Crypto

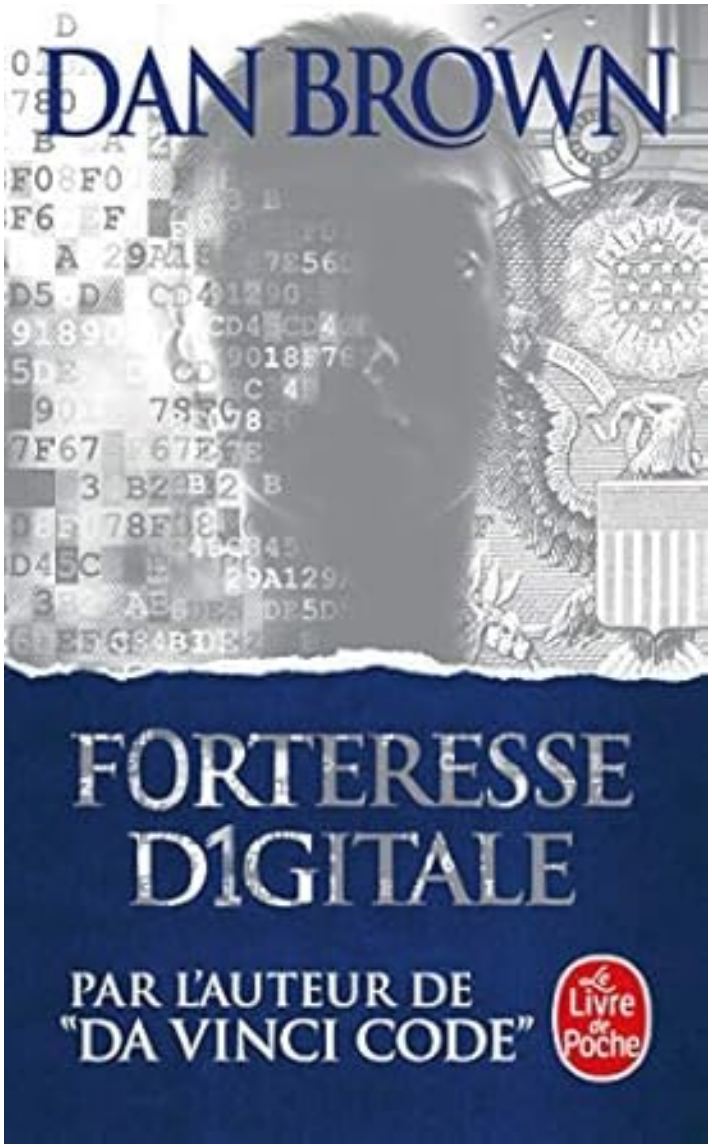
Andreas Enge

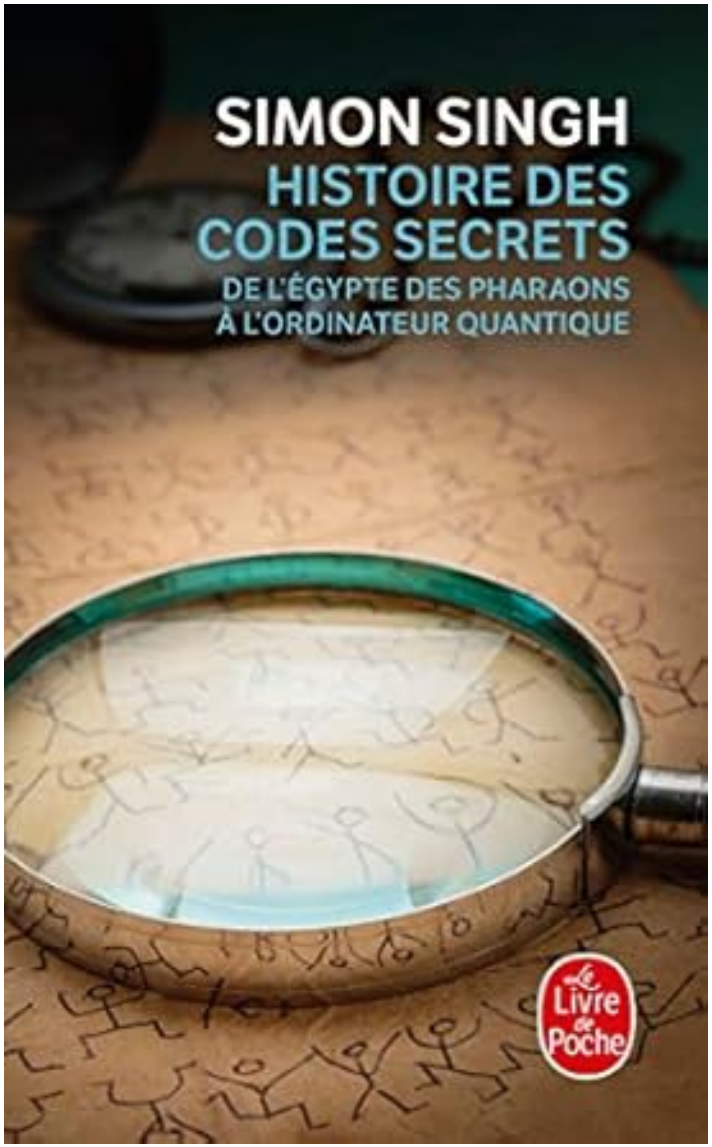
CANARI project-team
INRIA Bordeaux
andreas.enge@inria.fr
http://enge.math.u-bordeaux.fr/

