CRYPTOGRAPHIE

Résumé

haute école
neuchâtel berne jura
ingénierie
www.he-arc.ch

TABLE DES MATIERES

INTRODUCTION

QUELQUES DEFINITIONS

Etymologie : science du secret

Cryptographie : Science qui utilise les mathématiques pour le cryptage et le décryptage de données

Cryptanalyse : Etude des informations cryptée afin d'en découvrir le secret

Texte en clair : Donnée lisibles et compréhensibles sans intervention spécifique.

Sténographie : L'art de dissimuler.

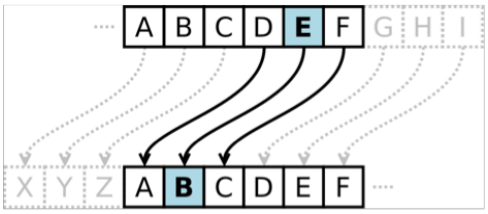
CHIFFREMENT MONOALPHABETIQUE

SCYTALE - SKYTALE (BATON DE PLUTARQUE) DE SPARTE

Le plus ancien dispositif de cryptographie militaire.

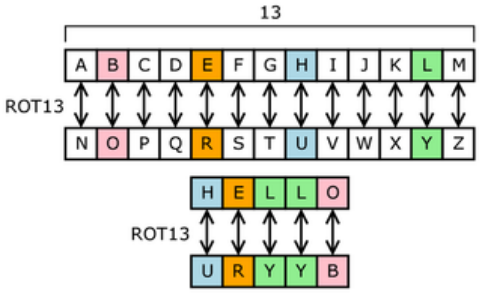
Pour le déchiffrer, le destinataire devait posséder un bâton d'un diamètre identique à celui utilisé pour l'encodage.

CHIFFREMENT DE CESAR - CHIFFREMENT PAR DECALAGE



CODE ROT13

Le ROT13 (rotate by 13 places) est un cas particulier du chiffre de César, un algorithme simpliste de chiffrement de texte. Comme son nom l'indique, il s'agit d'un décalage de 13 caractères de chaque lettre du texte à chiffrer.



CHIFFREMENT POLYALPHABETIQUE

CODE DE BLAISE DE VIGENERE

Principe

Ce chiffrement introduit la notion de clé. Une clé se présente généralement sous la forme d'un mot ou d'une phrase. Pour pouvoir chiffrer notre texte, à chaque caractère nous utilisons une lettre de la clé pour effectuer la substitution.

Évidemment, plus la clé sera longue et variée et mieux le texte sera chiffré. Il faut savoir qu'il y a eu une période où des passages entiers d'œuvres littéraires étaient utilisés pour chiffrer les plus grands secrets. Les deux correspondants n'avaient plus qu'à avoir en leurs mains un exemplaire du même livre pour s'assurer de la bonne compréhension des messages.

Table de Vigenère.

Clé utilisée	Lettre en clair																									
	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
26 lettres chiffrées																										
A	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
B	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A
C	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B
D	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C
E	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D
F	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E
G	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F
H	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G
I	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H
J	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I
K	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J
L	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K
M	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L
N	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M
O	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N
P	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O
Q	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P
R	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q
S	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R
T	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S
U	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T
V	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U
W	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V
X	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W
Y	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X
Z	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y

```
Texte en clair :   j'adore ecouter la radio toute la journee

Clé répétée    :   M USIQU EMUSIQU EM USIQU EMUSI QU EMUSIQU
                   ^ ^^^

                   | ||Colonne O, ligne I : on obtient la lettre W.
                   | |Colonne D, ligne S : on obtient la lettre V.
                   | Colonne A, ligne U : on obtient la lettre U.
                   Colonne J, ligne M : on obtient la lettre V.
```

CHIFFREMENT PAR TRANSPOSITION

Le chiffrement par transposition demande de découper le texte clair en blocs de taille identique. La même permutation est alors utilisée sur chacun des blocs. Le texte doit éventuellement être complété (procédé de bourrage) pour permettre ce découpage. La clef de chiffrement est la permutation elle-même.

Le nombre de permutations possibles d'une longueur donnée, qui est la factorielle de cette longueur, augmente donc rapidement avec celle-ci. Par exemple un mot de trois lettres ne peut être permuté que dans 6 (=3!) positions différentes. Ainsi "col" ne peut se transformer qu'en "col", "clo", "ocl", "olc", "lco" ou "loc".

Lorsque le nombre de lettres croît, le nombre d'arrangements augmente rapidement et il devient plus difficile de retrouver le texte original sans connaître la permutation, et sans aucune connaissance sur le texte clair. Ainsi pour un chiffre par transposition qui utilise des blocs de 20 caractères, il y a 20! possibilités, soit 2 432 902 008 176 640 000 combinaisons.

Exemple:

Message chiffré :

```
CARTM IELHX YEERX DEXUE VCCXP EXEEM OEUNM CMIRL XRTFO CXQYX EXISV NXMAH
GRSML ZPEMS NQXXX ETNIX AAEXV UXURA FOEAH XUEUT AFXEH EHTEN NMFXA XNZOR
ECSEI OAINE MRCFX SNSD PELXA HPRE
```

Clé de transposition :

```
8 4 9 14 1 2 16 10 3 17 15 19 11 5 20 6 7 12 13 18
```

Déchiffrement : le déchiffrement se fait en remplissant les colonnes verticalement, dans l'ordre défini par la clé. On commence par remplir de haut en bas la colonne numérotée 01 avec les huit premiers caractères du message chiffré : CARTMIEL. On continue en remplissant de la même façon la colonne numérotée 02 avec les huit caractères suivants HxYEERxD etc.

08	04	09	14	01	02	16	10	03	17	15	19	11	05	20	06	07	12	13	18
S	P	R	U	C	H	x	S	E	C	H	S	N	U	L	L	x	V	O	N
V	E	S	T	A	x	A	N	x	S	T	E	I	N	x	x	Q	U	E	E
N	x	M	A	R	Y	x	Q	U	E	E	N	x	M	A	R	Y	x	A	M
x	E	L	F	T	E	N	x	E	I	N	S	A	C	H	T	x	U	H	R
M	E	Z	x	M	E	Z	x	V	O	N	D	A	M	P	F	E	R	x	C
A	M	P	E	I	R	O	x	C	A	M	P	E	I	R	O	x	A	U	F
H	O	E	H	E	x	R	E	C	I	F	E	x	R	E	C	I	F	E	x
G	E	M	E	L	D	E	T	x	.	.	.	.	.	.	.	.	.	.	.

Message en clair : Spruch 60. Von VESTA An STEIN.

QUEEN MARY am Elften eins acht Uhr MEZ von Dampfer CAMPEIRO auf hoehe RECIFE gemeldet.

VERNAM CIPHER - MASQUE JETABLE - CHIFFRE DE VERNAM

Définition

Algorithme de cryptographie inventé par Gilbert Vernam (en) en 1917et perfectionné par Joseph Mauborgne, qui rajouta la notion de clé aléatoire.

Principe

Le chiffrement par la méthode du masque jetable consiste à combiner le message en clair avec une clé présentant les caractéristiques très particulières suivantes :

• La clé doit être une suite de caractères au moins aussi longue que le message à chiffrer.

