

# Cryptographie

IFT2105

H2008

(Alain Tapp)

# Introduction

Depuis fort longtemps, les hommes ont tenté de rendre sécuritaires leurs communications confidentielles. Différentes techniques ont été utilisées.

Au début, il s'agissait seulement de cacher l'existence du message. Cette technique s'appelle la stéganographie.

Puis, des techniques de plus en plus sophistiquées furent utilisées pour rendre les messages compréhensibles seulement par leurs destinataires légitimes.

Tout au cours de l'histoire, une difficile bataille eut lieu entre les constructeurs de code (cryptographes) et ceux qui essayaient de les briser (les cryptanalystes). Il n'est toujours pas clair, même aujourd'hui, qui sera le vainqueur.

# Stéganographie

Le plus ancien exemple de stéganographie a été rapporté par [Hérodote](#). C'était lors du conflit entre la Grèce et la Perse au [5ième siècle av. J.-C.](#)

Les Perses voulaient conquérir la Grèce et avaient préparé pendant 5 années une imposante armée. Heureusement pour les Grecques, [Damaratus](#), un Grec exilé en Perse eu vent de ce projet.

Il inscrivit son message sur des tablettes de bois et les recouvrit de cire. Les tablettes avaient donc l'air vierges. Elles n'attirèrent pas l'attention des gardes tout au long du parcours.

Les Grecques, une fois mis au courant de l'attaque perse à venir, eurent le temps de se préparer et lors de l'attaque, ils mirent l'armée perse en déroute.

# Stéganographie

Hérodote rapporte aussi l'histoire d'[Histaïaeus](#) qui, pour transmettre un message, rase la tête de son messager et inscrit le message sur son crane. Une fois les cheveux repoussés, le messager put circuler sans attirer l'attention.

Durant la Deuxième Guerre mondiale, les Allemands utilisaient la technique du [micropoint](#). Il s'agit de photographier avec un microfilm le document à transmettre. La taille du microfilm était de moins d'un millimètre de diamètre. On plaçait le micropoint à la place du point final d'une lettre apparemment anodine.

En 1941, le FBI repéra le premier micropoint. De nombreux messages furent par la suite interceptés.

# Chiffrement de César

Dans le célèbre film de Stanley Kubrick

## **2001: A Space Odyssey**

un des personnages principaux est un super ordinateur appelé

**HAL9000**

Le film a été réalisé en 1969.

Est-ce qu'il y a un message caché dans le nom de l'ordinateur?

# Chiffrement de César

Cette technique simple de chiffrement effectuant un décalage est appelé chiffrement de César.

Par exemple, avec un décalage de trois, mon nom devient

ALAIN TAPP = DODLQCWDSS

(On décale aussi les espaces...)

Cette technique de chiffrement est-elle sécuritaire?

# Chiffrement de César

On intercepte le message

FAGEMYREMPURZV\_EMZR\_R FMNMDAZR

Essayons différents décalages...

1: E\_FDLXQDLOTQYUZDLYQZQZELMLC\_YQ

2: DZECKWPCKNSPXTYCKXPYPYDKLKBZXP

3... 4... 5... 6... 7... 8... 9... 10... 11... 12...

13: TOUS\_LES\_CHEMINS\_MENENT\_A\_ROME

Clairement, le chiffrement de César n'est pas sécuritaire.

# Cryptosystème a clef courte

Principe de Kerckhoff

(La cryptographie militaire 1883):

*La sécurité d'un système de cryptographie ne doit pas dépendre de la préservation du secret de l'algorithme. La sécurité ne repose que sur le secret de la clef.*

Le masque jetable n'est pas pratique.

Peut-on chiffrer avec une clef courte de façon sécuritaire?

# Substitution mono-alphabétique

Essayons autre chose.

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

TOUS\_LES\_CHEMINS\_MENENT\_A\_ROME    devient  
FQLJRPAJRHCAE\_ZJREAZAZFRDRNQEA

Le décodage devrait être plus difficile. Peut-on essayer tous les décodages possibles?

Il y a  $27! = 10\ 888\ 869\ 450\ 418\ 352\ 160\ 768\ 000\ 000$  possibilités...

La substitution mono-alphabétique apparaît déjà dans le *kàma-sùtra* qui fut écrit au 5<sup>ème</sup> siècle mais qui est basé sur des écrits datant du 4<sup>ème</sup> siècle av. J.-C.

Le premier usage révélé de chiffrement par substitution dans un usage militaire est rapporté par Jules César dans *La guerre des Gaules*. César utilisait fréquemment le chiffrement et en particulier le décalage de trois caractères.

La substitution mono-alphabétique fut la technique de chiffrement la plus utilisée durant le premier millénaire. Nombreux savants de l'antiquité tenaient cette technique pour inviolable.

Ce sont les Arabes qui réussirent à briser ce code et qui inventèrent la cryptanalyse au 9<sup>ème</sup> siècle.

# Exemple

BQPSNRSJXJNXLDPCLDLPQBE\_QRKJXHNKPKSJPJIKSPUNBDKIQRBKPKQ  
PBQPZITEJQDQBT SKPELNIUNPHNKPBKPCCKSSQWKPSLXJPSNVVXSQCCKD  
JPBLDWPXBPSNVVXJPGKPJKDXIPZLCEJKPGKSPSJQJXSJXHNKSPGPLZZ  
NI IKDZKPGKSPGXVVKIKDJKSPBKJJIKS

Comment déchiffrer ce message?

Chaque lettre est chiffrée de la même façon...  
Certaines lettres sont utilisées plus souvent.

# Occurrence des lettres

En français

_	19.3	L	4.7	H	0.8
E	13.9	O	4.1	G	0.8
A	6.7	D	2.9	B	0.6
S	6.3	P	2.5	X	0.4
I	6.1	C	2.4	Y	0.3
T	6.1	M	2.1	J	0.3
N	5.6	V	1.3	Z	0.1
R	5.3	Q	1.3	K	0.0
U	5.2	F	0.9	W	0.0

Dans le cryptogramme

P	14.3	D	4.6	W	1.0
K	12.8	L	4.1	U	1.0
S	9.2	V	3.1	T	1.0
J	9.2	Z	2.6	_	0.5
X	5.6	G	2.6	O	0.0
Q	5.6	C	2.6	M	0.0
N	5.6	E	2.0	F	0.0
B	5.1	R	1.5	A	0.0
I	4.6	H	1.5	Y	0.0

Remplaçons P par \_ et K par E

BQ\_SNRSJXJNXLDCLDL\_QBE\_QREJXHNE\_ESJ\_JIES\_UNBDEIQRBE\_Q  
\_BQ\_ZITEJQDQBTSE\_ELNUN\_HNE\_BE\_CESSQWE\_SLXJ\_SNVVXSQCCED  
J\_BLDW\_XB\_SNVVXJ\_GE\_JEDXI\_ZLCEJE\_GES\_SJQJXSJXHNES\_G\_LZZ  
NI IEDZE\_GES\_GXVVEIEDJES\_BEJJIES

