Informatique Quantique
IFT6155
Cryptographie

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 cour 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'armé perse en déroute.

Stéganographie

Hérodote rapporte aussi l'histoire d'Histaïaeus qui, pour transmettre un message, rasa la tête de son messager et inscrivit 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.

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 5ième siècle mais qui est basé sur des écrits datant du 4ième 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 9ième siècle.

Exemple

BQPSNRSJXJNJXLDPCLDLPQBE_QRKJXHNKPKSJPJIKSPUN
BDKIQRBKPQPBQPZITEJQDQBTSKPELNIUNPHNKPBKPCKSS
QWKPSLXJPSNVVXSQCCKDJPBLDWPXBPSNVVXJPGKPJKDXI
PZLCEJKPGKSPSJQJXSJXHNKSPGPLZZNIIKDZKPGKSPGXV
VKIKDJKSPBKJJIKS

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_SNRSJXJNJXLD_CLDL_QBE_QREJXHNE_ESJ_JIES_UN
BDEIQRBE_Q_BQ_ZITEJQDQBTSE_ELNIUN_HNE_BE_CESS
QWE_SLXJ_SNVVXSQCCEDJ_BLDW_XB_SNVVXJ_GE_JEDXI
_ZLCEJE_GES_SJQJXSJXHNES_G_LZZNIIEDZE_GES_GXV
VEIEDJES_BEJJIES

Remplaçons **Q** par A et **B** par L

LA_SNRSJXJNJXLD_CLDL_ALE_AREJXHNE_ESJ_JIES_UN
LDEIARLE_A_LA_ZITEJADALTSE_ELNIUN_HNE_LE_CESS
AWE_SLXJ_SNVVXSACCEDJ_LLDW_XL_SNVVXJ_GE_JEDXI
_ZLCEJE_GES_SJAJXSJXHNES_G_LZZNIIEDZE_GES_GXV
VEIEDJES_LEJJIES

Remplaçons **S** par S et **G** par D

LA_S**NR**S**JXJNJXLD**_**CLDL**_AL**E**_A**R**E**JXHN**E_ES**J**_**JI**ES_**UN**
L**D**E**I**A**R**LE_A_LA_**ZITEJ**A**D**AL**T**SE_**ELNIUN**_**HN**E_LE_**C**ESS
A**W**E_S**LXJ**_S**NVVX**SA**CC**E**DJ**_L**LDW**_**X**L_S**NVVXJ**_DE_**J**E**DXI**
_**ZLCEJ**E_DES_S**J**A**JX**S**JXHN**ES_D_**LZZNII**E**DZ**E_DES_D**XV**
VE**I**E**DJ**ES_LE**JJI**ES

Remplaçons **J** par T et **I** par R

LA_S**NR**ST**X**T**N**T**XLD**_**CLDL**_AL**E**_A**R**ET**XHN**E_EST_TRES_**UN**
L**D**ERA**R**LE_A_LA_**Z**R**TE**TA**D**AL**T**SE_**ELN**R**UN**_**HN**E_LE_**C**ESS
A**W**E_S**LX**T_S**NVVX**SA**CC**E**D**T_L**LDW**_**X**L_S**NVVX**T_DE_TE**DX**R
_**ZLCE**TE_DES_STAT**X**ST**XHN**ES_D_**LZZN**RRE**DZ**E_DES_D**XV**
VERE**D**TES_LETTRES

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

LA_SU**R**STITUTI**LD**_**CLDL**_AL**E**_A**R**ETIQUE_EST_TRES_**U**U
L**D**ERA**R**LE_A_LA_**Z**R**TE**TA**D**AL**T**SE_**EL**UR**U**U_QUE_LE_**C**ESS
A**W**E_S**L**IT_SU**VV**ISA**CC**E**D**T_L**LDW**_IL_SU**VV**IT_DE_TE**D**IR
_**ZLCE**TE_DES_STATISTIQUES_D_**LZZ**URRE**DZ**E_DES_DI**V**
VERE**D**TES_LETTRES

Remplaçons **V** par F et **D** par N

LA_SU**R****S**TITUTI**L**N_**CL**N**L**_AL**E**_A**R**ETIQUE_EST_TRES_**U**U
LNERA**R**LE_A_LA_**Z**R**TE**TANAL**T**SE_**EL**UR**U**U_QUE_LE_**C**ESS
A**W**E_S**L**IT_SUFFISA**CC**ENT_L**L**N**W**_IL_SUFFIT_DE_TENIR
_**ZLCE**TE_DES_STATISTIQUES_D_**LZZ**URREN**Z**E_DES_DIF
FERENTES_LETTRES