• Les caractères composant la clé doivent être choisis de façon totalement aléatoire.

• Chaque clé, ou « masque », ne doit être utilisée qu'une seule fois (d'où le nom de masque jetable).

La méthode de combinaison entre le clair et la clé est suffisamment simple pour être employée « à la main » sans dispositif informatique, mécanique ou autre.

Chiffrement et déchiffrement à la main

Supposons que la clé aléatoire retenue, ou « masque », soit :

```
WMCKL
```

Cette clé est choisie à l'avance entre les deux personnes souhaitant communiquer. Elle n'est connue que d'eux.

On veut chiffrer le message « **HELLO** ». Pour cela, on attribue un nombre à chaque lettre, par exemple le rang dans l'alphabet, de **0 à 25**. Ensuite on additionne la valeur de chaque lettre avec la valeur correspondante dans le masque ; enfin si le résultat est supérieur à 25 on soustrait 26 (calcul dit « **modulo 26** ») :

```
   7 (H)   4 (E)  11 (L)  11 (L)  14 (O) message

+ 22 (W)  12 (M)   2 (C)  10 (K)  11 (L) masque

= 29      16      13      21      25     masque + message

=  3 (D)  16 (Q)  13 (N)  21 (V)  25 (Z) masque + message  modulo 26
```

Le texte reçu par le destinataire est « **DQNVZ** ».

Le déchiffrement s'effectue de manière similaire, sauf que l'on soustrait le masque au texte chiffré au lieu de l'additionner. Ici encore on ajoute éventuellement 26 au résultat pour obtenir des nombres compris entre 0 et 25 :

```
        3 (D)  16 (Q)  13 (N)  21 (V)  25 (Z) message chiffré

-  22 (W)  12 (M)   2 (C)  10 (K)  11 (L) masque

= -19       4      11      11      14     message chiffré - masque

=   7 (H)   4 (E)  11 (L)  11 (L)  14 (O) message chiffré - masque modulo
26
```

Chiffrement et déchiffrement avec un ordinateur

Si on essaie de faire une résolution en informatique, on va utiliser le XOR.

Le chiffrement consiste en l'ajout (mod 2) bit à bit du clair et de la clé:

```
c = m ⊕ K = m1 ⊕ K1 · · ·mn ⊕ Kn
```

Pour décrypter, on connait K:

```
m = c ⊕ K
```

Attention, si on connait déjà m et c, on peut en déduire K

```
K = m ⊕ c
```

Ce qui implique que la clé ne doit être utilisée qu'une fois!

CRYPTOGRAPHIE D'AUJOURD'HUI

La cryptographie se divise en **deux grands domaines**

- La cryptographie à **clé privée** (ou clé discrète ou cryptage symétrique)
- La cryptographie à **clé publique** ou cryptage asymétrique

Mais aussi :

- Standardisation des primitives cryptographiques
- Invention de la cryptographie à clé publique

PROBLEME DE LA CRYPTOGRAPHIE CLASSIQUE

Faibles

- Papier et crayon, et cryptosystèmes mécaniques sont devenus faible face des ordinateurs modernes.

Informels

- Constructions étaient ad hoc. Il n'y avait pas publiquement définitions de sécurité disponibles ou des preuves de la sécurité.

Fermé

- La connaissance et de la technologie de chiffrement a été principalement uniquement disponible pour les organismes militaires ou de renseignement.

La distribution des clés

- Le nombre de clés dans le système pousse quadratique avec le nombre de parties.

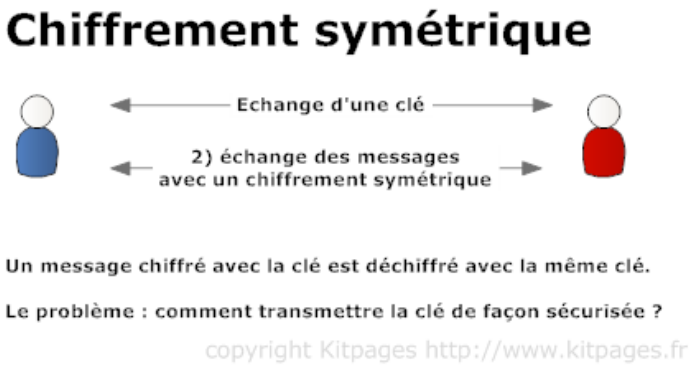
CHAPITRE 2 - CRYPTAGE SYMETRIQUE - CRYPTAGE A CLE PRIVEE

L'un des concepts fondamentaux de la cryptographie symétrique est la clé. Une clé est une donnée qui (traitée par un algorithme) permet de chiffrer et de déchiffrer un message. Toutes les méthodes de chiffrement n'utilisent pas de clé. Le ROT13, par exemple, n'a pas de clé. Quiconque découvre qu'un message a été codé avec cet algorithme peut le déchiffrer sans autre information. Une fois l'algorithme découvert, tous les messages chiffrés par lui deviennent lisibles.

CONCEPT

Le chiffrement symétrique utilise une **clé unique partagée entre les 2 interlocuteurs**. On encode et on décode le message avec la même clé.

Le **problème** de ce chiffrement est qu'il faut trouver un moyen de transmettre la clé unique entre les 2 interlocuteurs.



Chiffrement par flots

- Traitement bit par bit
- Exemple : RC4 (WEP, WPA, WPA2), E0 (Bluetooth), A5/1 (GSM)

Chiffrement par blocs

- Découpage des données en bloc de taille fixe
- Chiffrement de chaque bloc
- Exemple: AES, DES, 3DES, BlowFish

RC4

- RC4 = Rivest Cipher 4 (40-2048 taille de la clé)
- Simple à implémenter (autant logiciel que matériel)
- Rapide (10x plus rapide que le DES)

L'ESSENTIEL

RC4 est un algorithme de chiffrement à flot conçu en 1987 par Rivest et dédié aux applications logicielles. Il est largement déployé notamment dans le protocole SSL/TLS et la norme WEP pour les réseaux sans fil, IEEE 802.11. RC4 présente certaines faiblesses dues à son initialisation, qui est relativement faible, et qui ne prévoit pas de valeur initiale pour la re-synchronisation. Employé par exemple avec le protocole de re-synchronisation choisi dans la norme IEEE 802.11, RC4 s'avère extrêmement faible.

