

Mathématiques-Cryptographie

Anne Garcia-Sanchez

M2i cyber dev - CFA CCI Avignon
19 octobre 2023

Chiffrement par substitution mono-alphabétique

lettre de l'alphabet du message \rightarrow autre lettre du même alphabet

clair	A	B	C	D	E	F	G	H	I	J	K	L	M
chiffré	D	E	F	G	H	I	J	K	L	M	N	O	P

lettre de l'alphabet du message \rightarrow lettre d'un autre alphabet

clair	A	B	C	D	E	F	G	H	I	J	K	L	M
chiffré	β	δ	ε	φ	γ	η	λ	ζ	κ	μ	ν	ρ	π

Chiffrement par substitution mono-alphabétique

- Chiffrement par décalage - César
- ROT13, ROT47
- Chiffre Atbash, Atbah
- Chiffre Pigpen
- Carré de Polybe
- Chiffrement affine
- Cas général

Chiffrement affine

clés: a et b entiers compris entre 0 et 25 (avec a premier avec 26)

lettre du texte clair: rang m

$$c \equiv a \times m + b \pmod{26}$$

c : rang de la lettre chiffrée

Rappel: deux nombres entiers sont premiers entre eux s'ils n'ont pas de diviseur commun autre que 1

Nombres premiers

nombre premier (*prime number*): entier naturel qui n'admet comme diviseurs que 1 et lui-même.

2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43, 47, 53, 59, 61, 67, 71, 73, 79, 83, 89, et 97

nombre composé (*composite number*): entier qui est le produit de deux entiers strictement supérieurs à 1 et possède de ce fait au moins trois diviseurs.

Nombres premiers entre eux

Deux entiers sont **premiers entre eux** ou **coprimiers** s'ils n'ont pas de diviseur commun autre que 1 et -1.

Deux entiers a et b sont premiers entre eux si $\text{PGCD}(a, b) = 1$.

Remarques:

- les deux nombres ne sont pas forcément premiers:
9 n'est pas premier mais est premier avec 4
- un nombre premier n'est pas forcément premier avec un autre nombre:
13 est premier mais n'est pas premier avec 26
- deux nombres premiers distincts sont premiers entre eux

Chiffrement affine

a doit être premier avec 26

valeurs possibles pour a ?

1 ~~2~~ 3 ~~4~~ 5 ~~6~~ 7 ~~8~~ 9 ~~10~~ 11 ~~12~~ ~~13~~ ~~14~~ 15 ~~16~~ 17 ~~18~~ 19 ~~20~~ 21 ~~22~~ 23 ~~24~~ 25

Chiffrement affine

Exemple: pour chiffrer le message SECRET avec la clé $a = 3, b = 2$

clair	A	B	C	D	E	F	G	H	I	J	K	L	M	N
rang	0	1	2	3	4	5	6	7	8	9	10	11	12	13

clair	O	P	Q	R	S	T	U	V	W	X	Y	Z
rang	14	15	16	17	18	19	20	21	22	23	24	25

message clair	S	E	C	R	E	T
rangs	18	4	2	17	4	19
calcul $3x + 2$	56	14	8	53	14	59
réduction modulo 26	4	14	8	1	14	7
message chiffré	E	O	I	B	O	H

Déchiffrement affine

message clair	S	E	C	R	E	T
rangs	18	4	2	17	4	19
calcul $3x + 2$	56	14	8	53	14	59
réduction modulo 26	4	14	8	1	14	7
message chiffré	E	O	I	B	O	H

Déchiffrement affine

message clair	S	E	C	R	E	T
rangs	18	4	2	17	4	19
calcul $3x + 2$	56	14	8	53	14	59
réduction modulo 26	4	14	8	1	14	7
message chiffré	E	O	I	B	O	H

$$3x + 2 \equiv 4 \pmod{26}$$

$$3x \equiv 4 - 2 \pmod{26}$$

$$3x \equiv 2 \pmod{26}$$

Que vaut x ?

Déchiffrement affine

message clair	S	E	C	R	E	T
rangs	18	4	2	17	4	19
calcul $3x + 2$	56	14	8	53	14	59
réduction modulo 26	4	14	8	1	14	7
message chiffré	E	O	I	B	O	H

$$3x + 2 \equiv 4 \pmod{26}$$

$$3x \equiv 4 - 2 \pmod{26}$$

$$3x \equiv 2 \pmod{26}$$

$$3^{-1}3x \equiv 3^{-1}2 \pmod{26}$$

$$x \equiv 3^{-1}2 \pmod{26}$$

Déchiffrement affine

Cherchons une valeur pour 3^{-1} telle que $3 \times 3^{-1} \equiv 1 \pmod{26}$

1

2

3

4

5

6

7

8

9

10

...

