Introduction à la cryptographie

Le Reset - Dimanche 6 mai 2018

Scytale ou Bâton de Plutarque

Le chiffrement par substitution

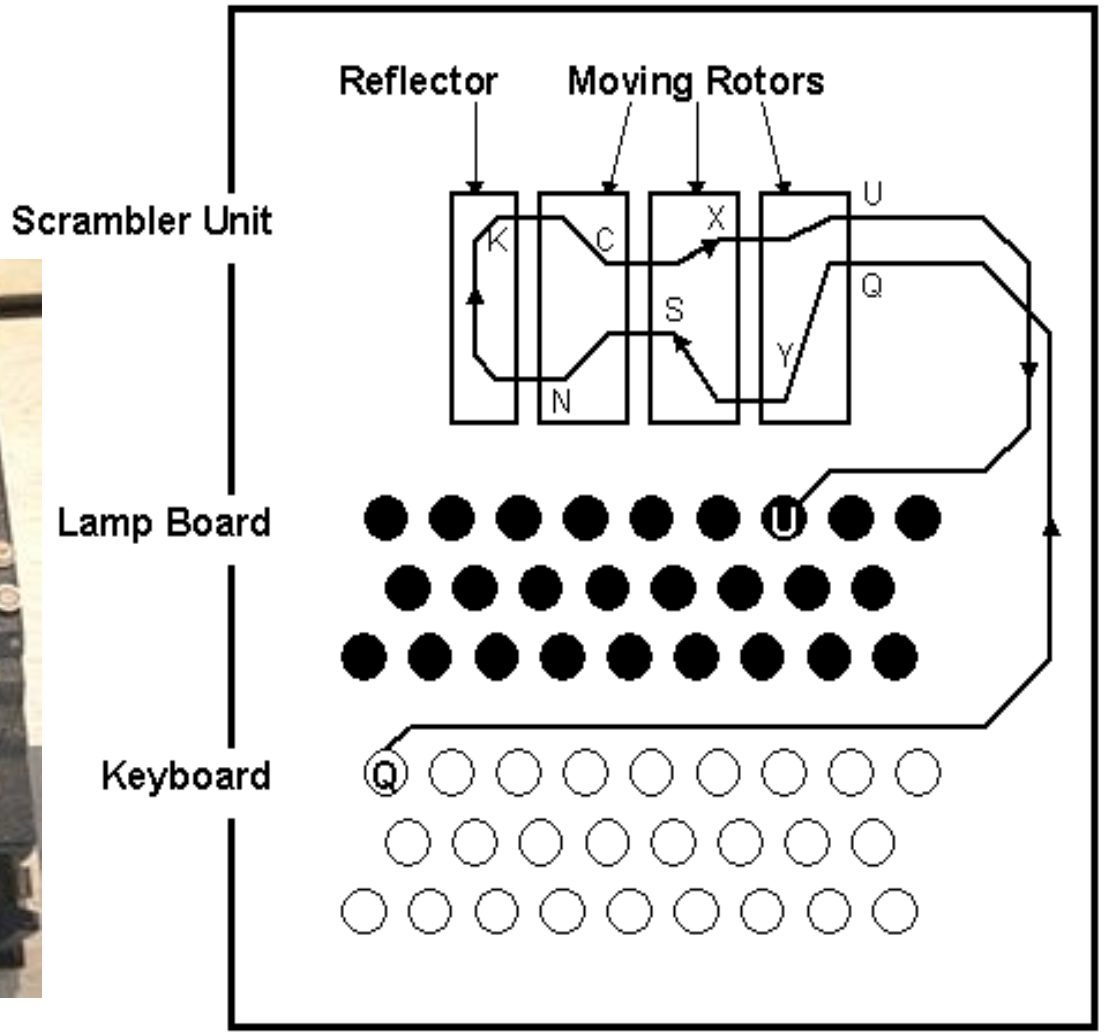
Atbash

Le chiffre de César

Le chiffre de Vigenère

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

Enigma


Reflector
Moving Rotors
Scrambler Unit
Lamp Board
Keyboard
K
C
X
U
Q
S
Y
N
U
Q

Travaux pratiques

Le chiffrement avec des coordonnées

Le 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

