Cryptographie avancée

Anne Garcia-Sanchez

M2i M1 - CCI Avignon

10 septembre 2024

Programme - 12 séances

- Révisions: chiffrements symétriques, fonctions de hachage
- Arithmétique pour les chiffrements asymétriques:
  - exponentiation modulaire
  - inverse modulaire
  - tests de primalité
  - factorisation
- Fonctions à sens unique
- Chiffrement RSA
- Attaques sur chiffrement RSA
- Problème du logarithme discret
- Mise en accord de clés de Diffie-Hellman
- Chiffrement ElGamal
- Authentification, signatures numériques
- Stéganographie

Révisions chiffrements symétriques

- 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

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 - chiffrements symétriques

- 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

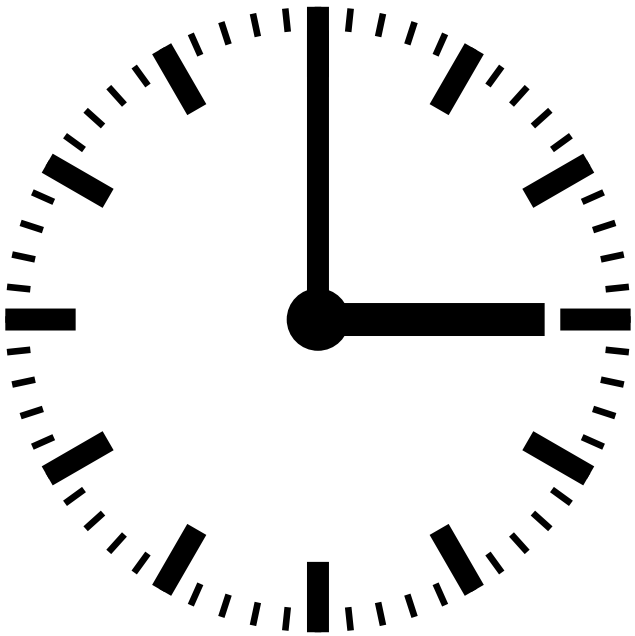
  Eve **décrypte** le message

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 $\{0, 1, ..., n-1\}$.

a: entier relatif quelconque

le représentant de a dans $\{0, 1, ..., n-1\}$ est:

le reste de la division euclidienne de a par n

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

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
- Chiffre Pigpen
- Templiers
- hommes dansants
- Carré de Polybe
- Chiffrement affine
- Cas général: permutation de l'alphabet

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

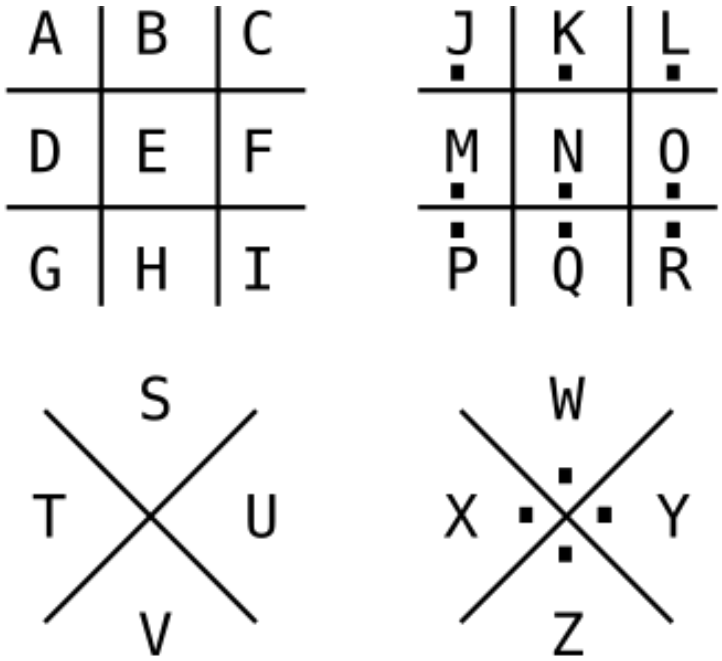
clair	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
chiffré	Q	R	S	T	U	V	W	X	Y	Z	A	B	C