Lycée Albert Claveille, Périgueux, 18/03/2025

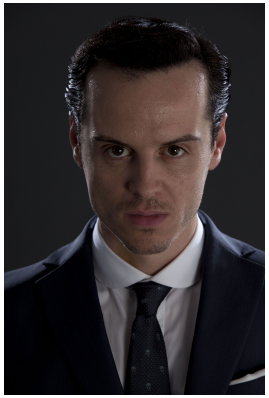
Cryptologie

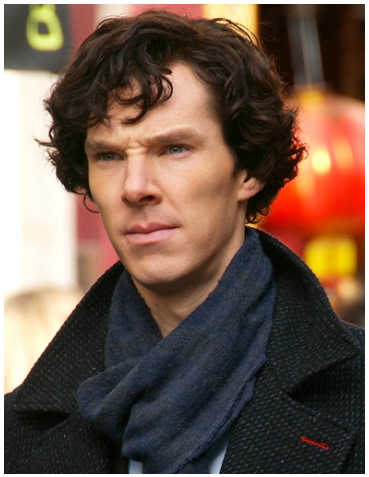
Robert M. Lavinsky, CC-BY-SA 3.0


DAN BROWN
FORTERESSE
D1GITALE
PAR L'AUTEUR DE
"DA VINCI CODE"
Le Livre de Poche


SIMON SINGH
HISTOIRE DES
CODES SECRETS
DE L'ÉGYPTE DES PHARAONS
À L'ORDINATEUR QUANTIQUE
Le Livre de Poche

Cryptologie

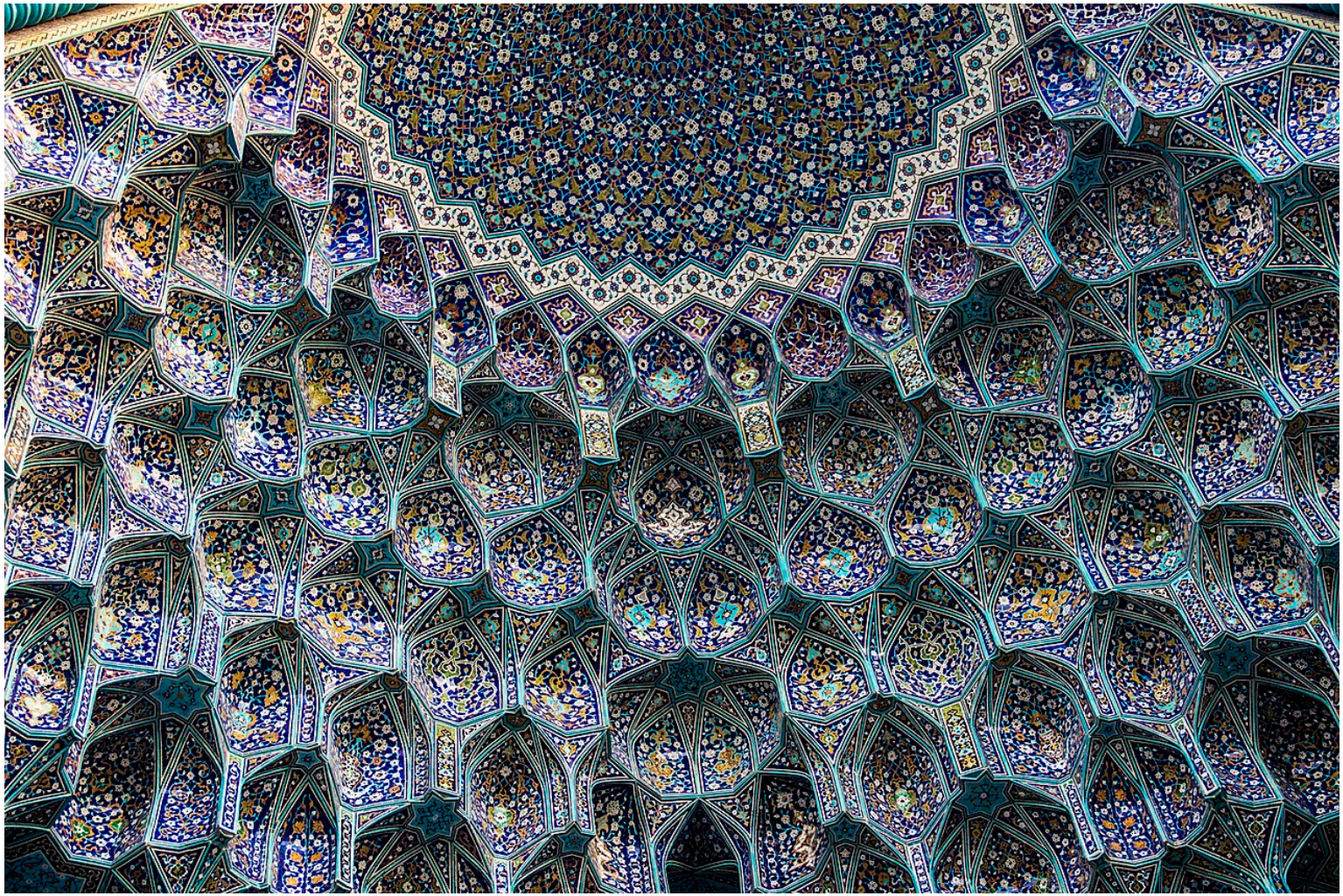




Vocabulaire

- Cryptologie
  - κρυπτός : caché
  - λόγος : mot
  - mot caché, science du secret
- Cryptographie
  - γράφω : écrire
  - écriture secrète = chiffrement
- Cryptanalyse
  - ἀνάλυσις
  - “cassage”, décryptage

Symétrie



Hhhamidhh, CC-BY-SA 4.0

Chiffrement de César

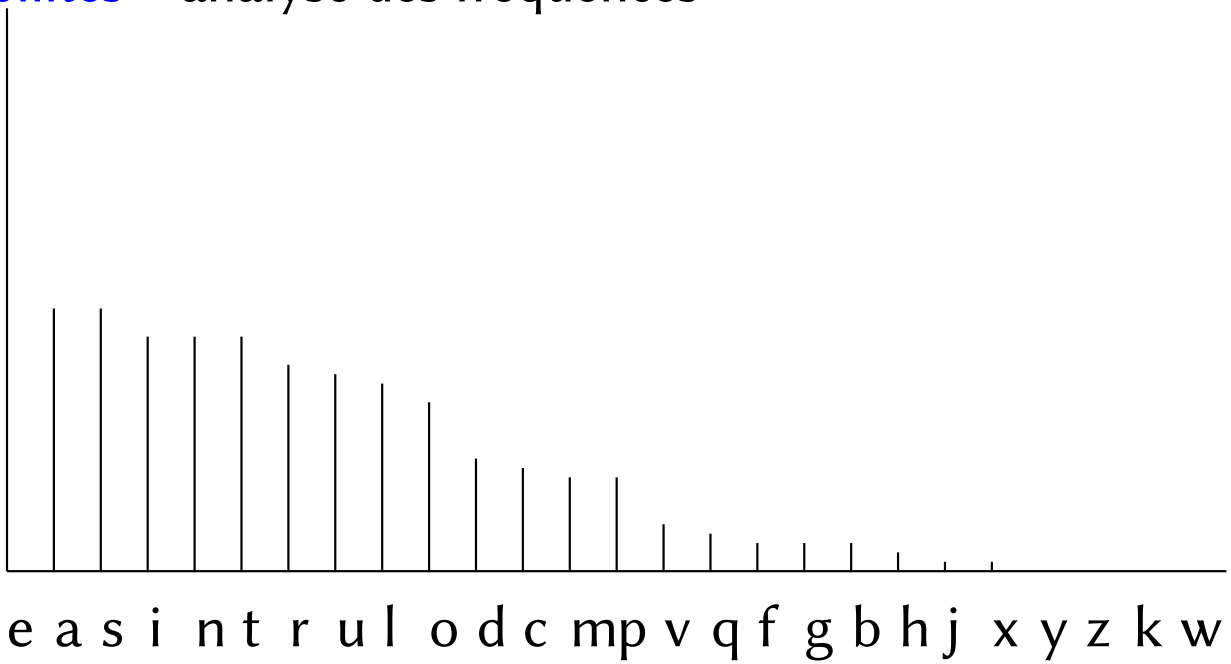
Décalage de l'alphabet de 3 lettres :

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
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

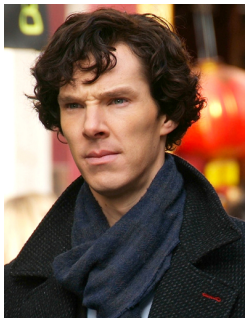
- Chiffrement
  JETAIME $\longrightarrow$ MHWDLPH
- Déchiffrement
  NLVV $\longrightarrow$ KISS

Cryptanalyse du chiffrement de César

- Il n'y a rien à analyser !
- Introduisons une clef – valeur du décalage
  - Recherche exhaustive
  - Probabilités – analyse des fréquences



La chaîne du chiffrement



clef

message

chiffrement

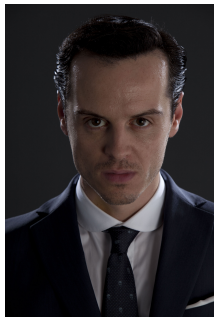
réseau

déchiffrement

clef

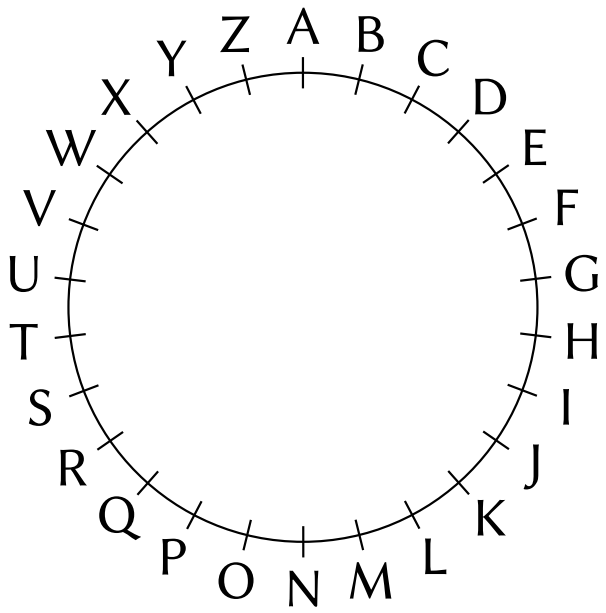
message

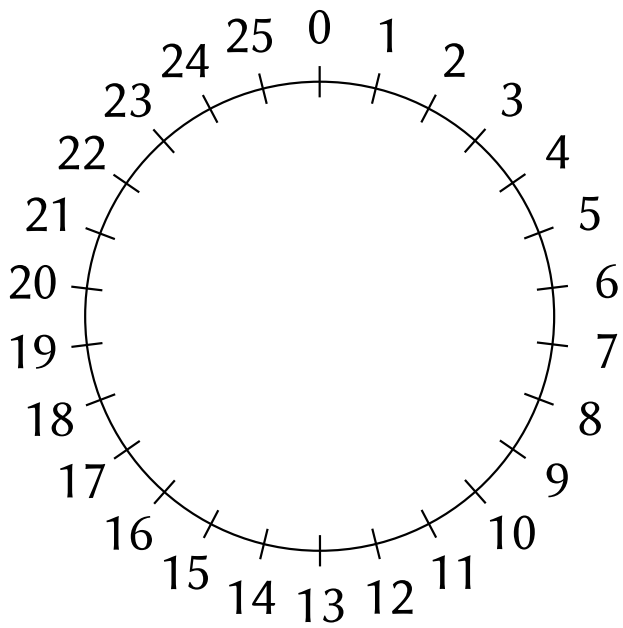
décryptage ?