Le carré de Playfair, XIX

sur la même ligne

```
* * * * *
* 0 Y R Z
* * * * *
* * * * *
* * * * *
```

alors, OR → YZ

sur la même colonne

```
* * 0 * *
* * B * *
* * * * *
* * R * *
* * Y * *
```

alors, OR → BY

forment un rectangle

```
Z * * 0 *
* * * * *
* * * * *
R * * X *
* * * * *
```

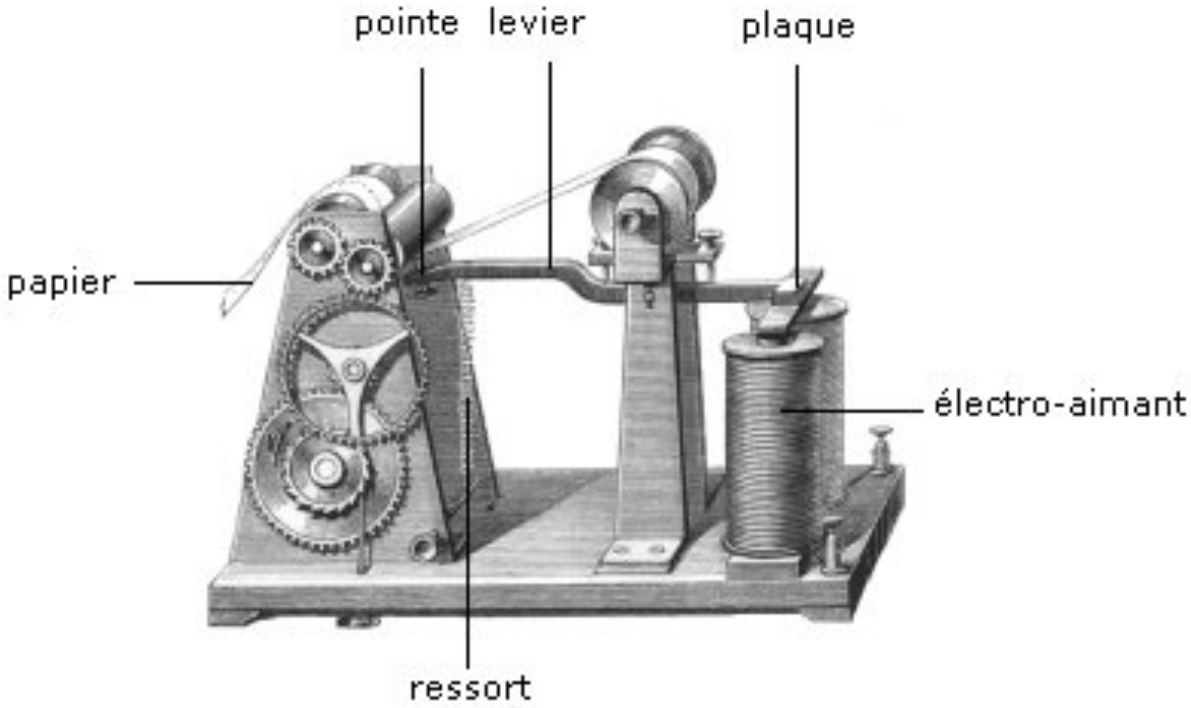
alors, OR → ZX

ADFGVX

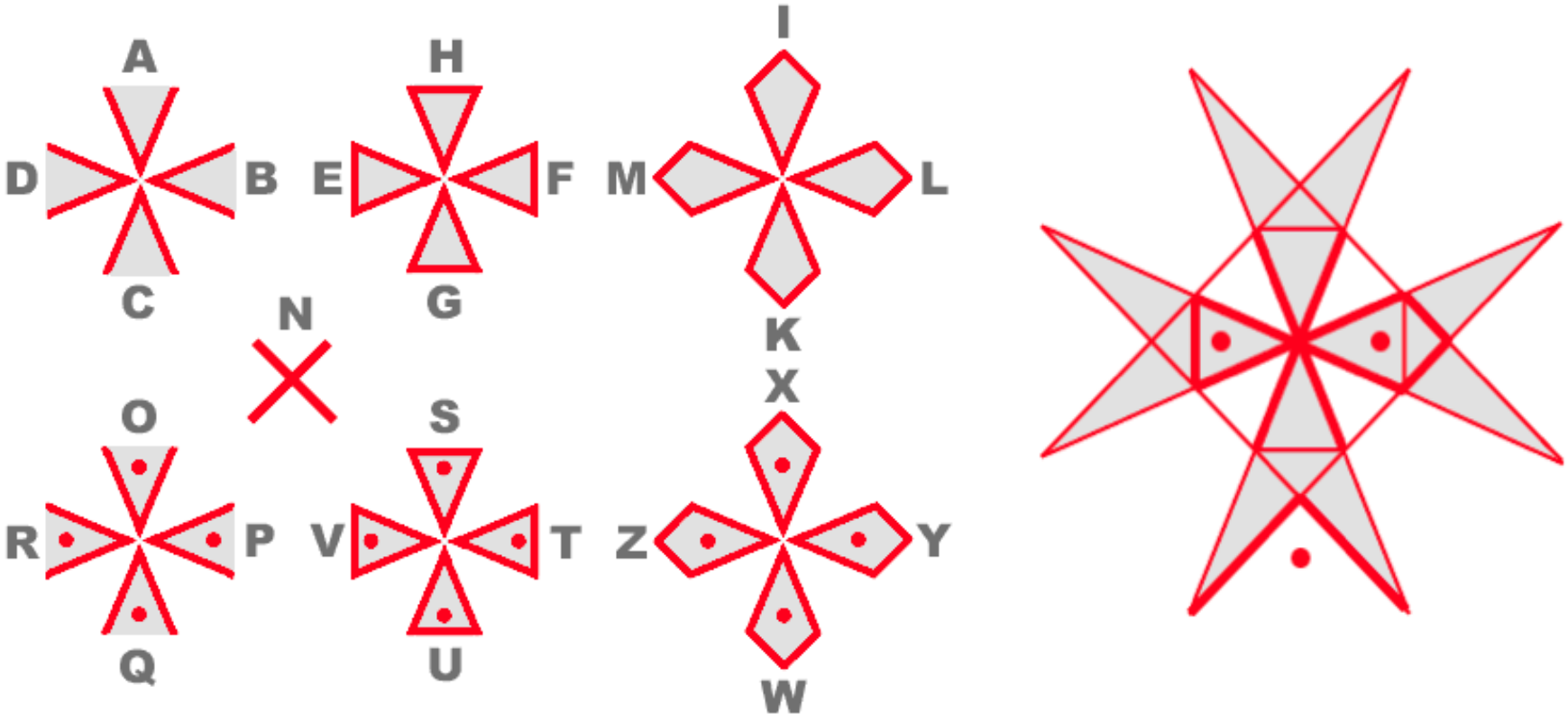
	A	D	F	G	V	X
A	S	U	B	J	E	C
D	T	A	D	F	G	H
F	I	K	L	M	N	O
G	P	Q	R	V	W	X
V	Y	Z	0	1	2	3
X	4	5	6	7	8	9

