

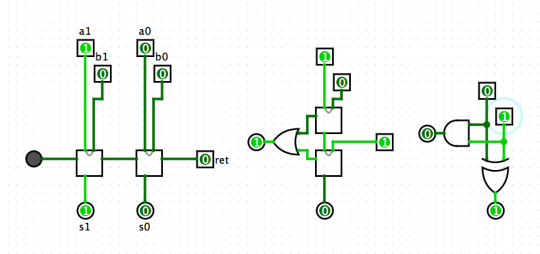
Concepts Informatiques I

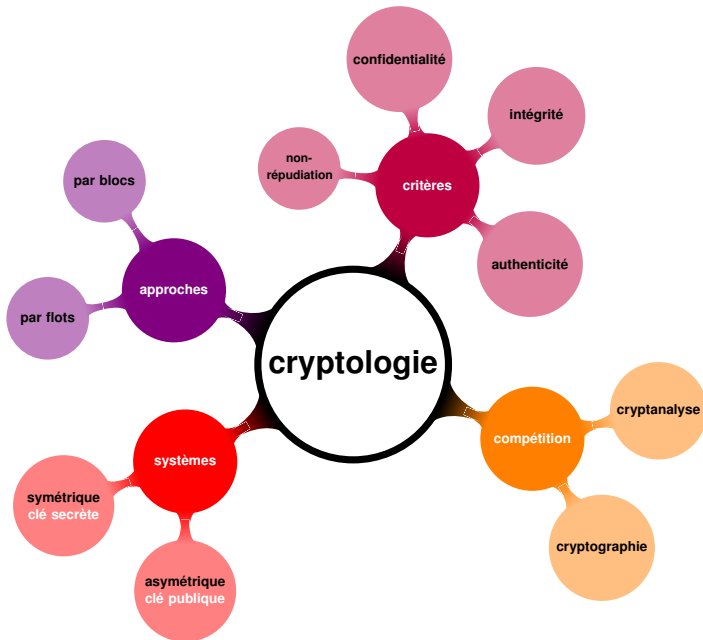
2025–2026

Matthieu Picantin



numération et arithmétique
 numération et arithmétique en machine
 codes, codages, compression,
 contrôle d'erreur (détection, correction)
crypto (confidentialité, authenticité, intégrité)
 logique et calcul propositionnel
 circuits numériques





Chiffre de César

- chiffrement mono-alphabétique par permutation de l'alphabet
- chaque lettre code l'un des 26 décalages cycliques possibles

clé **a** – pas de décalage

clé **b** – décalage d'une lettre de l'alphabet: $\tau_b(a) = b$, $\tau_b(b) = c$, etc

...

clé **z** – décalage de 25 lettres de l'alphabet: $\tau_z(a) = z$, $\tau_z(b) = a$, etc

Chiffre de Vigenère

- chiffrement poly-alphabétique par permutations de l'alphabet
- la clé est un mot **u** utilisé cycliquement et codant $|u|$ décalages:

$$\tau_u(w_0 \dots w_{|w|-1}) = \tau_{u_0}(w_0) \dots \tau_{u_{k \bmod |u|}}(w_k) \dots \tau_{u_{|w|-1 \bmod |u|}}(w_{|w|-1})$$

Faiblesse du chiffre de César

- calcul des fréquences des lettres
- comparaison avec une langue connue
- déduction du décalage utilisé

Solidité du chiffre de Vigenère

- plusieurs alphabets décalés utilisés
- pas de déduction directe évidente
- inattaquable pendant trois siècles

hegmmaehquphaijdeelzpv
 oqkeinezjadillpkvydpam
 hjsqdwsezwtzapsowqkzl
 gqzazyol **jpei**asthwtaniw
 vvdlabgwhdmjdmobwceoew
 wpwaksiywmwhnmepqxmjel
 auswpppwdiobjlrmsoszav
 lfvaagqlazkelwbqzydinp
 ngalmiav **jpe**zqfrexwmeej
 losijazplwlxtreaz **phdmj**
 dmobwcoeak **phdmj**lrz **asth**
 ebolwwkmcmkckovaieoiwz
 upvpaiappujmerkejfrevlz
 ckcjeiwqldkabltrctsei