Mettons des chiffres !

- Pourquoi ?
  - Implantation sur ordinateur
  - Preuves mathématiques pour la sécurité
- Calcul modulo 26





$$\vdots$$
$$25 = 25$$
$$26 \equiv 0$$
$$27 \equiv 1$$
$$28 \equiv 2$$
$$\vdots$$

Mettons des chiffres !

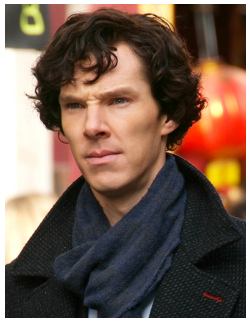
Chiffrement César = addition de 3 modulo 26

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
0	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

JETAIME $\longrightarrow$ 9 4 19 0 8 12 4

$\longrightarrow$ 12 7 22 3 11 15 7 $\longrightarrow$ MHWDLPH

La chaîne complète du chiffrement



clef

message

codage

chiffrement

réseau

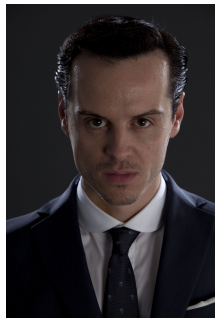
déchiffrement

décodage

clef

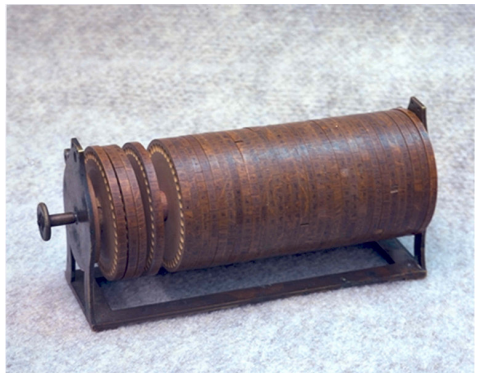
message

décryptage ?



Substitutions

- ATBASH — substitution utilisée dans la bible
  A = T, B = SH, ...
  Babylon = Sheshach
- 1412 : encyclopédie arabe contenant une section sur la cryptologie, fréquence des mots dans le coran
- substitution monoalphabétique avec homophones
- substitution polyalphabétique
  - inventée par Trithemius en 1518
  - attaquée par Kasiski en 1863