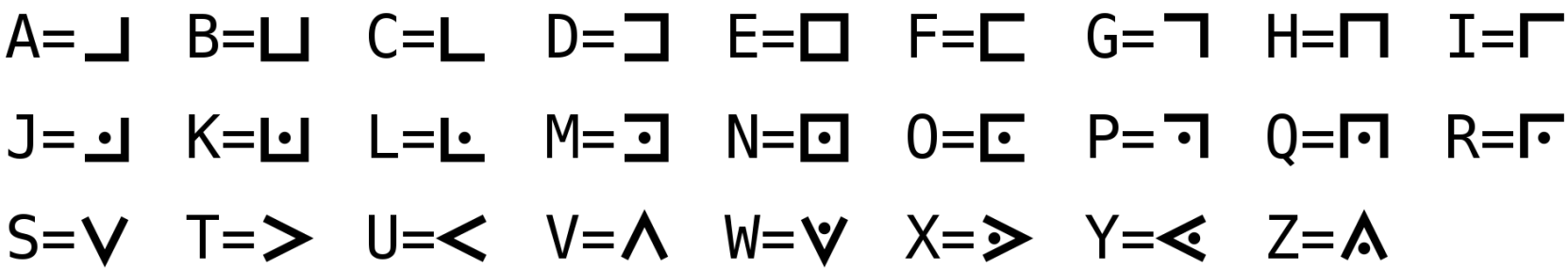
Chiffre Atbash

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

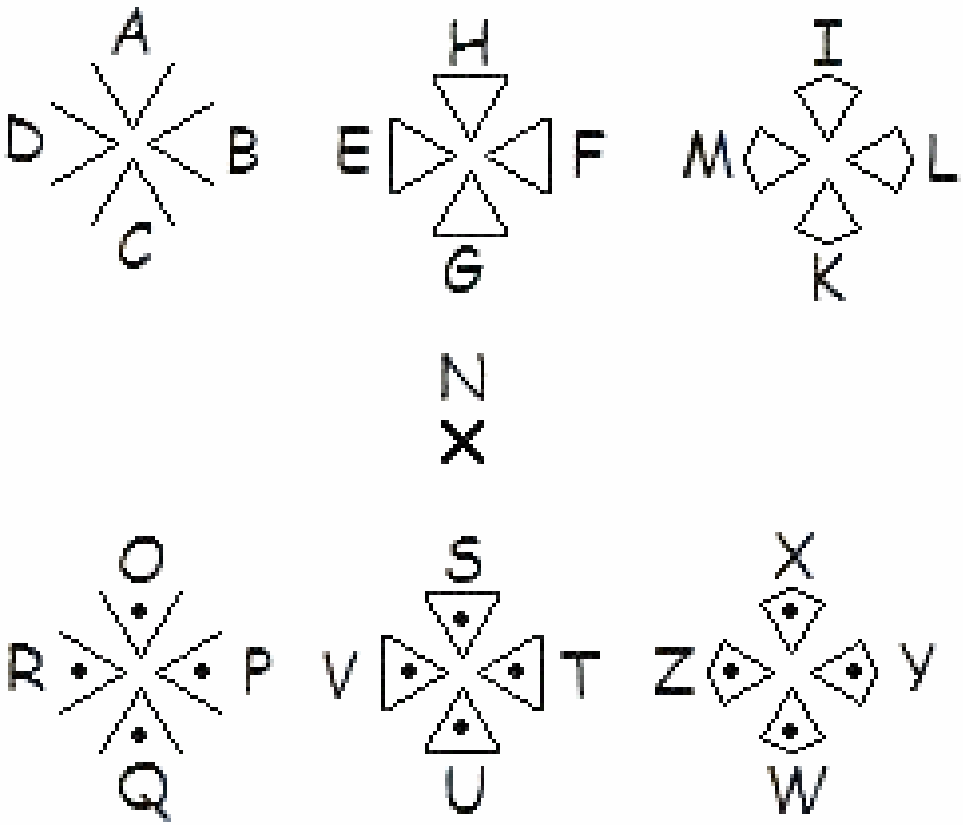
clair	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
chiffré	M	L	K	J	I	H	G	F	E	D	C	B	A

