Mathématiques-Cryptographie

Anne Garcia-Sanchez

M2i cyber dev - CFA CCI Avignon

14 septembre 2023

M2i - Programme de première année (L3)

- Chiffrements par substitution:
  - mono-alphabétiques:

    César, Rot13, Rot47, Atbash, Pigpen, Templiers, hommes dansants, Polybe, affine, permutation de l'alphabet
  - poly-alphabétiques:

    Vigenère, Hill, Beaufort, Enigma
- Chiffrements par transposition:

  dents de scie, scytale, permutation de colonnes
- Chiffrements par flux - OTP - LFSR
- Chiffrements par blocs - DES - 3DES - AES
- Fonctions de hachage

cryptologie, cryptographie, cryptanalyse

cryptologie:

1. **cryptographie**:

   étude et conception des procédés assurant la sécurité des communications

2. **cryptanalyse**:

   - cherche les failles dans ces procédés

   - cherche à retrouver les informations cachées

Principe général et terminologie

- Alice veut envoyer le message M à Bob

  M: **texte clair** - *plaintext*

- Alice **chiffre** le message M avec la clé K et obtient C

  chiffrement du message : *encryption*

  C: **texte chiffré** - *ciphertext*

- Bob **déchiffre** C avec la clé K et retrouve M

  déchiffrement du message : *decryption*

- Eve intercepte le chiffré C

  Elle ne connait pas la clé K

  Eve **décrypte** le message

environ 1500 av. J. C.

premier document chiffré: tablette d'argile (Mésopotamie)

recette secrète de vernis de poterie

environ 500 av. J. C.

Chiffre hébreu Atbash (sud Mésopotamie)

Aleph	Pari	Gimel	Daleth	Il h	Vav	Zayin	Het	Tet	Yodh	Kaph	Lamed	Mem	Religieuse	Samech	Ayin	Peh	Tzady	Koof	Reish	Tibia	Taw
א	ב	ג	ד	ה	ו	ז	ח	ט	י	כ	ל	מ	נ	ס	ע	פ	צ	ק	ר	ש	ת
Taw	Tibia	Reish	Koof	Tzady	Peh	Ayin	Samech	Religieuse	Mem	Lamed	Kaph	Yodh	Tet	Het	Zayin	Vav	Il h	Daleth	Gimel	Pari	Aleph
ת	ש	ר	ק	צ	פ	ע	ס	נ	מ	ל	כ	י	ט	ח	ז	ו	ה	ד	ג	ב	א

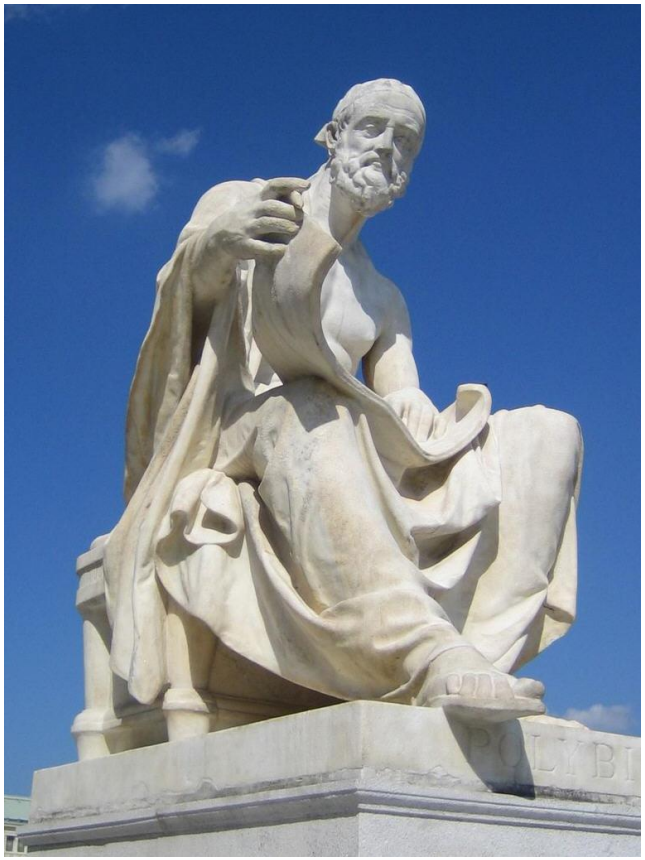
environ 500 av. J. C.

Scytale ou bâton de Plutarque (Grèce)

environ 150 av. J. C.

carré de Polybe (historien Grec)

	1	2	3	4	5
1	A	B	C	D	E
2	F	G	H	I/J	K
3	L	M	N	O	P
4	Q	R	S	T	U
5	V	W	X	Y	Z



environ 50 av. J. C.