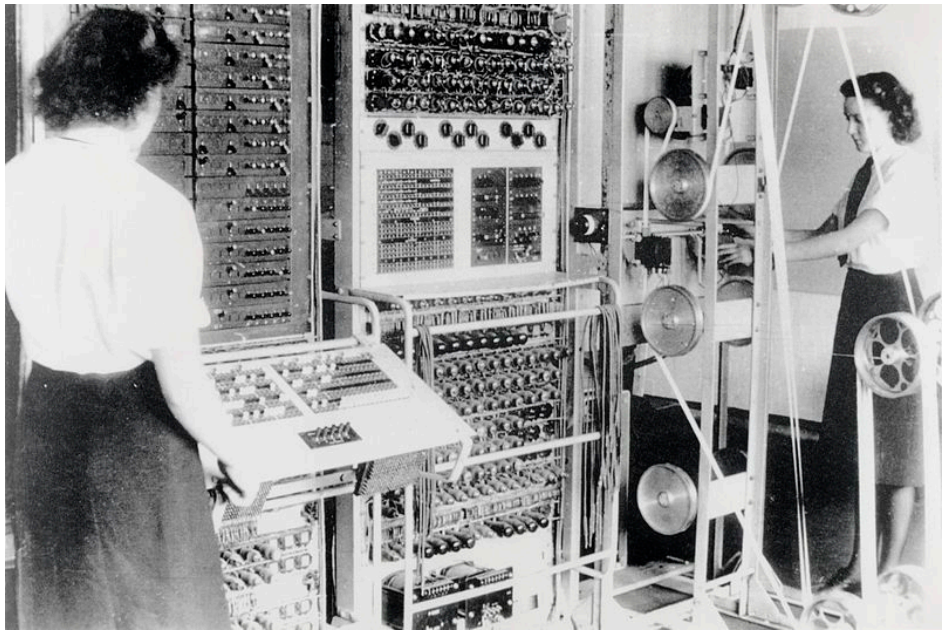
USA, Public Domain

Enigma

Karsten Sperling, Public Domain

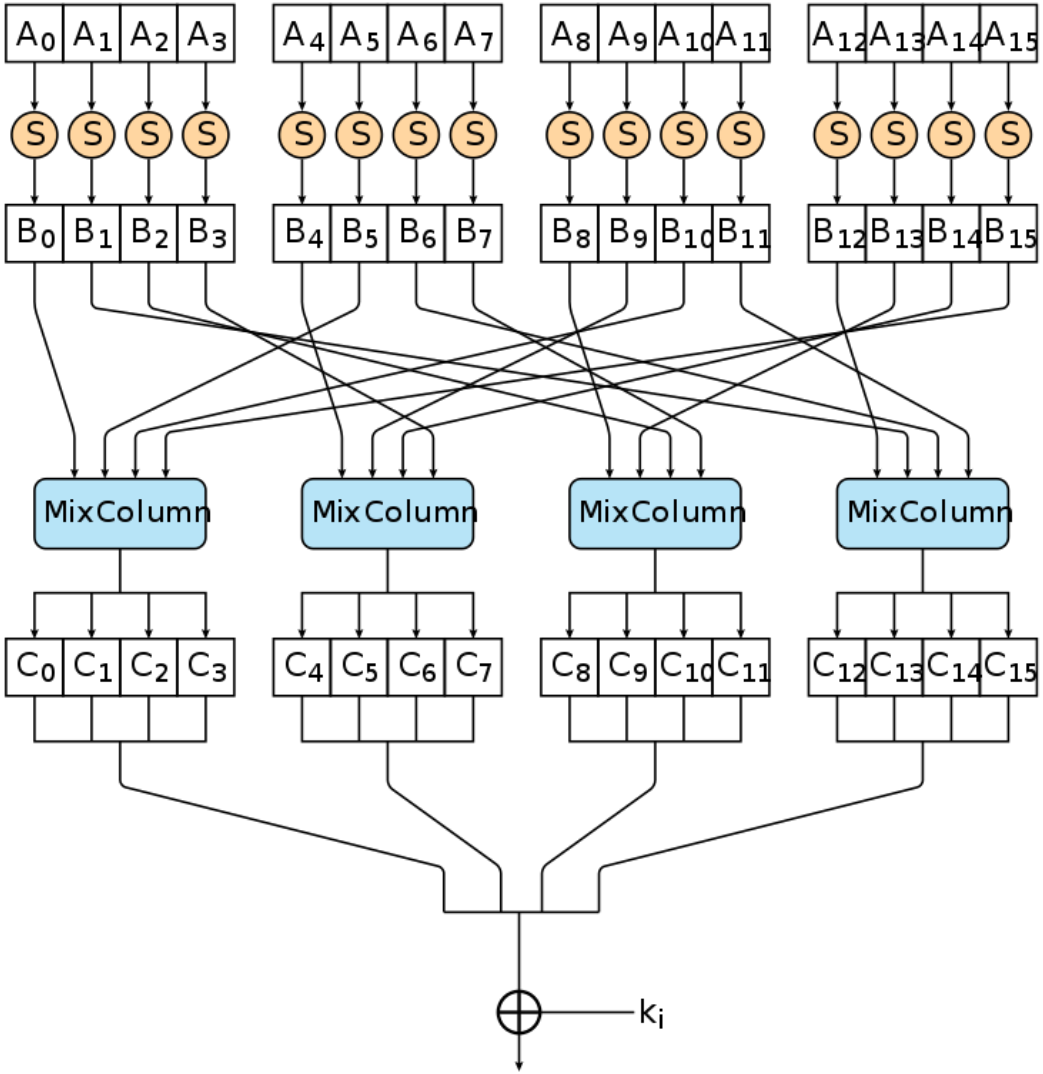
Bob Lord, CC-BY-SA 3.0

Bob Lord, CC-BY-SA 3.0



UK National Archive, Public Domain

Chiffrement symétrique moderne : AES



Lois de Kerckhoffs

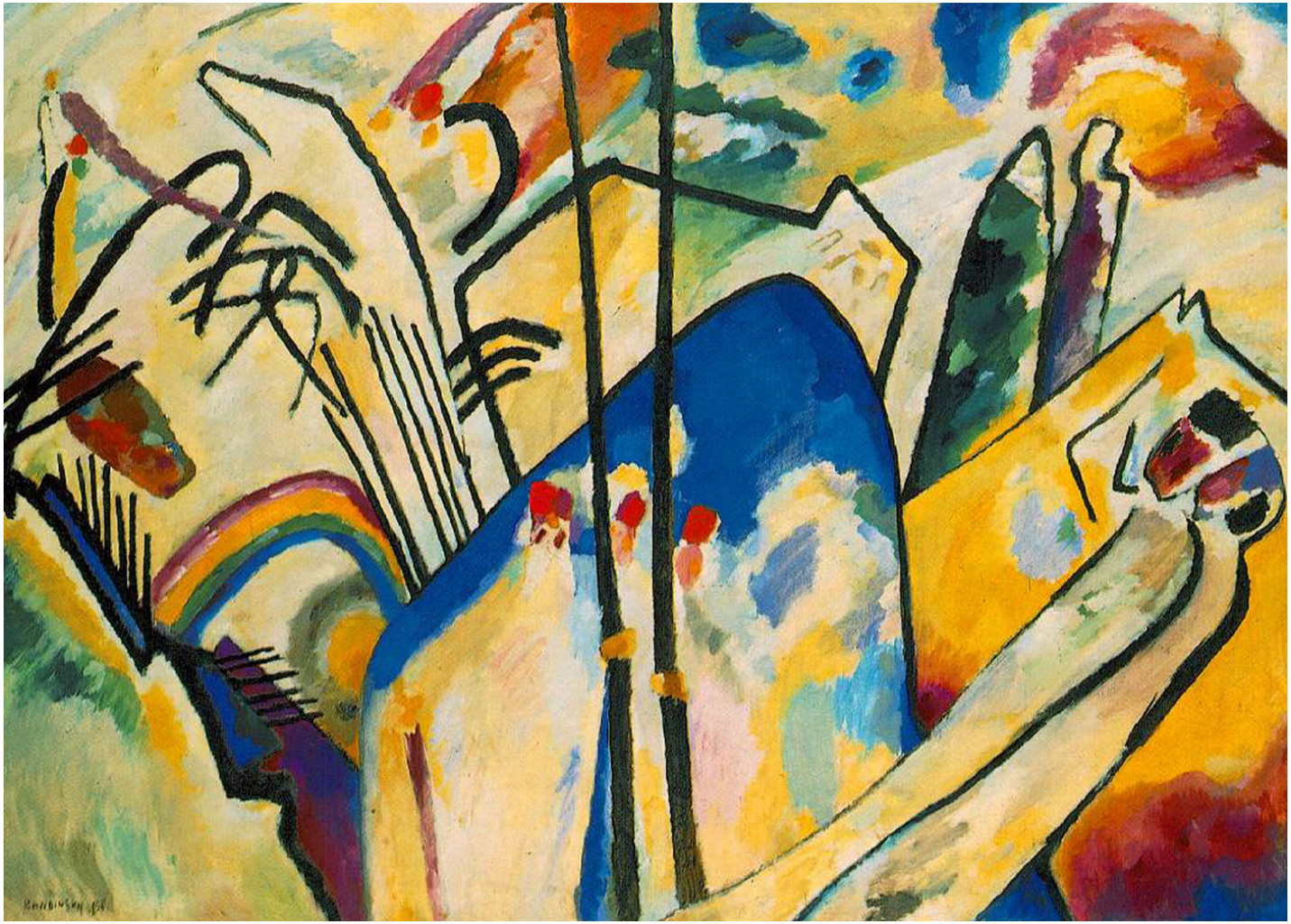
Journal des Sciences Militaires, janvier 1883

1. Le système doit être matériellement, sinon mathématiquement, indéchiffrable.
2. Il faut qu'il n'exige pas le secret, et qu'il puisse sans inconvénient tomber entre les mains de l'ennemi.
3. La clef doit pouvoir en être communiquée et retenue sans le secours de notes écrites, et être changée ou modifiée au gré des correspondants.
4. Il faut qu'il soit applicable à la correspondance télégraphique.
5. Il faut qu'il soit portatif, et que son maniement ou son fonctionnement n'exige pas le concours de plusieurs personnes.
6. Enfin, il est nécessaire, vu les circonstances qui en commandent l'application, que le système soit d'un usage facile, ne demandant ni tension d'esprit, ni la connaissance d'une longue série de règles à observer.

Buts de sécurité

- Confidentialité
  chiffrement
- Integrité
- Authentification
- Non-répudiation
  signatures numériques

Asymétrie



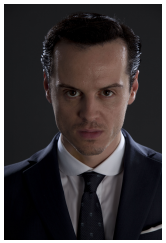
Vassily Kandinsky, Public Domain

Échange de clefs à la Diffie–Hellman (1976)

- Structure dans laquelle on peut additionner : nombres entiers
- Point de base $P = 3$
- $aP = \underbrace{P + P + \cdots + P}_{a \text{ fois}}$

clefs privées $a = 2$ $b = 5$

“clefs publiques” $\xrightarrow{aP=6}$



$\xleftarrow{bP=15}$

secret partagé $a(bP) = (ab)P = b(aP)$

$2 \times 15 = 10 \times 3 = 30 = 5 \times 6$

Chiffrement ElGamal (1985)

- Structure dans laquelle on peut additionner
- Point de base $P = 3 \bmod 26$
- Message, texte claire $m =$ COUCOU

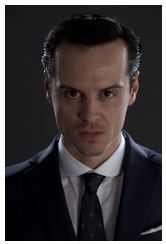
clef privée $b = 5$

clef publique $bP = 15$

aléa $a = 2$

chiffrement $(aP, c = E_{abP(m)}) \longrightarrow$

$= (6, \text{GSYGSY})$



déchiffrement $m = D_{baP}(c)$

Cryptanalyse de Diffie–Hellman

- Oscar connaît P et voit aP, bP.
- Il veut trouver abP (exercise : casse aussi ElGamal).
- Logarithme discret

Étant donné aP, trouver $a = \text{“}\log_P aP\text{”}$

- Exemple
  - $P = 3$
  - $aP = 6$, $bP = 15$
  - $a = \frac{aP}{P} = \frac{6}{3} = 2$
  - $abP = 2 \times 15 = 30$

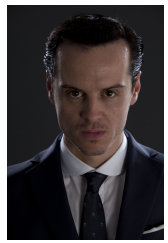
Ici, logarithme discret = division !