Le chiffrement par substitution de symboles

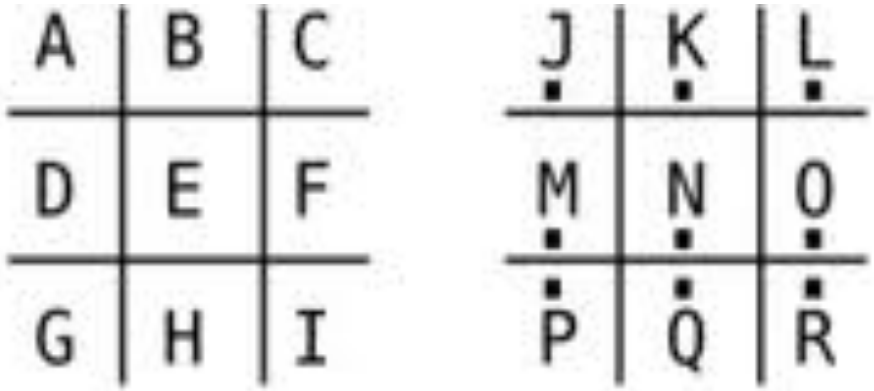
Le Morse



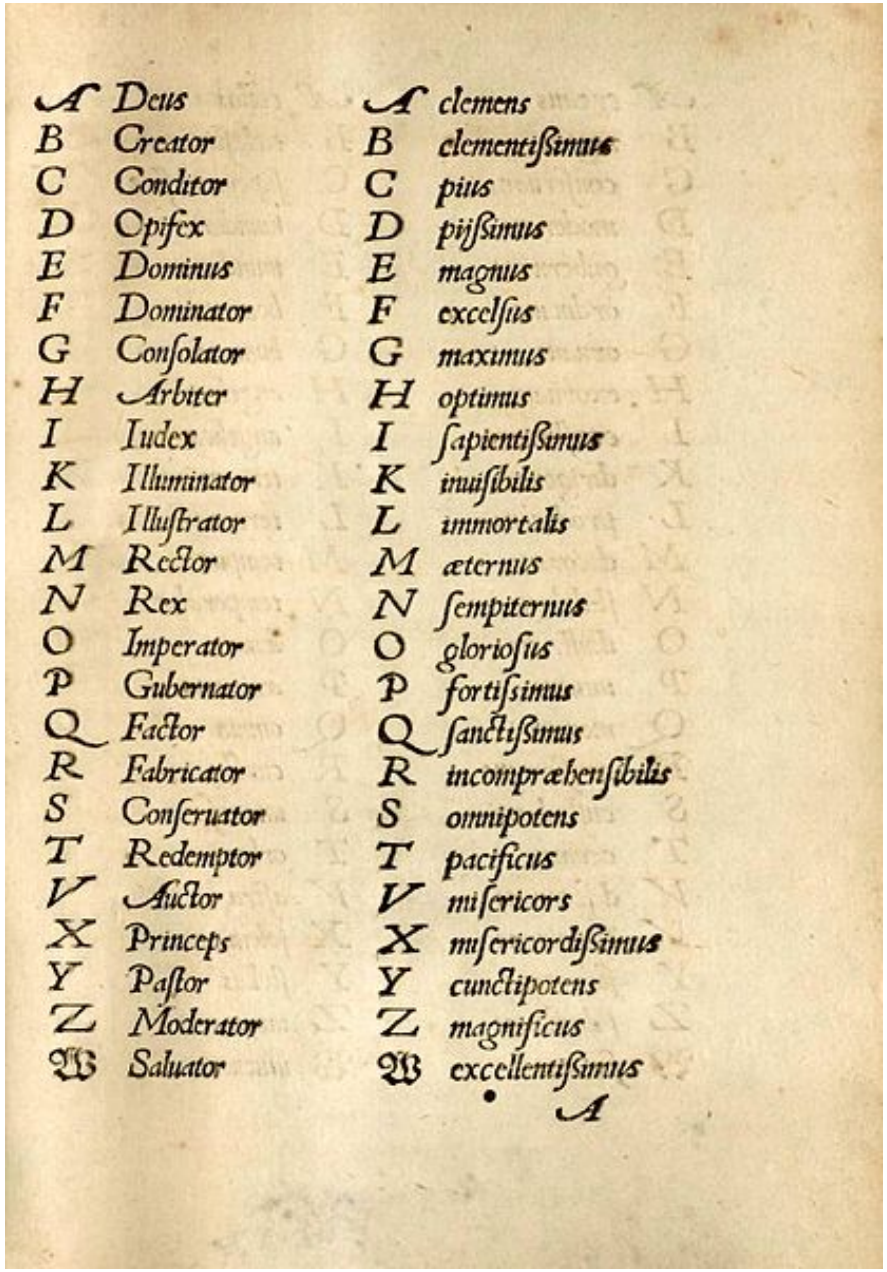
Le chiffre des Templiers



Le chiffre de Pigpen



Jean Trithème



A	Deus	A	clemens
B	Creator	B	clementiſsimus
C	Conditor	C	pius
D	Opifex	D	piiſsimus
E	Dominus	E	magnus
F	Dominator	F	excelſus
G	Conſolator	G	maximus
H	Arbiter	H	optimus
I	Iudex	I	ſapientiſsimus
K	Illuminator	K	inuiſibilis
L	Illuſtrator	L	immortalis
M	Rector	M	æternus
N	Rex	N	ſempiternus
O	Imperator	O	glorioſus
P	Gubernator	P	fortiſsimus
Q	Factor	Q	ſanctiſsimus
R	Fabricator	R	incompræhenſibilis
S	Conſeruator	S	omnipotens
T	Redemptor	T	pacificus
V	Auctor	V	miſericors
X	Princeps	X	miſericordiſsimus
Y	Paſtor	Y	cunctipotens
Z	Moderator	Z	magnificus
W	Saluator	W	excellentiſsimus