FONCTIONNEMENT

RC4 = générateur de bits pseudo-aléatoire combiné avec un **XOR** au texte clair

2 étapes :

1. **Initialisation à l'aide de la clé (5 à 256 octets)**
   - Mélange d'un tableau contenant des indices aléatoires (0 à 255) à partir de la clé
   - Utilisé lors de la phase de cryptage

```
Pour i de 0 à 255,
        S[i] ← i
j ← 0
Pour i de 0 à 255 faire
        j ← j + S[i] + K[i mod K] mod 256
        échanger S[i] et S[j]
```

2. **Chiffrement du texte clair**
   - Utilisation du tableau généré précédemment
   - Evolution du tableau à chaque tour

```
Tant que flux non vide:
        i = (i+1) mod 256
        j = (j+S[i]) mod 256
        echanger(S[i] , S[j])
        octCrypt = S[(S[i]+S[j]) mod 256]
        resultat = octetFlux xor octCrypt
```

EXEMPLE RC4

Voir code sur Github

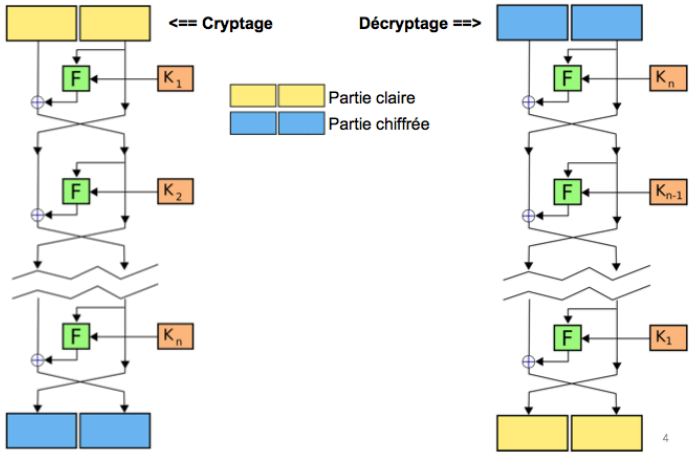
CHAPITRE 3 - DES (DATA ENCRYPTION STANDARD)

INTRODUCTION

Le **Data Encryption Standard** (DES) est un algorithme de chiffrement symétrique (chiffrement par bloc) utilisant des clés de 56 bits. Son emploi n'est plus recommandé aujourd'hui, du fait de sa lenteur à l'exécution et de son espace de clés trop petit permettant une attaque systématique en un temps raisonnable. Quand il est encore utilisé c'est généralement en Triple DES, ce qui ne fait rien pour améliorer ses performances. DES a notamment été utilisé dans le système de mots de passe UNIX.

- Clés de 56 bits
- Taille de bloc = 64 bits
- Cryptage à clé secrète, itératif, par blocs

EN BREF



Fonctionnement sur 3 étapes

1. Permutation initiale et fixe d'un bloc (sans aucune incidence sur le niveau de sécurité) ;
2. Le résultat est soumis à 16 itérations d'une transformation, ces itérations dépendent à chaque tour d'une autre clé partielle de 48 bits.

   Cette clé de tour intermédiaire est calculée à partir de la clé initiale de l'utilisateur (grâce à un réseau de tables de substitution et d'opérateurs XOR).

   Lors de chaque tour, le bloc de 64 bits est découpé en deux blocs de 32 bits, et ces blocs sont échangés l'un avec l'autre selon un schéma de Feistel. Le bloc de 32 bits ayant le poids le plus fort (celui qui s'étend du bit 32 au bit 64) subira une transformation ;

3. Le résultat du dernier tour est transformé par la fonction inverse de la permutation initiale.

CHAPITRE 4 - DIFFIE HELLMAN

CRYPTOGRAPHIE ASYMETRIQUE OU CLE PUBLIQUE

La cryptographie asymétrique, ou cryptographie à clé publique, est une méthode de chiffrement qui s'oppose à la cryptographie symétrique. Elle repose sur l'utilisation d'une clé publique (qui est diffusée) et d'une clé privée (gardée secrète), l'une permettant de coder le message et l'autre de le décoder.

Ainsi, l'expéditeur peut utiliser la clé publique du destinataire pour coder un message que seul le destinataire (en possession de la clé privée) peut décoder, garantissant la confidentialité du contenu. Inversement, l'expéditeur peut utiliser sa propre clé privée pour coder un message que le destinataire peut décoder avec la clé publique ; c'est le mécanisme utilisé par la signature numérique pour authentifier l'auteur d'un message.

PRINCIPE

- Un utilisateur possède deux clés: une clé publique et une clé privée.
- Un message peut être chiffré avec la clé publique et déchiffré avec la clé privée pour assurer la sécurité.
- Un message peut être chiffré avec la clé privée et déchiffré avec la clé publique pour fournir des signatures.

LEXIQUE

Fonction à sens unique : Une fonction qui est facile à calculer dans une direction, mais difficile à calculer dans l'autre.

Trapdoor one-way function : Une fonction à sens unique qui peut être facilement inversé avec une pièce supplémentaire de connaissances.

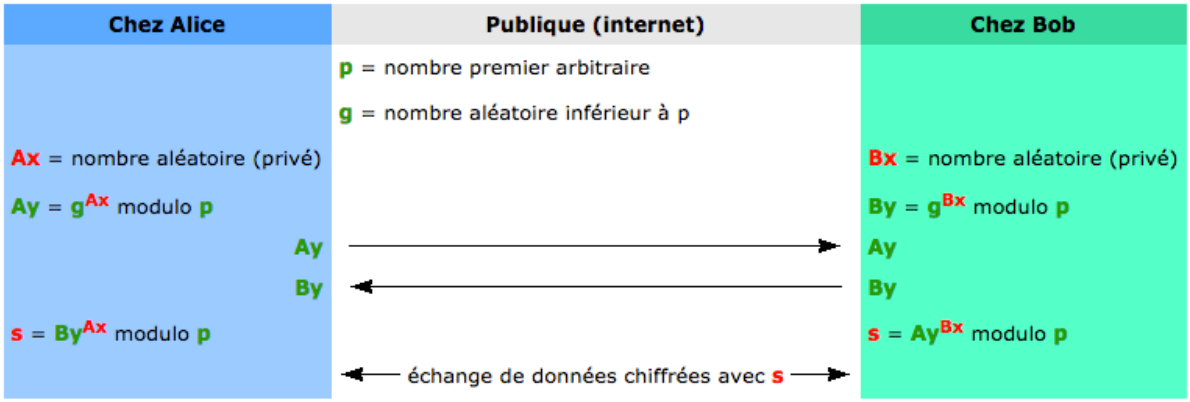
DIFFIE-HELLMAN

But

- Entre plusieurs personnes (2 ou plus)
- Etablissement d'une clé secrète commune
- Via canal non-sécurisé

PRINCIPE

Tout ce qui est en **vert** est publique (diffusé sur internet). Tout ce qui est en **rouge** est privé.



s est le secret commun d'Alice et Bob.

Un espion sera incapable de calculer **s** à partir de **p** et **g**, car il ne connait ni le nombre aléatoire **Ax** choisi par Alice, ni le nombre aléatoire **Bx** choisi par Bob. **Ay** et **By** échangés entre Alice et Bob ne l'aideront pas non plus à calculer **s**.