Chiffre Pigpen - chiffre des francs-maçons





Chiffre des templiers



Carré de Polybe

	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

clair	A	B	C	D	E	F	G	H	I/J	K	L	M	N
chiffré	11	12	13	14	15	21	22	23	24	25	31	32	33

Chiffrement affine

clé: 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

Cas général

exemple:

clair	A	B	C	D	E	F	G	H	I	J	K	L	M
chiffré	K	G	R	M	B	D	N	J	V	O	S	E	Z

clair	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
chiffré	T	Q	F	X	W	H	U	A	L	P	C	I	Y

permutation des lettres de l'alphabet

Nombre de clés?
$26 \times 25 \times 24... \times 4 \times 3 \times 2$

26! se lit **factorielle** 26 et vaut $\approx 400000000000000000000000000$

Analyse fréquentielle

substitution mono-alphabétique : conservation des fréquences d'apparition des lettres

Fréquence des lettres

E	A	S	I	N	T	R	L	U	O	D	C	M
17.35%	8.2%	7.93%	7.53%	7.17%	6.99%	6.65%	5.92%	5.73%	5.53%	4.01%	3.33%	2.97%
P	V	G	F	Q	H	B	X	J	Y	Z	K	W
2.92%	1.39%	1.09%	1.08%	1.04%	0.93%	0.92%	0.47%	0.34%	0.31%	0.1%	0.06%	0.03%

Chiffrement par substitution poly-alphabétique

une lettre correspond à plusieurs lettres selon sa position

- Chiffre de Vigenère
- Chiffre de Hill
- Chiffre de Beaufort
- Enigma

Chiffre de Vigenère

Blaise de Vigenère - XVI° siècle

Exemple: on chiffre le mot MESSAGE avec la clé KEY

clé	K	E	Y	K	E	Y	K
message clair	M	E	S	S	A	G	E
rang lettre du message	12	4	18	18	0	6	4
rang lettre de la clé	10	4	24	10	4	24	10
somme rangs	22	8	42	28	4	30	14
réduction modulo 26	22	8	16	2	4	4	14
message chiffré	W	I	Q	C	E	E	O

Chiffre de Hill

Exemple: chiffrer le mot MESSAGE avec la matrice clé $\begin{pmatrix} 6 & 7 \\ 15 & 21 \end{pmatrix}$

nombre de lettres du message impair: rajouter X à la fin

message clair	M	E	S	S	A	G	E	X
rang lettre du message	12	4	18	18	0	6	4	23

on obtient la matrice: $\begin{pmatrix} 12 & 18 & 0 & 4 \\ 4 & 18 & 6 & 23 \end{pmatrix}$

