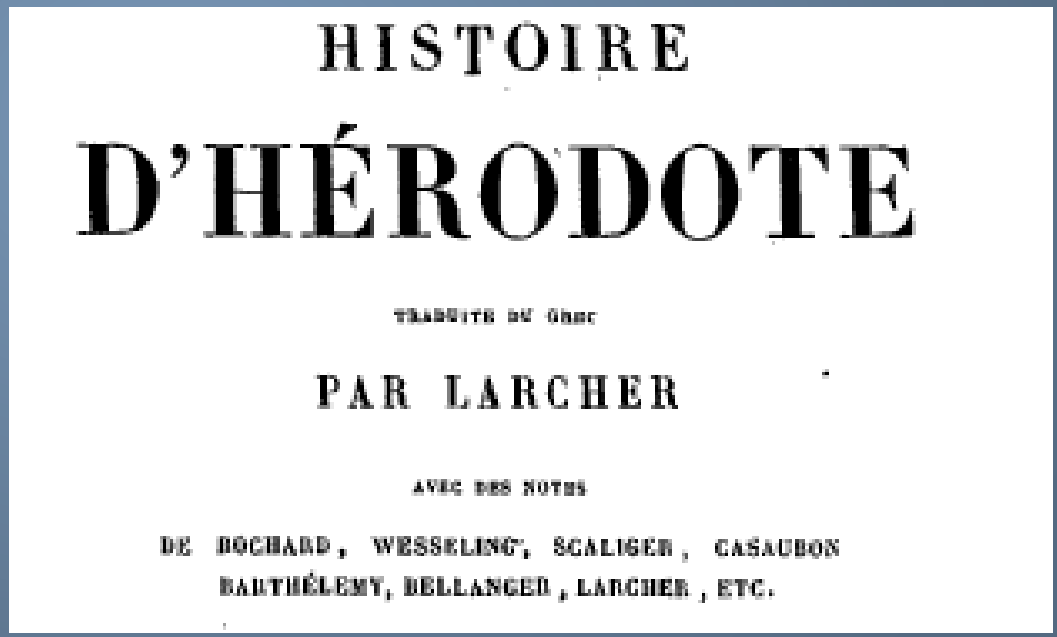
Algorithmes et protocoles de chiffrement

Ayitic
Port-au-Prince, Haïti.
11 - 16 Août 2014

Lucien Loiseau

Hérodote, *Histoire* - V^e siècle av. J-C

"Histiée est le tyran de la ville de Milet sous la suzeraineté de l'empire du roi perse Darius Ier. Il participe à l'expédition de ce dernier contre les et reçoit en récompense des riches domaines situés en Thrace. Il est retenu auprès de Darius, à Suse. Ne se plaisant pas à Suse, il organise la révolte de l'Ionie vers **499 av. J-C**. sous la direction d'Aristagoras. Pour lui donner les ordres de la révolte, Histiée utilise la **stéganographie** : il sélectionne son plus fidèle esclave, lui fait raser la tête et tatouer un ordre de révolte sur le crâne ; Dès que les cheveux eurent repoussé, il l'envoie à Aristagoras qui lui rase de nouveau la tête afin de lire le message."


HISTOIRE

D'HÉRODOTE

TRADUITE DU GREC

PAR LARCHER

AVEC DES NOTES

DE BOCHART, WESSELING, SCALIGER, CASAUBON

BARTHÉLEMY, BELLANGER, LARCHER, ETC.

(on n'avait pas la même notion de l'urgence à l'époque !)

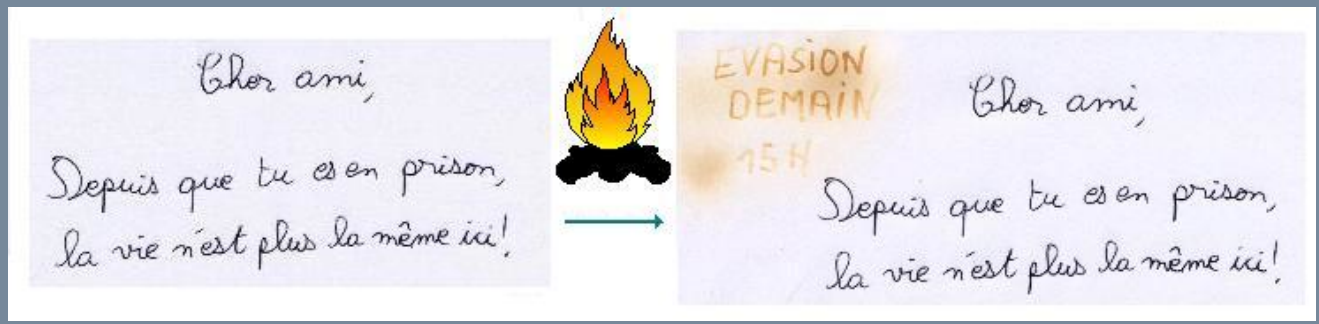
La stéganographie

Origine du mot

- *steganos* voulant dire couvert
- *graphein* voulant dire écriture

pendant 2000 ans après Hérodote, des formes diverses ont été utilisées dans le monde entier !

- Chine ancienne : message sur une fine soie, glissé dans une minuscule boule recouverte de cire
- I_{er} siècle : encre invisible avec du lait de l'euphorbe *tithymalus* (une plante)
  - procédé repris avec les encres sympathiques (invisibles)



- XVI^e siècle : cacher un message dans un œuf dur

Message envoyé par un espion allemand, 1947

"Apparently neutral's protest is thoroughly discounted and ignored. Ismam hard hit. Blockade issue affects pretext for embargo on by-products, ejecting suets and vegetable oils."

"Apparemment la protestation des pays neutres est totalement ignorée. Isman frappe fort. L'issue du blocus donne des prétextes pour un embargo sur certains produits, mis à part graisses animales et huiles végétales."

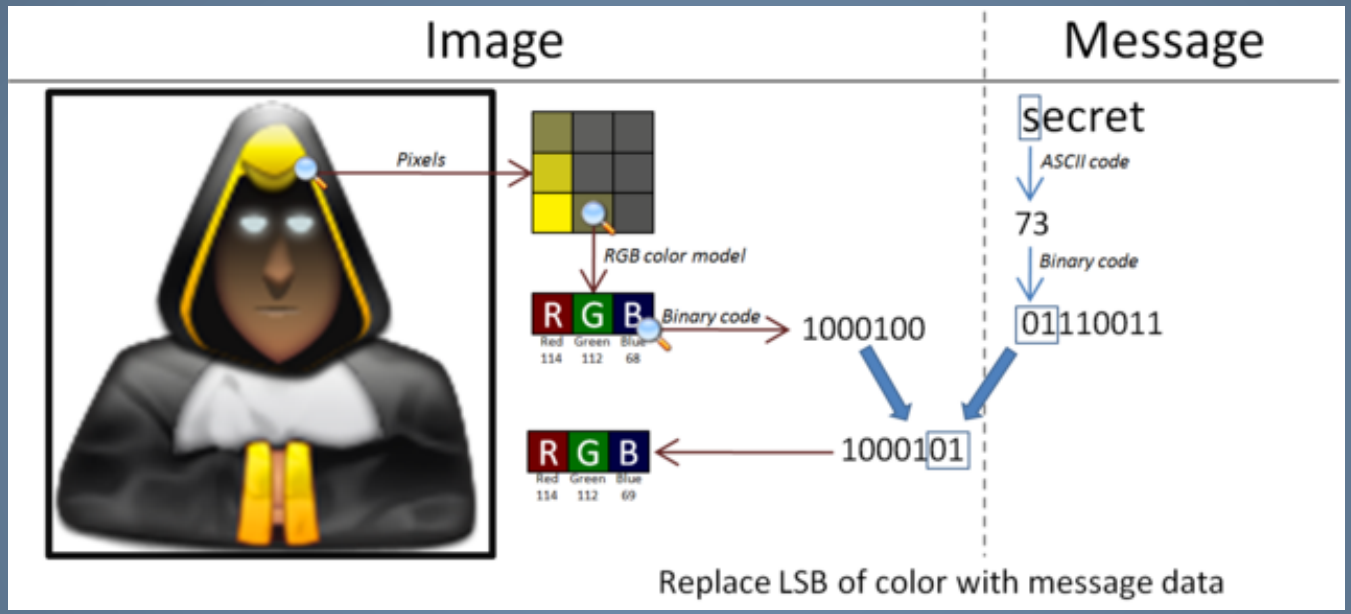
Message envoyé par un espion allemand, 1947

"APparently nEutral's pRotest iS tHoroughly dIscounted aNd iGnored. ISmam hArd hIt. BLockade iSsue aFfects pRetext fOr eMbargo oN bY-products, eJecting sUets aNd vEgetable oIls."

Pershing sails from NY June 1(le Pershing part de New-York le 1er juin)

La stéganographie numérique

- cacher un message numérique dans un fichier



- pratique pour "tatouer" une œuvre sous copyright !

Les faiblesses de la stéganographie

L'interception du message suffit à supprimer toute sécurité !

- si le messager est fouillé, le message est trouvé
- le message découvert, le contenu est révélé

Parallèlement à la *stéganographie* s'est développé la *cryptographie* dont le but n'est pas de cacher le message, mais de le brouiller (i.e. chiffrer)

- *transposition* : redistribution des lettres du message
- *substitution* : remplacer des lettres par d'autres lettres

Exemple de transposition : En dents de scie

TON SECRET EST TON PRISONNIER; S'IL FUIT TU DEVIENDRAS SON PRISONNIER

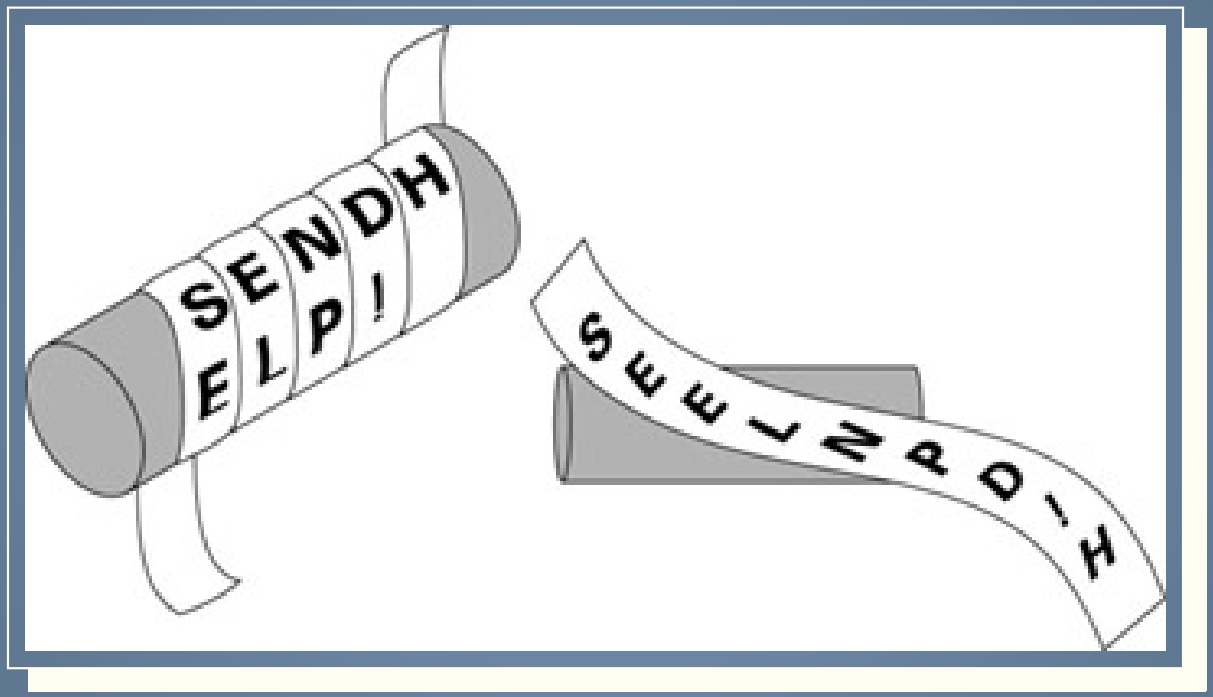
↓

T N E R T S T N R S N I R I F I T D V E D A S N R S N I R
O S C E E T O P I O N E S L U T U E I N R S O P I O N E

↓

TNERTSTNRSNIRIFITDVEDASNRSNIROSCEETOPIONESLUTUEINRSOPIONE

Exemple de transposition : La scytale spartiate (V^e siècle av J-C)



Chiffrement par substitution ou par bijection

Mathématiquement, la substitution est une bijection !