EXEMPLE PRATIQUE

1. Alice et Bob se mettent d'accord pour utiliser p=23 et g=5
2. Alice choisit un nombre entier secret : a=6, puis envoie à Bob : A = g^a mod p

```
A = 5^6 mod 23 A = 15'625 mod 23 A = 8
```

1. Bob choisit un entier secret : b=15, puis envoie à Alice : B = g^b mod p

```
B = 5^15 mod 23 B = 30'517'578'125 mod 23 B = 19
```

1. Alice calcule : s = B^a mod p

```
s = 196 mod 23 s = 47'045'881 mod 23 s = 2
```

1. Bob calcule : s = Ab mod p

```
s = 815 mod 23 s = 35’184’372’088’832 mod 23 s = 2
```

1. Alice et Bob ont maintenant un secret : s = 2. Explications :

```
s = 5^(6*15) mod 23

s = 5^(15*6) mod 23

s = 590 mod 23 s =
807’793’566’946’316’088’741’610’050’849’573’099’185’363’38 mod 23

s = 2
```

Autre exemple :

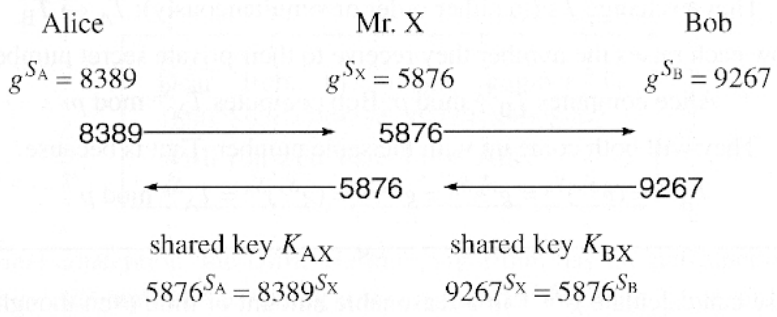
Chez Alice	Publique (internet)	Chez Bob
	On choisit un nombre premier arbitraire commun: **p = 419** On choisit un nombre aléatoire commun inférieur à p: **g = 7**	
Alice choisit un nombre aléatoire secret: **Ax = 178**		Bob choisit un nombre aléatoire secret: **Bx = 344**
Ay = 7^{178} modulo 419 = 208		**By = 7^{344} modulo 419 = 49**
Ay = 208 →		**Ay = 208**
By = 49	←	**By = 49**
s = 49^{178} modulo 419 = 107		**s = 208^{344} modulo 419 = 107**
	← échange de données chiffrées avec **s** →	

MAN IN THE MIDDLE

Cette attaque repose sur l'interception de g^ a et g^b, ce qui est facile puisqu'ils sont échangés en clair ; l'élément g étant supposé connu par tous les attaquants. Pour retrouver les nombres a et bet ainsi casser complètement l'échange, il faudrait calculer le logarithme discret de g^a et g^b, ce qui est impossible en pratique.

Mais un attaquant peut se placer entre Alice et Bob, intercepter la clé g^a envoyée par Alice et envoyer à Bob une autre clé g^a', se faisant passer pour Alice. De même, il peut remplacer la clé g^b envoyée par Bob à Alice par une clé g^b', se faisant passer pour Bob. L'attaquant communique ainsi avec Alice en utilisant la clé partagée g^(ab’) et communique avec Bob en utilisant la clé partagée g^(a’b), Alice et Bob croient communiquer directement. C'est ce que l'on appelle « attaque de l'homme du milieu ».

Alice et Bob croient ainsi avoir échangé une clé secrète alors qu'en réalité ils ont chacun échangé une clé secrète avec l'attaquant, l'homme du milieu.



CHAPITRE 5 - ARITHMETIQUE MODULAIRE

PGDC

```
pgcd(ac, bc) = |c| pgcd(a, b) pgcd(a, b) = pgcd(a, b + na)
```

Théorème d'Euclide

```
pgcd(a,0) = a pgcd(a,a) = a pgcd(a,b) = pgcd(a-b,b) pgcd(a,b) = pgcd(b,a
mod b)
```

NOMBRE PREMIER

Lorsque **pgcd(a,b) = 1** on dit que a et b sont premiers entre eux.

ARITHMETIQUE MODULAIRE

ADDITION EN ARITHMETIQUE MODULAIRE

Commutativité

```
x + y (mod n) = y + x (mod n)
```

Associativité

```
(x + y) + z (mod n) = x + (y + z) (mod n)
```

Elément neutre

```
0 + x = x + 0 = x (mod n)
```

Existence d'un opposé

```
x – x = 0 (mod n)
```

MULTIPLICATION EN ARITHMETIQUE MODULAIRE

- La multiplication conserve :
- La commutativité
- L'associativité
- L'élément neutre 1
- L'élément absorbant 0
- La distributivité par rapport à l'addition
- **Mais pas l'existence d'inverse**

L'inverse

```
X^(-1) est l'inverse de x modulo n ssi

x*x^(-1) mod n = 1
```

THEOREME DE BEZOUT

Soient a et b Z et **d = PGCD (a, b)** alors (u; v) Z^2 tels que

```
au + bv = d
```

Exemple

```
PGCD (15,24) = 3 -3*15 + 2*24 = 3 u=-3 et v=2
```

Théorème 2 (Théorème de Bézout).
Soient a, b des entiers. Il existe des entiers $u, v \in \mathbb{Z}$ tels que

$$au + bv = \text{pgcd}(a, b)$$

La preuve découle de l'algorithme d'Euclide. Les entiers u, v ne sont pas uniques. Les entiers u, v sont des ***coefficients de Bézout***. Ils s'obtiennent en «remontant» l'algorithme d'Euclide.

Exemple 8. Calculons les coefficients de Bézout pour $a = 600$ et $b = 124$. Nous reprenons les calculs effectués pour trouver $\text{pgcd}(600, 124) = 4$. La partie gauche est l'algorithme d'Euclide. La partie droite s'obtient de *bas en haut*. On exprime le pgcd à l'aide de la dernière ligne où le reste est non nul. Puis on remplace le reste de la ligne précédente, et ainsi de suite jusqu'à arriver à la première ligne.

$$\begin{array}{rcrcrcr} 600 & = & 124 & \times & 4 & + & 104 \\ 124 & = & 104 & \times & 1 & + & 20 \\ 104 & = & 20 & \times & 5 & + & 4 \\ 20 & = & 4 & \times & 5 & + & 0 \end{array}$$

$$\begin{array}{rcl} 4 & = & 124 \times (-5) + (600 - 124 \times 4) \times 6 = 600 \times 6 + 124 \times (-29) \\ 4 & = & 104 - (124 - 104 \times 1) \times 5 = 124 \times (-5) + 104 \times 6 \\ 4 & = & 104 - 20 \times 5 \end{array}$$

INVERSE MODULAIRE : ALGORITHME D'EUCLIDE

Le théorème de Bézout garantit l'existence des coefficients et donc de l'inverse d'un nombre modulo un nombre premier, et c'est l'algorithme d'Euclide qui permet de les calculer efficacement.
Dans sa version fondamentale, l'algorithme d'Euclide calcule le pgcd de deux nombres entiers. Le principe est : en supposant que a > b :

```
pgcd(a,b) = pgcd(a-b,b) = pgcd(a-2b,b) = ··· = pgcd(a modb,b)
```

Algorithme d'Euclide (Pseudo-code)

```
**Entrées Deux entiers a et b, a □ b.**
**Sorties pgcd(a,b)**
```

```
Si b = 0 Alors
       Renvoyer a; Sinon
       Calculer récursivement pgcd(b,a modb)et renvoyer le résultat;
Fin Si
```

ALGORITHME D'EUCLIDE ETENDU

La version dite «étendue » de l'algorithme d'Euclide permet, **en plus du calcul du pgcd de deux nombres**, **de trouver les coefficients de Bézout**. Il est étendu aussi parce qu'on veut le rendre un peu plus générique en lui donnant la possibilité de l'appliquer non seulement à des ensembles de nombres mais aussi à n'importe quel anneau euclidien.