Remplaçons **R** par B et **L** par O

LA_SUBSTITUTION_**C**ONO_AL**E**_A**R**ETIQUE_EST_TRES_**U**U
LNERABLE_A_LA_**Z**R**TE**TANAL**T**SE_**E**OUR**U**U_QUE_LE_**C**ESS
A**W**E_SOIT_SUFFISA**CC**ENT_LON**W**_IL_SUFFIT_DE_TENIR
_**Z**O**CE**TE_DES_STATISTIQUES_D_O**ZZ**URREN**Z**E_DES_DIF
FERENTES_LETTRES

Finalement

LA_SUBSTITUTION_MONO_ALPHABETIQUE_EST_TRES_VU
LNERABLE_A_LA_CRYPTANALYSE_POURVU_QUE_LE_MESS
AGE_SOIT_SUFFISAMMENT_LONG_IL_SUFFIT_DE_TENIR
_COMPTE_DES_STATISTIQUES_D_OCCURRENCE_DES_DIF
FERENTES_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

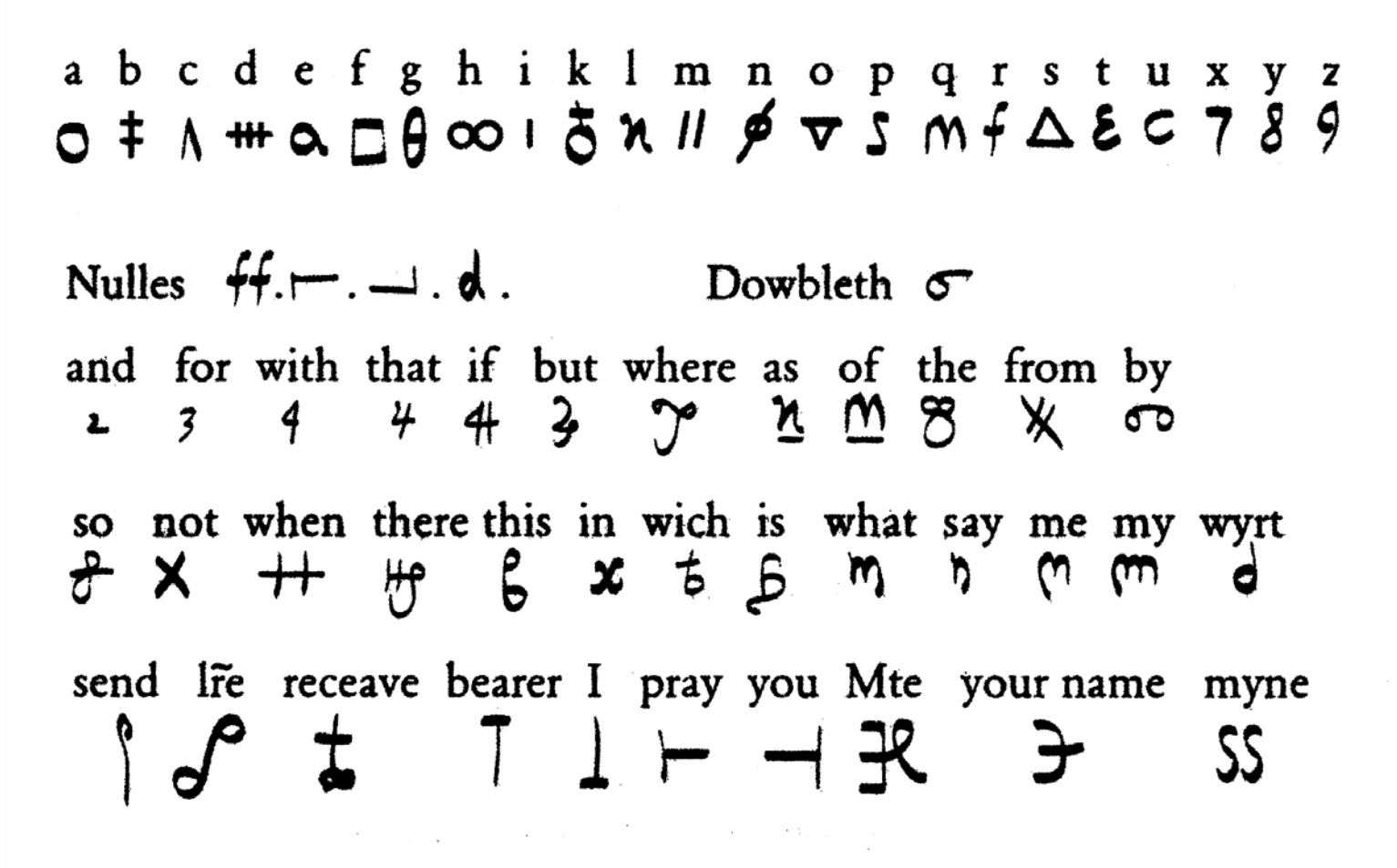
En 1586, Marie Stuart, reine d'Écosse fut jugée en Angleterre.