Échange de clefs à la Diffie–Hellman (1976)

- Structure dans laquelle on peut multiplier : nombres entiers
- Point de base $P = 3$
- $P^a = \underbrace{P \times P \times \cdots \times P}_{a \text{ fois}}$

clefs privées $a = 2$ $b = 5$

“clefs publiques” $\xrightarrow{P^a = 9}$ $\xleftarrow{P^b = 243}$



secret partagé $(P^b)^a = P^{ab} = (P^a)^b$

$243^2 = 3^{10} = 59049 = 9^5$

Chiffrement ElGamal (1985)

- Structure dans laquelle on peut multiplier
- Point de base $P = 3$
- Message, texte claire $m =$ COUCOU

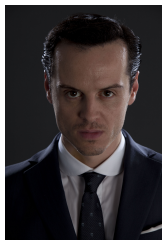
clef privée $b = 5$

clef publique $bP = 15$

aléa $a = 2$

chiffrement $(P^a, c = E_{Pab}(m)) \longrightarrow$

$= (9, \text{FRXFRX})$



déchiffrement $m = D_{Pba}(c)$

Cryptanalyse : Logarithme discret

- Oscar connaît P et voit P^a, P^b.
- Il veut trouver P^{ab} (exercise : casse aussi ElGamal).
- Logarithme discret

Étant donné P^a, trouver $a = \log_P P^a$

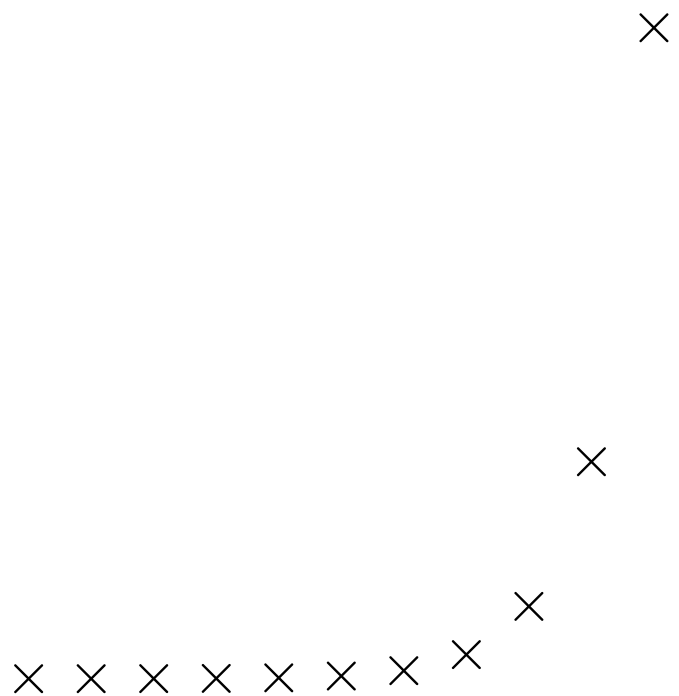
$P = 3$

$P^a = 9$

$a = \log_P(P^a) = \frac{\ln(P^a)}{\ln(P)}$

$= \frac{\ln(9)}{\ln(3)} = \frac{2{,}19\ldots}{1{,}09\ldots} = 2$

a	3^a
0	1
1	3
2	9
3	27
4	81
5	243
6	729
7	2187
8	6561
9	19683
10	59049



Calcul modulo m

- Principe : On remplace chaque nombre par son reste après division par m.
- Exemple
  - $m = 17$
  - $40 = 2 \times 17 + 6 \equiv 6$
- On peut additionner

$$3 + 5 = 8$$

$$15 + 5 = 20 \equiv 3$$

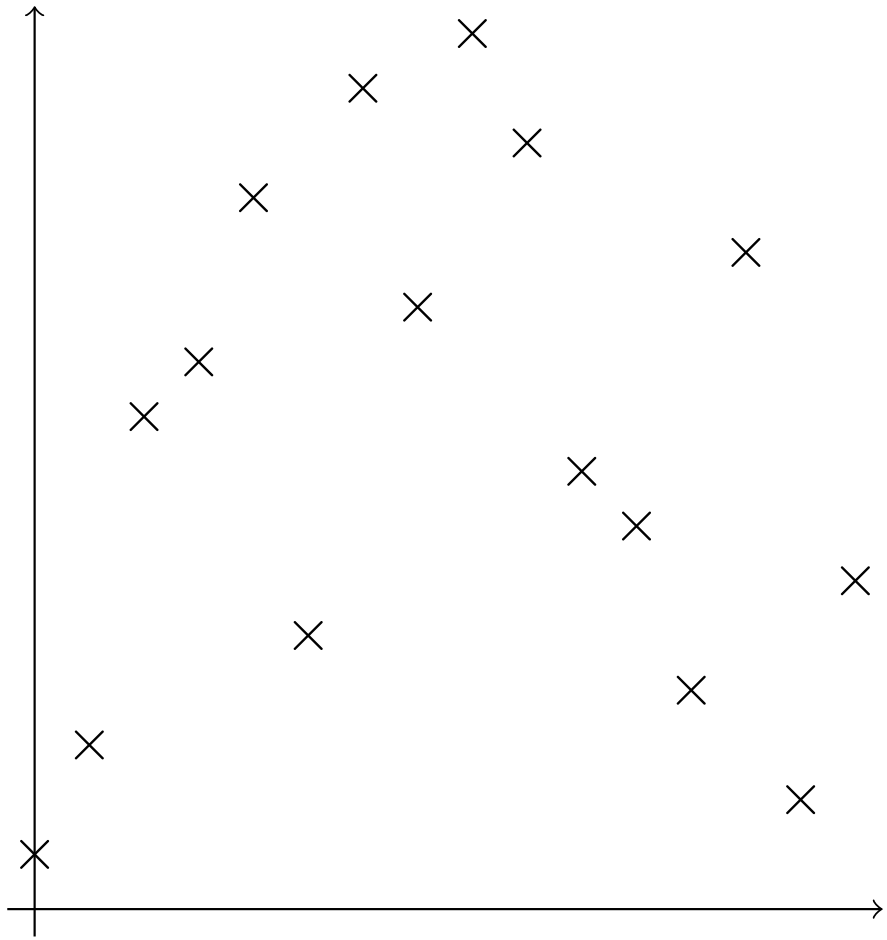
- On peut multiplier

$$15 \times 5 = 75 = 4 \times 17 + 7 \equiv 7$$

$$16 \times 16 = 256 = 15 \times 17 + 1 \equiv 1$$

Puissances modulo

a	$3^a \bmod 17$
0	1
1	3
2	9
3	10
4	13
5	5
6	15
7	11
8	16
9	14
10	8
11	7
12	4
13	12
14	2
15	6



On peut faire Diffie–Hellman et ElGamal,
et le log discret est (peut-être...) difficile à casser.

Algorithme de recherche exhaustive = force brute

- Base du logarithme : 3
- Nombre dont on cherche le logarithme : 2
- On cherche x avec $3^x \equiv 2$.

a	$3^a \bmod 17$
0	1
1	3
2	9
3	$27 = 1 \times 17 + 10 \equiv 10$
4	$81 = 4 \times 17 + 13 \equiv 13$
	$30 = 1 \times 17 + 13 \equiv 13$
5	$39 = 2 \times 17 + 5 \equiv 5$
6	15
7	$45 = 2 \times 17 + 11 \equiv 11$
8	$33 = 1 \times 17 + 16 \equiv 16$
9	$48 = 2 \times 17 + 14 \equiv 14$
10	$42 = 2 \times 17 + 8 \equiv 8$
11	$24 = 1 \times 17 + 7 \equiv 7$
12	$21 = 1 \times 17 + 4 \equiv 4$
13	12
14	$36 = 2 \times 17 + 2 \equiv 2$

$$\begin{aligned} 3^{14} &\equiv 2 \\ x &= 14 \end{aligned}$$

Vérification :

$$\begin{aligned} 3^{14} &= 4\,782\,969 \\ &= 281\,351 \times 17 + 2 \end{aligned}$$

Vers un algorithme intelligent : nombres premiers

- Nombre premier = avec exactement deux facteurs

  1 : 1 ~~1 : 1~~

  2 : 1, 2

  3 : 1, 3

  4 : 1, 2, 4 ~~4 : 1, 2, 4~~

  5 : 1, 5

  6 : 1, 2, 3, 6 ~~6 : 1, 2, 3, 6~~

  7 : 1, 7

  8 : 1, 2, 4, 8 ~~8 : 1, 2, 4, 8~~

  9 : 1, 3, 9 ~~9 : 1, 3, 9~~

- Tout nombre entier a une factorisation unique en nombres premiers.

