B^{pub}, k_B^{priv})$

Chiffrement du message
La fonction de chiffrement E est paramétrée par la partie **publique** de la clef du destinataire :

- Si Alice souhaite envoyer un message à Bob, elle chiffre son message m en utilisant la partie publique de la clef de Bob : $c = E_{k_B^{pub}}(m)$

Déchiffrement du message
La fonction de déchiffrement D est paramétrée par la partie **privée** de la clef du destinataire :

- Bob déchiffrera le message c en utilisant la partie privée de sa clef : $m = D_{k_B^{priv}}(c)$

Pour que ce système fonctionne, il faut que la partie publique et la partie privée de la clef permettent de définir des opérations E et D réciproques ($D_{k^{priv}} = E^{-1}_{k^{pub}}$) et que le calcul de la clef privée de quelqu'un connaissant sa clef publique soit infaisable dans des temps raisonnables.

Ce principe de la cryptographie asymétrique a été formalisé par Diffie et Hellmann en 1976 mais aucune solution concrète n'avait été proposée à ce moment. Il a fallu attendre le chiffrement **RSA**, proposé par Rivest, Shamir et Adleman un an plus tard pour pouvoir implémenter le chiffrement asymétrique.

Clef RSA

RSA propose une application concrète du principe du chiffrement asymétrique en se basant sur la difficulté à factoriser des entiers de grande taille.

Une clef RSA $k = (k^{pub}, k^{priv})$ est définie à partir des paramètres suivants :

- p et q sont deux grands nombres premiers distincts
- $n = pq$
- e et d sont des entiers tels que $ed \equiv 1 \mod \varphi(n)$ $(d \equiv e^{-1} \mod \varphi(n))$

Alors $k^{pub} = (n, e)$ et $k^{priv} = (n, d)$

Mais que signifie $\varphi(n)$?

Indicatrice d'Euler $\varphi(n)$

Définition

L'indicatrice d'Euler est définie par :

- $\varphi(1) = 1$
- $\forall n \in \mathbb{N}, n > 1, \quad \varphi(n) = Card\left(\left(\mathbb{Z}/n\mathbb{Z}\right)^*\right)$

- $\varphi(n)$ compte donc le nombre d'entiers premiers avec n et compris (au sens large) entre 1 et $n-1$.
- Si p est premier, alors $\varphi(p) = p-1$

Donner $\varphi(26)$ et $\varphi(17)$.

Propriétés

L'indicatrice d'Euler vérifie :

1. Pour tout p premier et tout $k \geq 1$, $\varphi\left(p^k\right) = p^k - p^{k-1}$
2. Pour tout m, n premiers entre eux, $\varphi(mn) = \varphi(m)\varphi(n)$

En utilisant les propriétés, donner $\varphi(25)$, $\varphi(49)$, $\varphi(64)$ et $\varphi(60)$

Avec ces propriétés, il est possible de trouver l'indicatrice d'Euler de n'importe quel nombre n ... **à condition de trouver la décomposition de n en facteurs premiers !**.

Par exemple :

- $\varphi(240) = \varphi(2^4 \times 3 \times 5) = \varphi(2^4) \times \varphi(3) \times \varphi(5) = (2^4 - 2^3) \times 2 \times 4 = 8 \times 2 \times 4 = 64$
- mais $\varphi(221)$?
- ou $\varphi(33741)$?

La décomposition en facteurs premiers n'est pas si évidente et le chiffrement RSA se base sur cette difficulté !

Application du chiffrement RSA

RSA

Alice souhaite envoyer le message $m = 10$ à Bob.
Ce dernier, pour définir sa clef $\left(k_B^{pub}, k_B^{priv}\right)$ a choisi deux nombres premiers[a] distincts : $p = 5$ et $q = 17$

1. Déterminer n et $\varphi(n)$.

Bob a ensuite choisi un entier $e = 5$ premier avec $\varphi(n)$

2. Déterminer k_B^{pub} et k_B^{priv}

a. Dans la pratique, ce sont de très grands nombres d'une centaine de chiffres

Nous avons les clefs RSA, mais quelle sont les fonctions de chiffrement/déchiffrement RSA ?

Principe du chiffrement RSA

Propriété (lemme du déchiffrement RSA)

Soit $n = pq$, le produit de deux nombres premiers distincts.
Soit d l'inverse de e modulo $\varphi(n)$.
Soient m le message en clair et c le message chiffré.
Si $c \equiv m^e \mod n$, alors $m \equiv c^d \mod n$.

La force du chiffrement RSA réside dans la difficulté de calculer d à partir n et e. En effet, d est l'inverse de e modulo $\varphi(n)$ mais $\varphi(n)$ ne peut se calculer qu'en ayant trouvé les deux nombres premiers p et q dont le produit donne n. Or, la factorisation en nombre premier est un problème actuellement insoluble dans des temps raisonnables dès que n est assez grand.