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

Code de Marie Stuart



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 a 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.

Ils furent tous exécutés, incluant Marie. La preuve était accablante.

Le chiffre indéchiffrable

Au 16ième 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.

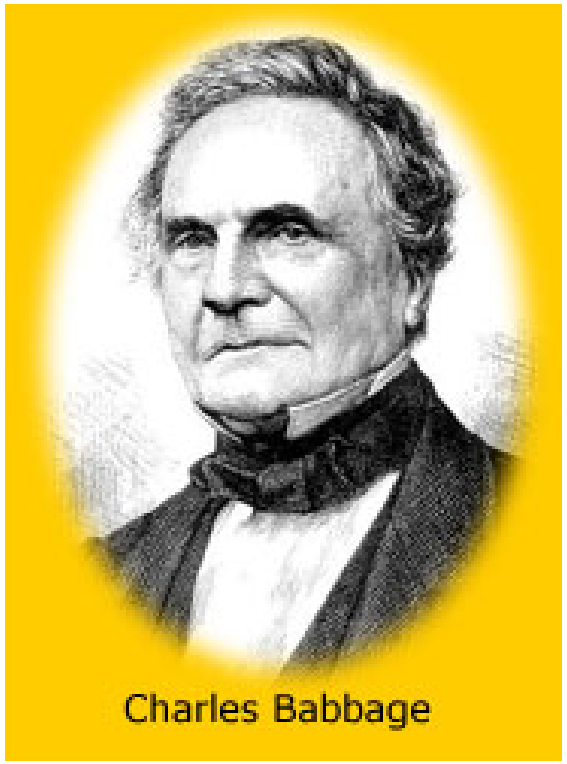
ALAIN=1,12,1,9,14

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!


Charles Babbage

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

Au 19ième siècle, Charles Babbage réussit à le briser.

La technique est relativement simple.

Exemple

OTDHRSIEGTD_LVISHFIESPVFLHDUOIWEGXJKLRMQHOEEEFMX
HFDVXTDQDOWZEGXNWIXNRBDRRBSED_TMDQIYLEYJCXPEIIXE
EFMXHOTFUOFFEQELHOYSHOJTLGDQDOPTQVYJXFDIHOPFCRPJ
IOVJWFSZYTIEOTDIHRSIDVIEHGXEXBDOHIDICTRKDBXEHBGT
UTDZQTDKRXWEOTDRHGWFJTDIRXXEHHVJCPWXHNDQ

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_LVISHFIESPVFLHDUOIWEGXJKLRMQHOEEEFMX
HFDVXTDQDOWZEGXNWIXNRBDRRBSED_TMDQIYLEYJCXPEIIXE
EFMXHOTFUOFFEQELHOYSHOJTLGDQDOPTQVYJXFDIHOPFCRPJ
IOVJWFSZYTIEOTDIHRSIDVIEHGXEXBDOHIDICTRKDBXEHBGT
UTDZQTDKRXWEOTDRHGWFJTDIRXXEHHVJCPWXHNDQ

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

Peut-on avoir un cryptosystème ayant une confidentialité absolue et qui soit impossible à briser?

Qu'arrive-t-il si on utilise le chiffre de Vigenère avec une clef aussi longue que le message?

Avec une clef aléatoire, on obtient le masque jetable.

Pour être inconditionnellement sécuritaire, la clef doit être choisie aléatoirement et être utilisée une seule fois.

Sécurité du masque jetable

Si la clef est: 12,7,24,3,26,11,5,21,0,25

ALAIN_TAPP devient MSYLMKYVPN

Pour toute interprétation du message, il existe une clef la justifiant.

Avec la clef: 11,4,11,2,25,22,20,22,16,14

BONJOUR___ devient **MSYLMKYVPN**

C'est Shannon en 1949 qui a démontré formellement que le masque jetable est inconditionnellement sécuritaire. L'inconvénient du masque jetable est la taille nécessaire de la clef.