A

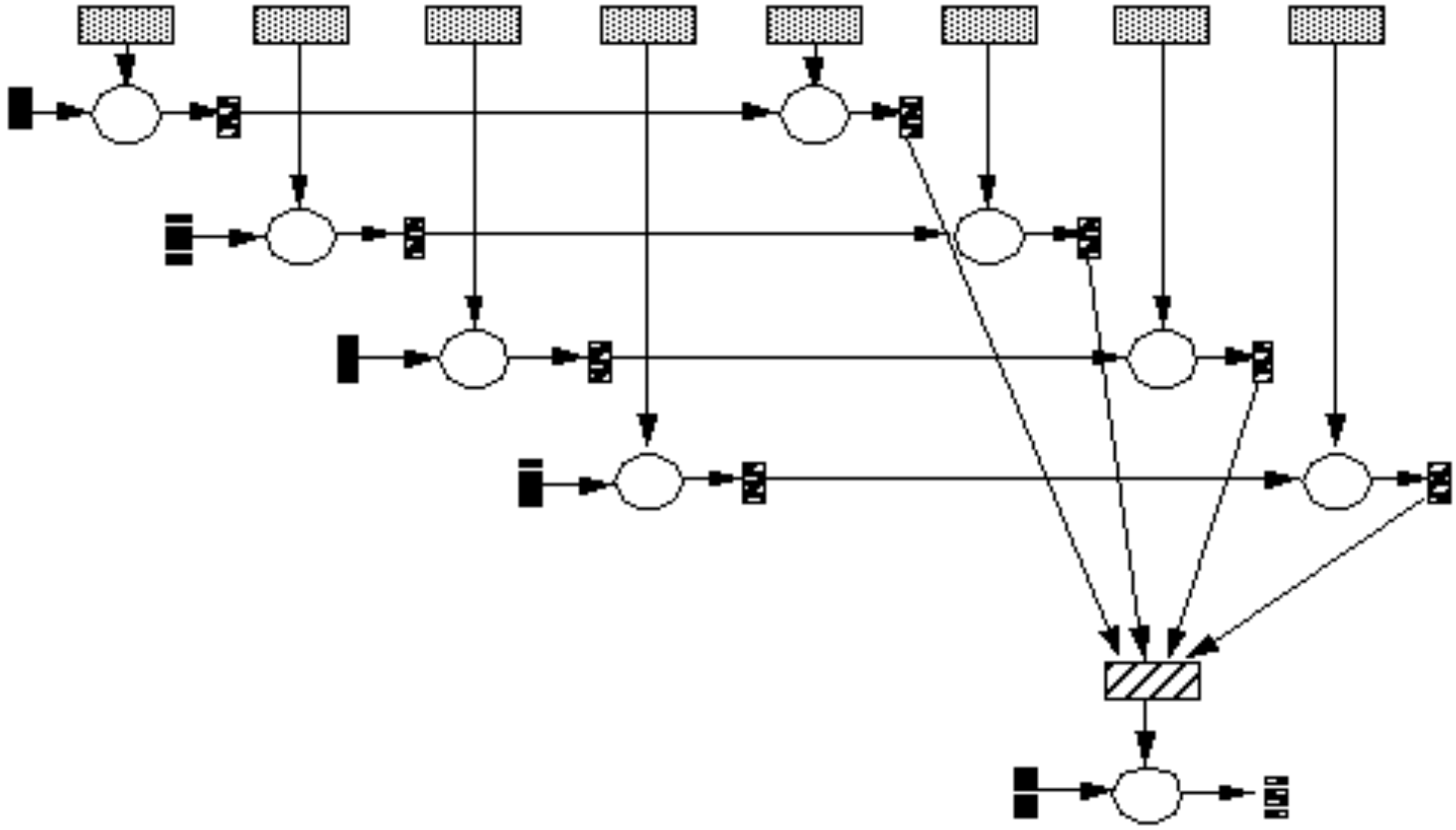
Le Grand Chiffre de Louis XIV

Les suites de nombres pseudo-aléatoires

Rivest Cipher 4, 1987

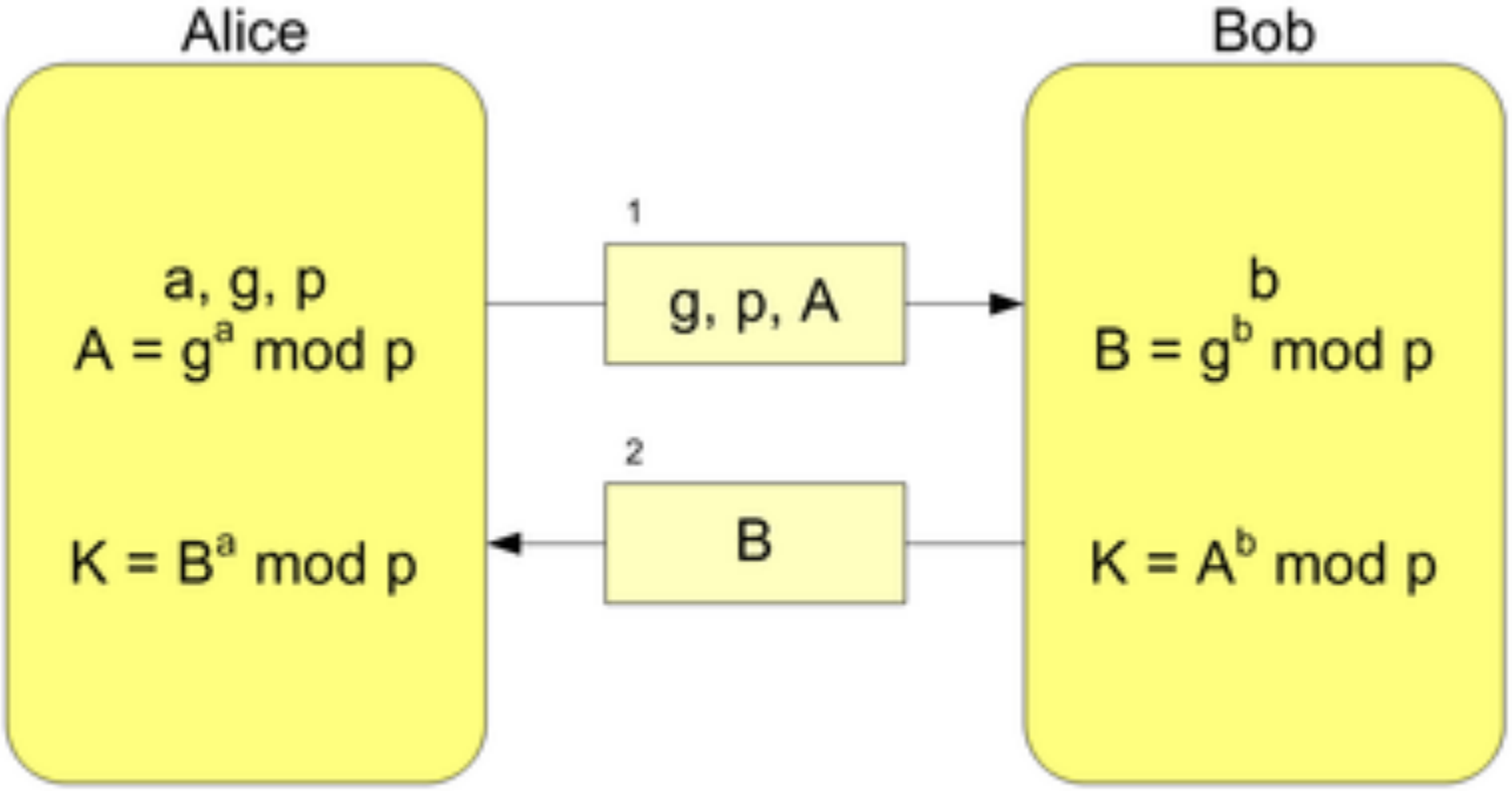
Les fonctions de hashage