  $4 = 2 \times 2 = 2^2$

  $6 = 2 \times 3$

  $8 = 2^3$

  $9 = 3^2$

Vers un algorithme intelligent

Qu'est-ce qui se passe modulo 17 ?

La factorisation n'est plus unique !

$3^3 = 27 \equiv 10 = 2 \times 5$

a	3^a	2^a
0	1	1
1	3	2
2	9	4
3	10	8
4	13	16
5	5	15

Magie

$$3^3 \equiv 2 \times 5 \quad \Rightarrow \quad 3^{12} \equiv 2^4 \times 5^4$$

$$3^5 \equiv 5 \quad \Rightarrow \quad 3^{25} \equiv 5^5$$

$$2^5 \equiv 3 \times 5$$

$$2^5 \times 3^{12} \equiv 2^4 \times 3 \times 5^5$$

$$\Leftrightarrow \quad 2 \times 3^{11} \equiv 5^5$$

$$2 \times 3^{11} \equiv 5^5 \equiv 3^{25}$$

$$\Leftrightarrow \quad \boxed{2 \equiv 3^{14}}$$

Algorithme intelligent

Remplacer la magie par des équations linéaires

Premiers	2	3	5
Logarithme en base 3 modulo 17	x	1	y

$$
\begin{aligned}
3^3 &\equiv 2 \times 5 \\
3^5 &\equiv 5 \\
2^5 &\equiv 3 \times 5 \\
\Leftrightarrow 3 &\equiv 2^5 \times 5^{-1}
\end{aligned}
$$

I)	3	=	x	+	y	
II)	5	=			y	
III)	1	=	$5x$	−	y	
IV)=I)+III)	4	=	$6x$			
V)=II)+III)	6	=	$5x$			
5×V) - 4×IV)	14	=	x			

Même avec des multiplications modulo, le log est plus facile qu'on ne le croît !

Courbes elliptiques

$$\begin{aligned} Y^2 &= X^3 + a - X + b \\ &= (X+1)X(X-1) \end{aligned}$$

Quand $X^3 - X < 0$

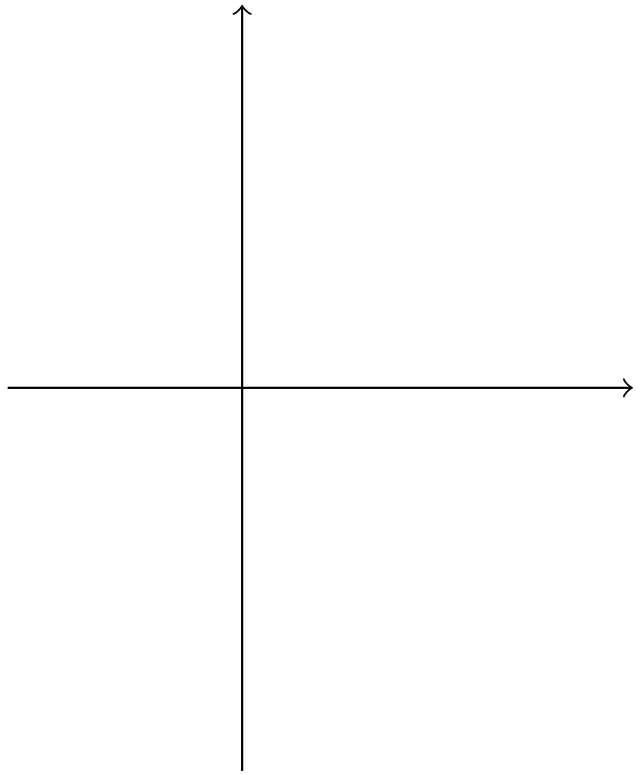
rien

Quand $X^3 - X = 0$

$$Y = 0$$

Quand $X^3 - X > 0$

$$\begin{aligned} Y &= +\sqrt{X^3 - X} \\ Y &= -\sqrt{X^3 - X} \end{aligned}$$

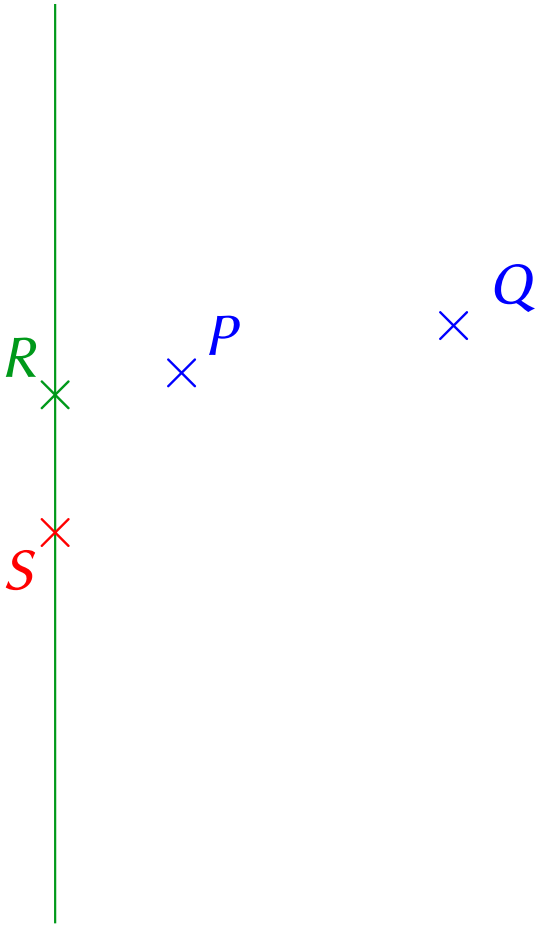


Addition

La somme des points sur une droite est 0.

Addition

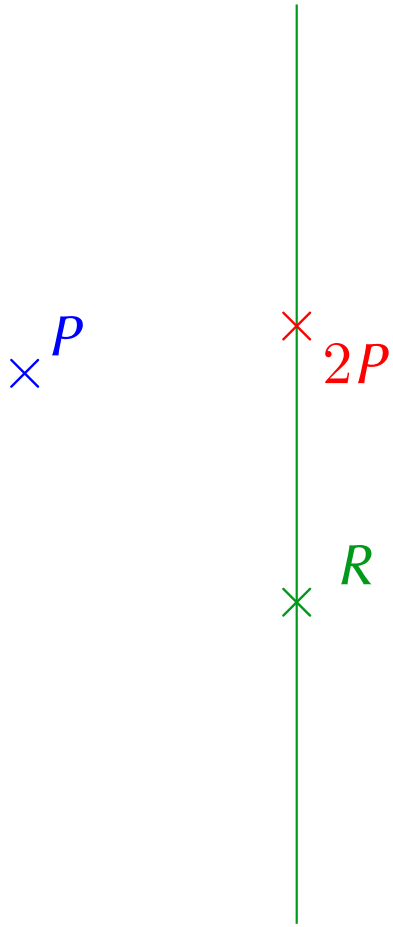
La somme des points sur une droite est 0.



$$\begin{aligned} P+Q+R &= 0 \\ R+S &= 0 \\ P+Q-S &= 0 \\ P+Q &= S \end{aligned}$$