Cryptosystème a clef courte

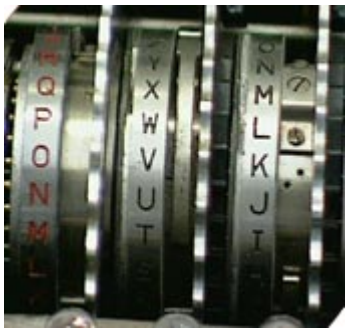
Principe de Kerckhoff
(La cryptographie militaire 1883):

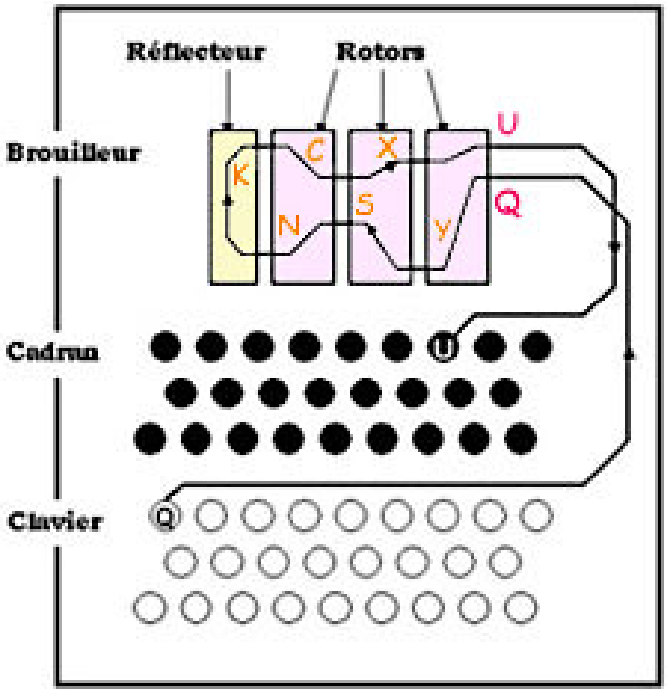
La sécurité d'un système de cryptographie ne doit pas dépendre de la préservation du secret de l'algorithme. La sécurité ne repose que sur le secret de la clef.

Le masque jetable n'est pas pratique.

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

Enigma


QPONML
YXWVUT
ZMLKJI


Réflecteur
Rotors
Brouilleur
Cadran
Cuvier
K
C
X
U
N
S
Y
Q
Q

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.
26x26x26=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

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 a déchiffrer des milliers de messages allemands.

Les Polonais on réussi là ou 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.

ABCDEFGHIJKLMNOPQRSTUVWXYZ
P M RX

Briser ENIGMA

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

ABCDEFGHIJKLMNOPQRSTUVWXYZ
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 x 17 576= 105 456 positionnements des rotors. Chacun donne lieu a une liste de chaînes avec des tailles caractéristiques. En une année, Marian réussit a 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

Un peu avant l'invasion allemande, les Polonais on 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 (72 057 594 037 927 936 clefs).

DES

X est le texte clair de 64 bits.

$(L_0, R_0)=IP(X)$
Pour i=1 à 16
$(L_i, R_i)=(R_{i-1}, L_{i-1}+F(R_{i-1},K_i))$
$Y=IP^{-1}(R_{16},L_{16})$

Y est le texte chiffré de 64 bits.

Chaque k_i est une chaîne de 48 bits provenant de K.

Pour déchiffrer, on utilise le même algorithme avec les clefs K_i utilisées dans l'ordre inverse.

DES

Seulement 56 bits de la clef de 64 bits sont utilisées.
Les 8 autres sont des bits de vérification.

K_1

10	51	34	60	49	17	33	57	2	9	19	42
3	35	26	25	44	58	59	1	36	27	18	41
22	28	39	54	37	4	47	30	5	53	23	29
61	21	38	63	15	20	45	14	13	62	55	31

K_2,...,K_{16} ont chacun leurs tableau spécifique.