MD5, Whirlpool, SHA-256



L'échange de clefs Diffie-Hellman

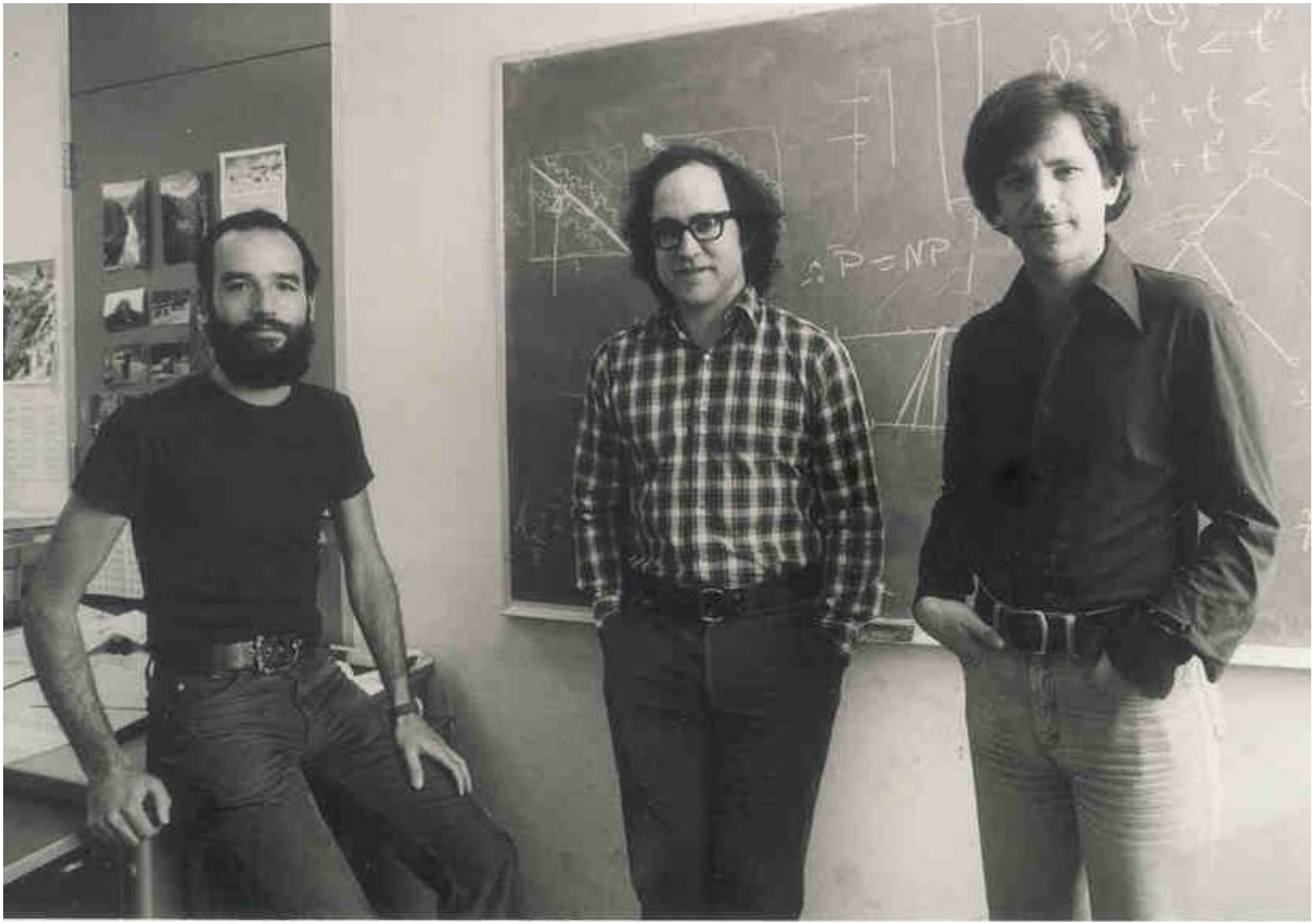
Diffie-Hellman



$K = A^b \bmod p = (g^a \bmod p)^b \bmod p = g^{ab} \bmod p = (g^b \bmod p)^a \bmod p = B^a \bmod p$

Le chiffrement asymétrique

RSA（1977）



La cryptographie quantique

L’importance de la clef

Principes de Kerckhoffs, 1883

« L'adversaire connaît le système »