Addition

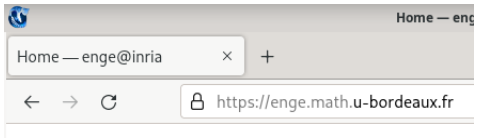
$P + P = ?$



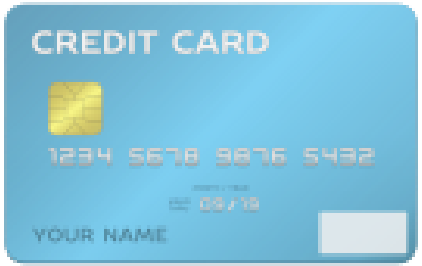
Crytographie avec courbes

のっとあっとおーる
CC-BY-SA 3.0

RainbowSilver2ndBackup
& Futurhit12
CC-BY-SA 4.0



Michael Romano, CC-BY-SA 3.0



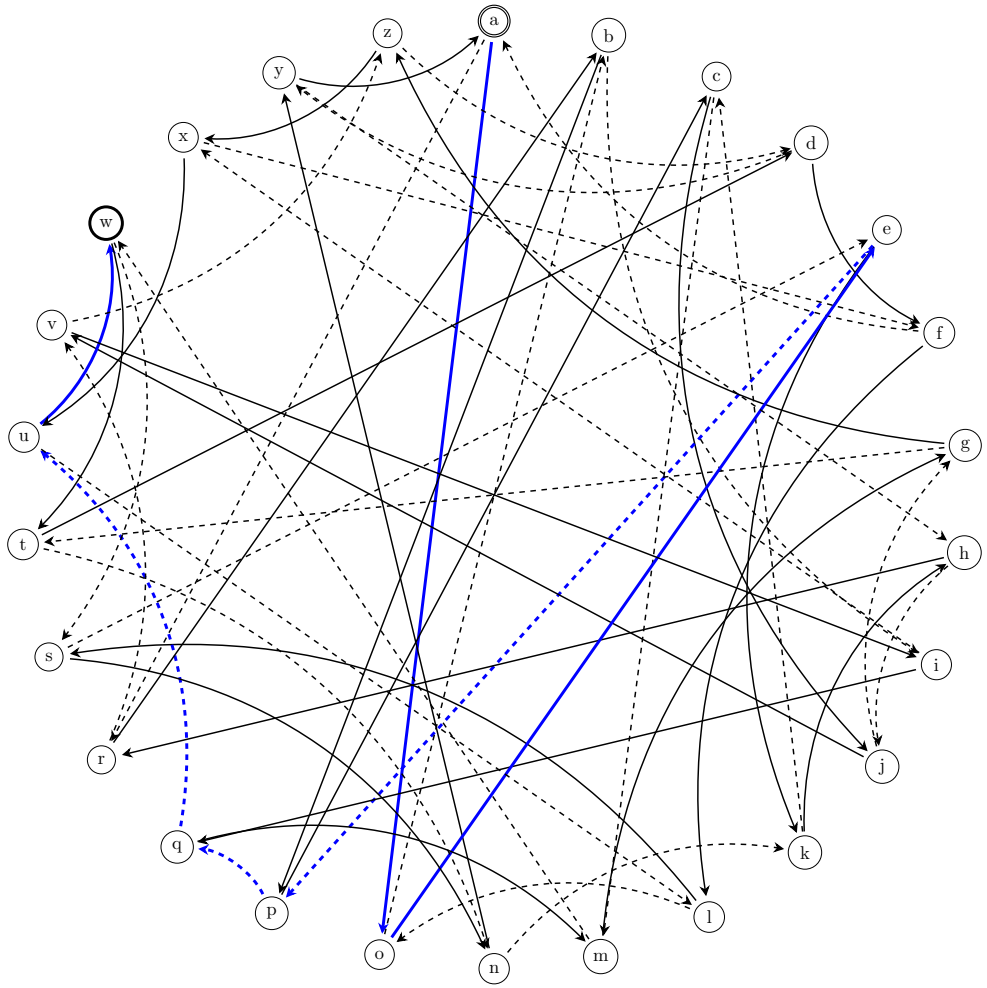
Pixabay, CC0

Postquantique

Chris Denny, CC-BY-SA 2.0

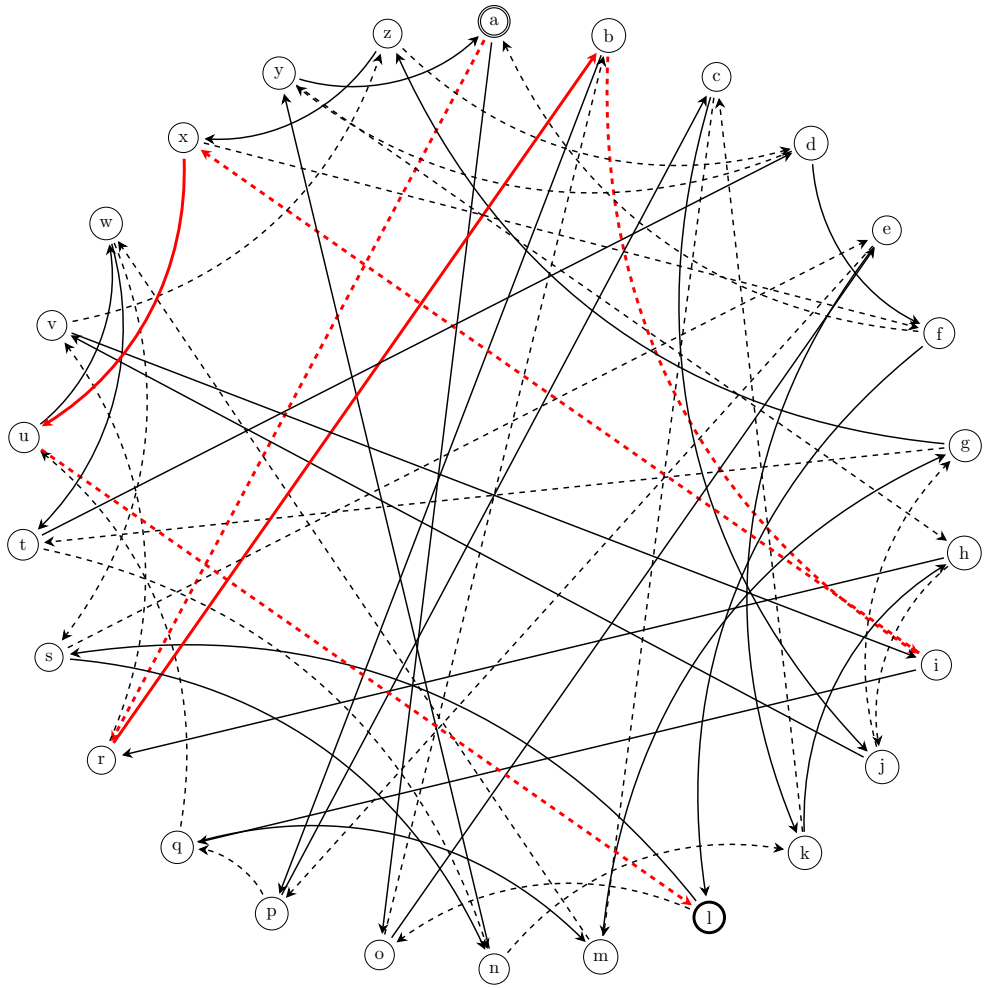
Cryptographie sur des graphes d'isogénies

Alice : 110001 a $\longrightarrow$ w (graphes par Damien Robert)