Remplaçons Q par A et B par L

LA\_SNRSJXJNXLD\_CLDL\_ALE\_AREJXHNE\_ESJ\_JIES\_UNLDEIARLE\_A  
\_LA\_ZITEJADALTSE\_ELNIUN\_HNE\_LE\_CESSAWE\_SLXJ\_SNVVXSACCED  
J\_LLDW\_XL\_SNVVXJ\_GE\_JEDXI\_ZLCEJE\_GES\_SJAJXSJXHNES\_G\_LZZ  
NI EDZE\_GES\_GXVVEIEDJES\_LEJJIES

Remplaçons S par S et G par D

LA\_SNRSJXJNJXLD\_CLDL\_ALE\_AREJXHNE\_ESJ\_JIES\_UNLDEIARLE\_A  
\_LA\_ZITEJADALTSE\_ELNIUN\_HNE\_LE\_CESSAWE\_SLXJ\_SNVVXSACCED  
J\_LLDW\_XL\_SNVVXJ\_DE\_JEDXI\_ZLCEJE\_DES\_SJAJXSJXHNES\_D\_LZZ  
NI IEDZE\_DES\_DXVVEIEDJES\_LEJJIES

Remplaçons **J** par T et **I** par R

LA\_SNRSTXTNTXLD\_CLDL\_ALE\_ARETXHNE\_EST\_TRES\_UNLDERARLE\_A  
\_LA\_ZRTETADALTSE\_ELNRUN\_HNE\_LE\_CESSAWE\_SLXT\_SNVVXSACCED  
T\_LLDW\_XL\_SNVVXT\_DE\_TEDXR\_ZLCETE\_DES\_STATXSTXHNES\_D\_LZZ  
NRREDZE\_DES\_DXVVEREDTES\_LETTRES

Remplaçons X par I, H par Q et N par U

LA\_SURSTITUTILD\_CLDL\_ALE\_ARETIQUE\_EST\_TRES\_UULDERARLE\_A  
\_LA\_ZRTETADALTSE\_ELURUU\_QUE\_LE\_CESSAWE\_SLIT\_SUVVISACCED  
T\_LLDW\_IL\_SUVVIT\_DE\_TEDIR\_ZLCETE\_DES\_STATISTIQUES\_D\_LZZ  
URREDZE\_DES\_DIVVEREDTES\_LETTRES

Remplaçons **V** par F et **D** par N

LA\_SURSTITUTILN\_CLNL\_ALE\_ARETIQUE\_EST\_TRES\_UULNERARLE\_A  
\_LA\_ZRTETANALTSE\_ELURUU\_QUE\_LE\_CESSAWE\_SLIT\_SUFFISACCEN  
T\_LLNW\_IL\_SUFFIT\_DE\_TENIR\_ZLCETE\_DES\_STATISTIQUES\_D\_LZZ  
URRENZE\_DES\_DIFFERENTES\_LETTRES

Remplaçons R par B et L par O

LA\_SUBSTITUTION\_MONO\_ALPHABETIQUE\_EST\_TRES\_VULNERABLE\_A  
\_LA\_CRYPTANALYSE\_POURVU\_QUE\_LE\_MESSAGE\_SOIT\_SUFFISAMMEN  
T\_LONG\_IL\_SUFFIT\_DE\_TENIR\_COMPTÉ\_DES\_STATISTIQUES\_D\_OCC  
URRENCE\_DES\_DIFFERENTES\_LETTRES

Finalemént

LA\_SUBSTITUTION\_MONO\_ALPHABETIQUE\_EST\_TRES\_VULNERABLE\_A  
\_LA\_CRYPTANALYSE\_POURVU\_QUE\_LE\_MESSAGE\_SOIT\_SUFFISAMMEN  
T\_LONG\_IL\_SUFFIT\_DE\_TENIR\_COMPTÉ\_DES\_STATISTIQUES\_D\_OCC  
URRENCE\_DES\_DIFFERENTES\_LETTRES

# Substitution+

Au lieu de faire la substitution mono-alphabétique, on peut rendre le code plus difficile à briser en faisant une substitution de mots. Chaque mot est remplacé par un nombre, d'où la nécessité d'un dictionnaire. On peut utiliser des synonymes.

Cette technique n'est pas vraiment pratique. La construction du dictionnaire est fastidieuse. Il faut se déplacer avec le dictionnaire qui pourrait être intercepté. Il est difficile de changer le code.

# Substitution++

Différentes techniques peuvent être utilisées pour rendre le chiffrement par substitution plus sécuritaire tout en gardant une clef de taille raisonnable.

Premièrement, on peut utiliser des synonymes. Par exemple, la lettre E se retrouve 14% du temps et on pourrait utiliser 14 symboles différents pour représenter E et ainsi de suite pour les autres symboles.

On obtient un code de 100 symboles.

On peut aussi utiliser des blancs (symbole sans signification).

On peut coder certains mots courants par un seul symbole.

etc....

# Marie Stuart (1556)



En 1586, Marie Stuart, reine d'Écosse fut jugée en Angleterre.

Elle était accusée d'avoir comploté pour assassiner la [reine Elizabeth](#).

Le complot eut lieu durant son emprisonnement en Angleterre mais Marie utilisait le chiffrement lors de ses communications avec ses complices.

La Reine était réticente à exécuter Marie car elle était sa cousine. Le déchiffrement des lettres rendrait la preuve accablante et ne laisserait aucune chance à Marie.

# Marie Stuart (1556)



a b c d e f g h i k l m n o p q r s t u x y z  
 O † ‡ # a □ θ ∞ | ð ñ || ø ∇ ∫ M f Δ ε c 7 8 9

Nulles ff. r. . \_ . d .

Dowbleth σ

and for with that if but where as of the from by  
 2 3 4 4 4 3 ρ ρ ρ ρ ρ ρ

so not when there this in wich is what say me my wyrt  
 ρ X † † † ρ x † ρ m n m m d

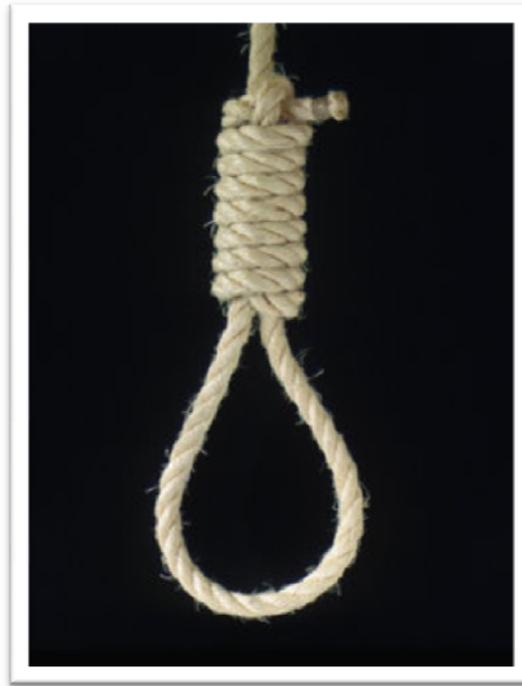
send lre receave bearer I pray you Mte your name myne  
 ρ ρ † T † † † † † † † SS

# Marie Stuart

**Gifford** transmettait secrètement les lettres de Marie mais c'était en fait un agent double et il transmettait aussi les lettres au services de renseignement de la Reine qui réussirent à briser le code utilisé par Marie.