CALCUL DE L'INVERSE MODULAIRE AVEC EUCLIDE ETENDU

Définition

Deux entiers a et b sont premiers entre eux (ou bien a est dit premier avec b) s'il n'ont pas de diviseurs premiers communs, ou bien, de manière équivalente, si **PGDC (a, b) = 1**.

Exemple

```
9^(−1)(mod 16)
       16 = 1 · 9 + 7;
       9 = 1 · 7 + 2;
       7 = 3 · 2 + 1;
       2 = 2 · 1 + 0 donc pgcd (16, 9) = 1
       a^p a mod p
```

Exemple 4. Calculons le pgcd de $a = 600$ et $b = 124$.

$$\begin{aligned} 600 &= 124 \times 4 + 104 \\ 124 &= 104 \times 1 + 20 \\ 104 &= 20 \times 5 + 4 \\ 20 &= 4 \times 5 + 0 \end{aligned}$$

Ainsi $\text{pgcd}(600, 124) = 4$.

Voici un exemple plus compliqué :

Exemple 5. Calculons $\text{pgcd}(9945, 3003)$.

$$\begin{aligned} 9945 &= 3003 \times 3 + 936 \\ 3003 &= 936 \times 3 + 195 \\ 936 &= 195 \times 4 + 156 \\ 195 &= 156 \times 1 + 39 \\ 156 &= 39 \times 4 + 0 \end{aligned}$$

Ainsi $\text{pgcd}(9945, 3003) = 39$.

PETIT THEOREME DE FERMAT

Théorème 4 (Petit théorème de Fermat).
Si p est un nombre premier et $a \in \mathbb{Z}$ alors

$$\boxed{a^p \equiv a \pmod{p}}$$

Corollaire 4. Si p ne divise pas a alors

$$\boxed{a^{p-1} \equiv 1 \pmod{p}}$$

Lemme 3. p divise $\binom{p}{k}$ pour $1 \leqslant k \leqslant p-1$, c'est-à-dire $\binom{p}{k} \equiv 0 \pmod{p}$.

Démonstration. $\binom{p}{k} = \frac{p!}{k!(p-k)!}$ donc $p! = k!(p-k)!\binom{p}{k}$. Ainsi $p \mid k!(p-k)!\binom{p}{k}$. Or comme $1 \leqslant k \leqslant p-1$ alors p ne divise pas $k!$ (sinon p divise l'un des facteurs de $k!$ mais il sont tous $< p$). De même p ne divise pas $(p-k)!$, donc par le lemme d'Euclide p divise $\binom{p}{k}$. □

Preuve du théorème. Nous le montrons par récurrence pour les $a \geqslant 0$.

- Si $a = 0$ alors $0 \equiv 0 \pmod{p}$.
- Fixons $a \geqslant 0$ et supposons que $a^p \equiv a \pmod{p}$. Calculons $(a+1)^p$ à l'aide de la formule du binôme de Newton :

$$(a+1)^p = a^p + \binom{p}{p-1}a^{p-1} + \binom{p}{p-2}a^{p-2} + \cdots + \binom{p}{1} + 1$$

Réduisons maintenant modulo p :

$$\begin{aligned}(a+1)^p &\equiv a^p + \binom{p}{p-1}a^{p-1} + \binom{p}{p-2}a^{p-2} + \cdots + \binom{p}{1} + 1 \pmod{p} \\ &\equiv a^p + 1 \pmod{p} \quad \text{grâce au lemme 3} \\ &\equiv a + 1 \pmod{p} \quad \text{à cause de l'hypothèse de récurrence}\end{aligned}$$

- Par le principe de récurrence nous avons démontré le petit théorème de Fermat pour tout $a \geqslant 0$. Il n'est pas dur d'en déduire le cas des $a \leqslant 0$.

□

Exemple 17. Calculons $14^{3141} \pmod{17}$. Le nombre 17 étant premier on sait par le petit théorème de Fermat que $14^{16} \equiv 1 \pmod{17}$. Écrivons la division euclidienne de 3141 par 16 :

$$3141 = 16 \times 196 + 5.$$

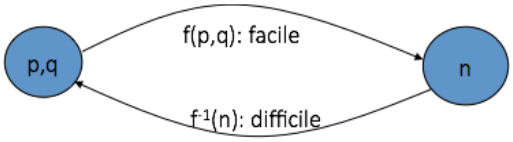
Alors

$$14^{3141} \equiv 14^{16\times 196+5} \equiv 14^{16\times 196} \times 14^5 \equiv \left(14^{16}\right)^{196} \times 14^5 \equiv 1^{196} \times 14^5 \equiv 14^5 \pmod{17}$$

Il ne reste plus qu'à calculer 14^5 modulo 17. Cela peut se faire rapidement : $14 \equiv -3 \pmod{17}$ donc $14^2 \equiv (-3)^2 \equiv 9 \pmod{17}$, $14^3 \equiv 14^2 \times 14 \equiv 9 \times (-3) \equiv -27 \equiv 7 \pmod{17}$, $14^5 \equiv 14^2 \times 14^3 \equiv 9 \times 7 \equiv 63 \equiv 12 \pmod{17}$. Conclusion : $14^{3141} \equiv 14^5 \equiv 12 \pmod{17}$.

CHAPITRE 6 - RSA

Se base sur la difficulté de factoriser un entier n en terme de deux nombres premiers.



FONCTIONNEMENT

1. On choisit **deux nombres premiers** p et q que l'on garde secrets et on pose n = p × q. Le principe étant que même connaissant n il est très difficile de retrouver p
   et q (qui sont des nombres ayant des centaines de chiffres).
2. La **clé secrète et la clé publique** se calculent à l'aide de l'**algorithme d'Euclide** et des **coefficients de Bézout**.
3. Les calculs de cryptage se feront **modulo n**.
4. Le **déchiffrement** fonctionne grâce à une variante du **petit théorème de Fermat**.

Dans cette section, c'est Bruno qui veut envoyer un message secret à Alice. Le processus se décompose ainsi :

1. Alice prépare une clé publique et une clé privée,
2. Bruno utilise la clé publique d'Alice pour crypter son message,
3. Alice reçoit le message crypté et le déchiffre grâce à sa clé privée.

ETAPE 1 - CALCUL DE LA CLE PUBLIQUE ET DE LA CLE PRIVEE

CHOIX DE DEUX NOMBRES PREMIERS

Alice effectue, une fois pour toute, les opérations suivantes (en secret) :
- elle choisit deux nombres premiers distincts p et q (dans la pratique ce sont de très grand nombres, jusqu'à des centaines de chiffres),
- Elle calcule $n = p \times q$,
- Elle calcule $\varphi(n) = (p-1) \times (q-1)$.

Exemple

$p = 5$ et $q = 17$
$n = p \times q = 85$
$\varphi(n) = (p-1) \times (q-1) = 64$

Vous noterez que le calcul de ϕ(n) n'est possible que si la décomposition de n sous la forme p × q est connue. D'où le caractère secret de ϕ(n) même si n est connu de tous.

CHOIX D'UN EXPOSANT ET CALCUL DE SON INVERSE

Alice continue :
- elle choisit un exposant e tel que $\text{pgcd}(e, \varphi(n)) = 1$,
- elle calcule l'inverse d de e module $\varphi(n)$: $d \times e \equiv 1 \pmod{\varphi(n)}$. Ce calcul se fait par l'algorithme d'Euclide étendu.