wakeupalicedearsaidher
 sisterwhywhatalongslee
 pyouvehadohivehadsucha
 curiousdreamsaidalicea
 ndshetoldhersisteraswe
 llasshecouldrememberth
 emallthesestrangeadven
 turesofhersthatyouhave
 justbeenreadingaboutan
 dwhenshehadfinishedher
 sisterkissedherandsaid
 itwasacuriousdreamdear
 certainlybutnowruninto
 yourteaitsgettinglate

distance 110 entre les deux occurrences de **jpe**

distance 15 entre les deux occurrences de **phdmj**

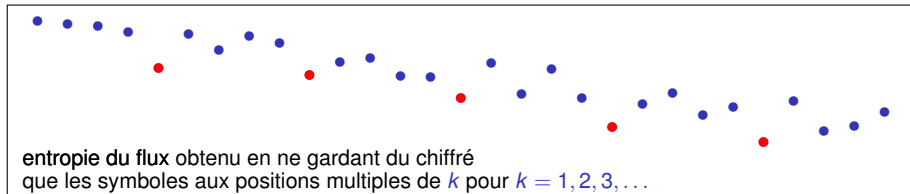
distance 160 entre les deux occurrences de **asth**

pgcd = **5** est une longueur probable pour la clé
 ce qui réduit la cryptanalyse à **5** cryptanalyses de César
 pour finalement découvrir la clé: **lewis**

```

hegmmaehquphaijdeelpzv
oqkeinezjadillpkvydpam
hjsqdwsezwtzapsowqkzl
ggzazyoljpeiasthwtaniw
vvdlabgwhdmjdmobwceoew
wpwaksiywmwhnmepqxmjel
auswpppwdiobjlrcmsozav
lfvaagqlazkelwbqzydinp
ngalmiavjpezqfrexwmeej
losijazplwlxtreazphdmj
dmobwcoeakphdmjlrzasth
ebolwwkmcmkckovaieoiwz
upvpiaypujmerkejfrevlz
ckcjeiwqldkabltrctsei

```





Alice chiffre son message, puis envoie le chiffré à **Bob**

Bob reçoit le chiffré, puis le déchiffre

Comment **Alice** et **Bob** s'accordent (à l'abri de **Eve**) sur leur **secret** partagé?

Protocole d'échange de clés de Diffie–Hellman–Merkle 1976 [prix Turing 2015]



Eve ne peut voir que
les couleurs c , ac , et bc



Alice et Bob choisissent une couleur commune c (publique)

Alice choisit une couleur a ,
mélange et diffuse ac

Bob choisit une couleur b ,
mélange et diffuse bc

Alice mélange a avec bc
et garde abc secret

Bob mélange b avec ac
et garde abc secret

Comment Alice et Bob s'accordent (à l'abri de Eve) sur leur **secret** partagé?

Protocole d'échange de clés de Diffie–Hellman–Merkle 1976 [prix Turing 2015]



Eve ne peut voir que les nombres p , g , $g^a \bmod p$ et $g^b \bmod p$



Alice et Bob choisissent un premier p et un nombre $g < p$ (publics)

Alice choisit un nombre a
et diffuse $A = g^a \bmod p$

Alice calcule et garde
secret $B^a \bmod p$



Bob choisit un nombre b
et diffuse $B = g^b \bmod p$

Bob calcule et garde
secret $A^b \bmod p$

Comment Alice et Bob s'accordent (à l'abri de Eve) sur leur **secret** partagé?



Eve ne peut voir le message en clair et ceci,
malgré la connaissance de la clé publique d'Alice



Alice envoie sa clé publique à **Bob** (ou la diffuse)

Bob chiffre avec la clé publique d'Alice, puis envoie

Alice reçoit le chiffré, puis le déchiffre avec sa clé privée

Comment **Bob** envoie un message secret à **Alice** sans clé secrète partagée?