En plus de lire toute sa correspondance et d'apprendre le contenu, ils ont **falsifié un message** demandant explicitement la liste des personnes impliquées.

# Une fin triste pour Marie Stuart



# Le chiffre indéchiffrable

Au 16<sup>ième</sup> siècle, on brisait les codes de façon routinière. La balle était dans le camp des cryptographes. *Vigenère* inventa un code simple et subtile. Il s'agit d'une amélioration du chiffre par décalage. On choisit un mot de code par exemple ALAIN et on l'utilise pour chiffrer.

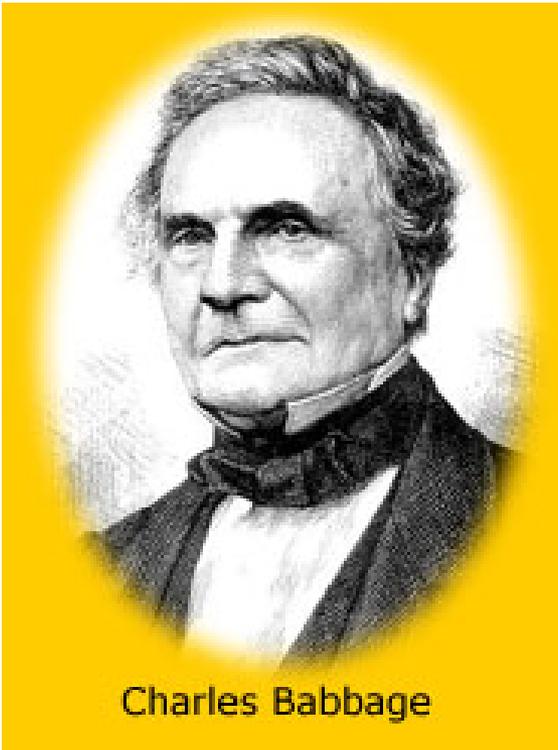
ALAIN=1,12,1,9,14

ALAINALAINALAINALAINALAINALAINALAINALAINALAINA  
LE\_CODE\_DE\_VIGENERE\_EST\_IL\_INDECHIFFRABLE  
MQALBEQAMSAGJPSOQSNNFDUIWMLJWRFOIRTGCBKZF

Clairement, une attaque statistique simple ne fonctionnera pas. Si le mot de code est suffisamment long (une phrase), essayer toutes les clefs est aussi impossible.

Le chiffre de Vigenère est-il indéchiffrable?

# Briser le chiffre indéchiffrable!



Les cryptanalystes furent déjoués pendant près de 3 siècles par le chiffre de Vigenère.

Au 19<sup>ème</sup> siècle, Charles Babbage réussit à le briser.

La technique est relativement simple.

# Exemple

OTDHRSEIETD\_LVISHFIESPVFLHDUOIEWEGXJKLRMQHOEEEFMXHFDVXTDQDO  
WZEGXNWIXNRBDRRBSSED\_TMDQIYLEYJCXPEIIXEEFMXHOTFUOFFEQELHOYS  
HOJTLGDQDOPTQVYJXFDIHOPFCRPJIOVJWFSZYTIEOTDIHRSIDVIEHGXE  
DOHIDICTRKDBXEHBGTUTDZQTDKRXWEOTDRHGWFJTDIRXXEHHVJCPWXHNDQ

1	2	3	4	5
9.5%	19.0%	9%	24.1% H	13.0%
	12.0%	11.7%	17.2% T	10.9%
		15.6%	27.6% D	15.2%
			22.4% E	13.0%
				17.4%
9.5%	15.5%	12.1%	22.8%	13.9%

En considérant que les caractères apparaissant le plus souvent sont soit \_ ou E, on peut essayer différentes possibilités. H=E, T=E, D=\_ et E=\_ donne comme mot de code CODE qui permet de déchiffrer le message.

OTDHRSIEGTD\_LVISHFIESPVFLHDUOIWEGXJKLRMQHOEEEFMXHFDVXTDQDO  
WZEGXNWIXNRBDRRBSSED\_TMDQIYLEYJCXPEIXEEFMXHOTFUOFFEQELHOYS  
HOJTLGDQDOPTQVYJXFDIHOPFCRPJIOVJWFSZYTIEOTDIHRSIDVIEHGEXB  
DOHIDICTRKDBXEHBGTUTDZQTDKRXWEOTDRHGWFJTDIRXXEHHVJCPWXHNDQ

LE CODE DE VIGENERE PARAIT PLUS DIFFICILE  
A BRISER QUE LA SUBSTITUTION MONO  
ALPHABETIQUE IL FUT BRISE PAR BABBAGE UNE  
FOIS LA LONGUEUR DE LA CLEF RETROUVEE LE  
DECODAGE EST UN JEU D ENFANT ENCORE UNE  
FOIS LE MESSAGE DOIT ETRE ASSEZ LONG

# Masque jetable Un code parfait?

Chiffrer un bit d'information avec un bit de clef.



Mensonge

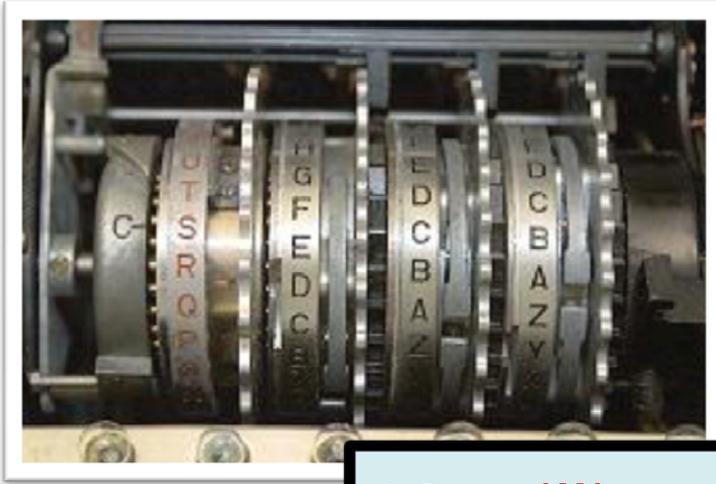


Vérité

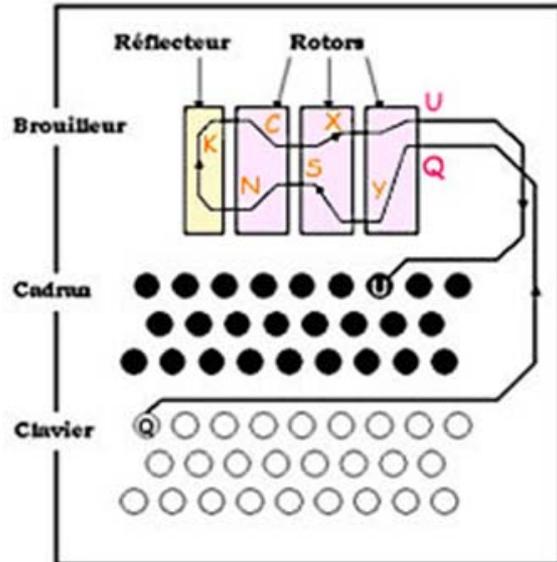
# Sécurité du masque jetable

Claude Shannon,  
*Communication Theory of Secrecy Systems*,  
Bell System Technical Journal,  
vol.28(4), page 656–715, 1949.