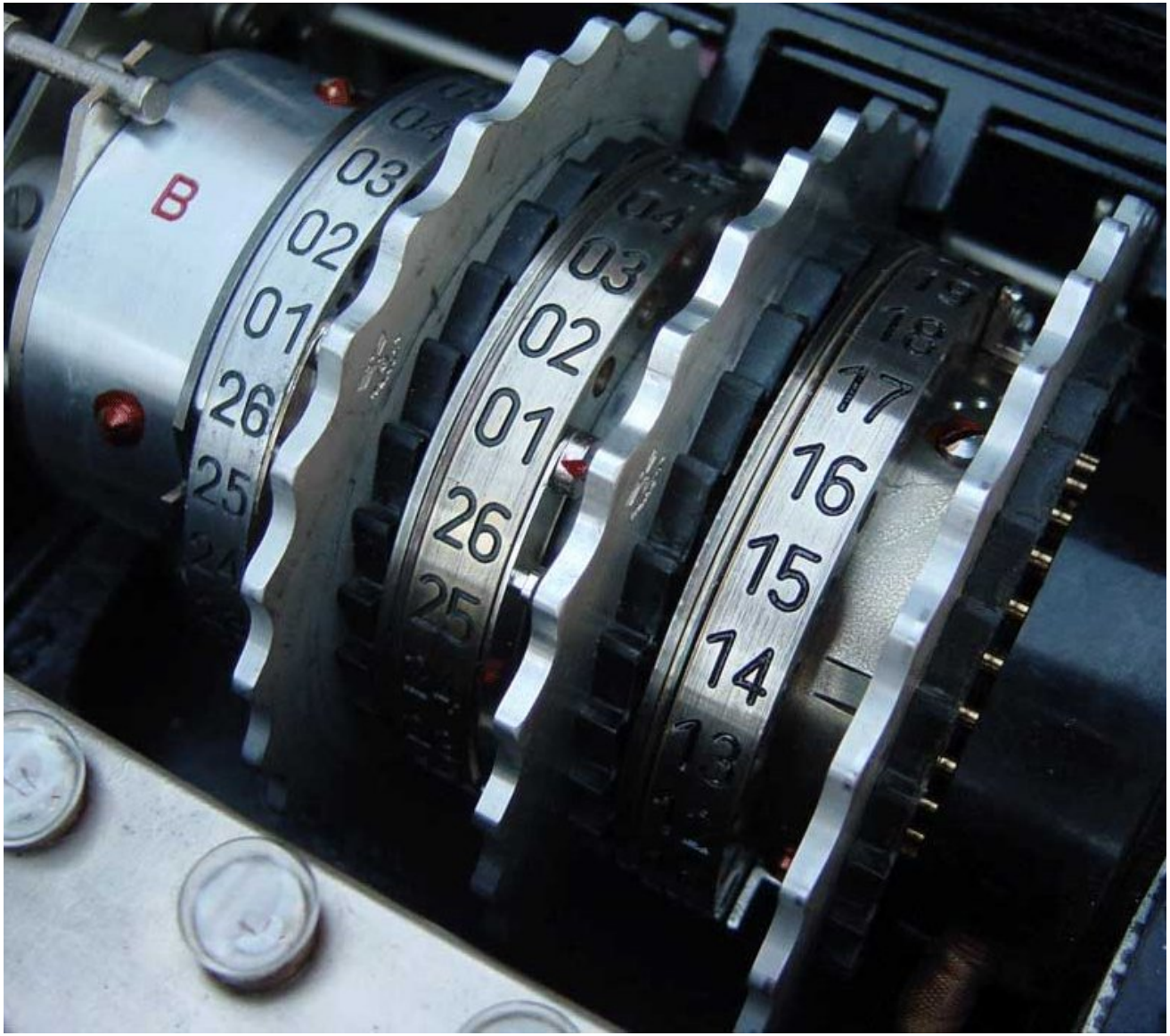
produit matriciel $\begin{pmatrix} 6 & 7 \\ 15 & 21 \end{pmatrix}$

$$\begin{pmatrix} 100 & 234 & 42 & 185 \\ 264 & 648 & 126 & 543 \end{pmatrix} \bmod 26 = \begin{pmatrix} 22 & 0 & 16 & 3 \\ 4 & 24 & 22 & 23 \end{pmatrix}$$