- On note $\mathcal{A}$ l'alphabet, par exemple $\mathcal{A} = a, b, ..., z$ est un alphabet de 26 lettres
- On choisit :
  - un ensemble $\mathcal{E}$ d'autant de signe que $\mathcal{A}$
  - une bijection c : $\mathcal{E} \to \mathcal{E}$
- On chiffre le message x par $x \mapsto c(x)$
- On déchiffre le message x' par $x' \mapsto c^{-1}(x')$

Exemple de substitution : Le chiffre de Jules-César (de -100 à -15)

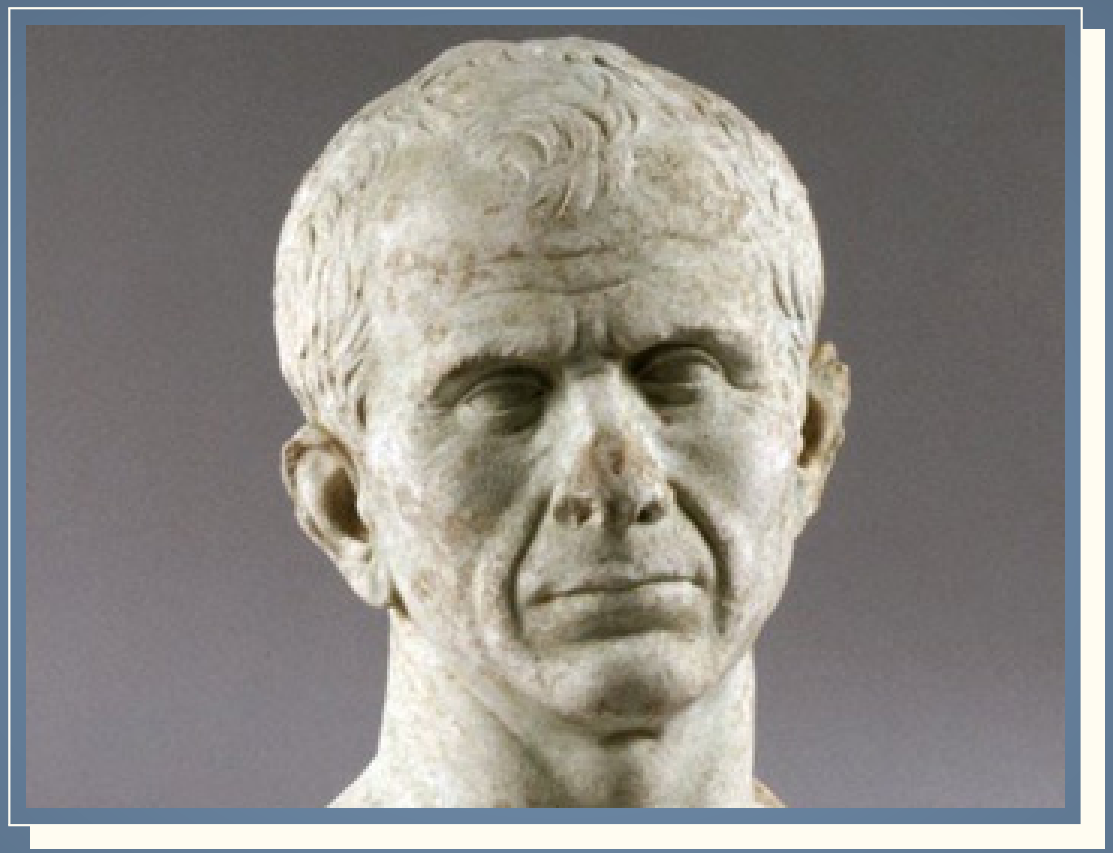


FIGURE: Le Monde, 16 mai 2008 ; tête repêchée dans le Rhône.

Exemple de substitution : Le chiffre de Jules-César (de -100 à -15)

Extrait de Suétone, *La vie des douze Césars* (120 après J-C) :

"On a conservé en outre ses lettres à Cicéron, et celles qu'il adressait à ses familiers sur ses affaires domestiques ; quand il avait à leur faire quelque communication secrète, il usait d'un chiffre, c'est-à-dire qu'il brouillait les lettres de telle façon qu'on ne pût reconstituer aucun mot : si l'on veut en découvrir le sens et les déchiffrer, il faut substituer à chaque lettre la troisième qui la suit dans l'alphabet, c'est-à-dire le D à l'A, et ainsi de suite."

Exemple de substitution : Le chiffre de Jules-César (de -100 à -15)

clair	A	B	C	D	E	F	G	H	...	S	T	U	V	W	X	Y	Z
chiffré	D	E	F	G	H	I	J	K	...	V	W	X	Y	Z	A	B	C

TABLE: Chiffre de césar avec clé de décalage $k = 3$

Exemple avec le mot REVOLUTION :

- $R \rightarrow U$
- $E \rightarrow H$
- ...
- REVOLUTION $\rightarrow$ UHYROXZLRA

Le déchiffrement se fait en inversant la procédure

Les mathématiques derrière le chiffrement de Jules César

$$J_k = c^{-1} \circ t_k \circ c$$

$$\begin{array}{ccc} \mathcal{A} & \xrightarrow{J_k} & \mathcal{E} = \mathcal{A} \\ \downarrow{\scriptstyle c} & & \downarrow{\scriptstyle c} \\ \frac{\mathbb{Z}}{26\mathbb{Z}} & \xrightarrow{t_k} & \frac{\mathbb{Z}}{26\mathbb{Z}} \end{array}$$

x	A	B	C	D	E	F	G	H	...	Z
c(x)	1	2	3	4	5	6	7	8	...	26

$$t_k : x \mapsto x + k \text{ mod } 26$$

Le chiffrement de césar est très faible

Après tout il n'y a que 26 clés différentes !

Clé de décalage	Texte chiffré
0	VIZSPYXMSR
1	UHYROXWLRQ
2	TGXQNWVKQP
3	SFWPMVUJPO
4	REVOLUTION
5	QDUNKTSHNM
6	PCTMJSRGML
...	...
26	WJATQZYNTS

Attaque brute-force : on teste toute les clés

Le chiffre de Jules-César

Exercice : déchiffrez

FDNYNHMJZN

Le chiffre de Jules-César

Exercice : déchiffrez

FDNYNHMJZN

AYITICHERI

L'énigme du scarabée d'or, Edgar Allan Poe, 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 ;‡ ? ;

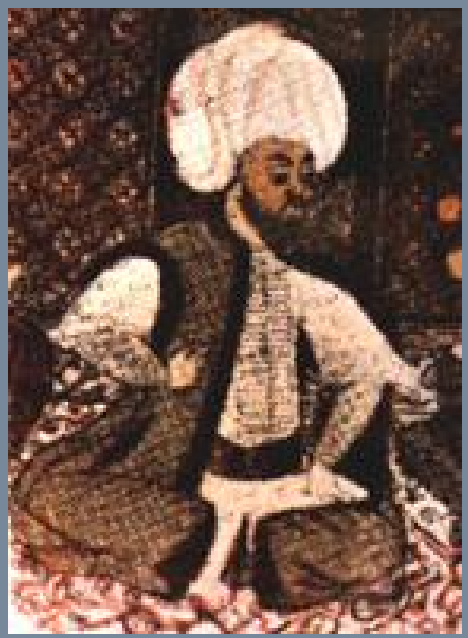
L'énigme du scarabée d'or, Edgar Allan Poe, 1843

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;‡?;

- 20 caractères différents : 8 ; 4 ‡) * 5 6 († 1 0 9 2 : 3 ? ¶ — .
- Pas possible de brute-force car plusieurs milliards de combinaisons possibles !

Attaque par analyse de fréquence décrite par Al Kindi (801-873)

manuscrit retrouvé en 1987 à Istanbul



≪ la façon d'élucider un message crypté, si nous savons dans quelle langue il est écrit, est de nous procurer un autre texte en clair dans la même langue, de la longueur d'un feuillet environ, et de compter alors les apparitions de chaque lettre. Ensuite, nous nous reportons au texte chiffré que nous voulons éclaircir et relevons de même ses symboles. Nous remplaçons le symbole le plus fréquent par la lettre première (la plus fréquente du texte clair), le suivant par la deuxième, le suivant par la troisième, et ainsi de suite jusqu'à ce que nous soyons venus à bout de tous les symboles du cryptogramme à résoudre ≫.

Application de l'analyse de fréquence sur l'énigme du scarabée d'or

signes	8	;	4	‡	)	*	5	6	(	†
occurrences	33	26	19	16	16	13	12	11	11	8

signes	1	0	9	2	:	3	?	¶	—	.
occurrences	8	6	5	5	4	4	3	2	1	1

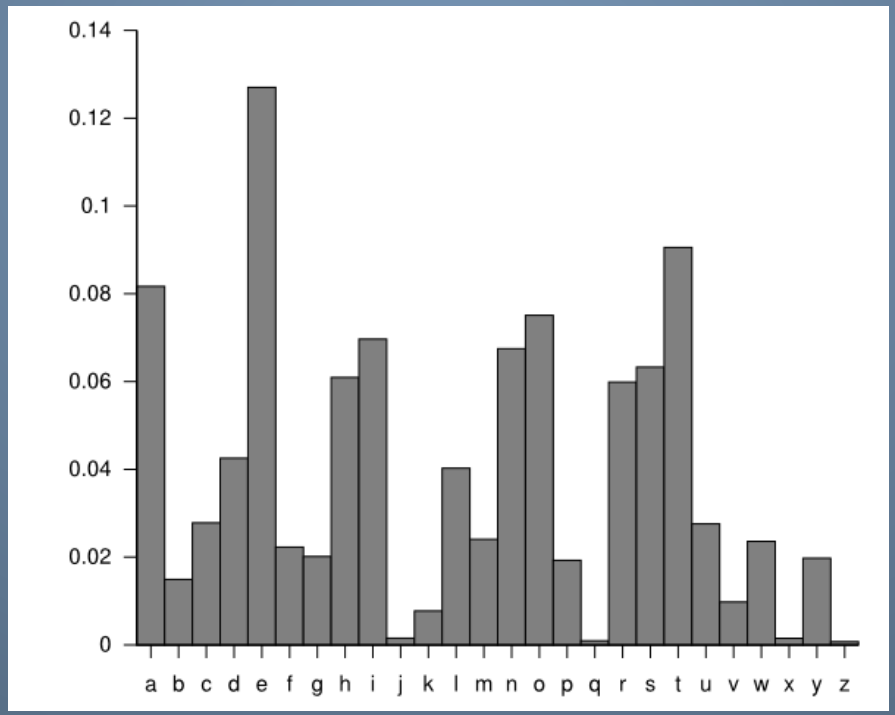


FIGURE: Distribution des lettres en Anglais

Application de l'analyse de fréquence sur l'énigme du scarabée d'or

On peut raisonnablement penser que 8 $\rightarrow$ e

53‡‡†305))6*;4e26)4‡.)4‡);e06*;4e‡e
¶60))e5;1‡(;:‡*e†e3(ee)5*†;46(;ee*96
?;e)‡(;4e5);5*†2:*‡(;4956*2(5*—4)e
¶e*;40692e5);)6†e)4‡‡;1(‡9;4e0e1;e:e‡
1;4e†e5;4)4e5†52ee06*e1(‡9;4e;(ee;4
(‡?34;4e)4‡;161;:1ee;‡?;

Application de l'analyse de fréquence sur l'énigme du scarabée d'or

en anglais le mot le plus utilisé est "the", on en déduit que " ;48" $\rightarrow$ "the" et donc que :

- ; $\rightarrow$ t
- 4 $\rightarrow$ h
- 8 $\rightarrow$ e

53‡‡†305))6*the26)h‡.)4‡)te06*the‡e
¶60))e5t1‡(t :‡*e†e3(ee)5*†th6(tee*96
?te)‡(the5)t5*†2 :*‡(th956*2(5*—)he
¶e*th0692e5)t)6†e)h‡‡t1(‡9the0e1te :e‡
1the†e5th)he5†52ee06*e1(‡9thet(eeth
(‡?3htheh)‡t161t :1eet‡?t

Application de l'analyse de fréquence sur l'énigme du scarabée d'or

On en arrive rapidement à la solution :

agoodglassinthebishopshostelinthede
vilsseatfortyonedegreesandthirteenmi
nutesnortheastandbynorthmainbranchse
venthlimbeastsideshootfromthelefteyeo
fthedeathsheadabeelinefromthetreeth
roughtheshotfiftyfeetout

« A good glass in the bishop's hostel in the devil's seat / forty-one degrees and thirteen minutes / north east and by north / main branch seventh limb east side / shoot from the left eye of the death's head / a bee line from the tree through the shot fifty feet out. »

D'autres chiffrements monoalphabétique

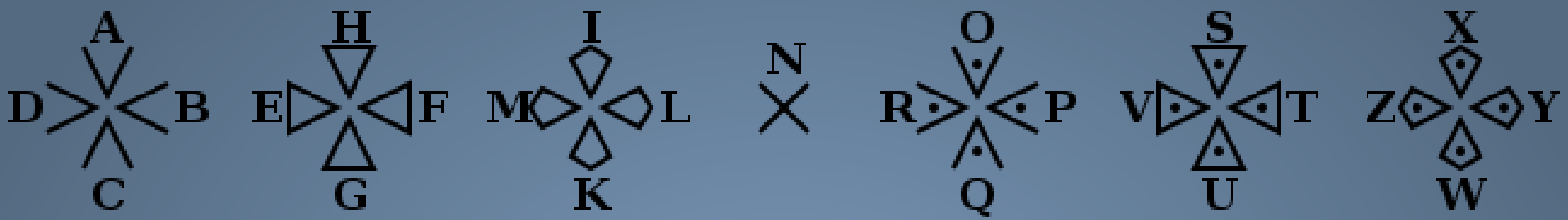
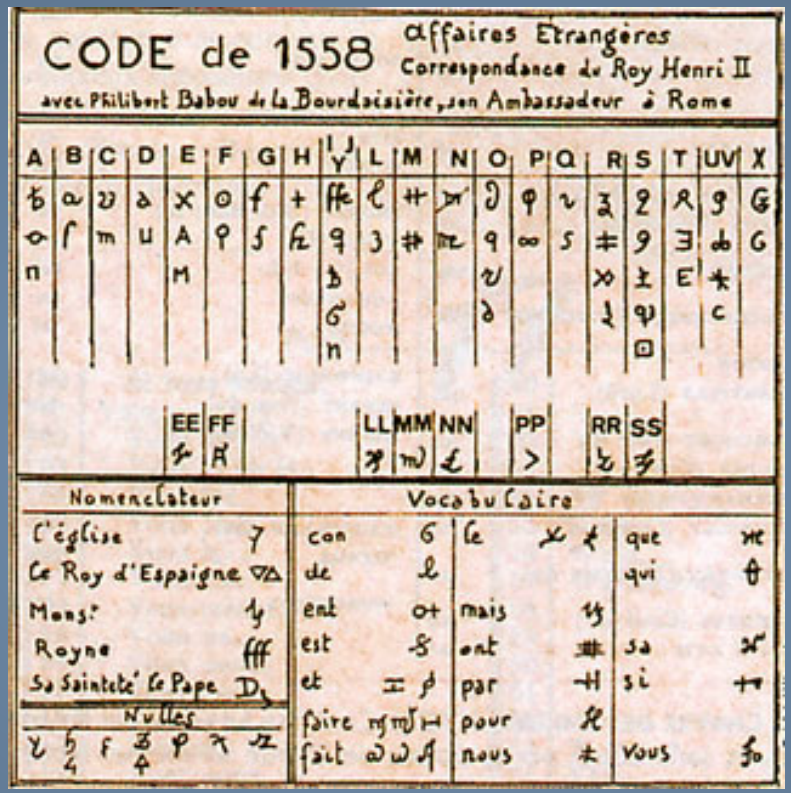