Claude Shannon, 1949

Un code incassable

Clé aléatoire

Au moins aussi longue que M

À masque jetable

Problème

Impossible en chiffrement asymétrique

Chiffrement symétrique

→ Problème de distribution des clefs

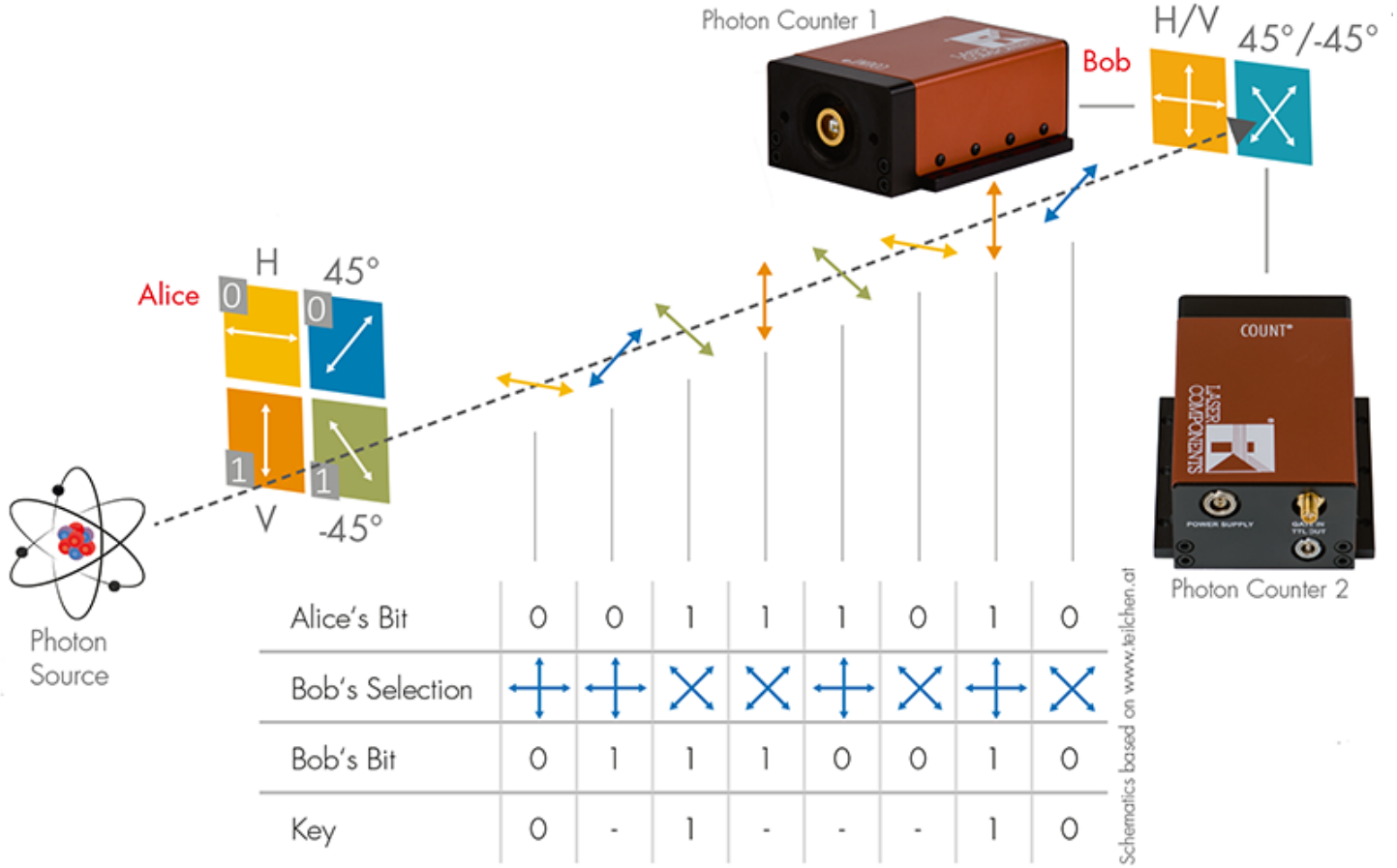
La mesure quantique

Paradoxe de Schrödinger

→ Impact de la mesure

Principe de décohérence quantique

Comment ça marche ?



Les limitations

Capacité d'écoute d'Eve

Moyens nécessaires

- Manipulation les particules
- Isolation du bruit (-50°C)
- Distance (Genève-Lausanne ≈ 67 km en 2002)

Les maths (faciles) derrière le RSA

Le Reset - Dimanche 6 mai 2018

Chiffrer / déchiffrer

m est le message en clair

c est le message chiffré

$m \to c$ (chiffrement)

$c \to m$ (déchiffrement)

Quelques principes mathématiques

- encodage de caractères
- multiplication et factorisation
- congruence sur les entiers
- indicatrice d'Euler
- théorème d'Euler

Exemple d'encodage : l'ascii

0	NUL	16	DLE	32	SP	48	0	64	@	80	P	96	`	112	p
1	SOH	17	DC1	33	!	49	1	65	A	81	Q	97	a	113	q
2	STX	18	DC2	34	"	50	2	66	B	82	R	98	b	114	r
3	ETX	19	DC3	35	#	51	3	67	C	83	S	99	c	115	s
4	EOT	20	DC4	36	$	52	4	68	D	84	T	100	d	116	t
5	ENQ	21	NAK	37	%	53	5	69	E	85	U	101	e	117	u
6	ACK	22	SYN	38	&	54	6	70	F	86	V	102	f	118	v
7	BEL	23	ETB	39	'	55	7	71	G	87	W	103	g	119	w
8	BS	24	CAN	40	(	56	8	72	H	88	X	104	h	120	x
9	HT	25	EM	41	)	57	9	73	I	89	Y	105	i	121	y
10	LF	26	SUB	42	*	58	:	74	J	90	Z	106	j	122	z
11	VT	27	ESC	43	+	59	;	75	K	91	[	107	k	123	{
12	FF	28	FS	44	,	60	<	76	L	92	\	108	l	124	|
13	CR	29	GS	45	-	61	=	77	M	93	]	109	m	125	}
14	SO	30	RS	46	.	62	>	78	N	94	^	110	n	126	~
15	SI	31	US	47	/	63	?	79	O	95	_	111	o	127	DEL

Le module de chiffrement

p est un nombre premier

q est un nombre premier

$$n = p*q$$

$$15 = 3*5$$

Congruence sur les entiers

$13 \equiv 1 \pmod{12}$

$22 \equiv 10 \pmod{12}$

Propriétés :

$a \equiv b \ (n) \rightarrow a^k \equiv b^k \ (n)$

$a \equiv b \ (n) \rightarrow k \star a \equiv k \star b \ (n)$

La fonction indicatrice d'Euler

Fonction qui à tout entier naturel n non nul associe le nombre d'entiers compris entre 1 et n (inclus) et premiers avec n.