Crypto-système RSA de Rivest–Shamir–Adleman 1977 [prix Turing 2002]



Eve ne peut voir que les couleurs \bar{a} et $m\bar{a}$



Alice choisit une couleur privée a

Alice calcule et diffuse la couleur \bar{a}

Alice reçoit $m\bar{a}$, y ajoute son a privé
pour déchiffrer et retrouver le m de Bob

Bob mélange son message
coloré secret m avec \bar{a}

Bob envoie le chiffré $m\bar{a}$

Comment Bob envoie un message secret à Alice sans clé secrète partagée?

Une **fonction à sens unique** est une fonction **facile à calculer** et **difficile à inverser**.
Une **fonction à porte dérobée** est une fonction facile à calculer et difficile à inverser
sauf si l'on possède une information spéciale.

Pour l'analogie imagée avec les couleurs, on considère *facile* de mélanger des couleurs données, mais on estime *difficile* de trouver la couleur complémentaire d'une couleur donnée ou de séparer deux couleurs une fois mélangées.

Candidat algorithmique: pb du sac-à-dos

Pour F et $E \subseteq F$ des ensembles d'entiers, il est facile de calculer $E \mapsto s = \sum_{e \in E} e$. Inversement, pour F, s fixés, il est difficile de trouver $E \subseteq F$ vérifiant $\sum_{e \in E} e = s$.

Si tout élément de F est plus grand que la somme des plus petits, l'inversion devient *facile*.

Candidat arithmétique: pb du logarithme discret

Pour e, n des entiers, il est facile de calculer l'exponentiation modulaire $m \mapsto c = m^e \bmod n$. Inversement, pour e, n, c fixés, il est difficile de trouver m vérifiant $m^e \bmod n = c$.

Si on connaît la décomposition de n en facteurs premiers, l'inversion devient *facile*.

Une **fonction à sens unique** est une fonction **facile à calculer** et **difficile à inverser**.
 Une **fonction à porte dérobée** est une fonction facile à calculer et difficile à inverser
sauf si l'on possède une information spéciale.

Pour l'analogie imagée avec les couleurs, on considère *facile* de mélanger des couleurs données, mais on estime *difficile* de trouver la couleur complémentaire d'une couleur donnée ou de séparer deux couleurs une fois mélangées.

Indicatrice d'Euler:

$$\varphi(n) = \#\{1 \leq h \leq n : \text{pgcd}(h, n) = 1\}$$

$$\varphi(8) = 4 = \varphi(12) \quad \varphi(p) = p - 1 \quad \varphi(ab) = \varphi(a)\varphi(b)$$

pour p premier pour $\text{pgcd}(a, b) = 1$

Théorème d'Euler: $m^{\varphi(n)} = 1 \bmod n$

$$m^{ed} = m \bmod n \quad \text{pour} \quad d = \frac{k\varphi(n) + 1}{e}$$

Candidat arithmétique: pb du *logarithme discret*

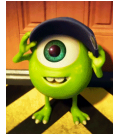
Pour e, n des entiers, il est facile de calculer l'exponentiation modulaire $m \mapsto c = m^e \bmod n$.
 Inversement, pour e, n, c fixés, il est difficile de trouver m vérifiant $m^e \bmod n = c$.

Si on connaît la décomposition de n en facteurs premiers, l'inversion devient *facile*.

Crypto-système RSA de Rivest–Shamir–Adleman 1977 [prix Turing 2002]



Eve ne connaît que (N, e)
et ne voit que c



Alice choisit deux premiers p et q ,
pose $N = pq$ et calcule $\varphi(N)$

Alice choisit e premier avec $\varphi(N)$
et calcule $d = (k\varphi(N) + 1)/e$

Alice diffuse sa clé publique (N, e)
et cache sa clé privée (N, d)

Alice reçoit c et récupère $m = c^d \bmod N$

Bob envoie le chiffré $c = m^e \bmod N$
de son message m

Comment **Bob** envoie un message secret à **Alice** sans clé secrète partagée?