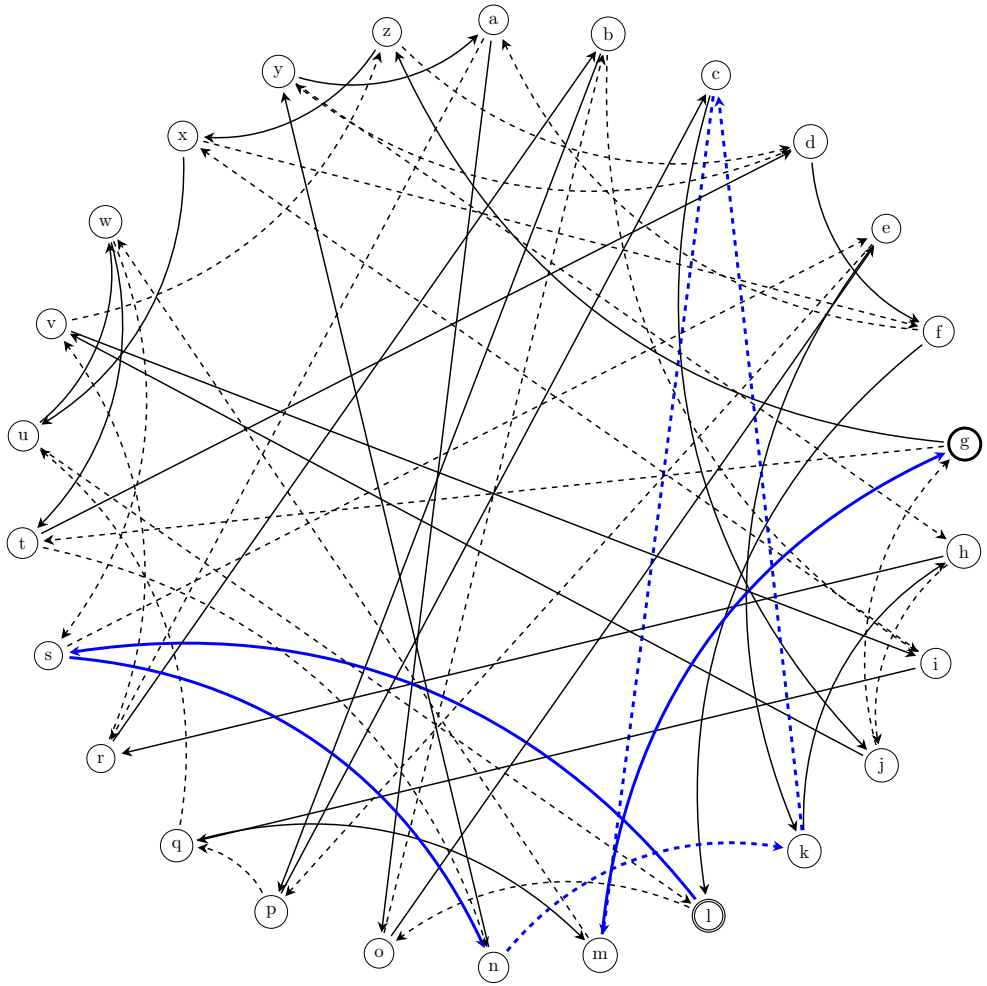
Cryptographie sur des graphes d'isogénies

Bob : 010010 $\quad a \longrightarrow l$



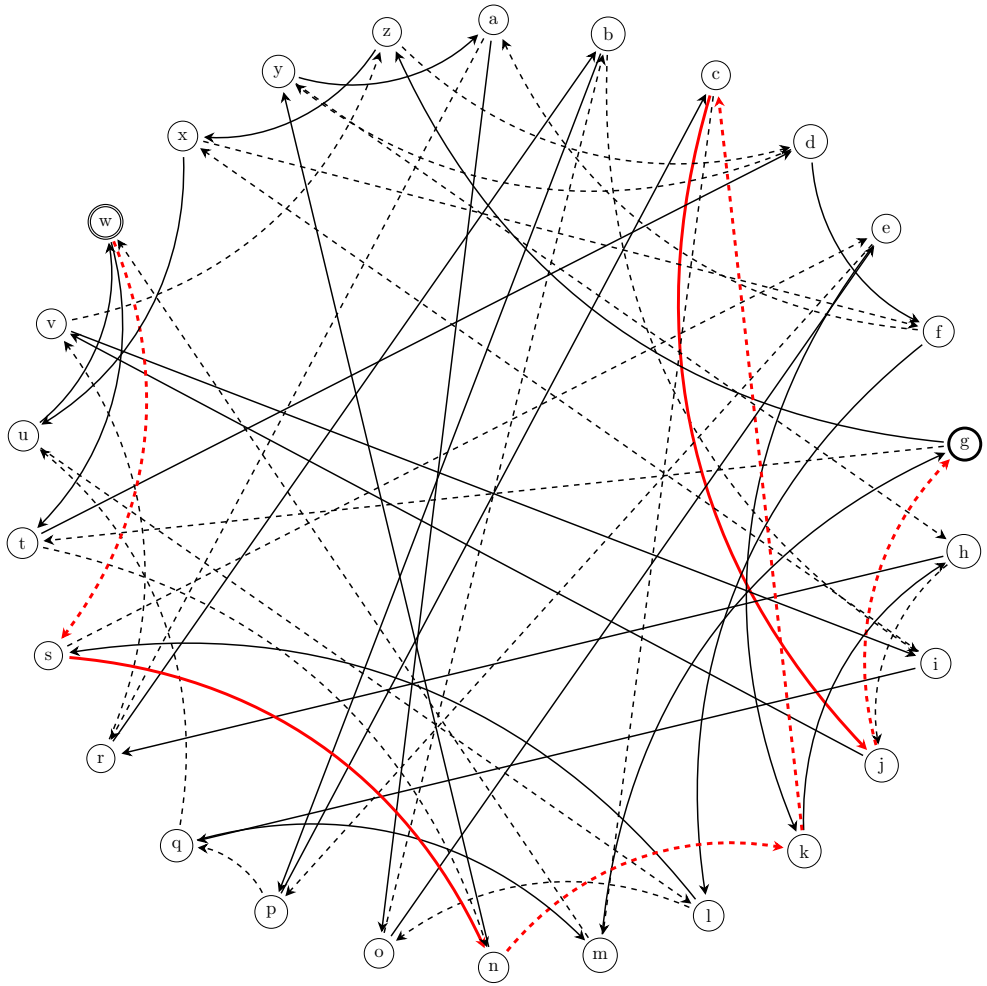
Cryptographie sur des graphes d'isogénies

Bob + Alice : 110001 $\quad l \longrightarrow g$



Cryptographie sur des graphes d'isogénies

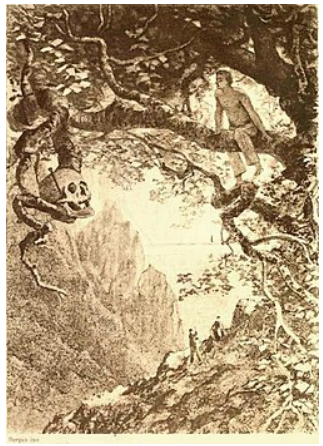
Alice + Bob : 010010 $\quad w \longrightarrow g$



Littérature

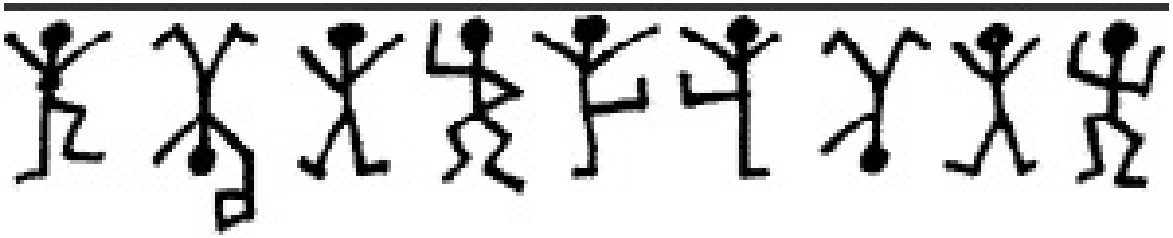
Poe, *Le scarabée d'or*, 1843

```
53‡‡†305))6*;4826)4‡.)4‡);806*;48†8
¶60))85;1‡(;:‡*8†83(88)5*†;46(;88*96
*?;8)*‡(;485);5*†2:*‡(;4956*2(5*-4)8
¶8*;4069285);)6†8)4‡‡;1(‡9;48081;8:8‡
1;48†85;4)485†528806*81(‡9;48;(88;4
(‡?34;48)4‡;161;:188;‡?;
```



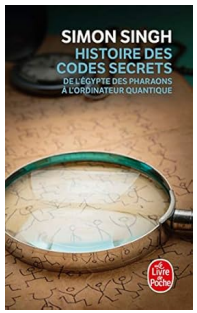
Herpin, Public Domain

Doyle, *Les hommes dansants*, 1903



조재범, CC-BY-SA 3.0

Singh, *L'Histoire des codes secrets : De l'Égypte des pharaons à l'ordinateur quantique*, 1999



Stephenson, *Cryptonomicon*, 1999