# ENIGMA



10 millions de milliards de clés



# ENIGMA

La première version d'ENIGMA était utilisée comme suit.

Agencement des 3 rotors.

123, 132, 213, 231, 312, 321

6 possibilités.

Position des trois rotors, 3 lettres.

$26 \times 26 \times 26 = 17\,576$  possibilités.

Connexions des fiches (6 connexions).

100 391 791 500 possibilités.

Exemple de clef: (231,DFT,AD,BE,CM,FY,UI,LP)

Nombre total de clefs:

$6 * 17\,576 * 100\,391\,791\,500 = 10\,586\,916\,764\,424\,000$

10 million de milliard de possibilités...

# Briser ENIGMA

Sur une période de 10 ans, les Allemands se dotèrent de plus de 30 000 machines ENIGMA.

ENIGMA est un véritable cauchemar pour les cryptanalystes.

Toute attaque statistique est inutile puisque chaque lettre du message est chiffré de façon différente.

Inutile d'essayer de deviner la clef. Il y en a trop.

La plupart des cryptanalystes abandonnèrent rapidement espoir de briser ENIGMA. Il y avait une exception. Les Polonais avaient peur d'une invasion Allemande. Pour eux, briser ENIGMA était vitale.

# Briser ENIGMA

Les services de renseignement polonais ont obtenu par l'intermédiaire d'un informateur une description de la machine, ainsi que son mode d'utilisation.

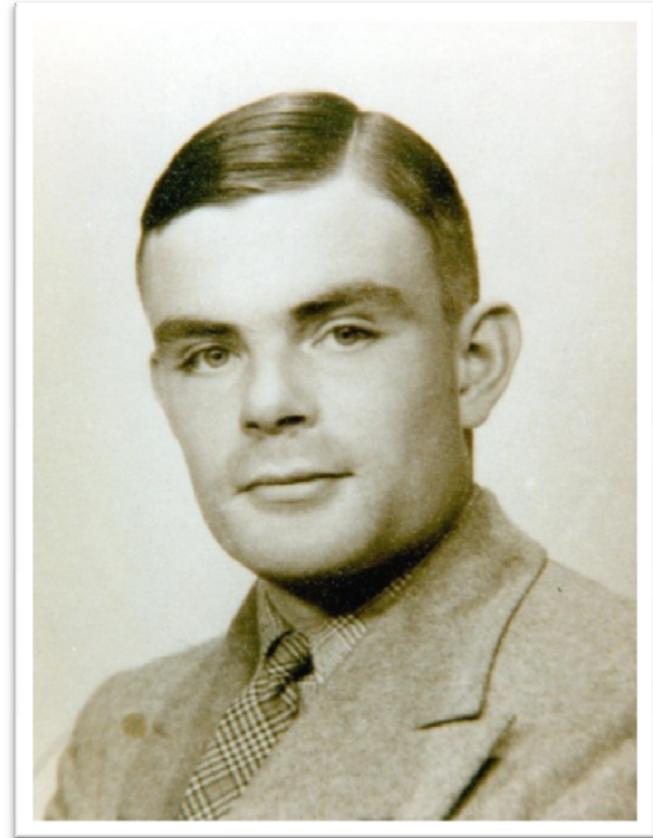
Un livre de code donnait pour chaque jour la clef utilisée. Pour éviter que tous les utilisateurs d'ENIGMA utilisent la même clef, l'opérateur choisissait trois lettres au hasard qu'il chiffrait avec la clef du jour, deux fois. Ensuite la position des rotors était modifiée en fonction de ces trois lettres.

Chaque message était donc chiffré avec une clef différente.

# Briser ENIGMA 1932-1944



Marian Rejewski  
Polonais



Alan Turing  
Britannique

# Briser ENIGMA



Marian Rejewski

Le code ENIGMA fut brisé en décembre 1932 par Marian Rejewski, travaillant pour les services de renseignement polonais. A partir de 1933, les Polonais ont réussi à déchiffrer des milliers de messages allemands.

Les Polonais ont réussi là où les autres services de renseignement ont échoué.

# Briser ENIGMA

La clef du succès de Marian Rejewski fut de se concentrer sur le fait que chaque message commençait par une répétition de 3 lettres.

Par exemple, pour quatre messages interceptés, on pouvait obtenir les données suivantes:

LOKRGM  
MVTXZE  
JKTMPE  
DVYPZX

Chacun de ces chiffres dépend de l'agencement des rotors, du positionnement des fiches et bien sûr, des trois caractères choisis. Examinons la première et la quatrième lettre.

ABCDEFGHIJKLMN OPQRSTUVWXYZ  
P M RX

# Briser ENIGMA

Avec l'interception de plusieurs messages, on peut compléter le tableau.

ABCDEFGHIJKLMN OPQRSTUVWXYZ  
FQHPLWOGBMVRXUYCZITNJEASDK

Ce tableau dépend de la clef du jour. Marian eu une intuition remarquable.

A-F-W-A	3 LIENS
B-Q-Z-K-V-E-L-R-I-B	9 LIENS
C-H-G-O-Y-D-P-C	7 LIENS
J-M-X-S-T-N-U-J	7 LIENS

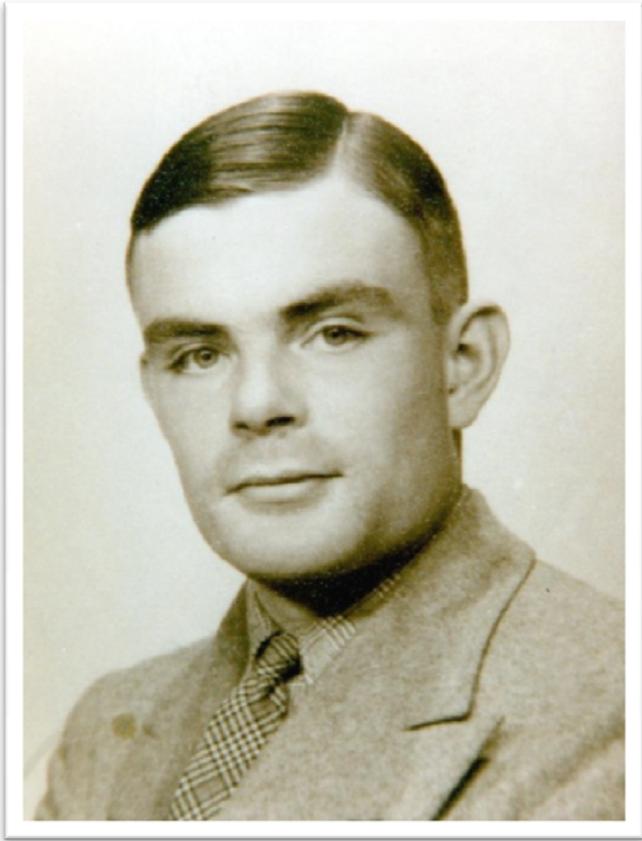
Le même exercice peut être réalisé avec les lettres numéro 2 et 5, ainsi que 3 et 6. Marian remarqua que la longueur des chaînes changeait à chaque jour. Si on change la position des fiches, les lettres des chaînes vont changer mais pas leurs longueurs. La longueur des chaînes ne dépend que de la position des rotors.