Exemple

Alice choisit par exemple $e = 5$ et on a bien $\text{pgcd}(e, \varphi(n)) = \text{pgcd}(5, 64) = 1$,
Alice applique l'algorithme d'Euclide étendu pour calculer les coefficients de Bézout correspondant à $\text{pgcd}(e, \varphi(n)) = 1$. Elle trouve $5 \times 13 + 64 \times (-1) = 1$. Donc $5 \times 13 \equiv 1 \pmod{64}$ et l'inverse de e modulo $\varphi(n)$ est $d = 13$.

CLE PUBLIQUE

La clé publique d'Alice est constituée des deux nombres : **n et e**

```
n = 85 et e = 5
```

CLE PRIVEE

Alice détruit en secret p, q et ϕ(n) qui ne sont plus utiles. Elle conserve secrètement sa clé privée.

Alice garde pour elle sa clé privée : **d**

```
d = 13
```

ETAPE 2 - CHIFFREMENT DU MESSAGE

Bruno veut envoyer un message secret à Alice. Il se débrouille pour que son message soit un entier (quitte à découper son texte en bloc et à transformer chaque bloc en un entier).

MESSAGE

Le message est un **entier m**, tel que 0 < m < n

Exemple

Bruno veut envoyer le message m

```
m = 10
```

MESSAGE CHIFFRE

Bruno récupère **la clé publique d'Alice : n et e** avec laquelle il calcule, à l'aide de l'algorithme d'exponentiation rapide, le message chiffré :

$$x \equiv m^e \pmod{n}$$

Il transmet ce message **x à Alice**

Exemple $m = 10$, $n = 85$ et $e = 5$ donc

$$x \equiv m^e \pmod{n} \equiv 10^5 \pmod{85}$$

On peut ici faire les calculs à la main :

$$10^2 \equiv 100 \equiv 15 \pmod{85}$$
$$10^4 \equiv (10^2)^2 \equiv 15^2 \equiv 225 \equiv 55 \pmod{85}$$
$$x \equiv 10^5 \equiv 10^4 \times 10 \equiv 55 \times 10 \equiv 550 \equiv 40 \pmod{85}$$

Le message chiffré est donc $x = 40$.

ETAPE 3 - DECHIFFREMENT DU MESSAGE

Alice reçoit le **message x** chiffré par Bruno, elle le décrypte à l'aide de sa **clé privée d**, par l'opération :

$$m \equiv x^d \pmod{n}$$

qui utilise également l'algorithme d'exponentiation rapide.
Nous allons prouver dans le lemme 4, que par cette opération Alice retrouve bien le message original m de Bruno.

Exemple

Exemple $c = 40$, $d = 13$, $n = 85$ donc

$$x^d \equiv (40)^{13} \pmod{85}.$$

Calculons à la main $40^{13} \equiv \pmod{85}$ on note que $13 = 8 + 4 + 1$, donc $40^{13} = 40^8 \times 40^4 \times 40$.

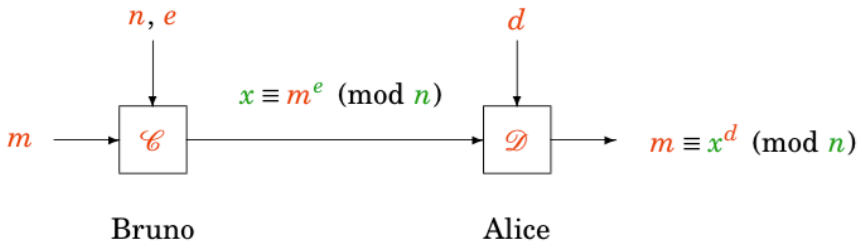
$$40^2 \equiv 1600 \equiv 70 \pmod{85}$$
$$40^4 \equiv (40^2)^2 \equiv 70^2 \equiv 4900 \equiv 55 \pmod{85}$$
$$40^8 \equiv (40^4)^2 \equiv 55^2 \equiv 3025 \equiv 50 \pmod{85}$$

Donc

$$x^d \equiv 40^{13} \equiv 40^8 \times 40^4 \times 40 \equiv 50 \times 55 \times 40 \equiv 10 \pmod{85}$$

qui est bien le message m de Bruno.

SCHEMA RECAPITULATIF



Clés d'Alice :
- publique : n, e
- privée : d

DECHIFFREMENT

Alice reçoit le message x chiffré par Bruno, elle le décrypte à l'aide de sa clé privée d, par l'opération :

$$\boxed{m \equiv x^d \pmod{n}}$$

qui utilise également l'algorithme d'exponentiation rapide.
Nous allons prouver dans le lemme 4, que par cette opération Alice retrouve bien le message original m de Bruno.

Exemple $c = 40$, $d = 13$, $n = 85$ donc

$$x^d \equiv (40)^{13} \pmod{85}.$$

Calculons à la main $40^{13} \equiv \pmod{85}$ on note que $13 = 8 + 4 + 1$, donc $40^{13} = 40^8 \times 40^4 \times 40$.

$$\begin{aligned} 40^2 &\equiv 1600 \equiv 70 \pmod{85} \\ 40^4 &\equiv (40^2)^2 \equiv 70^2 \equiv 4900 \equiv 55 \pmod{85} \\ 40^8 &\equiv (40^4)^2 \equiv 55^2 \equiv 3025 \equiv 50 \pmod{85} \end{aligned}$$

Donc

$$x^d \equiv 40^{13} \equiv 40^8 \times 40^4 \times 40 \equiv 50 \times 55 \times 40 \equiv 10 \pmod{85}$$

qui est bien le message m de Bruno.

QUELQUES EXPLICATIONS SUR LE DECHIFFREMENT (LEMME 4)

Le principe de déchiffrement repose sur le petit théorème de Fermat amélioré.

Lemme 4. Soit d l'inverse de e modulo $\varphi(n)$.

$$\text{Si } c \equiv m^e \pmod{n} \text{ alors } m \equiv x^d \pmod{n}.$$

Ce lemme prouve bien que le message original m de Bruno, chiffré par clé publique d'Alice (e,n) en le message x, peut-être retrouvé par Alice à l'aide de sa clé secrète d.

Démonstration. – Que d soit l'inverse de e modulo $\varphi(n)$ signifie $d \cdot e \equiv 1 \pmod{\varphi(n)}$. Autrement dit, il existe $k \in \mathbb{Z}$ tel que $d \cdot e = 1 + k \cdot \varphi(n)$.