DES

IP

58	50	42	34	26	18	10	2
60	52	44	36	28	20	12	4
62	54	46	38	30	22	14	6
64	56	48	40	32	24	16	8
57	49	41	33	25	17	9	1
59	51	43	35	27	19	11	3
61	53	45	37	29	21	13	5
63	55	47	39	31	23	15	7

IP^{-1}

40	8	48	16	56	24	64	32
39	7	47	15	55	23	63	31
38	6	46	14	54	22	62	30
37	5	45	13	53	21	61	29
36	4	44	12	52	20	60	28
35	3	43	11	51	19	59	27
34	2	42	10	50	18	58	26
33	1	41	9	49	17	57	25

DES

$R_i = F(R_{i-1}, K_i)$

R_{i-1}: 32 bits
K_i: 48 bits
R_i: 32 bits
E: 32 bits dans 48 bits
S_i: 6 bits dans 4 bits

$B_1B_2B_3B_4B_5B_6B_7B_8 = E(R_{i-1}) + K_i$

$R_i = P(S_1(B_1)S_2(B_2)...S_8(B_8))$

DES

P

16	7	20	21
29	12	28	17
1	15	23	26
5	18	31	10
2	8	24	14
32	27	3	9
19	13	30	6
22	11	4	25

E

32	1	2	3	4	5
4	5	6	7	8	9
8	9	10	11	12	13
12	13	14	15	16	17
16	17	18	19	20	21
20	21	22	23	24	25
24	25	26	27	28	29
28	29	30	31	32	1

DES

$B_j = b_1 b_2 b_3 b_4 b_5 b_6$ $l_i = b_1 b_6$ $c_i = b_2 b_3 b_4 b_5$

S_1

14	4	13	1	2	15	11	8	3	10	6	12	5	9	0	7
0	15	7	4	14	2	13	1	10	6	12	11	9	5	3	8
4	1	14	8	13	6	2	11	15	12	9	7	3	10	5	0
15	12	8	2	4	9	1	7	5	11	3	14	10	O	6	13

$S_2,\ldots,S_8$ ont leurs tableaux respectifs

Briser DES

De nos jours, une machine comportant 1024 processeurs de 1 GHz, spécialisée pour le problème peut explorer toutes les clefs en moins d'une journée.

DES n'est plus considéré sécuritaire mais est toujours utilisé. Certains utilisent triple DES, qui paraît plus sûr.

Plusieurs autres cryptosystèmes à clef privée sont aussi utilisés.

BLOWFISH IDEA SEAL RC4

Problème de l’échange de clef

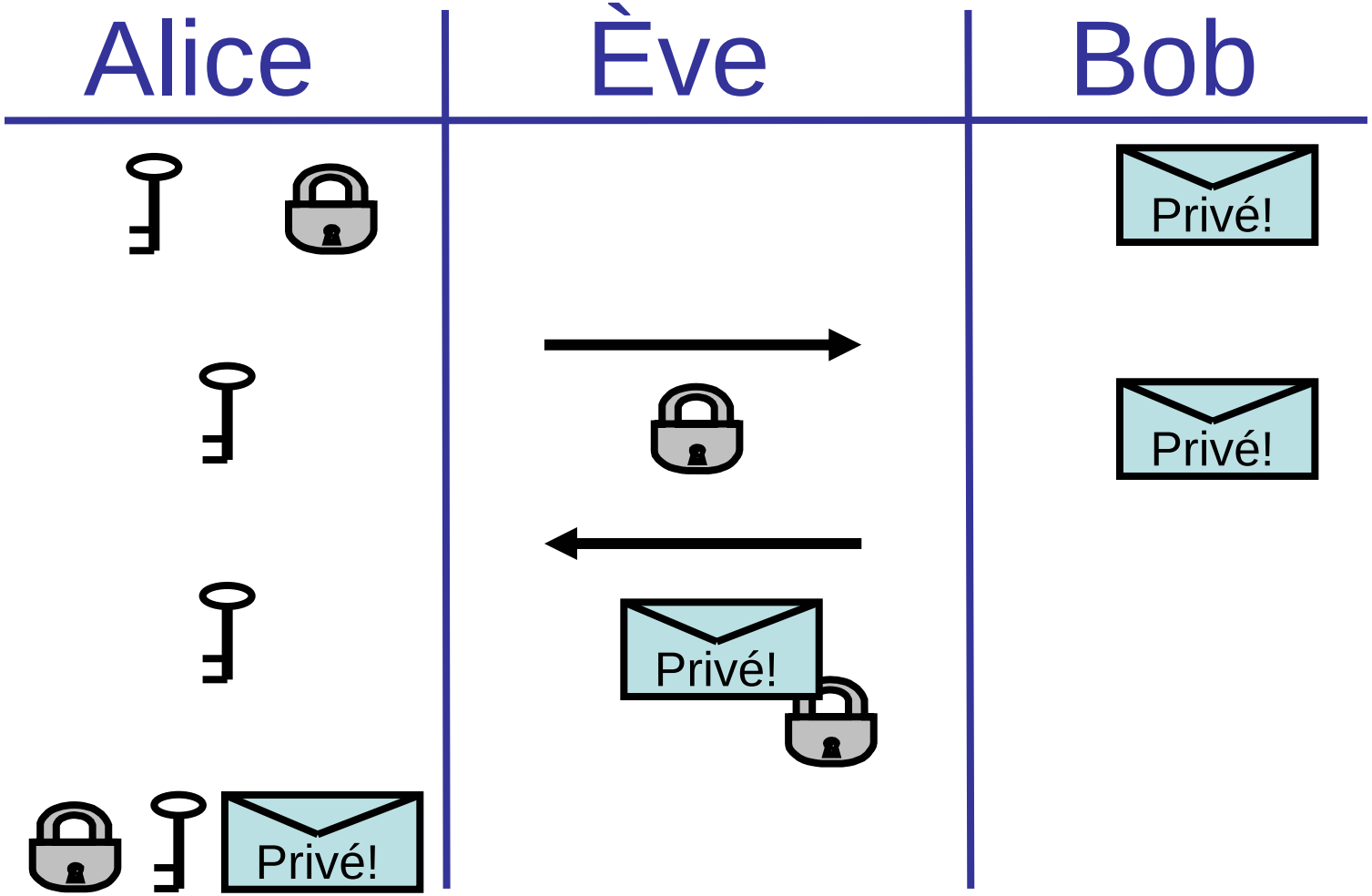
Même avec un cryptosystème très sécuritaire, un problème subsiste. Il faut distribuer les clefs secrètes qui seront utilisées sans qu’elles soient interceptées par des curieux. Ces clefs peuvent être échangées à l’aide d’un courrier diplomatique ou en temps de guerre, elles peuvent être distribuées aux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