Fonctions de chiffrement/déchiffrement RSA

Rappel : La clef du chiffrement/déchiffrement RSA est $k = (k^{pub}, k^{priv})$ avec $k^{pub} = (n, e)$ et $k^{priv} = (n, d)$

Chiffrement :

$$E_{k^{pub}} : \mathbb{Z}/n\mathbb{Z} \to \mathbb{Z}/n\mathbb{Z}$$
$$m \mapsto c = m^e \mod n$$

Déchiffrement

$$D_{k^{priv}} : \mathbb{Z}/n\mathbb{Z} \to \mathbb{Z}/n\mathbb{Z}$$
$$c \mapsto m = c^d \mod n$$

Essayer de calculer $c \equiv 10^5 \mod 85$... Pas si facile a priori...
Pour terminer ce cours, nous allons voir deux astuces pour faciliter l'exponentiation "à la main" :

1. le théorème d'Euler
2. la technique de l'exponentiation rapide

Théorème d'Euler

Propriété (théorème d'Euler)

Si a est un entier premier avec n, alors $a^{\varphi(n)} \equiv 1 \mod n$.

- **Petit théorème de Fermat** : Lorsque $n = p$ avec p premier, le théorème d'Euler donne :
  Si a est un entier premier avec p, alors $a^{p-1} \equiv 1 \mod p$
- **Cas particulier utilisé pour le déchiffrement RSA** : Lorsque $n = pq$ avec p, q premiers, cela devient :
  Si a est un entier premier avec n, alors $a^{(p-1)(q-1)} \equiv 1 \mod n$
- Le lemme du déchiffrement RSA se démontre grâce au théorème d'Euler (voir démo sur Moodle).

Montrer que $17^{1717} \equiv 7 \mod 10$ sachant que $1717 = 4 \times 429 + 1$

Exponentiation rapide

L'exponentiation rapide est une technique utilisée pour calculer rapidement de grandes puissances de nombres entiers. Elle est particulièrement utile pour l'exponentiation modulaire dans laquelle les nombres manipulés reste limités par le modulo. Étant donné les entiers a et e, et l'entier non nul m, cette technique vise donc à calculer b dans l'expression suivante :
$a^e \equiv b \mod m$

Description de la méthode :

Tout d'abord, il s'agit de donner la décomposition binaire de e : $e = \sum_{i=0}^{n-1} c_i 2^i$ avec n la longueur de e en bits, et $c_i = 0$ ou 1 pour tout i compris entre 0 et $n-1$.

Ainsi, a^e peut s'écrire comme le produit des a^{2^i} pour les c_i non nuls.

Il suffit donc ensuite de réaliser les carrés successifs de a (modulo m) puis de faire le produit (modulo m) pour obtenir b.

Exemple : Calculons b tel que $7^{18} \equiv b \mod 10$

1. Décomposition binaire de l'exposant : $18 = 16 + 2 = 2^4 + 2^1$
2. On a donc $7^{18} = 7^{2^4} \times 7^{2^1}$
3. Calcul des carrés successifs modulo 10 :
   $7^{2^1} \equiv 7^2 \equiv 49 \equiv 9 \mod 10$
   $7^{2^2} \equiv (7^2)^2 \equiv 9^2 \equiv 81 \equiv 1 \mod 10$
   $7^{2^3} \equiv ((7^2)^2)^2 \equiv 1^2 \equiv 1 \mod 10$
   $7^{2^4} \equiv (((7^2)^2)^2)^2 \equiv 1^2 \equiv 1 \mod 10$
4. Produit et conclusion :

$$\begin{aligned} 7^{18} &\equiv 7^{2^4} \times 7^{2^1} \mod 10 \\ &\equiv 1 \times 9 \mod 10 \\ &\equiv 9 \mod 10 \end{aligned}$$

Refaire le même exemple en utilisant le théorème d'Euler.

RSA (suite et fin)

Rappel de l'énoncé : Alice souhaite envoyer le message $m = 10$ à Bob.

Nous avons $p = 5$ et $q = 17$,

$n =$

$\varphi(n) =$

$k_B^{pub} =$

$k_B^{priv} =$

3. Alice utilise la fonction de chiffrement RSA. Calculer le chiffré c reçu par Bob.
4. Bob utilise la fonction de déchiffrement RSA. Retrouver le message m envoyé par Alice.

Comparaison

Cryptographie symétrique :

+ Algorithmes (souvent) rapides
- Nécessite la transmission préalable d'une clef secrète

Cryptographie asymétrique :

+ Ne nécessite pas la transmission préalable d'informations secrètes
- Algorithmes complexes, lents sur des données de grandes tailles

Les deux types de cryptographies paraissent complémentaires.

Problématique

Alice veut transmettre un message m à Bob de façon confidentielle.

Elle essaye d'abord d'utiliser RSA pour chiffrer son message mais son message est long et le chiffrement prend trop de temps. Elle perd patience...

En utilisant un algorithme de cryptographie symétrique, Alice réussit à rapidement chiffrer son message mais elle n'arrive pas à transmettre la clef à Bob de façon sécurisée...

Que faire ?
Serait-il possible de profiter des avantages des deux techniques ?

En pratique

Il est possible d'utiliser de manière conjointe les deux techniques cryptographiques de façon à profiter des forces de chacune.