– On rappelle que par le petit théorème de Fermat généralisé : lorsque m et n sont premiers entre eux

$$m^{\varphi(n)} \equiv m^{(p-1)(q-1)} \equiv 1 \pmod{n}$$

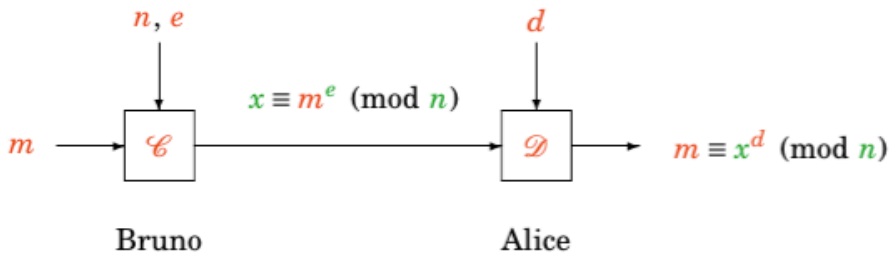
– **Premier cas** $\text{pgcd}(m,n) = 1$.
Notons $c \equiv m^e \pmod{n}$ et calculons x^d :

$$x^d \equiv (m^e)^d \equiv m^{e \cdot d} \equiv m^{1+k\cdot\varphi(n)} \equiv m \cdot m^{k\cdot\varphi(n)} \equiv m \cdot (m^{\varphi(n)})^k \equiv m \cdot (1)^k \equiv m \pmod{n}$$

– **Deuxième cas** $\text{pgcd}(m,n) \neq 1$.
Comme n est le produit des deux nombres premiers p et q et que m est strictement plus petit que n alors si m et n ne sont pas premiers entre eux cela implique que p divise m ou bien q divise m (mais pas les deux en même temps). Faisons l'hypothèse $\text{pgcd}(m,n) = p$ et $\text{pgcd}(m,q) = 1$, le cas $\text{pgcd}(m,n) = q$ et $\text{pgcd}(m,p) = 1$ se traiterait de la même manière.
Étudions $(m^e)^d$ à la fois modulo p et modulo q à l'image de ce que nous avons fait dans la preuve du théorème de Fermat amélioré.
– modulo p : $m \equiv 0 \pmod{p}$ et $(m^e)^d \equiv 0 \pmod{p}$ donc $(m^e)^d \equiv m \pmod{p}$,
– modulo q : $(m^e)^d \equiv m \times (m^{\varphi(n)})^k \equiv m \times (m^{q-1})^{(p-1)k} \equiv m \pmod{q}$.
Comme p et q sont deux nombres premiers distincts, ils sont premiers entre eux et on peut écrire comme dans la preuve du petit théorème de Fermat amélioré que

$$(m^e)^d \equiv m \pmod{n}$$

SCHEMA RECAPITULATIF



Clés d'Alice :
– publique : n, e
– privée : d

THEOREME DES RESTES CHINOIS

Soient p, q avec PGDC(p,q) = 1. Si :

x = y (mod p)

x = y (mod q)

alors x = y (mod pq)

Exemple

Cherchons à résoudre le système de congruences suivant :

$$\begin{cases} x \equiv 1 \pmod 3 \\ x \equiv 2 \pmod 5 \\ x \equiv 3 \pmod 7 \end{cases}$$

On pose $M = 3 \times 5 \times 7 = 105$

$$\begin{array}{lll} M_1 = 105/3 = 35 & y_1 \times 35 \equiv 1 \pmod 3 & y_1 = 2 \\ M_2 = 105/5 = 21 & y_2 \times 21 \equiv 1 \pmod 5 & y_2 = 1 \\ M_3 = 105/7 = 15 & y_3 \times 15 \equiv 1 \pmod 7 & y_3 = 1 \end{array}$$

$$x \equiv 1 \times 35 \times 2 + 2 \times 21 \times 1 + 3 \times 15 \times 1 \equiv 157 \equiv 52 \pmod{105}$$

L'EXPONENTIATION RAPIDE OU EXPONENTIATION RAPIDE

Nous aurons besoin de calculer rapidement des puissances modulo n. Pour cela il existe une méthode beaucoup plus efficace que de calculer d'abord a^k puis de le réduire modulo n. Il faut garder à l'esprit que les entiers que l'on va manipuler ont des dizaines voir des centaines de chiffres.
Voyons la technique sur l'exemple de $5^{11} \pmod{14}$. L'idée est de seulement calculer $5, 5^2, 5^4, 5^8 \ldots$ et de réduire modulo n à chaque fois. Pour cela on remarque que $11 = 8+2+1$ donc

$$5^{11} = 5^8 \times 5^2 \times 5^1.$$

Calculons donc les $5^{2^i} \pmod{14}$:

$$\begin{aligned}
5 &\equiv 5 \pmod{14} \\
5^2 &\equiv 25 \equiv 11 \pmod{14} \\
5^4 &\equiv 5^2 \times 5^2 \equiv 11 \times 11 \equiv 121 \equiv 9 \pmod{14} \\
5^8 &\equiv 5^4 \times 5^4 \equiv 9 \times 9 \equiv 81 \equiv 11 \pmod{14}
\end{aligned}$$

à chaque étape est effectuée une multiplication modulaire. Conséquence :

$$5^{11} \equiv 5^8 \times 5^2 \times 5^1 \equiv 11 \times 11 \times 5 \equiv 11 \times 55 \equiv 11 \times 13 \equiv 143 \equiv 3 \pmod{14}.$$

Nous obtenons donc un calcul de $5^{11} \pmod{14}$ en 5 opérations au lieu de 10 si on avait fait $5 \times 5 \times 5 \cdots$.
Voici une formulation générale de la méthode. On écrit le développement de l'exposant k en base 2 : $(k_\ell, \ldots, k_2, k_1, k_0)$ avec $k_i \in \{0,1\}$ de sorte que

$$k = \sum_{i=0}^{\ell} k_i 2^i.$$

On obtient alors

$$x^k = x^{\sum_{i=0}^{\ell} k_i 2^i} = \prod_{i=0}^{\ell} (x^{2^i})^{k_i}.$$

Par exemple 11 en base 2 s'écrit $(1,0,1,1)$, donc, comme on l'a vu :

$$5^{11} = (5^{2^3})^1 \times (5^{2^2})^0 \times (5^{2^1})^1 \times (5^{2^0})^1.$$

Voici un autre exemple : calculons $17^{154} \pmod{100}$. Tout d'abord on décompose l'exposant $k = 154$ en base 2 : $154 = 128+16+8+2 = 2^7+2^4+2^3+2^1$, il s'écrit donc en base 2 : $(1,0,0,1,1,0,1,0)$.

Ensuite on calcule $17, 17^2, 17^4, 17^8, \ldots, 17^{128}$ modulo 100.

$$\begin{aligned}
17 &\equiv 17 \pmod{100} \\
17^2 &\equiv 17 \times 17 \equiv 289 \equiv 89 \pmod{100} \\
17^4 &\equiv 17^2 \times 17^2 \equiv 89 \times 89 \equiv 7921 \equiv 21 \pmod{100} \\
17^8 &\equiv 17^4 \times 17^4 \equiv 21 \times 21 \equiv 441 \equiv 41 \pmod{100} \\
17^{16} &\equiv 17^8 \times 17^8 \equiv 41 \times 41 \equiv 1681 \equiv 81 \pmod{100} \\
17^{32} &\equiv 17^{16} \times 17^{16} \equiv 81 \times 81 \equiv 6561 \equiv 61 \pmod{100} \\
17^{64} &\equiv 17^{32} \times 17^{32} \equiv 61 \times 61 \equiv 3721 \equiv 21 \pmod{100} \\
17^{128} &\equiv 17^{64} \times 17^{64} \equiv 21 \times 21 \equiv 441 \equiv 41 \pmod{100}
\end{aligned}$$

Il ne reste qu'à rassembler :

$$17^{154} \equiv 17^{128} \times 17^{16} \times 17^8 \times 17^2 \equiv 41 \times 81 \times 41 \times 89 \equiv 3321 \times 3649 \equiv 21 \times 49 \equiv 1029 \equiv 29 \pmod{100}$$

Congruence

- En arithmétique modulaire, deux entiers relatifs sont **congrus modulo n** s'ils ont même reste dans la division euclidienne par n. On peut aussi dire qu'ils sont congrus modulo n si leur différence est un multiple de n.