FIGURE: Chiffre des templiers (XII^e siècle)

FIGURE: Chiffre des francs-maçons ($XVIII^e$ siècle)

Ces chiffrements ne résistent pas à l'analyse de fréquence

Le chiffre de Philibert Babou, cryptanalyste de François I_{er} et Henri II (XVI^e)


CODE de 1558 affaires Etrangeres
Correspondance du Roy Henri II
avec Philibert Babou de la Bourdaisière, son Ambassadeur à Rome

A B C D E F G H I/J L M N O P Q R S T UV X

EE FF LL MM NN PP RR SS

Nomenclateur

L'église
Le Roy d'Espaigne
Mons.r
Royne
Sa Saintete' le Pape

Nulles

Vocabulaire

con de ent est et faire fait

le mais ont par pour nous

que qui sa si vous

Parades contre l'analyse de fréquences

- substitution homophonique (appelé renversement de fréquence)
- codage de mots entiers
- signes nuls

Le chiffre de vigenère, 1586

	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

Principe

- Introduit la notion de clé qui est un mot ou une phrase
- À chaque lettre de la clé correspond un décalage (comme le chiffrement de césar)

Texte en clair	TOUJOURSAIMERTOUJOURSSOUFFRIRTOUJOURSMOURIR
Clé	IREMIREMIREMIREMIREMIREMIREMIREMIREMIREMIRE
Texte chiffré	BFYVWLVEIZQQZKSGRFYDAJSGNWVUZKSGRFYDADSGZZV

Le chiffre de vigenère, 1586

Un bon chiffre mais peu utilisé

- Le chiffre de Vigenère était robuste pour l'époque (il faudra attendre 3 siècles pour le casser)
- Usage pas évident, l'effort requis découragea beaucoup
- Pendant des siècles ont utilisa des variantes du chiffre mono-alphabétique

Giovanna Battista Della Porta (vers 1535-40, 1615)

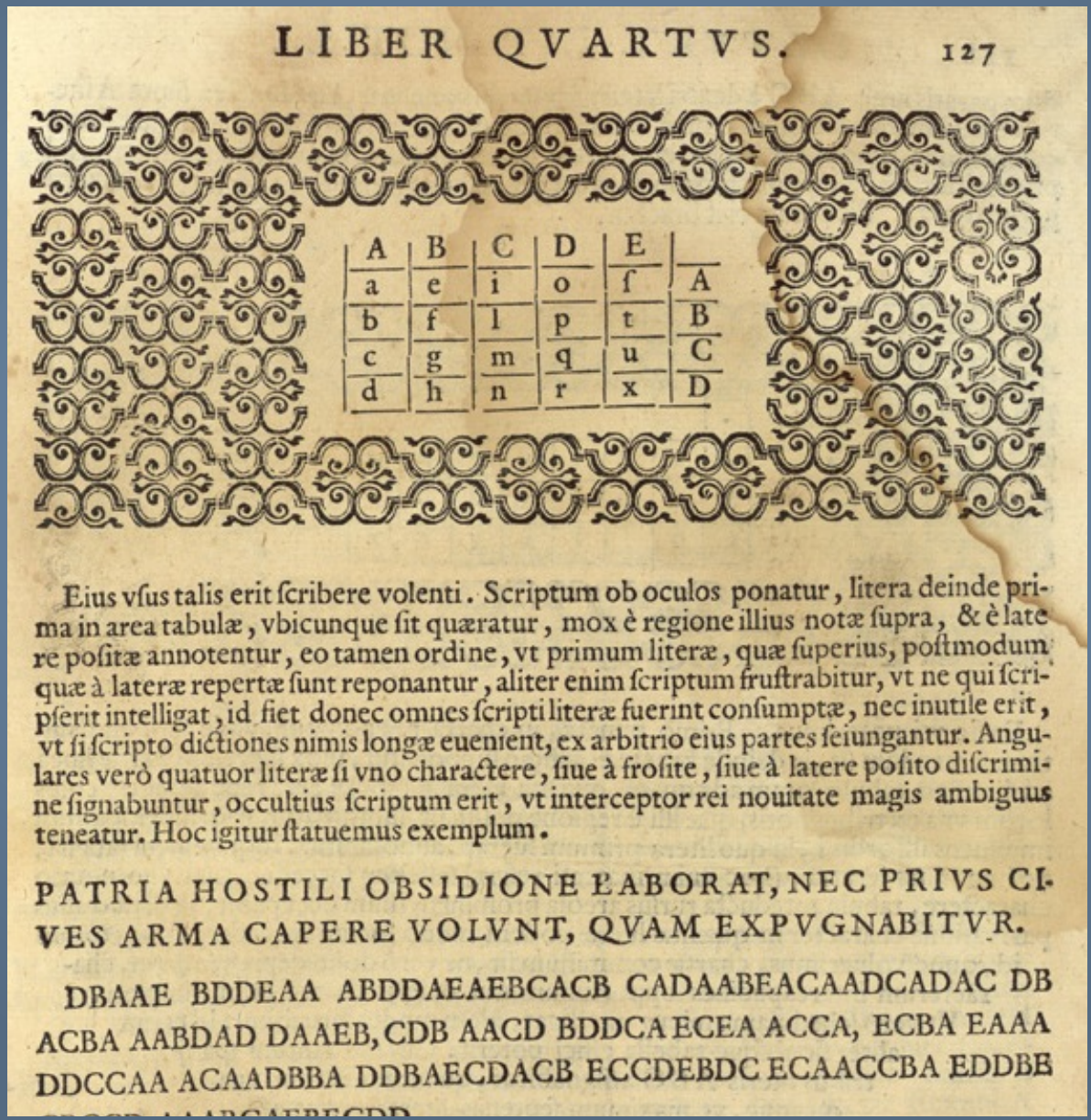
Traités de magie (1558), d'agriculture et botanique (1583,1584, 1588, 1592), d'optique (1589), d'astronomie (1601), de mathématiques et hydraulique (1602), d'art militaire (1606), de météorologie (1609), de chimie (1610) ; lignes de la main (1581 publié seulement en 1677). 14 comédies, une tragédie, un drame. . .

De Furtivis Literarum Notis, vulgo de ziferis


DE FVRTIVIS
LITERARVM NOTIS
VVLGO
DE ZIFERIS
Libri Quinque.
Altero libro superaddi, & quamplurimis in locis locupletati.
IO. BAPTISTA PORTA NEAPOLITANO
AVCTORE.
NEAPOLI, Apud Ioannem Baptistam Subtilem. MDCII.

Naples, 1563 et 1602.

Chiffrement des vingt lettres abcdefghilmnopqrstux par des couples



LIBER QVARTVS. 127

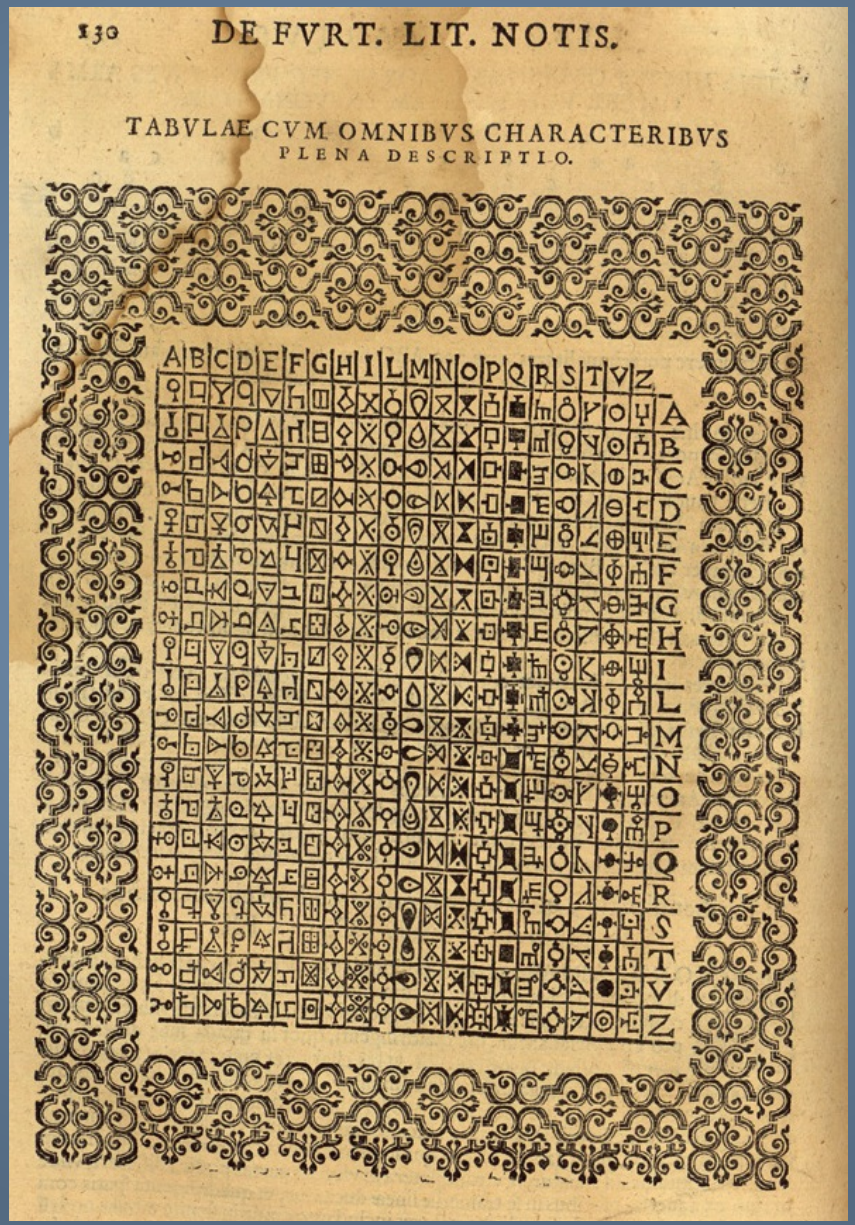
A	B	C	D	E	
a	e	i	o	ſ	A
b	f	l	p	t	B
c	g	m	q	u	C
d	h	n	r	x	D

Eius vſus talis erit ſcribere volenti. Scriptum ob oculos ponatur, litera deinde prima in area tabulæ, vbicunque ſit quæratur, mox è regione illius notæ ſupra, & è latere poſitæ annotentur, eo tamen ordine, vt primum literæ, quæ ſuperius, poſtmodum quæ à lateræ repertæ ſunt reponantur, aliter enim ſcriptum fruſtrabitur, vt ne qui ſcripſerit intelligat, id fiet donec omnes ſcripti literæ fuerint conſumptæ, nec inutile erit, vt ſi ſcripto dictiones nimis longæ euenient, ex arbitrio eius partes ſeiungantur. Angulares verò quatuor literæ ſi vno charactere, ſiue à froſite, ſiue à latere poſito diſcrimine ſignabuntur, occultius ſcriptum erit, vt interceptor rei nouitate magis ambiguus teneatur. Hoc igitur ſtatuemus exemplum.

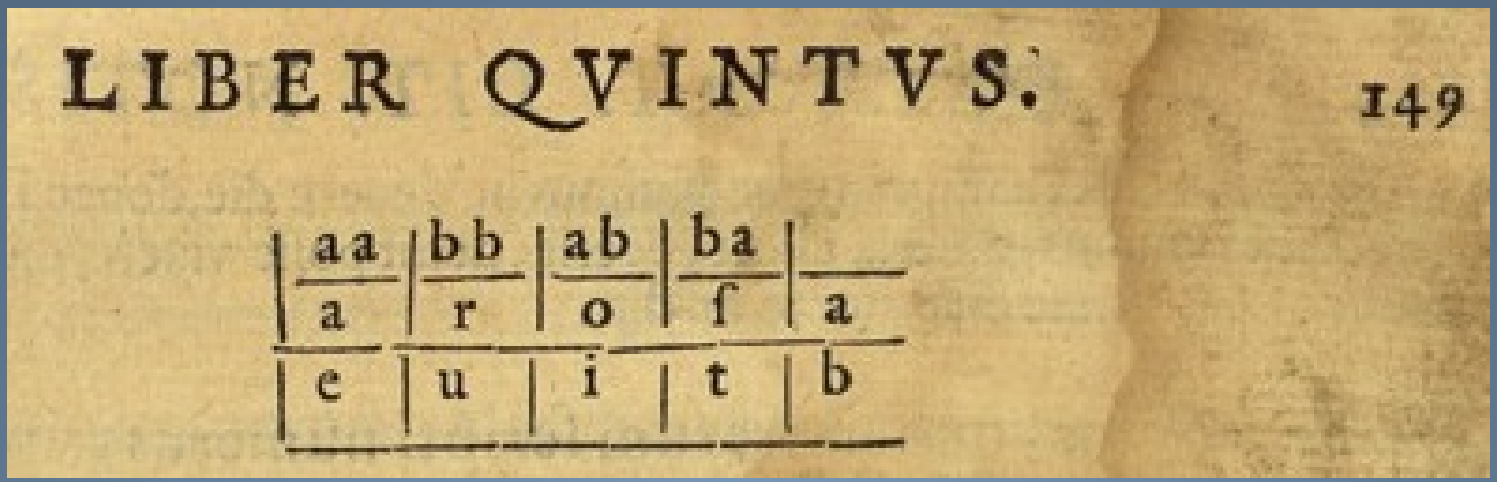
PATRIA HOSTILI OBSIDIONE LABORAT, NEC PRIVS CIVES ARMA CAPERE VOLVNT, QVAM EXPVGNABITVR.