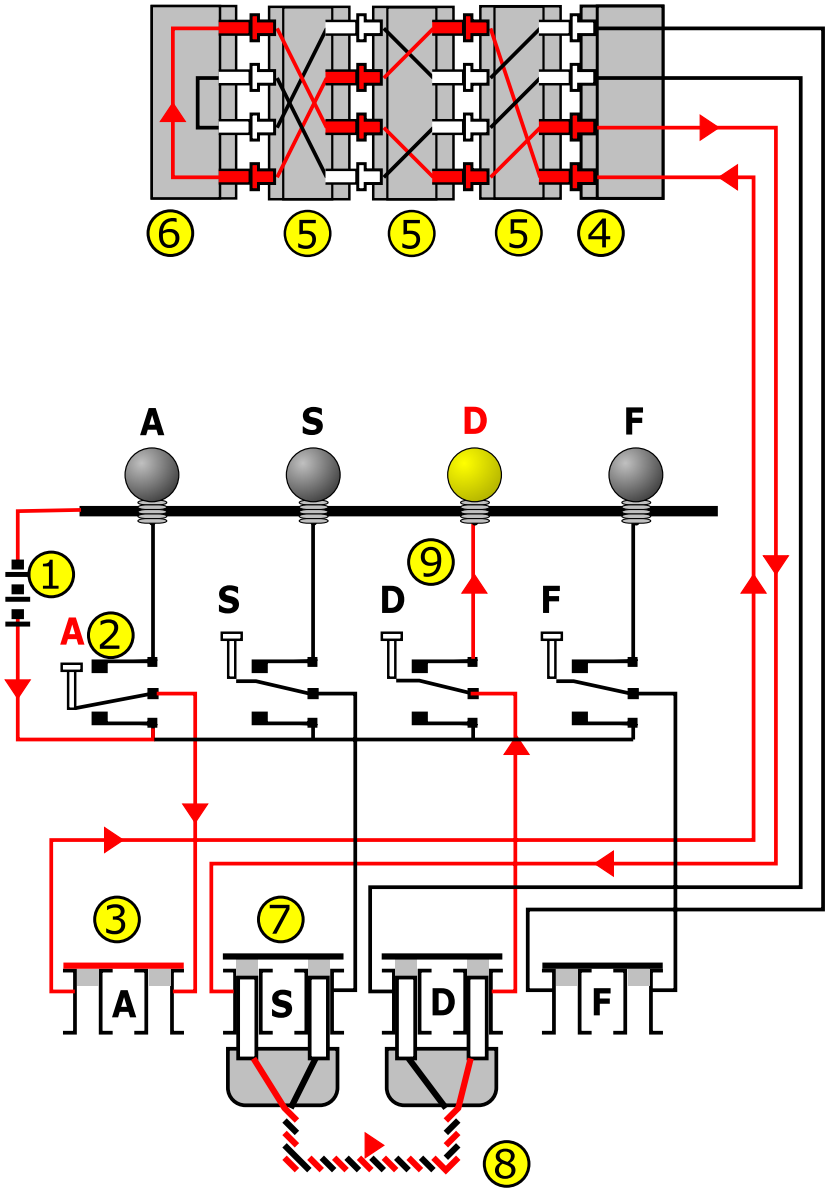
On obtient le message chiffré: WEAYQWDX

Machine Enigma

Machine Enigma: les rotors



Machine Enigma



Chiffrements par transposition

ordre des lettres du texte clair est modifié

- Chiffrement à dents de scie
- Scytale
- Chiffrement par transposition de colonnes

Chiffrement à dents de scie - Railfence cipher - Zigzag cipher

CECI EST MON MESSAGE SECRET:

C C E T O M S A E
E I S M N E S G S

chiffré: CCETOMSAEERTEISMNESGSCE

Scytale

600 av JC

clé: nombre de lettres sur la circonférence

Scytale

Exemple: circonférence 4 lettres

'VOICI UN MESSAGE SECRET SUR UNE SCYTALE'

V	O	I	C	I	U	N	M	E
S	S	A	G	E	S	E	C	R
E	T	S	U	R	U	N	E	S
C	Y	T	A	L	E			

VSECOSTYIASTCGUAIERLUSUENEN.MCE.ERS.