$\Phi(8)= ?$

La fonction indicatrice d'Euler

$\Phi(8) = ?$

1
2
3
4
5
6
7
8

La fonction indicatrice d'Euler

$\Phi(8) = 4$

1
2
3
4
5
6
7
8

Propriétés

Si p est premier,

$\Phi(p)=p-1$

$\Phi(3) = 2$
$\Phi(5) = 4$

Si a et b sont premiers entre eux,

$\Phi(a*b)=\Phi(a)*\Phi(b)$

$\Phi(3)*\Phi(5) = 8$

Propriétés

$n=p*q$ *(module de chiffrement)*

$\Phi(n) = \Phi(p*q)$

$\Phi(a*b)=\Phi(a)*\Phi(b)$

$\Phi(n)=\Phi(p)*\Phi(q)$

$\Phi(p)=p-1$

$\Phi(n)=(p-1)*(q-1)$

$$n=p*q$$

$$\Phi(n) = \Phi(p*q)$$

$$\Phi(n)=\Phi(p)*\Phi(q)$$

$$\Phi(n)=(p-1)*(q-1)$$

$$15=3*5$$

$$\Phi(15)=\Phi(3*5)$$

$$\Phi(15)=\Phi(3)*\Phi(5)$$

$$\Phi(15)=2*4$$

$$\Phi(15) = 8$$

1	6	11
2	7	12
3	8	13
4	9	14
5	10	15

$n=p*q$

$\Phi(n) = \Phi(p*q)$

$\Phi(n)=\Phi(p)*\Phi(q)$

$\Phi(n)=(p-1)*(q-1)$

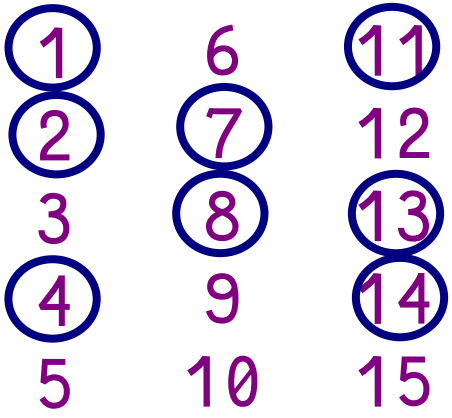
$15=3*5$

$\Phi(15)=\Phi(3*5)$

$\Phi(15)=\Phi(3)*\Phi(5)$

$\Phi(15)=2*4$

$\Phi(15) = 8$



Le théorème d'Euler

Pour tout entier $n > 0$ et tout entier a premier avec n

$$m^{\Phi(n)} \equiv 1 \pmod{n}$$

Le théorème d'Euler

$m^{\phi(n)} \equiv 1 \pmod{n}$

$m^{\phi(n)} * m \equiv m * 1 \pmod{n}$

$m^{\phi(n)+1} \equiv m \pmod{n}$

$a \equiv b \pmod{n} \rightarrow k * a \equiv k * b \pmod{n}$

Qu'est-ce qu'on cherche déjà ?

m → c (chiffrement)

$m^e \equiv c \pmod{n}$

e : Clef de chiffrement

$8^2 \equiv 64 \pmod{12}$

$8^2 \equiv 4 \pmod{12}$

c → m (déchiffrement)

$c^d \equiv m \pmod{n}$

d : Clef de déchiffrement

$4^{2,5} \equiv 32 \pmod{12}$

$4^{2,5} \equiv 8 \pmod{12}$

Par définition : $c \equiv m^e \pmod n$

On veut que : $c^d \equiv m \pmod n$

→ $c^d \equiv m^{e*d} \equiv m \pmod n$

On a vu que : $m^{\Phi(n)+1} \equiv m \pmod n$

(théorème d'Euler)

Donc : $e*d = \Phi(n)+1$

Donc : $e*d = 1+\Phi(n)$

$$d = \frac{\Phi(n)+1}{e}$$

$\Phi(n)=(p-1)*(q-1)$

$$d = \frac{(p-1)*(q-1)+1}{e}$$

$m = 7$ (message en clair)

$p = 3$ (nombre premier)

$q = 5$ (nombre premier)

$e = 3$ (clef de chiffrement, au hasard)

m = 7 (message en clair)

p = 3 (nombre premier)

q = 5 (nombre premier)

e = 3 (clef de chiffrement, au hasard)

module de chiffrement :

$n=p*q \rightarrow 15=3*5$

m = 7 (message en clair)

p = 3 (nombre premier)

q = 5 (nombre premier)

e = 3 (clef de chiffrement)

n = 15 (module de chiffrement)

message chiffré :

$m^e \equiv c \pmod{n} \rightarrow 7^3 \equiv 343 \equiv 13 \pmod{15}$

c : message chiffré

m = 7 (message en clair)

p = 3 (nombre premier)

q = 5 (nombre premier)

e = 3 (clef de chiffrement)

n = 15 (module de chiffrement)

c = 13 (message chiffré)

Déchiffrement :

$c^d \equiv m \pmod{n} \rightarrow 13^d \equiv 7 \pmod{15}$

m = 7

p = 3

q = 5

e = 3

n = 15

c = 13

$$d = \frac{\Phi(n) + 1}{e}$$

$$d = \frac{(p - 1) * (q - 1) + 1}{e}$$

$$d = \frac{(3 - 1) * (5 - 1) + 1}{3}$$

$$d = \frac{(2) * (4) + 1}{3}$$

$$d = \frac{9}{3} = 3$$

m = 7 (message en clair)

p = 3 (nombre premier)

q = 5 (nombre premier)

e = 3 (clef de chiffrement)

n = 15 (module de chiffrement)

c = 13 (message chiffré)

d = 3 (clef de déchiffrement)

$c^d \equiv m \pmod{n} \rightarrow 13^3 \equiv 2197 \equiv 7 \pmod{15}$

m : message déchiffré

En résumé

$c^d \equiv m^{e*d} \equiv m \pmod{n}$

(n, e) = clef publique

(p, q) = clef privée