DBAAE BDDEAA ABDDAEAEBCACB CADAABEACAADCADAC DB ACBA AABDAD DAAEB, CDB AACD BDDCA ECEA ACCA, ECBA EAAA DDCCAA ACAADBBA DDBAECDACB ECCDEBDC ECAACCBA EDDBE

Chiffrement des couples



Chiffrement par deux lettres



LIBER QVINTVS. 149

aa	bb	ab	ba	
a	r	o	ſ	a
e	u	i	t	b

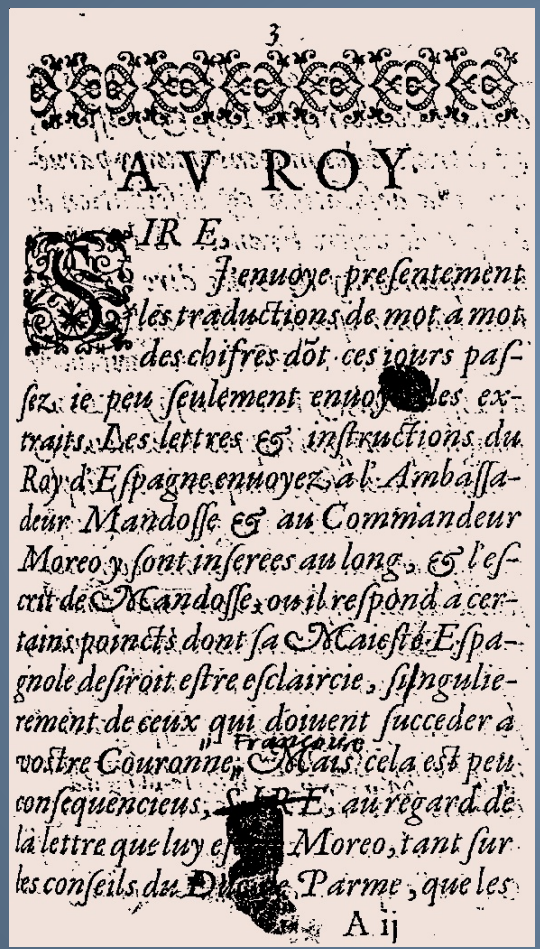
Exemplum.

PVGNATE VIRILITER, NAM VENIAM, VT CIVITATEM IN LIBERTATEM ASSERAM.

In duas literas A B ita reduximus.

babbbb a b abaaaaaba ba ab, bbb a bbbb aa bbbbb a bbbbab aa bbb a, b aa aaa bb a bbb aa bb aaa bb aaabba bbbb ab aaaa bbbbbabbba b aaa ba b aa bbb aa bbb aa bbb a bbbbb aa bbb ab ab aaa ba baa bbb a aaa baa baa aa bbb a aaa bb a.

François viète, cryptanalyste du roi Henri IV (XVI^e)



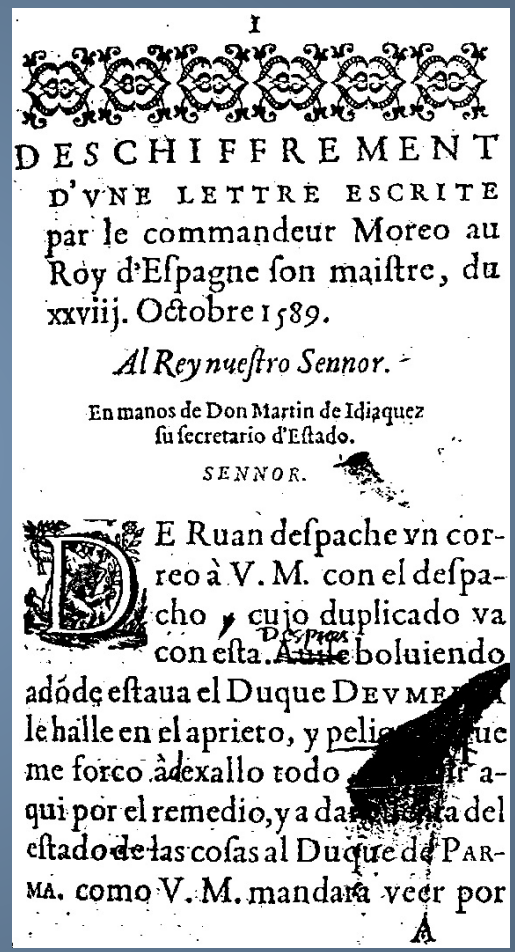
3

AV ROY.

SIRE,

Ie enuoye presentement les traductions de mot à mot des chifres dõt ces iours passez ie peu seulement enuoyer les extraits, Des lettres & instructions du Roy d'Espagne enuoyez à l'Ambassadeur Mandosse & au Commandeur Moreo, y sont inserees au long, & l'escrit de Mandosse, ou il respond à certains poincts dont sa Maiesté Espagnole desiroit estre esclaircie, singulierement de ceux qui doiuent succeder à vostre Couronne. Mais cela est peu consequencieus, SIRE, au regard de la lettre que luy escript Moreo, tant sur les conseils du Duc de Parme, que les

A ij



I

DESCHIFFREMENT D'VNE LETTRE ESCRITE par le commandeur Moreo au Roy d'Espagne son maistre, du xxviij. Octobre 1589.

Al Rey nuestro Sennor.

En manos de Don Martin de Idiaquez su secretario d'Estado.

SENNOR.

DE Ruan despache vn correo à V. M. con el despacho, cujo duplicado va con esta. A ... boluiendo adõde estaua el Duque DE VME... le halle en el aprieto, y peli... que me forco à dexallo todo ... ir aqui por el remedio, y a da... ta del estado de las cosas al Duque de PARMA. como V. M. mandara veer por

A

FIGURE: Deschiffrement d'une lettre escripte par le Commandeur Moreo au Roy d'Espagne son maître, du 28 octobre 1589

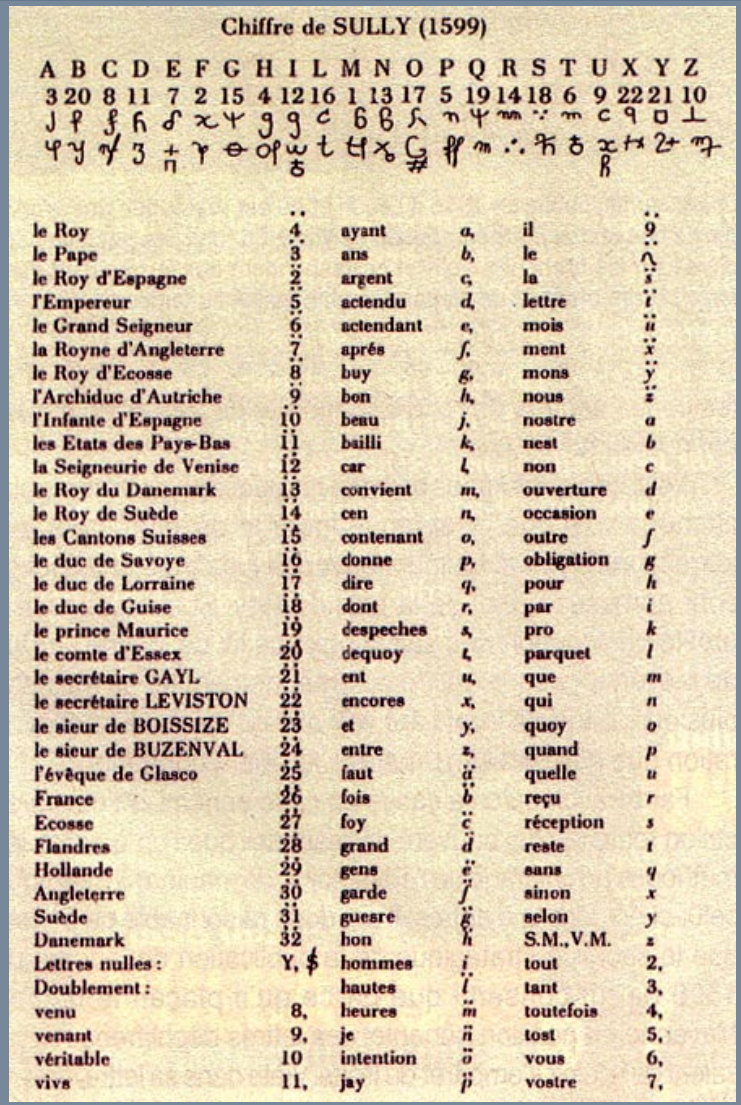
François viète, cryptanalyste du roi Henri IV (XVI^e)

père de la cryptanalyse, il décrit sa méthode dans un mémoire

- principe de base du déchiffrage :
  - identifier le type de chiffrement
  - utiliser des renseignements sur le contexte du message
  - faire une analyse cryptographique fondée sur une étude des fréquences des différents signes et de leurs associations.
- Une autre arme pour le décryptage est la recherche de mots probables. Viète explore trois pistes :
  - la présence de nombres dans le document (dates, effectifs militaires, sommes d'argent) livre des codages de mots tels que : janvier, fantassins, cavaliers, ducats...
  - la structure du document livre des codages de mots tels que : mémoire, instructions, chapitre, idem...
  - les en-têtes des doubles livrent des codages de mots tels que : copie de la lettre, copie du chapitre...

François viète et le chiffre de sully, 1599

Le chiffre de sully vraisemblablement composé par viète



Chiffre de SULLY (1599)

A	B	C	D	E	F	G	H	I	L	M	N	O	P	Q	R	S	T	U	X	Y	Z
3	20	8	11	7	2	15	4	12	16	1	13	17	5	19	14	18	6	9	22	21	10

le Roy	4	ayant	*a,*	il	9
le Pape	3	ans	*b,*	le	
le Roy d'Espagne	2	argent	*c,*	la	*s*
l'Empereur	5	actendu	*d,*	lettre	*t*
le Grand Seigneur	6	actendant	*e,*	mois	*u*
la Royne d'Angleterre	7	aprés	*f,*	ment	*x*
le Roy d'Ecosse	8	buy	*g,*	mons	*y*
l'Archiduc d'Autriche	9	bon	*h,*	nous	*z*
l'Infante d'Espagne	10	beau	*j,*	nostre	*a*
les Etats des Pays-Bas	11	bailli	*k,*	nest	*b*
la Seigneurie de Venise	12	car	*l,*	non	*c*
le Roy du Danemark	13	convient	*m,*	ouverture	*d*
le Roy de Suède	14	cen	*n,*	occasion	*e*
les Cantons Suisses	15	contenant	*o,*	outre	*f*
le duc de Savoye	16	donne	*p,*	obligation	*g*
le duc de Lorraine	17	dire	*q,*	pour	*h*
le duc de Guise	18	dont	*r,*	par	*i*
le prince Maurice	19	despeches	*s,*	pro	*k*
le comte d'Essex	20	dequoy	*t,*	parquet	*l*
le secrétaire GAYL	21	ent	*u,*	que	*m*
le secrétaire LEVISTON	22	encores	*x,*	qui	*n*
le sieur de BOISSIZE	23	et	*y,*	quoy	*o*
le sieur de BUZENVAL	24	entre	*z,*	quand	*p*
l'évêque de Glasco	25	faut	*ä*	quelle	*u*
France	26	fois	*b*	reçu	*r*
Ecosse	27	foy	*c*	réception	*s*
Flandres	28	grand	*d*	reste	*t*
Hollande	29	gens	*ë*	sans	*q*
Angleterre	30	garde	*f*	sinon	*x*
Suède	31	guesre	*g*	selon	*y*
Danemark	32	hon	*h*	S.M.,V.M.	*z*
Lettres nulles :	Y, $	hommes	*i*	tout	2,
Doublement :		hautes	*l*	tant	3,
venu	8,	heures	*m*	toutefois	4,
venant	9,	je	*n*	tost	5,
véritable	10	intention	*o*	vous	6,
vivs	11,	jay	*p*	vostre	7,

Antoine Rossignol et le **Grand Chiffre** $XVII^e$ siècle

cryptanalyste du roi Louis XIV

- chiffrement par substitution à répertoire
  - on code les syllabes ou les mots plutôt que les lettres
  - emploi simple et rapide
  - sécurité repose sur le répertoire qui peut être perdu, copié ou volé
- 587 nombres différents
- réputé incassable, les archives sont restés secrètes pendant 200 ans
- cassé en 1893 par Étienne Bazeries

FIGURE: Étienne Bazeries (1846 - 1931)

Les cabinets noirs

La cryptanalyse devient une industrie au $XVIII^e$ siècle

- chaque puissance européenne avait son *cabinet noir*
- lieu de déchiffrement des messages

Exemple du *Geheime Kabinets-Kanzlei* de Vienne ($XVIII^e$ siècle)

- 7h : courrier destiné aux embassades étrangères arrive au cabinet
- les sceaux étaient fondus
- une équipe de sténographes copiait les lettres
- puis les lettres étaient replacées dans l'enveloppe et re-scellées
- 10h : le courrier est retourné au bureau de poste
- une centaine de courrier intercepté chaque jour

Les cabinets noirs

Une redoutable efficacité

- les cabinets sont venus à bout de toutes les formes de chiffres monoalphabétiques
- passage forcé au chiffre poly-alphabétique de Vigenère

Charles Babbage (1791 - 1871)

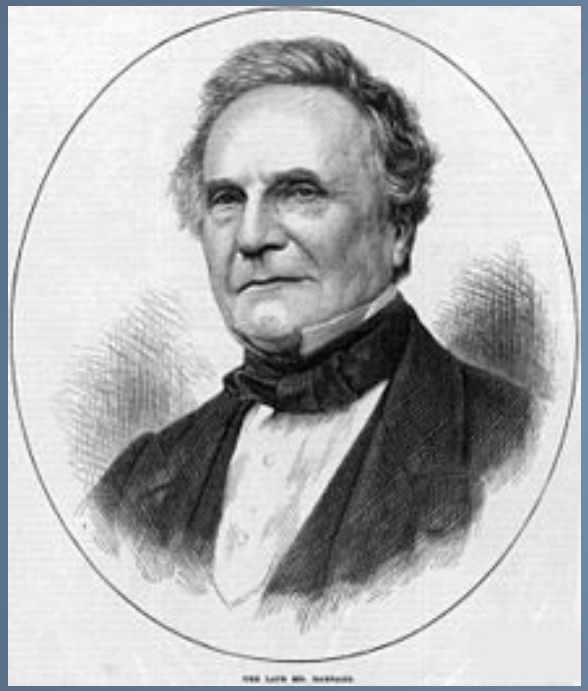


FIGURE: Charles Babbage

Vagabondage scientifique

- Un ingénieur et inventeur
  - compteur de vitesse
  - pare buffle
- Un scientifique
  - métrologie
  - statistiques (table de mortalité)
  - La machine a calculer
- Un cryptanalyste
  - **Cassage du chiffre de Vigenère**

Rappel du chiffre de vigenère

Texte en clair	TOUJOURSAIMERTOUJOURSSOUFFRIRTOUJOURSMOURIR
Clé	IREMIREMIREMIREMIREMIREMIREMIREMIREMIREMIRE
Texte chiffré	BFYVWLVEIZQQZKSGRFYDAJSGNWVUZKSGRFYDADSGZZV

Cryptanalyse du chiffre de vigenère par Babbage, 1854

Étape 1 : Analyse des répétitions pour trouver la taille de la clé

- Une répétition signifie :
  - la même séquence de lettres du texte clair a été chiffrée avec la même partie de la clef. (très probable)
  - deux séquences différentes dans le texte clair ont engendré la même séquence dans le texte chiffré (peu probable)

- BFYVWLVEIZQQZKSGRFYDAJSGNWVUZKSGRFYDADSGZZV
  - Distance entre les répétitions de 16 (RE chiffre OU = FY)
- BFYVWLVEIZQQZKSGRFYDAJSGNWVUZKSGRFYDADSGZZV
  - Distance entre les répétitions de 8 (EM chiffre OU = SG)
- la taille de la clé est nécessairement un diviseur de 16 et de 8 sinon les motifs répétés ne seraient pas alignés.