Déchiffrement affine

$$3 \times 9 \equiv 1 \pmod{26}$$

9 est l'inverse de 3 modulo 26.

Déchiffrement affine

$$3 \times 9 \equiv 1 \pmod{26}$$

9 est l'inverse de 3 modulo 26.

$$x \equiv 3^{-1}2 \pmod{26}$$

$$x \equiv 9 \times 2 \pmod{26}$$

$$x \equiv 18 \pmod{26}$$

Inverse modulaire

L'inverse modulaire d'un entier relatif a modulo n est un entier u satisfaisant l'équation :

$$a \times u \equiv 1 \pmod{n}$$

u peut être noté a^{-1}

L'inverse de a modulo n existe si et seulement si a et n sont premiers entre eux.

Inverse modulaire

Exemple: quel est l'inverse de 2 modulo 7?

Python:

```
>>> pow(2, -1, 7)
4
>>>
```

on vérifie:

$$2 \times 4 \equiv 1 \pmod{7}$$

Comment calculer l'inverse de a modulo b ?

Identité de Bézout:

Soient a et b deux entiers relatifs.

Il existe deux entiers relatifs u et v tels que

$$a \times u + b \times v = PGCD(a, b).$$

u et v : coefficients de Bézout

algorithme d'Euclide \rightarrow calcul de $PGCD(a, b)$

algorithme d'Euclide étendu \rightarrow calcul de u, v et $PGCD(a, b)$

a et b premiers entre eux donc $PGCD(a, b) = 1$

$$a \times u + b \times v = 1 \text{ donc } a \times u = 1 - b \times v \text{ donc } a \times u \equiv 1 \pmod{b}$$

Algorithme d'Euclide

a et b entiers avec $a > b$, alors $PGCD(a, b) = PGCD(b, a \bmod b)$

Exemple: calcul du PGCD de 120 et 23

$$120 = 23 \times 5 + 5$$

$$23 = 5 \times 4 + 3$$

$$5 = 3 \times 1 + 2$$

$$3 = 2 \times 1 + 1$$

$$2 = 1 \times 2 + 0$$

Algorithme d'Euclide étendu

Cherchons l'inverse de 23 modulo 120

$$120 = 23 \times 5 + 5$$

$$23 = 5 \times 4 + 3$$

$$5 = 3 \times 1 + 2$$

$$3 = 2 \times 1 + 1$$

$$2 = 1 \times 2 + 0$$

r											=	u	×	a	+	v	×	b			
120											=	1	×	120	+	0	×	23			
23											=	0	×	120	+	1	×	23			
5	=	120	-	5	×	23					=	1	×	120	+	-5	×	23			
3	=	23	-	4	×	5	=	1×23		-	4	×	(1×120 - 5×23)	=	-4	×	120	+	21	×	23
2	=	5	-	1	×	3	=	(1×120 - 5×23)		-	1	×	(-4×120 + 21×23)	=	5	×	120	+	-26	×	23
1	=	3	-	1	×	2	=	(-4×120 + 21×23)		-	1	×	(5×120 - 26×23)	=	-9	×	120	+	47	×	23

donc $1 = -9 \times 120 + 47 \times 23$ ou $23 \times 47 = 1 + 9 \times 120$

donc l'inverse de 23 modulo 120 est 47

Déchiffrement affine

c : rang de la lettre chiffrée

m : rang de la lettre du message en clair

$$c \equiv a \times m + b \pmod{26}$$

$$a \times m + b \equiv c \pmod{26}$$

$$a \times m \equiv c - b \pmod{26}$$

$$m \equiv a^{-1}(c - b) \pmod{26}$$

a^{-1} **inverse modulaire**: $a \times a^{-1} \equiv 1 \pmod{26}$

Chiffrement affine

Nombre de clés?

a : 1 3 5 7 9 11 15 17 19 21 23 25 : 12 possibilités

b : 0 1 2 3 4 5 6 7 8 9 10 11 12...25: 26 possibilités

$$12 \times 26 = 312$$

substitution: cas général

permutation des lettres de l'alphabet

Exemple: GTLUMWZVCOKYEQDIFASHBJNXPR

clair	ABCDEFGHIJKLMNOPQRSTUVWXYZ
chiffré	GTLUMWZVCOKYEQDIFASHBJNXPR

substitution: cas général

Nombre de clés?

$$26 \times 25 \times 24 \dots \times 4 \times 3 \times 2$$

26! se lit **factorielle** $26 \approx 4000000000000000000000000000$