Chiffrement par permutation de colonnes

1	2	3	4
M	E	S	S
A	G	E	S
U	P	E	R
S	E	C	R
E	T	X	X

devient

3	4	2	1
S	S	E	M
E	S	G	A
E	R	P	U
C	R	E	S
X	X	T	E

Chiffré: SEECXSSRRXEGPETMAUSE

Chiffrement par transposition défini par permutation

Exemple: transposition sur message de longueur 10

position clair	1	2	3	4	5	6	7	8	9	10
position chiffré	3	7	5	1	9	6	2	10	8	4

'VOICI MON MESSAGE SUPER SECRET'

'VOICI MON |MESSAGE SU|PER SECRET'

Question: où sont les clés?

- César
- Rot13
- Atbash
- Pigpen
- Templiers
- hommes dansants
- Polybe
- affine
- permutation de l'alphabet
- Vigenère
- Hill
- dents de scie
- scytale
- permutation de colonnes
- Enigma

Chiffrement de Vernam

Chiffre de Vernam - Chiffre à masque jetable - One time pad (OTP)

alphabet: n lettres

clé de chiffrement: suite de nombres **aléatoires et indépendants**, compris entre 0 et $n-1$.

message chiffré: décalage de chaque lettre du message clair par le nombre donné par la clé comme dans le chiffre de Vigenère.

Chiffrement de Vernam

Exemple: on chiffre le mot MESSAGE avec la clé HZOZGFL

clé	H	Z	O	Z	G	F	L
message clair	M	E	S	S	A	G	E
rang lettre du message	12	4	18	18	0	6	4
rang lettre de la clé	7	25	14	25	6	5	11
somme rangs	19	29	32	43	6	11	15
réduction modulo 26	19	3	6	17	6	11	15
message chiffré	T	D	G	R	G	L	P

Chiffrement de Vernam: chiffrement parfait

Claude Shannon a prouvé en 1949 que ce chiffrement est **parfait** si:

- la clé est une suite de caractères au moins aussi longue que le message à chiffrer
- la clé est clé choisie de façon totalement aléatoire
- la clé est utilisée une seule fois

Chiffrement de Vernam: messages binaires

opération bit à bit de *ou exclusif* ou *xor* noté $\oplus$

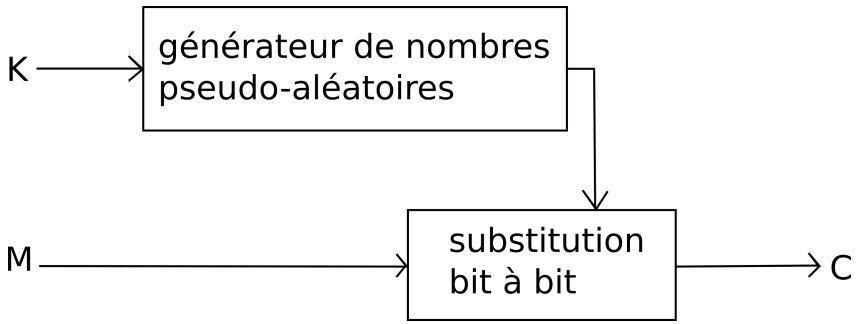
correspond à l'addition modulo 2 pour chaque bit

Table de vérité de XOR		
A	**B**	**R = A ⊕ B**
0	0	0
0	1	1
1	0	1
1	1	0

texte clair: 011010000110010101101100011011000110111
clé: 011000101001001001001010101101010010111 0
texte chiffré: 000010101111011100100110110110010100000 1

Chiffrements par flot

Chiffrement par flot (*stream cipher*), par flux, à la volée



principe du chiffrement de Vernam

Chiffrements par flot

Exemples de chiffrements par flot:

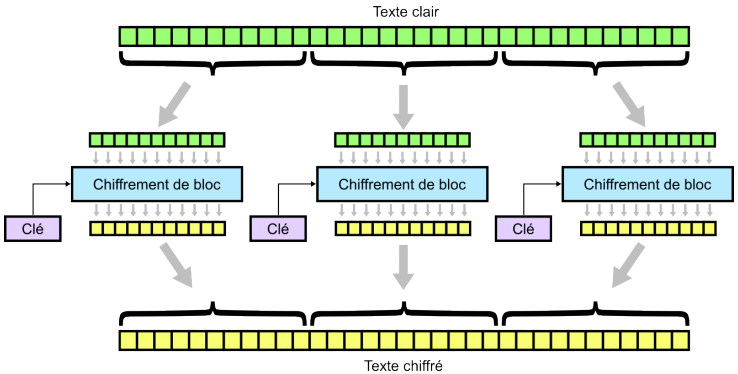
- A5/1: basé sur des LFSR - plusieurs attaques publiées
- RC4 - plusieurs attaques publiées
- Chacha20

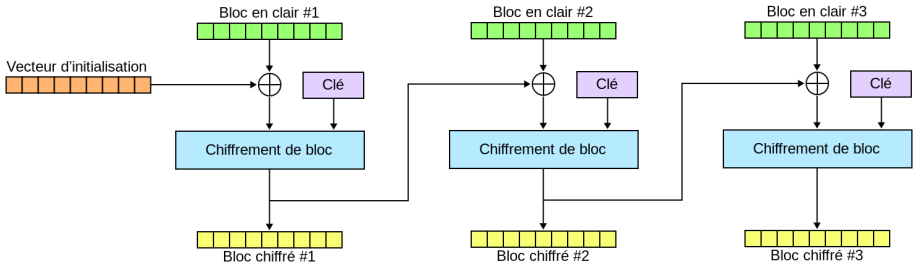
Chiffrements par blocs

le message est découpé en blocs de longueur fixe.