Cryptanalyse du chiffre de vigenère par Babbage, 1854

Éxemple sur un texte plus long

KQOWEFVJPUJUUNUKGLMEKJINMWUXFQMKJBGWRLFNFGHUDWUUMBSVLPS
NCMUEKQCTESWREEKOYSSIWCTUAXYOTAPXPLWPNTCGOJBGFQHTDWXIZA
YGFFNSXCSEYNCTSSPNTUJNYTGGWZGRWUUNEJUUQEAPYMEKQHUIDUXFP
GUYTSMTFFSHNUOCZGMRUWEYTRGKMEEDCTVRECFBDJQCUSWVBPNLGOYL
SKMTEFVJJTWWMFMWPNMEMTMHRSPXFSSKFFSTNUOCZGMDOEOYEEKCPJR
GPMURSKHFRSEIUEVGOYCWXIZAYGOSAANYDOEOYJLWUNHAMEBFELXYVL
WNOJNSIOFRWUCCESWKVIDGMUCGOCRUWGNMAAFFVNSIUDEKQHCEUCPFC
MPVSUDGAVEMNYMAMVLFMAOYFNTQCUAFVFJNXKLNEIWCWODCCULWRIFT
WGMUSWOVMATNYBUHTCOCWFYTNMGYTQMKBBNLGFBTWOJFTWGNTEJKNEE
DCLDHWTYYIDGMVRDGMPLSWGJLAGOEEKJOFEKUYTAANYTDWIYBNLNYNP
WEBFNLFYNAJEBFR

Cryptanalyse du chiffre de vigenère par Babbage, 1854

KQOWEFVJPUJUUNUKGLMEKJINMWUXFQMKJBGWRLFNFGHUDWUUMBSVLPS
NCMUEKQCTESWREEKOYSSIWCTUAXYOTAPXPLWPNTCGOJBGFQHTDWXIZA
YGFFNSXCSEYNCTSSPNTUJNYTGGWZGRWUUNEJUUQEAPYMEKQHUIDUXFP
GUYTSMTFFSHNUOCZGMRUWEYTRGKMEEDCTVRECFBDJQCUSWVBPNLGOYL
SKMTEFVJJTWWMFMWPNMEMTMHRSPXFSSKFFSTNUOCZGMDOEOYEEKCPJR
GPMURSKHFRSEIUEVGOYCWXIZAYGOSAANYDOEOYJLWUNHAMEBFELXYVL
WNOJNSIOFRWUCCESWKVIDGMUCGOCRUWGNMAAFFVNSIUDEKQHCEUCPFC
MPVSUDGAVEMNYMAMVLFMAOYFNTQCUAFVFJNXKLNEIWCWODCCULWRIFT
WGMUSWOVMATNYBUHTCOCWFYTNMGYTQMKBBNLGFBTWOJFTWGNTEJKNEE
DCLDHWTYYIDGMVRDGMPLSWGJLAGOEEKJOFEKUYTAANYTDWIYBNLNYNP
WEBFNLFYNAJEBFR

Séquence répétée	Distance entre répétition	2	3	5	19
WUU	95			x	x
EEK	200	x		x	
WXIZAYG	190	x		x	x
NUOCZGM	80	x		x	
DOEOY	45		x	x	
GMU	90	x	x	x	

La clé a donc une taille de 5 !

Cryptanalyse du chiffre de vigenère par Babbage, 1854

Étape 2 : Analyse par fréquence

- Il ne reste plus qu'a découper le texte en plusieurs sous texte (5 dans notre cas)
- chacun de ces sous textes a été chiffré avec le même décalage
- On applique alors la cryptanalyse connu par analyse de fréquence

```
12345123451234512345123451234512345123451234512345123451234512345
KQOWEFVJPUJUUNUKGLMEKJINMWUXFQMKJBGWRLFNFGHUDWUUMBSVLPS
NCMUEKQCTESWREEKOYSSIWCTUAXYOTAPXPLWPNTCGOJBGFQHTDWXIZA
YGFFNSXCSEYNCTSSPNTUJNYTGGWZGRWUUNEJUUQEAPYMEKQHUIDUXFP
GUYTSMTFFSHNUOCZGMRUWEYTRGKMEEDCTVRECFBDJQCUSWVBPNLGOYL
SKMTEFVJJTWWMFMWPNMEMTMHRSPXFSSKFFSTNUOCZGMDOEOYEEKCPJR
GPMURSKHFRSEIUEVGOYCWXIZAYGOSAANYDOEOYJLWUNHAMEBFELXYVL
WNOJNSIOFRWUCCESWKVIDGMUCGOCRUWGNMAAFFVNSIUDEKQHCEUCPFC
MPVSUDGAVEMNYMAMVLFMAOYFNTQCUAFVFJNXKLNEIWCWODCCULWRIFT
WGMUSWOVMATNYBUHTCOCWFYTNMGYTQMKBBNLGFBTWOJFTWGNTEJKNEE
DCLDHWTYYIDGMVRDGMPLSWGJLAGOEEKJOFEKUYTAANYTDWIYBNLNYNP
WEBFNLFYNAJEBFR
```

Auguste Kerckhoffs (1835-1903)

- *La cryptographie militaire* janvier et février 1883
- Lois de Kerckhoffs : il préconise un système cryptographique :
  - mathématiquement indéchiffrable
  - qui n'exige pas le secret, que nos voisins pourraient connaître et même copier
  - applicable à la correspondance télégraphique
  - portatif, pour une seule personne
  - usage facile.

- Principes toujours d'actualité !
- Les systèmes de sécurité par obscurité finissent toujours par être cassé

Le chiffre en danger

À la fin du XIX^e siècle, la cryptographie est dans un état désastreux

- Vigenère est cassé
- La communication par télégraphe se démocratise
  - Câbles France-Angleterre : 1850-1851.
  - Câbles transatlantiques :1858-1865
  - 103 000 km de câbles sont anglais sur 118 000 en 1877
- Invention de la TSF (Télégraphie sans fil) en 1896
  - facilité de communication
  - facilité d'interception
- Première guerre mondial qui se profil et toujours pas de chiffrage sûr..
  - aucune découverte d'importance entre 1914 et 1918
  - un catalogue d'échec de la cryptographie
  - et un florilège de success story de la cryptanalyse

1917 le télégramme de Zimmermann, ministre allemand des affaires étrangères

- 16 janvier : télégramme au Mexique pour le faire entre en guerre contre les Etats-Unis
- 17 janvier : télégramme doit passer par Londres où il est décrypté (Room 40)
- 5 février : le télégramme arrivé au Mexique est récupéré par les Anglais.
- 24 février : le télégramme est transmis aux Etats-Unis
- 2 avril : entrée en guerre des Etats-Unis.

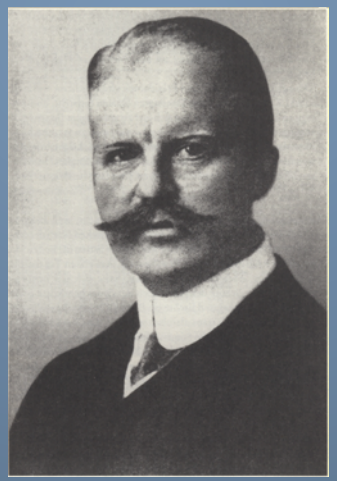
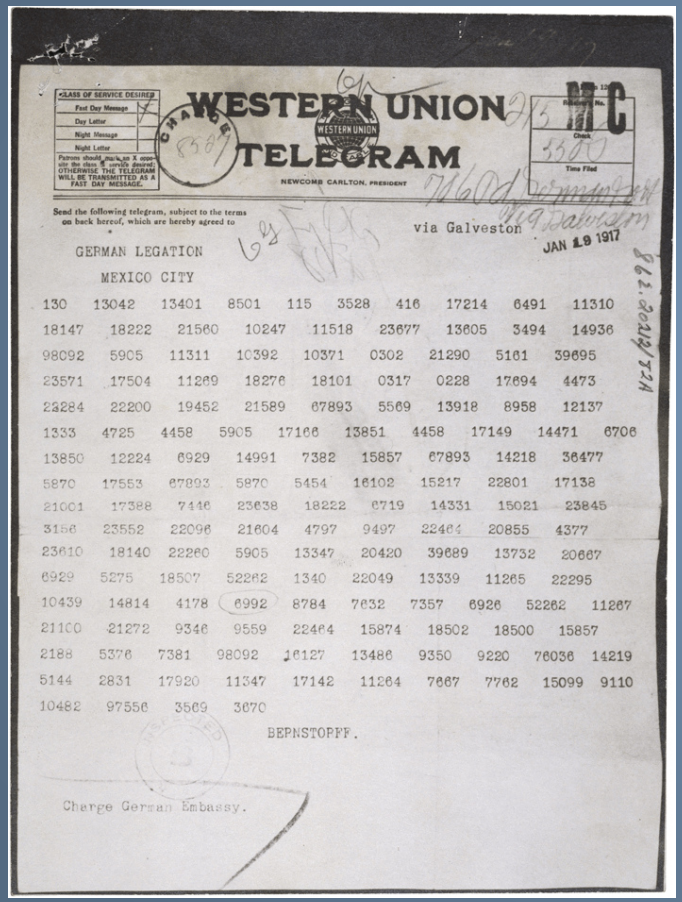


FIGURE: Arthur Zimmermann

1917 le télégramme de Zimmermann, ministre allemand des affaires étrangères



WESTERN UNION TELEGRAM

NEWCOMB CARLTON, PRESIDENT

Send the following telegram, subject to the terms on back hereof, which are hereby agreed to

via Galveston

JAN 19 1917

GERMAN LEGATION

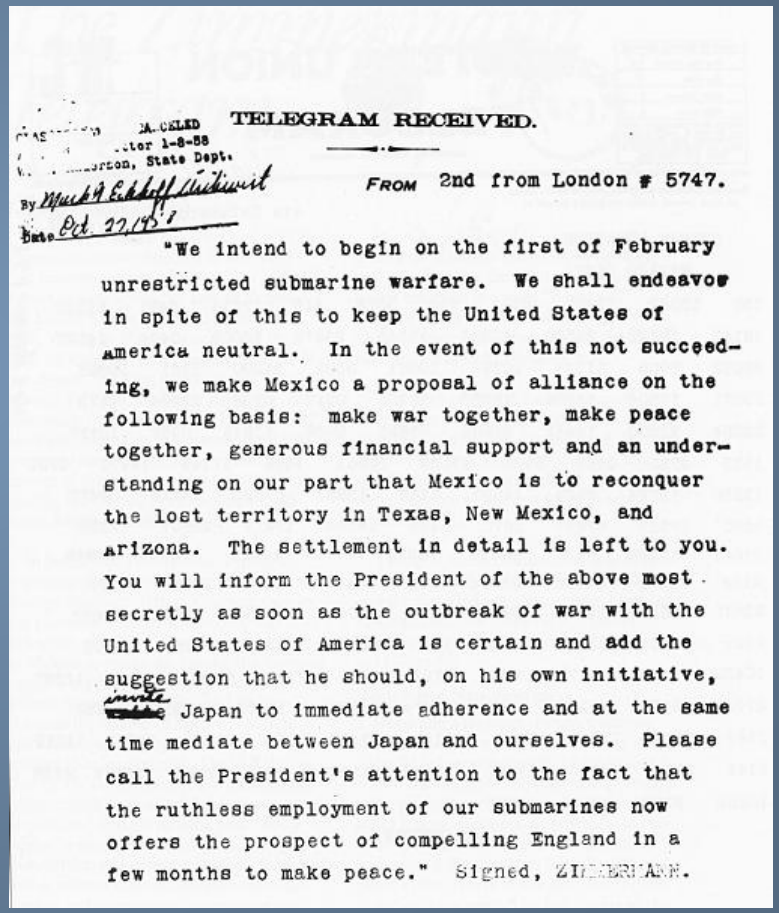
MEXICO CITY

130 13042 13401 8501 115 3528 416 17214 6491 11310
18147 18222 21560 10247 11518 23677 13605 3494 14936
98092 5905 11311 10392 10371 0302 21290 5161 39695
23571 17504 11269 18276 18101 0317 0228 17694 4473
23284 22200 19452 21589 67893 5569 13918 8958 12137
1333 4725 4458 5905 17166 13851 4458 17149 14471 6706
13850 12224 6929 14991 7382 15857 67893 14218 36477
5870 17553 67893 5870 5454 16102 15217 22801 17138
21001 17388 7446 23638 18222 6719 14331 15021 23845
3156 23552 22096 21604 4797 9497 22464 20855 4377
23610 18140 22260 5905 13347 20420 39689 13732 20667
6929 5275 18507 52262 1340 22049 13339 11265 22295
10439 14814 4178 6992 8784 7632 7357 6926 52262 11267
21100 21272 9346 9559 22464 15874 18502 18500 15857
2188 5376 7381 98092 16127 13486 9350 9220 76036 14219
5144 2831 17920 11347 17142 11264 7667 7762 15099 9110
10482 97556 3569 3670

BERNSTORFF.