# Briser ENIGMA

Il existe  $6 \times 26^3 = 105\,456$  positionnements des rotors. Chacun donne lieu à une liste de chaînes avec des tailles caractéristiques. En une année, Marian réussit à construire une table de toutes les possibilités. Pour identifier la position des rotors, il suffisait d'intercepter quelques messages, calculer la longueur des chaînes, et regarder dans la table.

Il restait maintenant à trouver la position des fiches. Une fois les rotors bien positionnés, si on laisse le tableau des fiches vierge, l'opération de déchiffrement donnera un message illisible mais facile à briser. Les lettres sont simplement permutées suivant la position des fiches. Une attaque statistique trouve facilement les branchements.

# ENIGMA et Turing



Alan Turing  
Britannique

Un peu avant l'invasion allemande, les Polonais ont dévoilé leurs techniques pour briser ENIGMA aux Britanniques. La partie n'était pas complètement gagnée. ENIGMA fut modifié durant la guerre. Des rotors furent ajoutés et à un certain moment, les Allemands ont cessé de répéter les trois lettres de la clef. Il y eut donc de courtes périodes pendant lesquelles les Alliés furent incapables de déchiffrer les messages allemands, mais des techniques de plus en plus sophistiquées et un appareillage électrique de plus en plus imposant leur permirent de déjouer les cryptographes allemands.

# DES

En 1973, le *National Bureau of Standards* des États-Unis lance un appel d'offre pour un système de cryptographie.

En 1975 DES, développé par IBM est adopté.

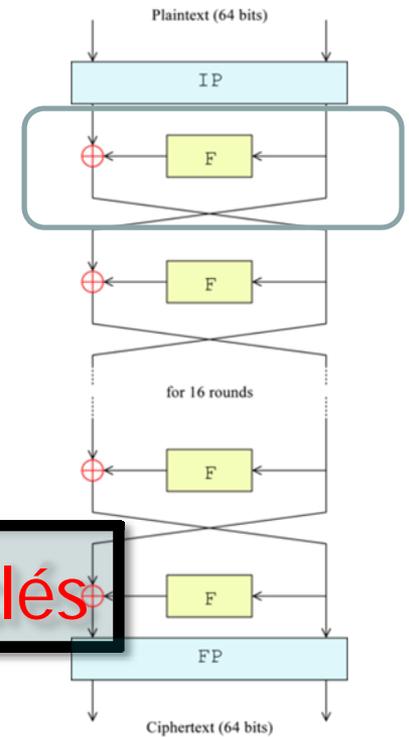
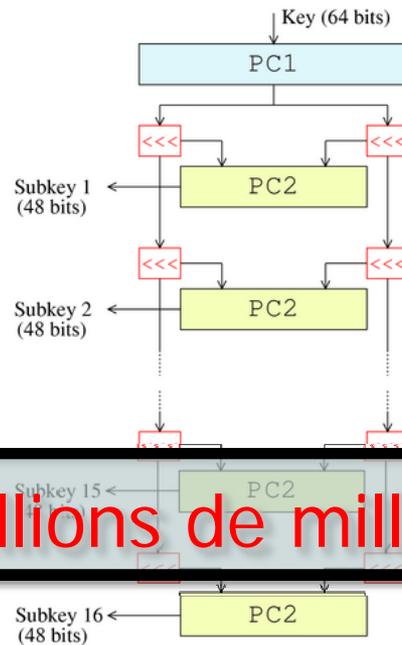
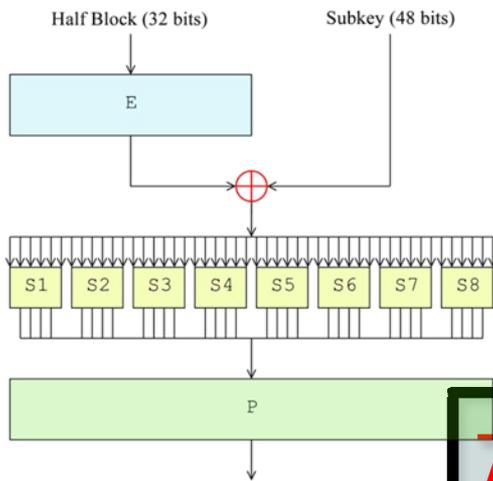
Cryptosystème le plus utilisé dans le monde.

Chiffrement de blocs de 64 bits.

Clef de 56 bits.