Inverse modulaire

12 * 12^(-1) = 1 mod 7

~~12 * 1 mod 7 = 5~~

~~12 * 2 mod 7 = 3~~

12 * 3 mod 7 = 1 (36 et 35)

THEOREME ET DEMONSTRATION

Théorème *(Petit théorème de Fermat)*

Pour tout entier a et tout nombre premier p, $a^p \equiv a \pmod p$

Lemme

Soient p un nombre premier, *A UN ENTIER PREMIER AVEC P, B ET C DEUX ENTIERS QUELCONQUES,*

$A \cdot B \equiv A \cdot C \pmod P \Rightarrow B \equiv C \pmod P$

Démonstration du théorème

Si $a \equiv 0 \pmod p$, le résultat est évident.

Si a est non nul modulo p, a est inversible modulo p. Le théorème peut donc se formuler de la façon suivante en multipliant les deux membres de l'énoncé par a^{-1} :
$a^{p-1} \equiv 1 \pmod p$ pour p premier et a non nul modulo p.

Considérons l'ensemble $E = \{1 \cdot a , 2 \cdot a , 3 \cdot a , \dots , (p-1) \cdot a\}$.
D'après le lemme, les éléments de E sont distincts modulo p, et aucun d'eux n'est nul modulo p (sinon, toujours d'après le lemme, $0 \cdot a = k \cdot a \pmod p \Rightarrow 0 = k$ modulo p ; or $k < p$).
Ainsi modulo p, l'ensemble E qui contient p-1 éléments distinct non nuls est égal à l'ensemble $N = \{1 , 2 , 3 , \dots , (p-1)\}$.

Par suite :

$1a \cdot 2a \cdot 3a \cdot \dots \cdot (p-1)a \equiv 1 \cdot 2 \cdot 3 \cdot \dots \cdot (p-1) \pmod p$,
$(1 \cdot 2 \cdot 3 \cdot \dots \cdot (p-1)) \cdot a^{p-1} \equiv 1 \cdot 2 \cdot 3 \cdot \dots \cdot (p-1) \pmod p$,
$(p-1)! \cdot a^{p-1} \equiv (p-1)! \pmod p$.

Comme p et (p-1) ! n'ont pas de facteurs communs, (p - 1) ! est non nul modulo p et le lemme s'applique : $a^{p-1} \equiv 1 \pmod p$.

Lemme

Soient p un nombre premier, *A UN ENTIER PREMIER AVEC P, B ET C DEUX ENTIERS QUELCONQUES*,

$A \cdot b \equiv A \cdot C \pmod P \Rightarrow B \equiv C \pmod P$

Démonstration

$A \cdot b \equiv A \cdot C \pmod P \Rightarrow$ p divise $(A \cdot b - A \cdot C) = A (b - c)$.
Comme a ne contient pas le facteur premier *P*, (b - c) doit le contenir, puisque la décomposition en produit de facteurs premiers est unique d'après le théorème fondamental de l'arithmétique.

p divise donc (b - c) $\Rightarrow B \equiv C \pmod P$.

Théorème

a et b sont congrus modulo n si et seulement si a et b ont le même reste de la division par n.

Démonstration

a et b sont congrus modulo n $\Leftrightarrow$ b - a = k · n.
a = nq + r , 0 ≤ r < n (division euclidienne de a par n)
b = nq' + r' , 0 ≤ r' < n (division euclidienne de b par n)
a = b mod n $\Leftrightarrow$ n divise b - a $\Leftrightarrow$ n divise [(nq + r) - nq' + r')]
$\Leftrightarrow$ n divise [nq -nq') + (r - r')] $\Leftrightarrow$ n | (r - r') $\Leftrightarrow$ r - r' = 0 (r et r' sont positifs, inférieurs à n).

Propriété

a ≡ b (mod n) et c ≡ d (mod n) $\Rightarrow$ a + c ≡ b + d (mod n)

Démonstration

a ≡ b (mod n) $\Rightarrow$ b - a = k · n

c ≡ d (mod n) $\Rightarrow$ d - c = k' · n

Ainsi, (b+d) - (a+c) = (k + k') · n $\Rightarrow$ a+c ≡ b+d (mod n).

Propriété

a ≡ b (mod n) et c ≡ d (mod n) $\Rightarrow$ a · c ≡ b · d (mod n)

Démonstration

a ≡ b (mod n) $\Rightarrow$ b - a = kn

c ≡ d (mod n) $\Rightarrow$ d - c = k'n

Ainsi, (b · d) = (a + nk) (c + nk') = a · c + (ak' + ck + nkk') · n,
ce que montre que a · c ≡ b · d (mod n).

Propriété

Pour tout entier strictement positif k, $a \equiv b \pmod n \Rightarrow a^k \equiv b^k \pmod n$

Démonstration (par récurrence sur k)

Le résultat est vrai pour k = 1 par hypothèse.
Supposons que $a^k \equiv b^k \pmod n$ pour un entier strictement positif k.
Alors, en utilisant la compatibilité de la loi $\cdot$ pour la congruence modulo n,
$a^k \cdot a \equiv b^k \cdot b \pmod n \Rightarrow a^{k+1} \equiv b^{k+1} \pmod n$.

Théorème

a est inversible modulo n si et seulement si a et n sont premiers entre eux

Démonstration

Supposons qu'il existe un nombre a^{-1} tel que $a \cdot a^{-1} \equiv 1 \pmod n$.
Alors, $a \cdot a^{-1} = 1 + k \cdot n$ et $a \cdot a^{-1} - k \cdot n = 1$.
Par le *théorème de Bézout*, D(a,n) = 1.

Supposons D(a,n) = 1. Par le théorème de Bézout, il existe deux entiers relatifs u et v
tels que $a \cdot u + b \cdot n = 1$.
Ainsi, $a \cdot u = 1 + b \cdot n$ et $a \cdot u \equiv 1 \pmod n$.
L'inverse a^{-1} de a est donc u.

Théorème

$(\mathbb{Z}/n\mathbb{Z}, +, \cdot)$ est un corps si et seulement si n est premier

Démonstration

$(\mathbb{Z}/n\mathbb{Z}, +, \cdot)$ est un anneau commutatif, unitaire.
Il suffit donc de montrer que tout élément non nul de $\mathbb{Z}/n\mathbb{Z}$ est inversible si et seulement si n est premier.

Si n est premier, D(a,n) = 1 pour tout $a \in \{1, 2, .., n-1\}$ et a est inversible modulo n.

Si $\mathbb{Z}/n\mathbb{Z}$ est un corps, tout $a \in \{1, 2, .., n-1\}$ est inversible modulo n et D(a,n) =1. Comme aucun des entiers entre 2 et n-1 ne divise n, n est premier.