Charge German Embassy.

FIGURE: Le télégramme original



TELEGRAM RECEIVED.

FROM 2nd from London # 5747.

"We intend to begin on the first of February unrestricted submarine warfare. We shall endeavor in spite of this to keep the United States of America neutral. In the event of this not succeeding, we make Mexico a proposal of alliance on the following basis: make war together, make peace together, generous financial support and an understanding on our part that Mexico is to reconquer the lost territory in Texas, New Mexico, and Arizona. The settlement in detail is left to you. You will inform the President of the above most secretly as soon as the outbreak of war with the United States of America is certain and add the suggestion that he should, on his own initiative, ~~invite~~ Japan to immediate adherence and at the same time mediate between Japan and ourselves. Please call the President's attention to the fact that the ruthless employment of our submarines now offers the prospect of compelling England in a few months to make peace." Signed, ZIMMERMANN.

FIGURE: Le télégramme déchiffré

Le chiffre de Vernam ou le masque jetable (one time pad)

Du Vigenère avec des contraintes sur la clef

- La clef doit être aussi longue que le texte à chiffrer
- La clef doit être choisie aléatoirement
- La clef ne doit servir qu'une fois

Feuille 1

P	L	M	O	E
Z	Q	K	J	Z
L	R	T	E	A
V	C	R	C	B
Y	N	N	R	B

Feuille 2

O	I	W	V	H
P	I	Q	Z	E
T	S	E	B	L
C	Y	R	U	P
D	U	V	N	M

Feuille 3

J	A	B	P	R
M	F	E	C	F
L	G	U	X	D
D	A	G	M	R
Z	K	W	Y	I

Clef	`PLMOEZQKJZLRTEAVCRCBY`
Texte Clair	`ATTAQUEZLAROUTEALAUBE`
Texte Chiffré	`PEFOUTUJUZCFNXEVNRWCC`

Le chiffre de Vernam ou le masque jetable

Robustesse du système

- Si les contraintes sur la clé sont respectées, le système est parfait et inviolable !
- Il n'est cependant pas facile à mettre en œuvre
  - Difficulté pour produire des clés aléatoires en grande quantité
  - Problème de transmission des clés (valises diplomatiques)
  - La tentation de réutiliser une clef affaiblit énormément le système

Usage

- KGB
- Che Guevara avec Fidel Castro
- Le téléphone rouge (entre Washington et Moscou), 1963

Naissance Enigma (1925)

- Arthur scherbius (1878 - 1929)
- 1925 : première enigma, incompréhensibilité des messages allemands
- Français et Anglais renoncent à déchiffrer Énigma !

FIGURE: photographie de la machine Enigma utilisée par les allemands

Principes d'Énigma : le brouilleur

- un rotor est une version électrique du disque d'alberti
- une pression sur la lettre 'B' sera chiffrée en 'A'

FIGURE: disque d'alberti (XVI^e siècle)

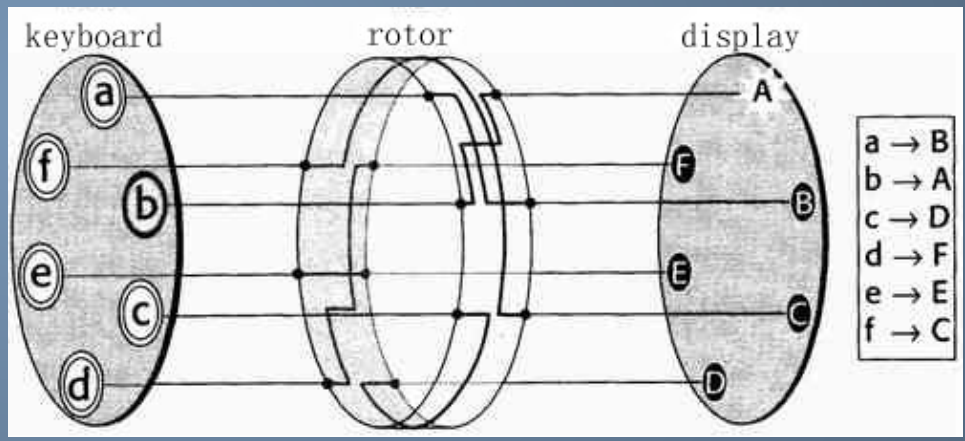
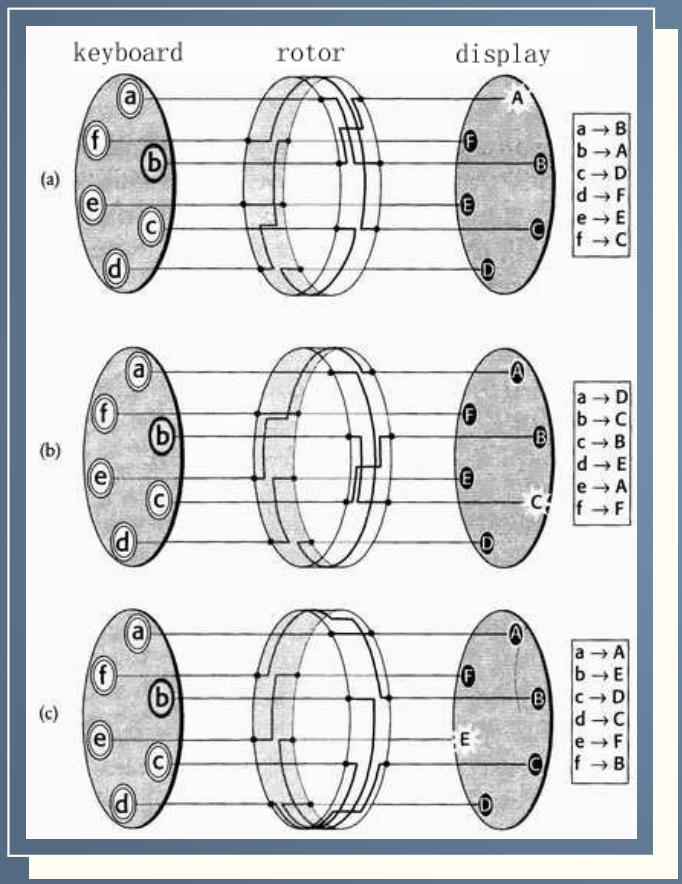


FIGURE: principe d'un rotor d'Énigma

Principes d'Énigma : rotation du brouilleur

Chaque pression sur une touche fait tourner le rotor de un cran

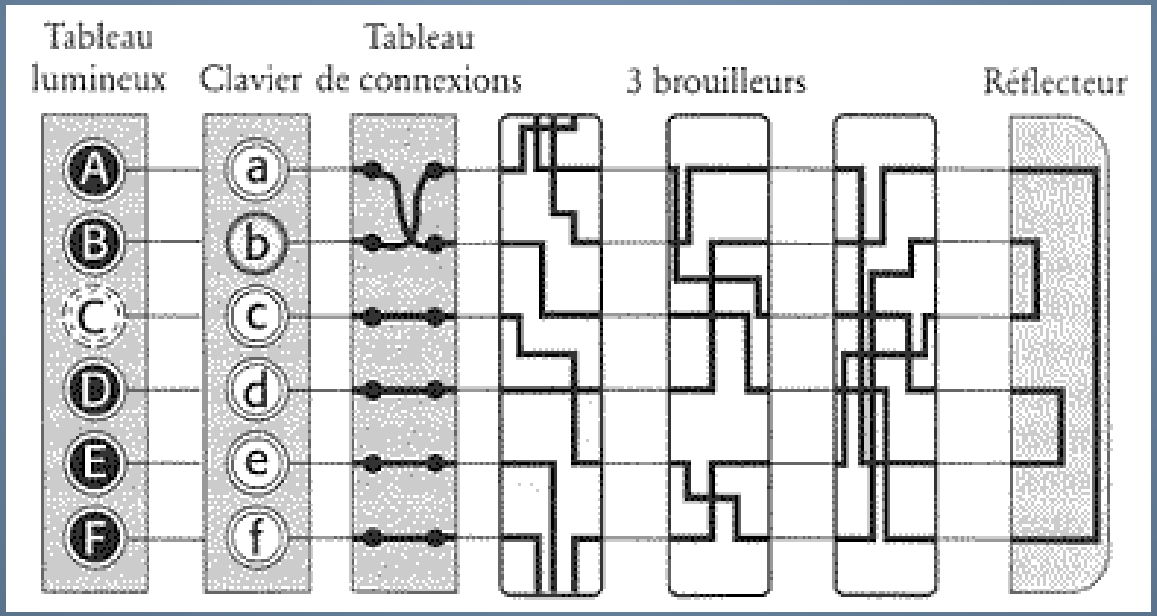


- 1ère pression : 'B' chiffrée en 'A'
- 2ème pression : 'B' chiffrée en 'C'
- 3ème pression : 'B' chiffrée en 'E'

tout les 26 lettres, c'est toujours la même substitution $\rightarrow$ attaque par fréquence ? !

Principes d'Énigma : trois brouilleur, un réflecteur et un tableau de connexion

- trois brouilleurs soit $26 \times 26 \times 26 = 15576$ positions différentes
- un réflecteur statique pour que $c(c(x)) = x$
- un tableau de connexion



FIGURE

Énigma : Calcul de la taille de la clef

- trois brouilleurs soit $26 \times 26 \times 26 = 15576$ positions différentes
- 6 disposition des brouilleurs différentes
- Tableau de connexion à fiche : $C_2^{26} \times C_2^{24} \times C_2^{22} \times C_2^{20} \times C_2^{18} \times C_2^{16} = 72282089880000$
- soit un total de :

$$15576 \times 6 \times 72282089880000 \ = 6.10^{18}$$

- le tableau permet d'avoir un grand nombre de clefs
- les rotors permettent de déjouer l'analyse de fréquence

À l'assault d'Énigma

Énigma sera vaincu en deux temps

- d'abord par Rajewski en exploitant une faiblesse du protocole d'échange de clé (chaque clé du jour était répétée deux fois)
- puis par Alan Turing qui exploita la méthode des mots connus (bulletin météo envoyé tout les matins à 6h)

FIGURE: Marian Rejewski

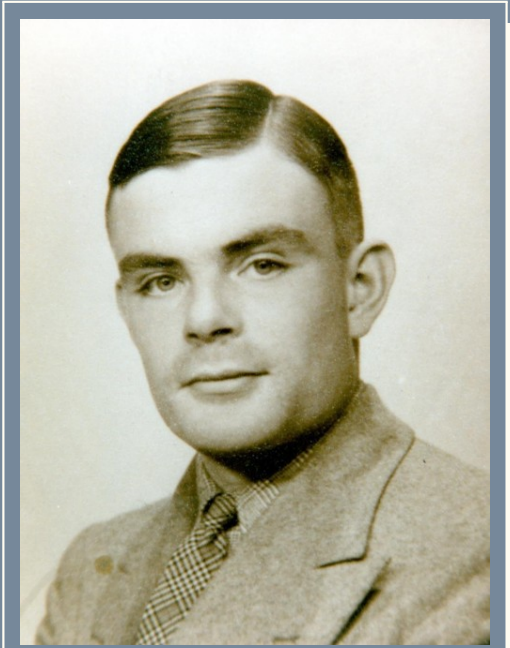


FIGURE: Alan Turing

À l'assault d'Énigma

Construction de *bombes* pour automatiser la découverte des clés

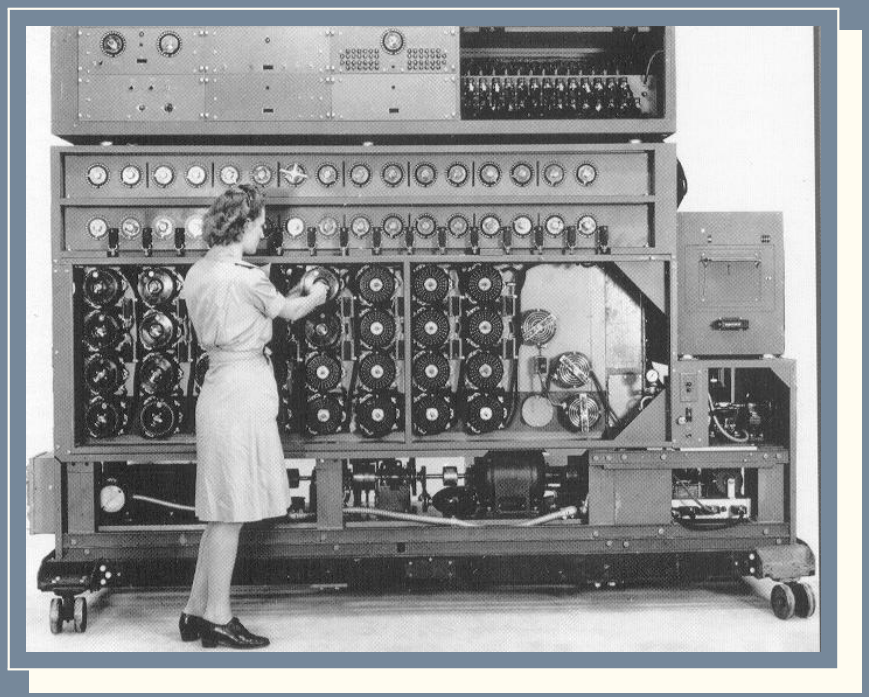


FIGURE: Une *bombe* d'Alan Turing

L'informatique et la cryptographie moderne

L'informatique manipule des 0 et des 1

On peut chiffrer un message en utilisant l'operation XOR sur chaque bit du message

		XOR
0	0	0
0	1	1
1	0	1
1	1	0

	A	B	C
Message (p)	0 1 0 0 0 0 0 1	0 1 0 0 0 0 1 0	0 1 0 0 0 0 1 1
Key (k)	0 0 0 1 0 0 1 1	0 1 1 0 0 1 0 1	0 0 1 1 1 0 0 1
$E(k,p) = p \oplus k$	0 1 0 1 0 0 1 0	0 0 1 0 0 1 1 1	0 1 1 1 1 0 1 0
	R	'	Z

- Le texte clair est "`ABC`" (le code ASCII est représenté)
- le texte chiffré $p \oplus k$ est "`R'Z`"

Le masque jetable (encore)

Un système parfait

Même si l'attaquant a un calculateur avec des ressources infini, il ne peut pas casser le code. Le masque jetable fournis une confidentialité parfaite. La clé dois être une suite de bits aléatoire de la même taille que le texte à chiffrer.