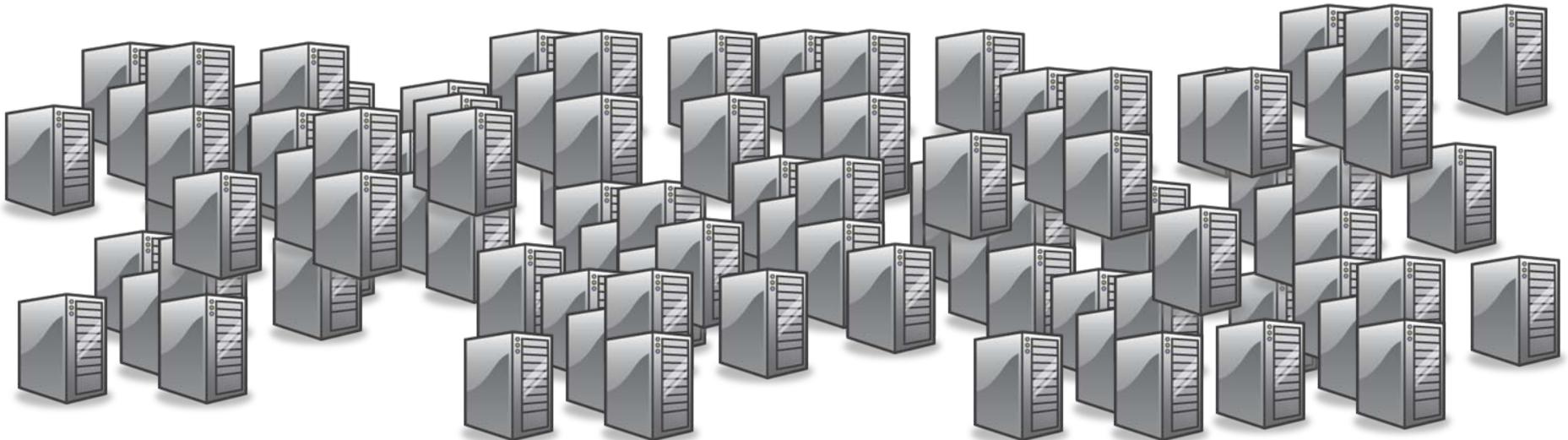
# DES

Data Encryptions Standard  
IBM 1975

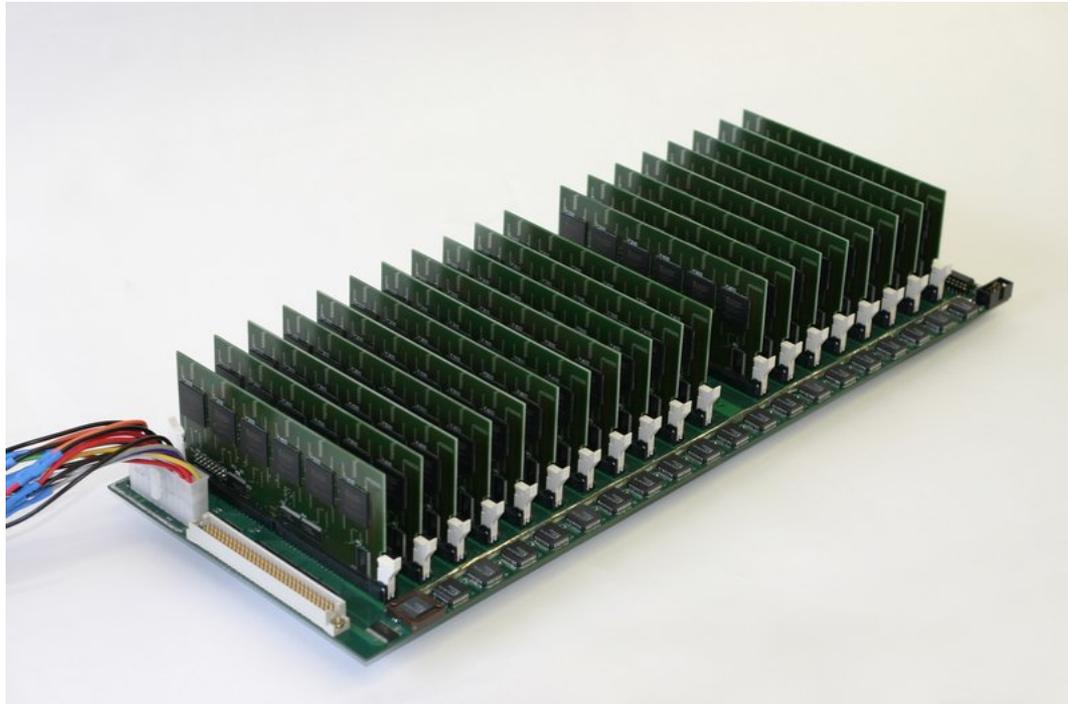


72 millions de milliards de clés

# Briser DES



# COPACOBANA



Brise DES en 6.4 jours (moyenne)  
\$100,000

# Cryptographie symétrique

- AES
- Blowfish
- Triple DES
- Serpent
- Twofish

# Problème de l'échange de clef

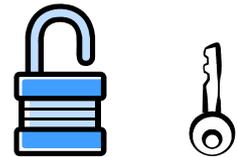
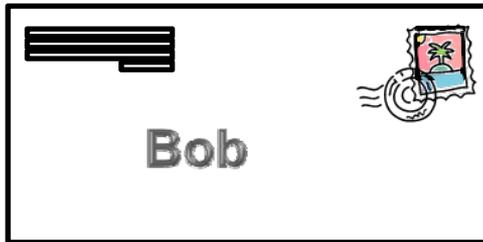
Même avec un cryptosystème très sécuritaire, un problème subsiste. Il faut distribuer les clefs secrètes qui seront utilisées sans qu'elles soient interceptées par des curieux. Ces clefs peuvent être échangées à l'aide d'un courrier diplomatique ou en temps de guerre, elles peuvent être distribuées aux unités avant leur départ.

Qu'arrive-t-il si on manque de clefs?

Pas très pratique sur Internet!

Y a-t-il une solution?

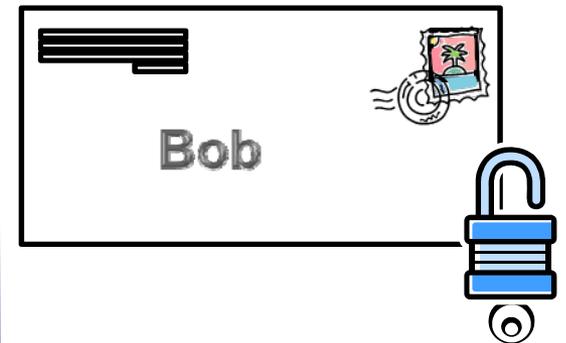
# Cryptographie à clef publique



# Cryptographie à clef publique



# Cryptographie à clef publique



# Arithmétique modulaire

$$x \equiv y \pmod{n} \quad \text{ssi} \quad x = kn + y \quad \text{avec} \quad y < n$$

$$27 = 3 * 7 + 6 \quad \text{alors} \quad 27 \equiv 6 \pmod{7}$$

$$x \pmod{n} + y \pmod{n} \equiv x + y \pmod{n}$$

$$9 + 11 = 20 \equiv 6 \pmod{7} \quad \text{et}$$

$$9 \pmod{7} + 11 \pmod{7} \equiv 2 + 4 \equiv 6 \pmod{7}$$

$$x \pmod{n} * y \pmod{n} \equiv x * y \pmod{n}$$

$$9 * 11 = 99 = 14 * 7 + 1 \equiv 1 \pmod{7} \quad \text{et}$$

$$9 \pmod{7} * 11 \pmod{7} \equiv 2 * 4 \equiv 8 \equiv 1 \pmod{7}$$

# Exponentiation modulaire

Comment calculez  $165789^{23456781} \pmod{456712}$

$$x^8 = \left( (x^2)^2 \right)^2 \quad \text{donc pour calculer } x^{(2^k)} \pmod{n}$$