Jules César: chiffre de César (Rome)

Chiffrement par substitution

remplacer chaque symbole du texte clair par d'autres symboles sans modifier l'ordre

clair	M	E	S	S	A	G	E
chiffré	C_1	C_2	C_3	C_4	C_5	C_6	C_7

le chiffrement par transposition modifie l'ordre des symboles

Chiffrement par substitution mono-alphabétique

lettre de l'alphabet du message $\longrightarrow$ 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 $\longrightarrow$ 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

Chiffrements par substitution mono-alphabétique

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

Chiffrement par décalage - *shift cipher* - César

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

clair	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
chiffré	Q	R	S	T	U	V	W	X	Y	Z	A	B	C

Chiffrement par décalage - *shift cipher* - César

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

lettre	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
rang	13	14	15	16	17	18	19	20	21	22	23	24	25

Espace des clés

La valeur de décalage k est appelée *clé de chiffrement*.

26 clés possibles pour le chiffrement de César

Chiffrement par décalage - *shift cipher* - César

clé $k = 3$

lettre en clair	A	B	C	D	E	F	G	H	I	J	K	L	M
rang	0	1	2	3	4	5	6	7	8	9	10	11	12
rang + k	3	4	5	6	7	8	9	10	11	12	13	14	15
% 26	3	4	5	6	7	8	9	10	11	12	13	14	15
lettre chiffrée	D	E	F	G	H	I	J	K	L	M	N	O	P

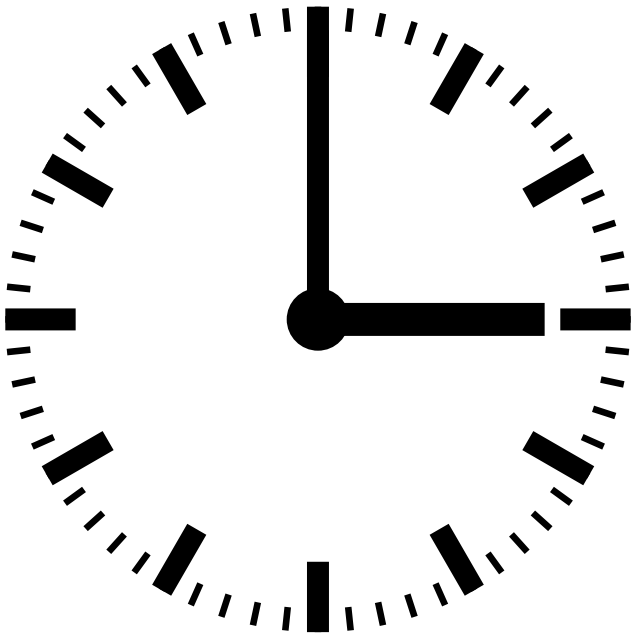
lettre en clair	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
rang	13	14	15	16	17	18	19	20	21	22	23	24	25
rang + k	16	17	18	19	20	21	22	23	24	25	26	27	28
% 26	16	17	18	19	20	21	22	23	24	25	0	1	2
lettre chiffrée	Q	R	S	T	U	V	W	X	Y	Z	A	B	C

Congruences

$a \equiv b \pmod{n}$ se lit «a est congru à b modulo n»

On peut passer de a à b en ajoutant ou retranchant un certain nombre de fois n

$a = b + kn$ avec k entier



exemple: $15 \equiv 3 \pmod{12}$

Congruences

exemples:

$28 \equiv 2 \pmod{26}$ car $28 = 2 + 1 \times 26$

$40 \equiv 4 \pmod{12}$ car $40 = 4 + 3 * 12$

$29 \equiv 15 \pmod{7}$ car $29 = 15 + 2 * 7$

Congruences avec Python

```
>>> 28 % 26
2
>>> 40 % 12
4
>>> 29 % 7
1
>>> 15 % 7
1
>>>
```

Congruences

Notation

On note $\mathbb{Z}/n\mathbb{Z}$ l'ensemble de tous les éléments de $\mathbb{Z}$ modulo n.

Rappel: $\mathbb{Z}$ est l'ensemble des entiers relatifs comme -10 -2 5 34

$\mathbb{Z}/n\mathbb{Z}$ contient n éléments qui peuvent être représentés par $\{0, 1, ..., n-1\}$.

Pour un entier $a \in \mathbb{Z}$ quelconque, son représentant dans $\{0, 1, ..., n-1\}$ correspond au reste de la division euclidienne de a par n.

chiffrement par décalage (César)

- fonction de chiffrement de décalage k:

  si r est le rang de la lettre à chiffrer

  calcul du rang c de la lettre chiffrée: $c \equiv r + k \pmod{26}$

  on prend le plus petit représentant: $c < 26$

- fonction de déchiffrement de décalage k:

  $r \equiv c - k \pmod{26}$

  on prend le plus petit représentant: $r < 26$

Chiffrement ROT13 ou chiffre Albam

ROT13 - *rotation 13*: décalage de 13

correspond au chiffre hébreu Albam

13 est la moitié de 26 donc
fonction de déchiffrement = fonction de chiffrement

clair	A	B	C	D	E	F	G	H	I	J	K	L	M
chiffré	N	O	P	Q	R	S	T	U	V	W	X	Y	Z

clair	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
chiffré	A	B	C	D	E	F	G	H	I	J	K	L	M