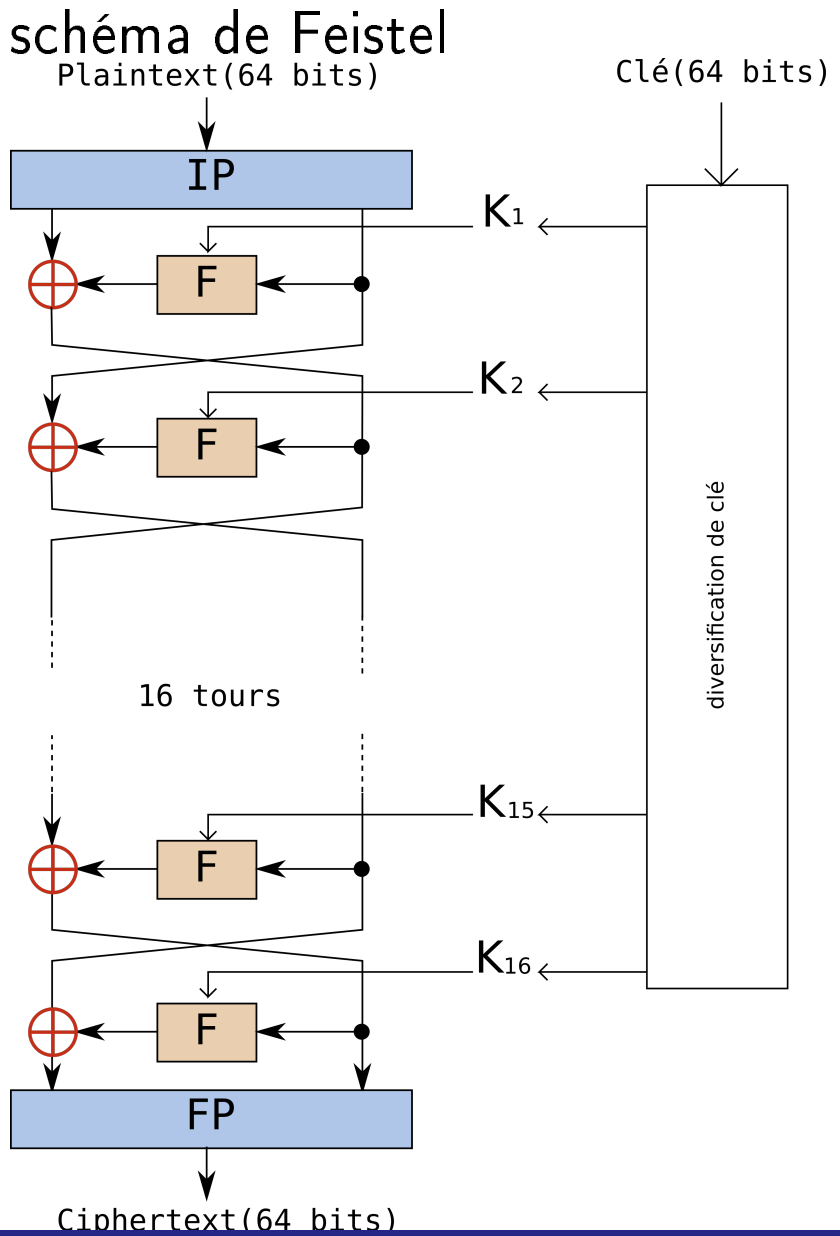
- DES
- AES

- modes opératoires: ECB, CBC, CTR, GCM
différentes façons d'enchaîner le chiffrement de plusieurs blocs
- rembourrage, padding



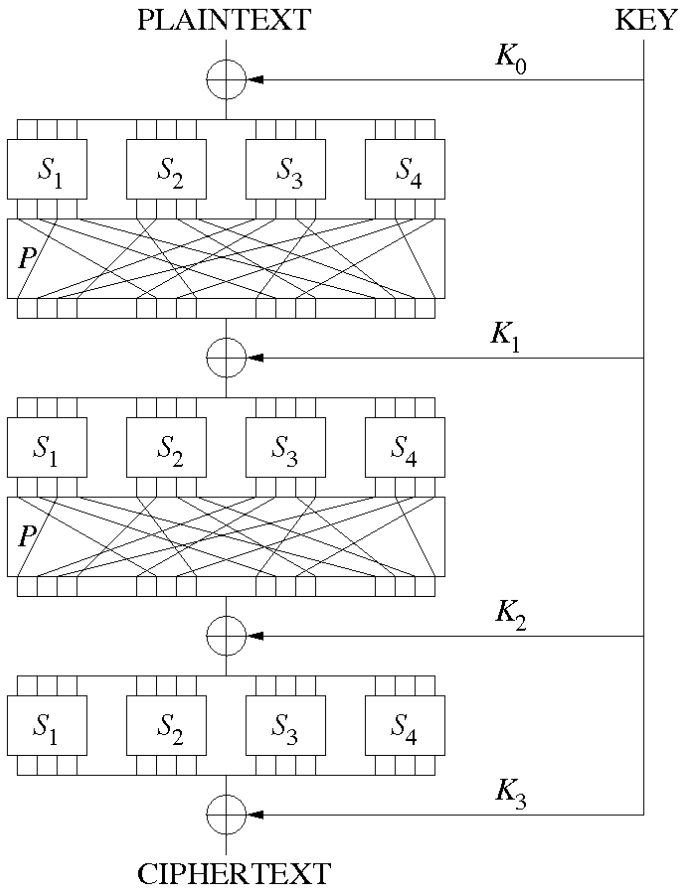


Chiffrement DES



Chiffrement AES - Advanced Encryption Standard

- chiffrement de type réseau de substitutions-permutations
- blocs de 128 bits
- clés de 128, 192 ou 256 bits



- 10, 12 ou 14 tours

Limites du chiffrement symétrique

chiffrements sûrs, rapides

Problème: comment échanger la clé en toute sécurité?