Arithmétique modulaire

$x \equiv y (\mathrm{mod}\, n)$ ssi $x = kn + y$ avec $y < n$

$27 = 3*7 + 6$ alors $27 \equiv 6 (\mathrm{mod}\, 7)$

$x (\mathrm{mod}\, n) + y (\mathrm{mod}\, n) \equiv x + y (\mathrm{mod}\, n)$

$9 + 11 = 20 \equiv 6 (\mathrm{mod}\, 7)$ et

$9 (\mathrm{mod}\, 7) + 11 (\mathrm{mod}\, 7) \equiv 2 + 4 \equiv 6 (\mathrm{mod}\, 7)$

$x (\mathrm{mod}\, n) * y (\mathrm{mod}\, n) \equiv x * y (\mathrm{mod}\, n)$

$9*11 = 99 = 14*7 + 1 \equiv 1 (\mathrm{mod}\, 7)$ et

$9 (\mathrm{mod}\, 7) + 11 (\mathrm{mod}\, 7) \equiv 2*4 \equiv 8 \equiv 1 (\mathrm{mod}\, 7)$

Exponentiation modulaire

Comment calculez $165789^{23456781} (\mathrm{mod}\, 456712)$

$x^8 = \left(\left(x^2\right)^2\right)^2$ donc pour calculer $x^{(2^k)} (\mathrm{mod}\ n)$

on calcule $x \leftarrow x^2 (\mathrm{mod}\, n)$ k fois

$21 = 10101 = 2^4 + 2^2 + 2^0$ et

$5^2 = 8 (\mathrm{mod}\ 17)$ $5^4 = 13 (\mathrm{mod}\ 17)$

$5^8 = 16 (\mathrm{mod}\ 17)$ $5^{16} = 1 (\mathrm{mod}\ 17)$

$5^{21} (\mathrm{mod} 17) = 5^{16} 5^4 5^1 (\mathrm{mod} 17) = 1 * 13 * 5 = 14 (\mathrm{mod} 17)$

PGCD

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

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

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 $PGCD(a,m) = 1$

$(m, a, 1, 0)$

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

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, 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

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

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

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

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

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

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

Briser RSA

La seule technique connue pour briser RSA consiste à calculer l'exposant de déchiffrement.
$d=e^{-1} mod\ (p-1)(q-1)$ 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
3570693524573389783059712356395870505898907514759929002687954354 1
=
3490529510847650949147849619903898133417764638493387843990820577
*
3276913299326670954996198819083446141317764296799294253979828853 3
```

- 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	Prix ($US)	Décimales
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

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.