on calcule  $x \leftarrow x^2 \pmod{n}$   $k$  fois

$$21 = 10101 = 2^4 + 2^2 + 2^0 \quad \text{et}$$

$$5^2 = 8 \pmod{17} \quad 5^4 = 13 \pmod{17}$$

$$5^8 = 16 \pmod{17} \quad 5^{16} = 1 \pmod{17}$$

$$5^{21} \pmod{17} = 5^{16} 5^4 5^1 \pmod{17} = 1 * 13 * 5 = 14 \pmod{17}$$

# PGCD

$PGCD(a, b) \quad a > b$

$(a, b) \rightarrow (b, a \bmod b)$

si  $b = 1$  alors répondre  $a$

$$PGCD(42, 30) = 6$$

$$(42, 30)$$

$$(30, 12)$$

$$(12, 6)$$

$$(6, 1)$$

$$PGCD(105, 45) = 5$$

$$(105, 45)$$

$$(45, 15)$$

$$(15, 1)$$

# Inverse multiplicatif

$a^{-1} \bmod m$  avec  $\text{PGCD}(a, m) = 1$

$(m, a, 1, 0)$

$(a, b, c, d) \rightarrow (b, a \bmod b, d - c(a \text{ div } b) \bmod m, c)$

si  $b = 1$  alors répondre  $c$

$$5^{-1} \equiv 8 \bmod 13$$

$(13, 5, 1, 0)$

$$(5, 3, 0 - 1 * (2) \bmod 13, 1) = (5, 3, 11, 1)$$

$$(3, 2, 1 - 11 * (1) \bmod 13, 11) = (3, 2, 3, 11)$$

$$(2, 1, 11 - 3 * (1) \bmod 13, 3) = (2, 1, 8, 3)$$

$$5 * 8 = 40 \equiv 1 \bmod 13$$

$$7^{-1} \equiv 19 \bmod 22$$

$(22, 7, 1, 0)$

$$(7, 1, 0 - 1 * (3) \bmod 22, 1) = (7, 1, 19, 1)$$

$$7 * 19 = 133 = 6 * 22 + 1 \equiv 1 \bmod 22$$

Avec un ordinateur, on calcule le PGCD et l'inverse multiplicatif de très grands nombres efficacement.

# RSA

Inventé par Rivest, Shamir et Adleman en 1978.

On choisit  $p$  et  $q$  de très grands nombres premiers. ( $n=pq$ )

On choisit  $e$  ( $1 < e < n$ ,  $\text{PGCD}(e, (p-1)(q-1)) = 1$ ).

On calcule  $d$ , l'inverse de  $e$  modulo  $m=(p-1)(q-1)$

Clef Publique:  $(n, e)$

Clef Privée:  $(d)$

$$E(m) = m^e \pmod{n}$$

$$D(c) = c^d \pmod{n}$$

On croit qu'il est difficile de retrouver la clef privée a partir de la clef publique.

# Exemple

$$p = 5, q = 7, n = 35, (p - 1)(q - 1) = 24$$

$$e = 5, PGCD(5, 24) = 1, d = e^{-1} = 5, 5 * 5 = 25 \equiv 1(\text{mod } 24)$$

$$E(3) \equiv 3^5 \equiv 243 \equiv 33(\text{mod } 35)$$

$$D(33) \equiv 33^5 \equiv 39135393 \equiv 3(\text{mod } 35)$$

$$E(5) \equiv 5^5 \equiv 10(\text{mod } 35)$$

$$D(10) \equiv 10^5 \equiv 5(\text{mod } 35)$$

# Briser RSA

La seule technique connue pour briser RSA consiste à calculer l'exposant de déchiffrement.

$d = e^{-1} \text{ mod } (p-1)(q-1)$  où  $pq = n$ .

Pour ce faire, il faut **factoriser**  $n$ .

Par contre, comme l'algorithme de chiffrement est connu publiquement, si on devine le message, on peut vérifier facilement que c'est le bon.

# Factorisation

Pour factoriser un nombre de  $n$  bits.

Algorithme naïf:  $O(2^{n/2})$

Crible algébrique:  $O(e^{cn^{1/3}(\log n)^{2/3}})$

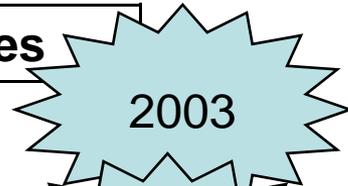
# Concours RSA-129

```
1143816257578888676692357799761466120102182967212423625625618429
35706935245733897830597123563958705058989075147599290026879543541
=
3490529510847650949147849619903898133417764638493387843990820577
*
32769132993266709549961988190834461413177642967992942539798288533
```

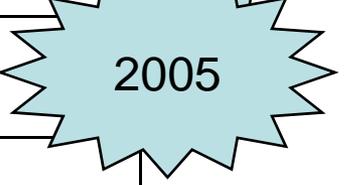
- En 1994, il a fallu 8 mois à 600 ordinateurs pour factoriser ce nombre!
- La vérification se fait en moins d'un millième de seconde.
- **THE MAGIC WORDS ARE SQUEAMISH OSSIFRAGE**

# Concours RSA (1991-2007)

<b>Concours</b>	<b>Prix</b>	<b>Décimales</b>
RSA-576	\$10,000	174
RSA-640	\$20,000	193
RSA-704	\$30,000	212
RSA-768	\$50,000	232
RSA-896	\$75,000	270
RSA-1024	\$100,000	309
RSA-1536	\$150,000	463
RSA-2048	\$200,000	617



2003



2005

# Signature utilisant RSA

Le problème de la signature est l'inverse du problème du chiffrement à clef publique. Seul le signataire doit avoir la capacité de signer mais tous peuvent vérifier la signature.

Avec RSA, on a que

$D(E(m))=m$  mais aussi  $E(D(M))=m$ .

Pour signer un document, on applique l'algorithme de déchiffrement au message et tout ceux qui connaissent l'algorithme publique de chiffrement peuvent vérifier la signature.

Pour signer un document, il faut connaître la clef privée!

# Infrastructure à clef publique

Lorsqu'on utilise une clef publique, il faut s'assurer que c'est bien la clef de la personne avec qui on désire communiquer secrètement, ou de qui on désire vérifier une signature.

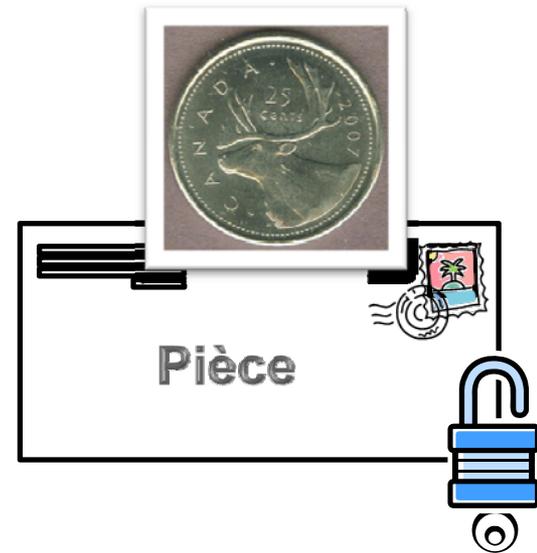
Si Alice possède la clef publique de Bob et Bob la clef publique de Charlie alors Bob peut signer la clef de Charlie et la transmettre à Alice qui peut vérifier sa signature.

C'est la transitivité de la confiance.