HELLO chiffré URYYB chiffré HELLO

Chiffre ROT47

ROT47 permet de chiffrer lettres, chiffres et des caractères spéciaux

alphabet de 94 caractères:

table ASCII entre le caractère 33 et le caractère 126

```
 !"#$%&'()*+,-./
0123456789:;<=>?
@ABCDEFGHIJKLMNO
PQRSTUVWXYZ[\]^_
`abcdefghijklmno
pqrstuvwxyz{|}~
```

hello chiffré 96==@ chiffré hello

Chiffre Atbash

chiffre hébreu

alphabet inversé

pour l'alphabet latin:

clair	A	B	C	D	E	F	G	H	I	J	K	L	M
chiffré	Z	Y	X	W	V	U	T	S	R	Q	P	O	N

clair	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
chiffré	M	L	K	J	I	H	G	F	E	D	C	B	A

Le chiffre Atbah

chiffre hébreu

associe les lettres par groupe de quatre :

lettres A B C D associées aux lettres F G H I ordonnées à l'envers

lettres J K L M associées aux lettres O P Q R ordonnées à l'envers

lettres S T U V associées aux lettres W X Y Z ordonnées à l'envers

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

clair	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
chiffré	E	M	L	K	J	Z	Y	X	W	V	U	T	S

chiffre de Wolseley

Lord Garnet Joseph Wolseley: général anglais fin du 18° siècle

chiffre Atbash amélioré grâce à une clé

une lettre de l'alphabet supprimée: J en anglais ou W en français

choix d'une clé (ici CRYPTO) puis reste de l'alphabet sans J ou W

séquence de lettres écrite dans l'ordre inverse

clair	C	R	Y	P	T	O	A	B	D	E	F	G	H
chiffré	Z	X	V	U	S	Q	N	M	L	K	J	I	H

clair	I	J	K	L	M	N	Q	S	U	V	X	Z
chiffré	G	F	E	D	B	A	O	T	P	Y	R	C

chiffre de Wolseley

C	R	Y	P	T
O	A	B	D	E
F	G	H	I	J
K	L	M	N	Q
S	U	V	X	Z

clair	C	R	Y	P	T	O	A	B	D	E	F	G	H
chiffré	Z	X	V	U	S	Q	N	M	L	K	J	I	H

clair	I	J	K	L	M	N	Q	S	U	V	X	Z
chiffré	G	F	E	D	B	A	O	T	P	Y	R	C

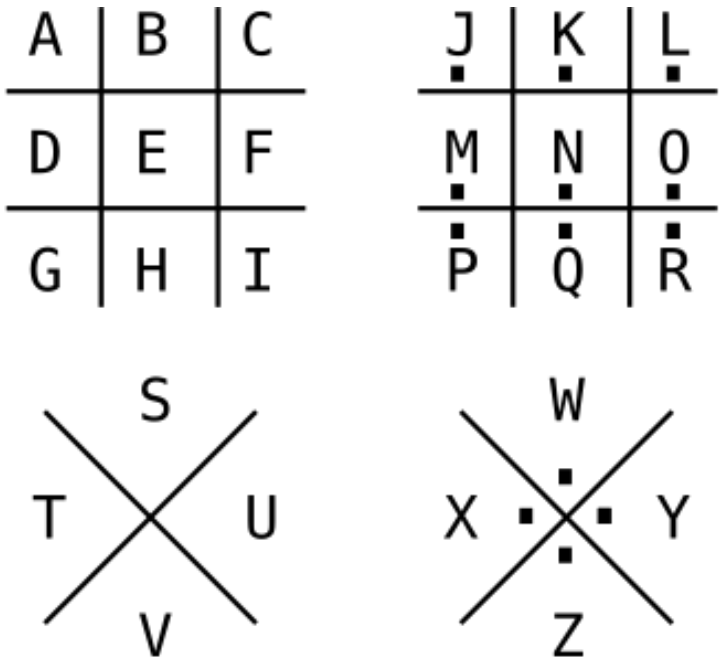
chiffrements réversibles

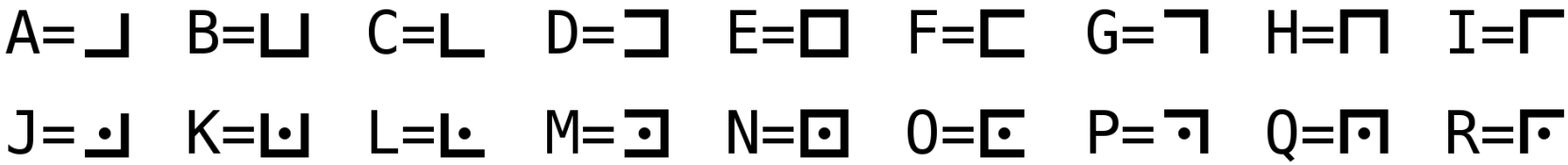
Rot13, Rot47, Atbash, Atbah, Wolseley: chiffres réversibles

message chiffré deux fois redonne le message en clair

Chiffre Pigpen - chiffre des francs-maçons

le parc à cochons:





Chiffre des templiers