Chiffrement : soit le texte clair $p_1, p_2, p_3, \ldots$
le texte chiffré est $p_1 \oplus k_1, p_2 \oplus k_2, p_3 \oplus k_3, \ldots$

Déchiffrement : soit le texte chiffré $c_1, c_2, c_3, \ldots$
le texte clair est $c_1 \oplus k_1, c_2 \oplus k_2, c_3 \oplus k_3, \ldots$

Correction : on remarque que $p_1 = k_1 \oplus (k_1 \oplus p_1)$

- Cela n'est cependant pas pratique pourquoi ?

Le masque jetable (encore)

Un système parfait

Même si l'attaquant a un calculateur avec des ressources infini, il ne peut pas casser le code. Le masque jetable fournis une confidentialité parfaite. La clé dois être une suite de bits aléatoire de la même taille que le texte à chiffrer.

Chiffrement : soit le texte clair $p_1, p_2, p_3, \ldots$
le texte chiffré est $p_1 \oplus k_1, p_2 \oplus k_2, p_3 \oplus k_3, \ldots$

Déchiffrement : soit le texte chiffré $c_1,\ c_2,\ c_3,\ \ldots$
le texte clair est $c_1 \oplus k_1,\ c_2 \oplus k_2,\ c_3 \oplus k_3,\ \ldots$

Correction : on remarque que $p_1 = k_1 \oplus (k_1 \oplus p_1)$

- Cela n'est cependant pas pratique pourquoi ?
- La plupart des systèmes cryptographique ne sont pas parfait, ils sont juste d'une grande complexité

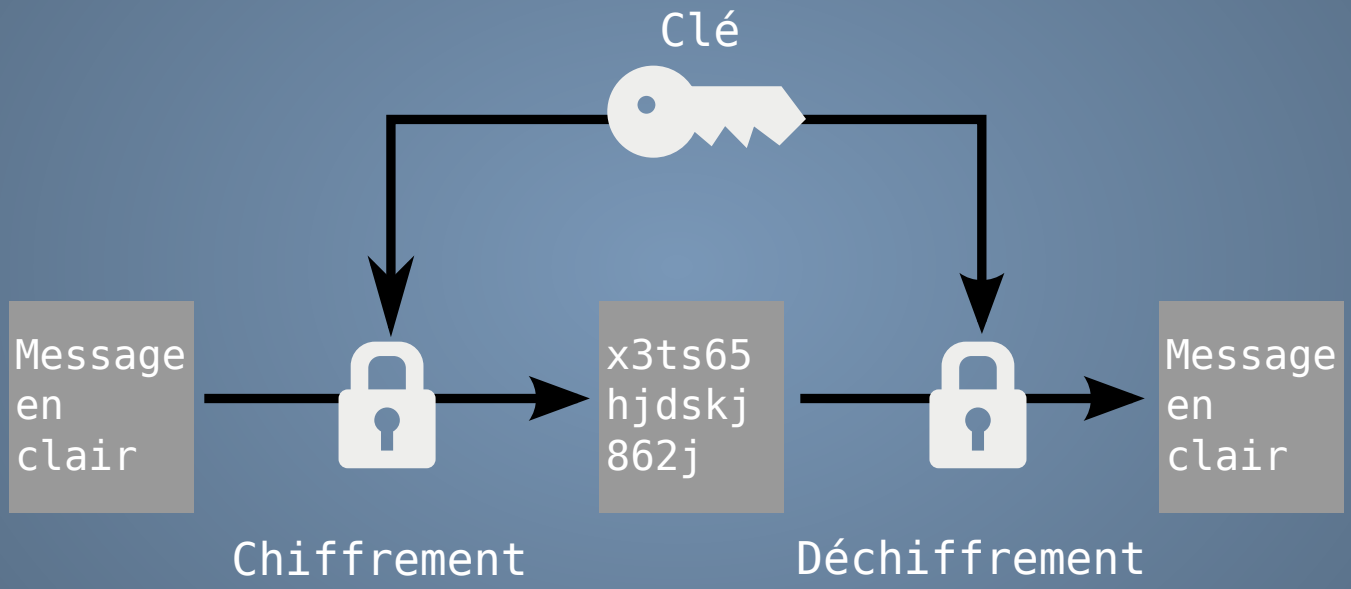
Objectifs de sécurité

Confidentialité Je veux des messages secrets

- Le chiffrement symmétrique
- Le chiffrement asymmétrique

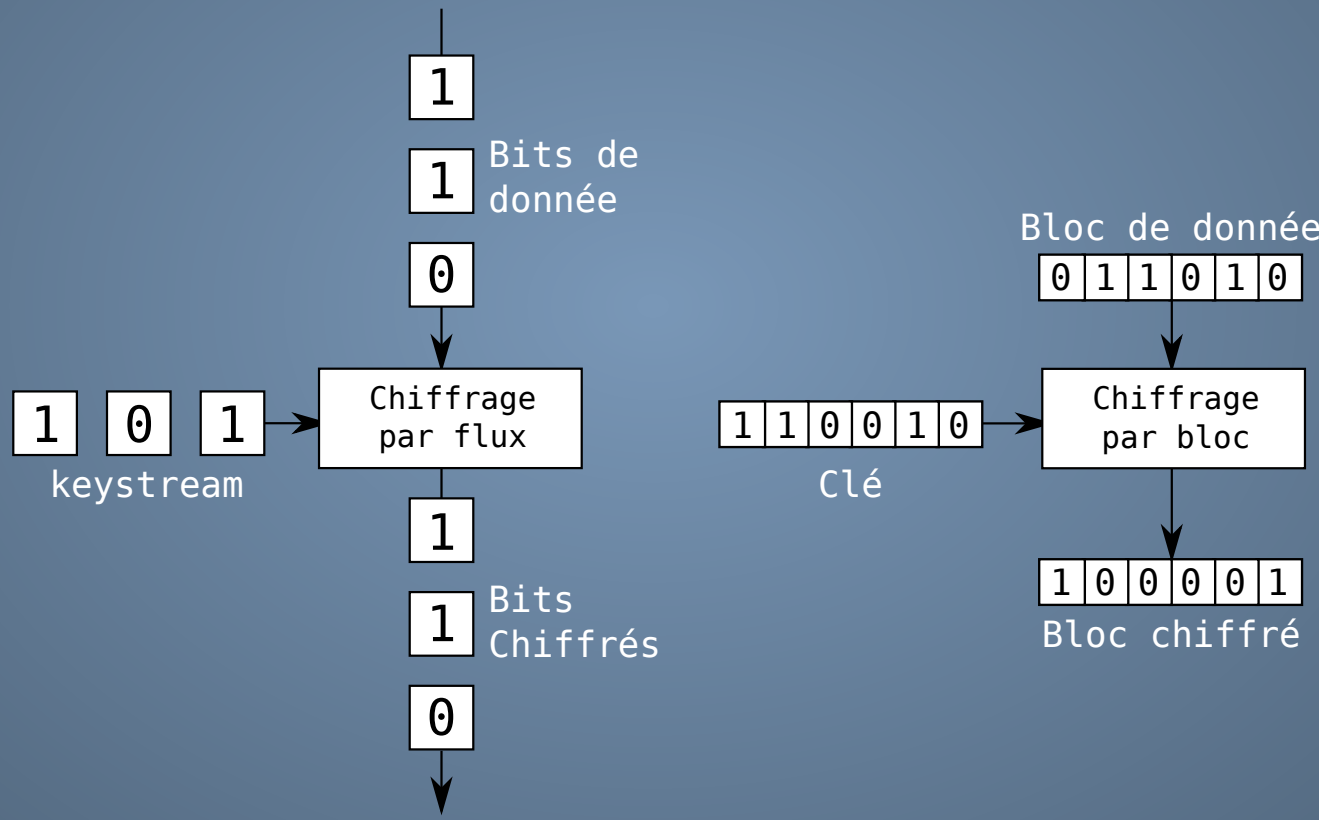
Chiffrement Symétrique

- La même clé est utilisée pour chiffrer et déchiffrer un message

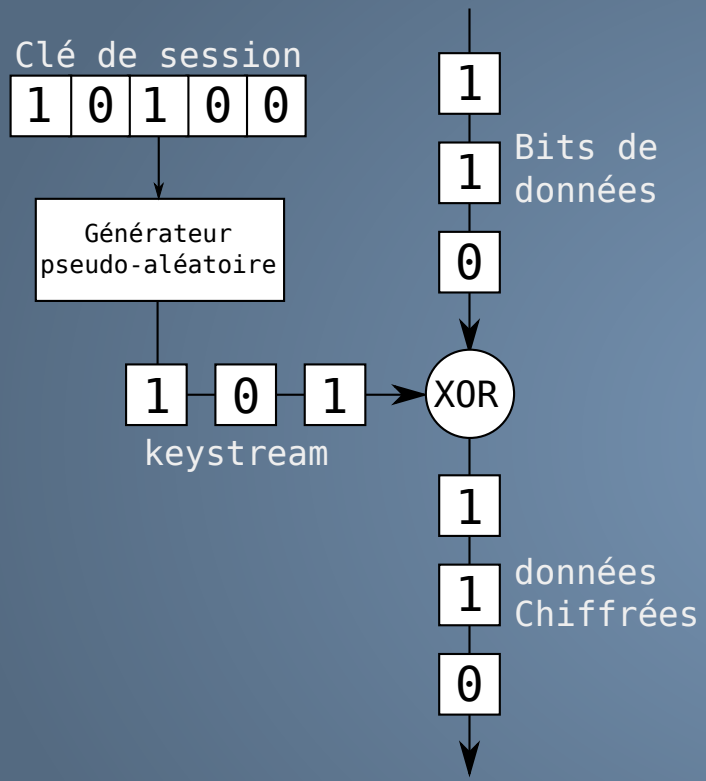


Chiffrement Symétrique

- La même clé est utilisée pour chiffrer et déchiffrer un message
- Deux types de chiffrement symétrique



Chiffrement Symétrique : Chiffrement par flux



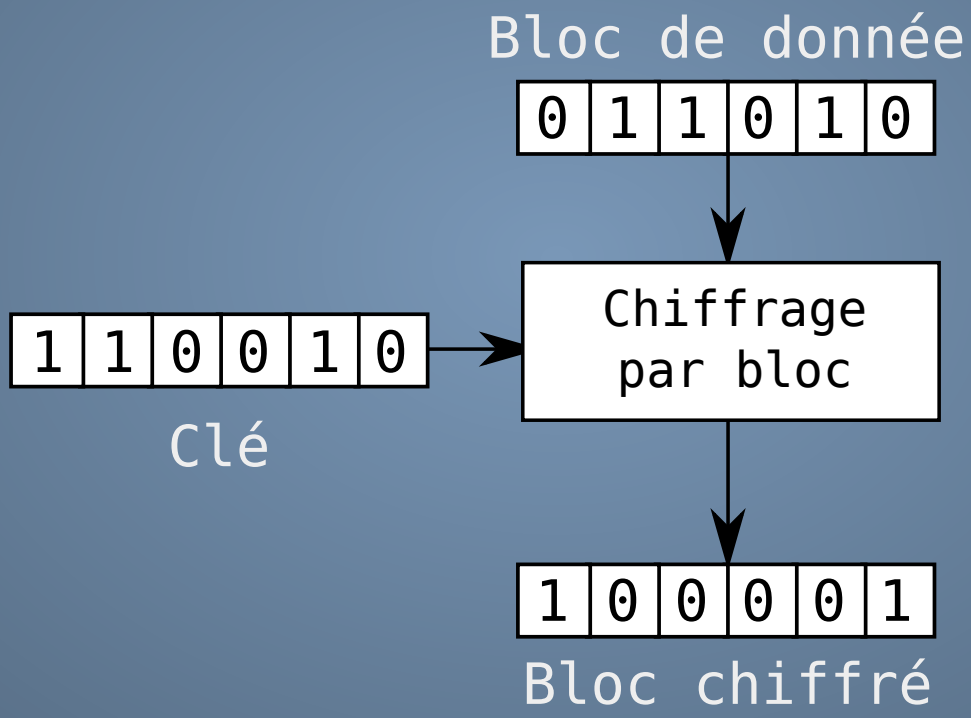
Principe proche du masque jetable

- générer une suite pseudo-aléatoire de bits à partir d'une clé (**keystream**)
- XOR cette suite, bit à bit, sur les données à chiffrer

Quelques exemples

- Enigma est un algorithme de chiffrement par flux mécanique
- GSM : A5/2, A5/1
- WiFi (WEP) : RC4

Chiffrement Symétrique : Chiffrement par bloc



Chiffrement Symétrique : Chiffrement par bloc

Principes

- on découpe les données en blocs

  Données : 10011010111010010111001000000011011101

  Blocs : 10011010111010 | 01011100100000 | 01101110110000

- On effectue un certain nombre de transformation à ces blocs qui dépendent de la clé