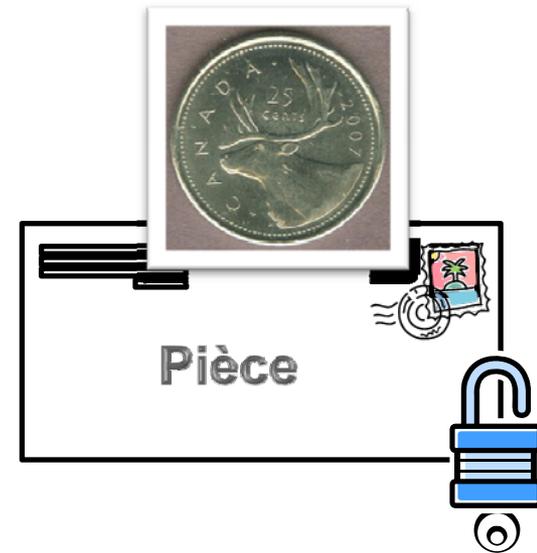
# Mise en gage (Pile ou face)



# Mise en gage (Pile ou face)



# Mise en gage (Pile ou face)



# Mise en gage

Supposons qu'Alice connaisse le gagnant de la finale de Hockey. Alice ne veut pas dire à Bob le nom de l'équipe gagnante mais elle aimerait qu'après coup, Bob reconnaisse qu'elle avait raison.

Il suffit pour Alice d'écrire le nom du gagnant sur un bout de papier, de le mettre dans un coffre fort et de le donner à Bob. Comme Bob ne connaît pas la combinaison, il n'apprendra pas le gagnant. Après la partie, Alice lui donne le code du coffre. Il l'ouvre et vérifie qu'Alice avait raison.

Existe-t-il une solution informatique à ce problème?

Peut-on utiliser le chiffrement??

# Mise en gage

Un cryptosystème à clef privé ne fera pas l'affaire car Alice peut, à l'ouverture, choisir la clef en fonction du message qu'elle désire révéler.

Avec RSA, il n'existe qu'un seul façon de déchiffrer étant donné une clef publique donnée.

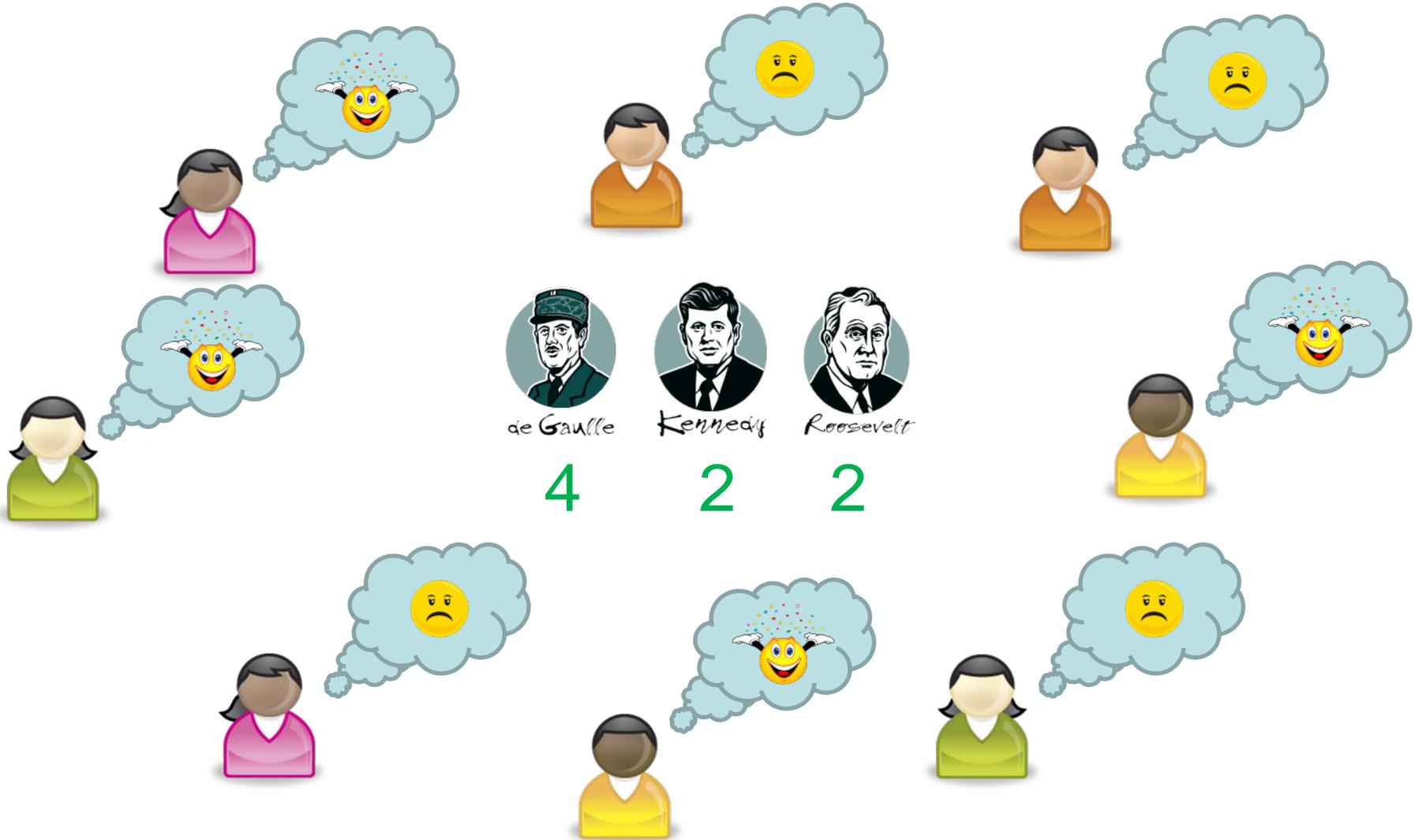
Pour se mettre en gage, Alice rend publique une clef et chiffre le message.

Pour ouvrir la mise en gage, elle donne la clef privée à Bob qui vérifie le tout.

# Vote



# Vote



# Calcul multi party

Soit  $F(x_1, \dots, x_n)$ .

Obtenir la même chose que:

- Chaque participant donne  $x_i$  au *juge*
- Le *juge* fait le calcul  $F(x_1, \dots, x_n)$
- Le *juge* annonce le résultat

Applications:

- «The matchmaking problem»
- Vote
- Message publique anonyme
- Statistique médicale (ou autre sujet privé ou tabou)
- Enchère électronique
- Etc...

# Calcul multi party

Broadcast: moins de  $N/2$  malhonnête

Pas de broadcast: moins de  $N/3$  malhonnête.

Avec OT: pas d'autre hypothèse

# La cryptographie à l'U de M

Quatre professeurs du DIRO travaille sur différents aspects de la cryptographie classique et quantique.

Michel Boyer

Gilles Brassard

Louis Salvail

Alain Tapp

Le cours de cryptographie et d'informatique quantique se donnent au niveau de la maîtrise. Quelques cours de mathématiques et d'informatique théorique sont préalables.