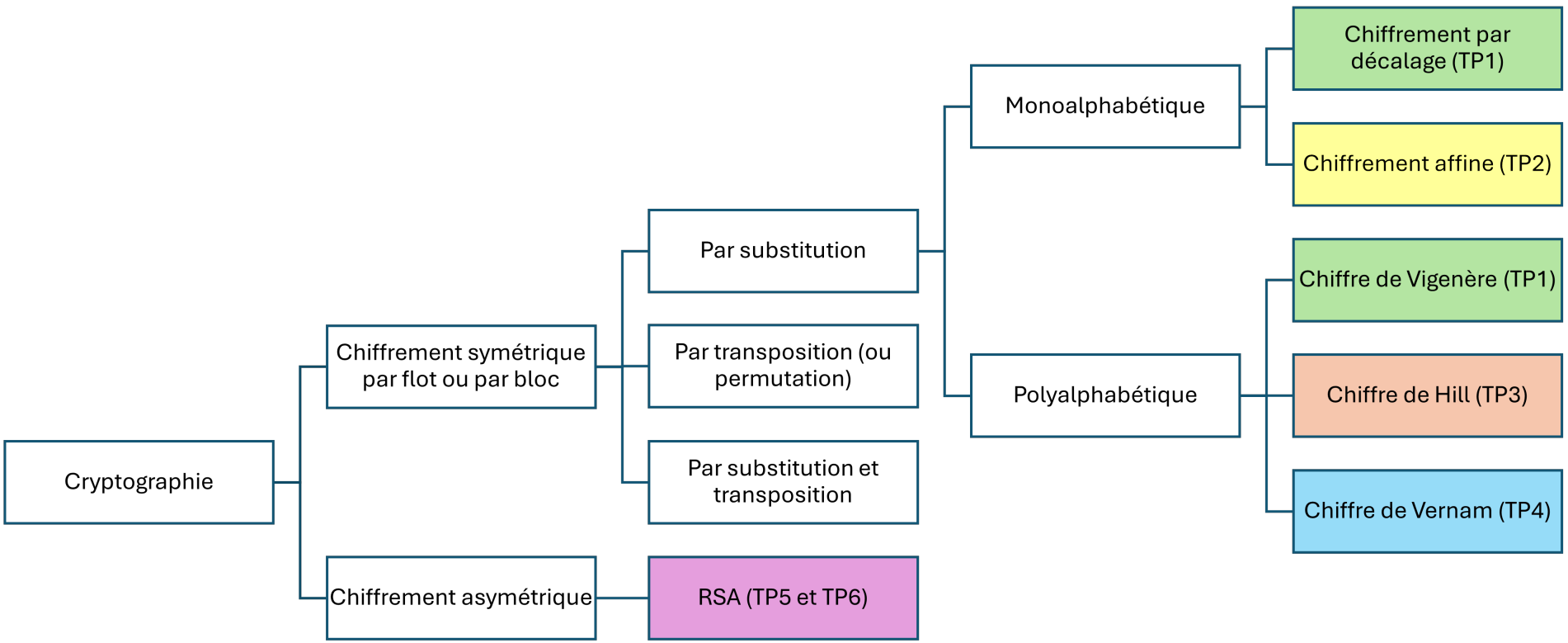
Les algorithmes de cryptographie **symétriques** permettent de chiffrer **le message en clair** tandis que les algorithmes de cryptographie **asymétriques**, plus sûrs et plus lents, peuvent permettre de chiffrer des données de faible longueur et donc **la clef de chiffrement** utilisée pour le chiffrement symétrique !

Il s'agit là d'un exemple de protocole de chiffrement...

A suivre en R4.B.10

- Hachage, signature, stockage des mots de passe
- Cryptographie symétrique plus récentes (par ex. : DES, AES...)
- Protocole SSL et certificats
- Intégrité des données (codes correcteurs...)

Annexe 1 : Récapitulatif des techniques vues en Cours/TP



Annexe 2 : quelques propriétés des exposants

- $a^m \times a^n = a^{m+n}$
- $(a^m)^n = a^{m \times n}$
- $a^{(m^n)} = (((a^m)^m)^m)^m)...$ (mis à la puissance n fois)

Annexe 3 : Rang des lettres dans l'alphabet

On considère souvent qu'une lettre est représentée par son rang dans l'alphabet en partant de 0. Ainsi, pour vous aider dans vos calculs, le tableau de correspondance suivant vous est fourni. La dernière ligne vous donne l'équivalent du rang en négatif dans $\mathbb{Z}/26\mathbb{Z}$.

A	B	C	D	E	F	G	H	I	J	K	L	M
0	1	2	3	4	5	6	7	8	9	10	11	12
0	-25	-24	-23	-22	-21	-20	-19	-18	-17	-16	-15	-14

N	O	P	Q	R	S	T	U	V	W	X	Y	Z
13	14	15	16	17	18	19	20	21	22	23	24	25
-13	-12	-11	-10	-9	-8	-7	-6	-5	-4	-3	-2	-1