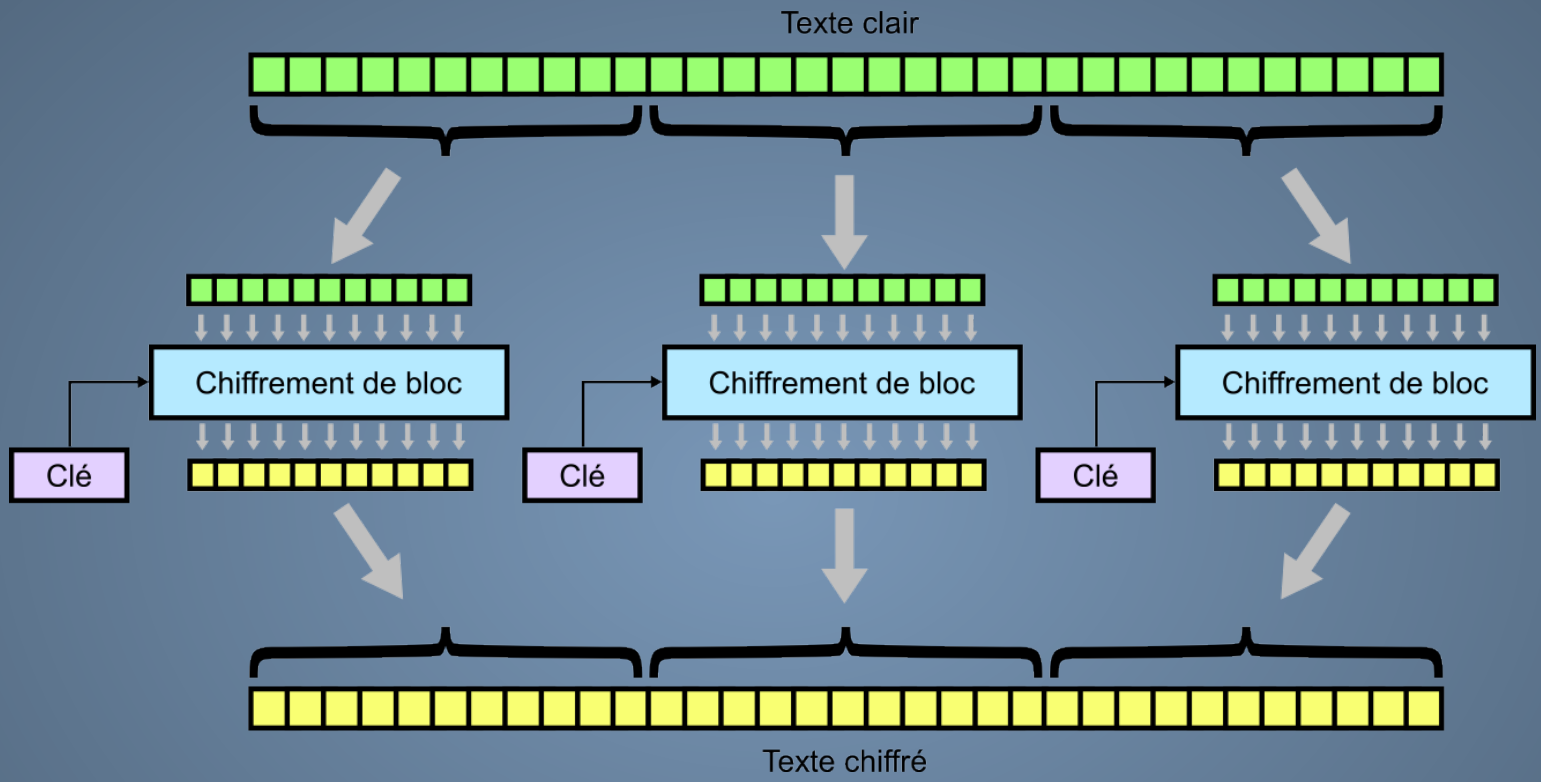
  Confusion : Rendre la relation entre la clé et le texte chiffré la plus complexe possible
  Possible grâce à la substitution

  Diffusion : Un biais en entrée ne doit pas se retrouver en sortie
  Possible grâce à la transposition

Quelques exemples

- ~~DES, 3DES, bluefish~~ (obsolète)
  - clé et blocs de 64 bits
- twofish, **Advanced Encryption Standard** (AES)
  - clé et blocs de 128, 192 et 256 bits

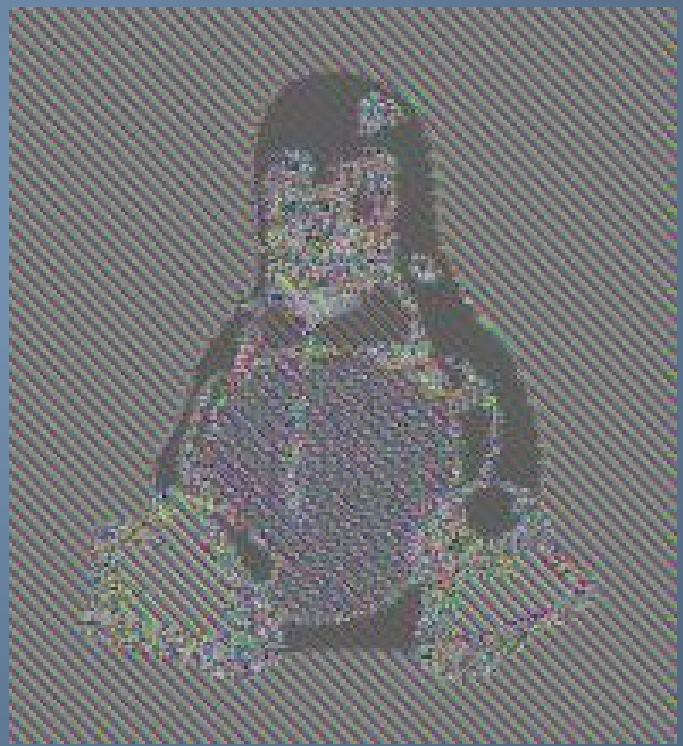
Chiffrement Symétrique par blocs : Le mode d'opération ECB



- Problème : Deux blocs de données identiques seront chiffrés pareil

Chiffrement Symétrique par blocs : Le mode d'opération ECB

```
openssl aes-128-ecb -in tux -out tux-ecb
```



Chiffrement Symétrique par blocs : Les modes d'opérations CBC et CTR

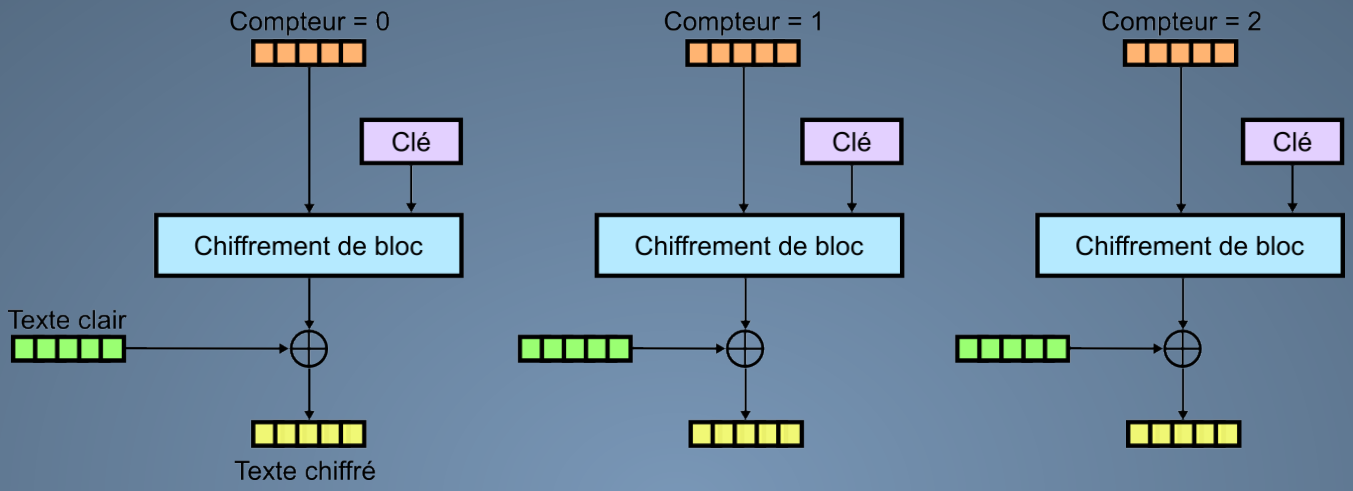


FIGURE: Mode d'opération CTR

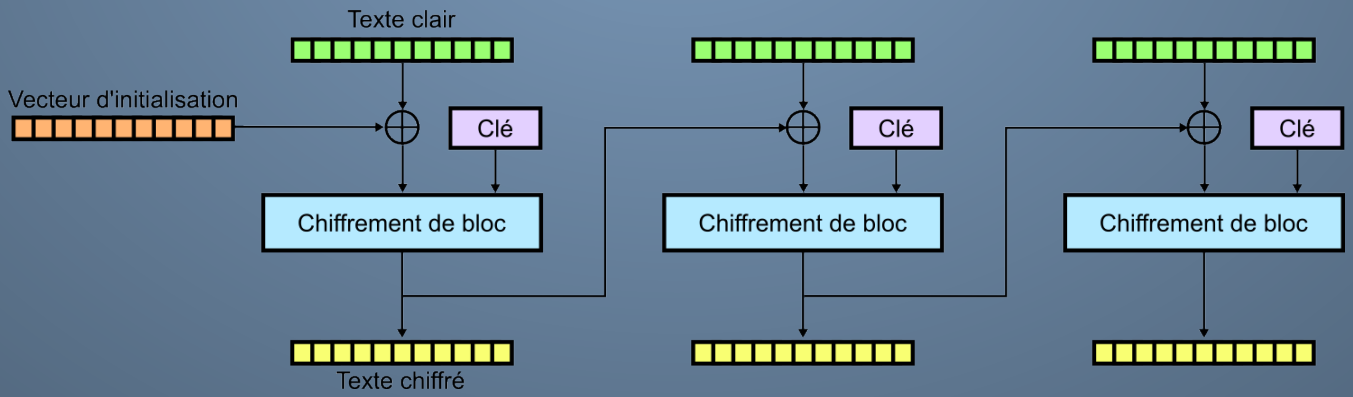


FIGURE: Mode d'opération CBC

Chiffrement Symétrique par blocs : Les modes d'opérations CBC et CTR

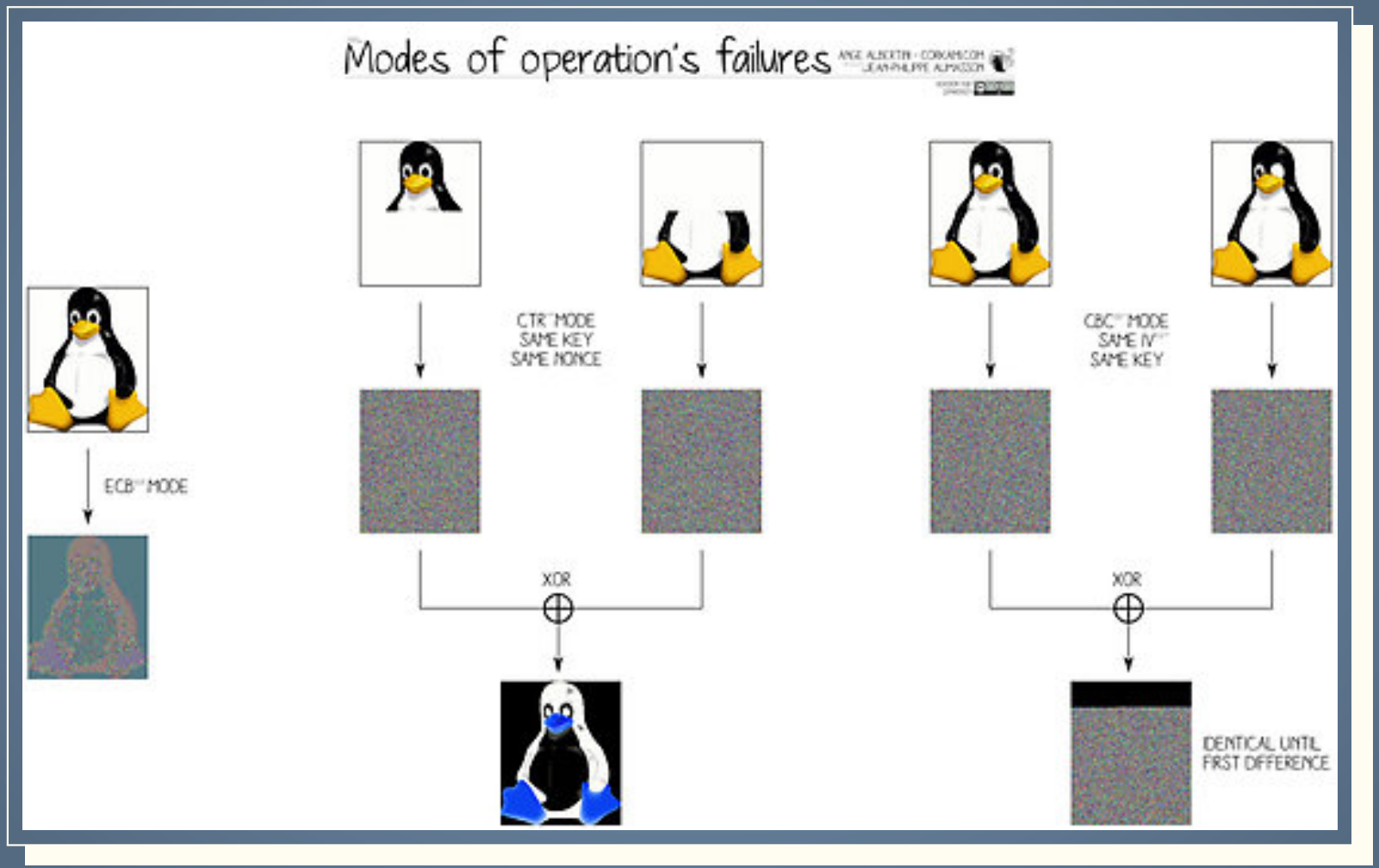


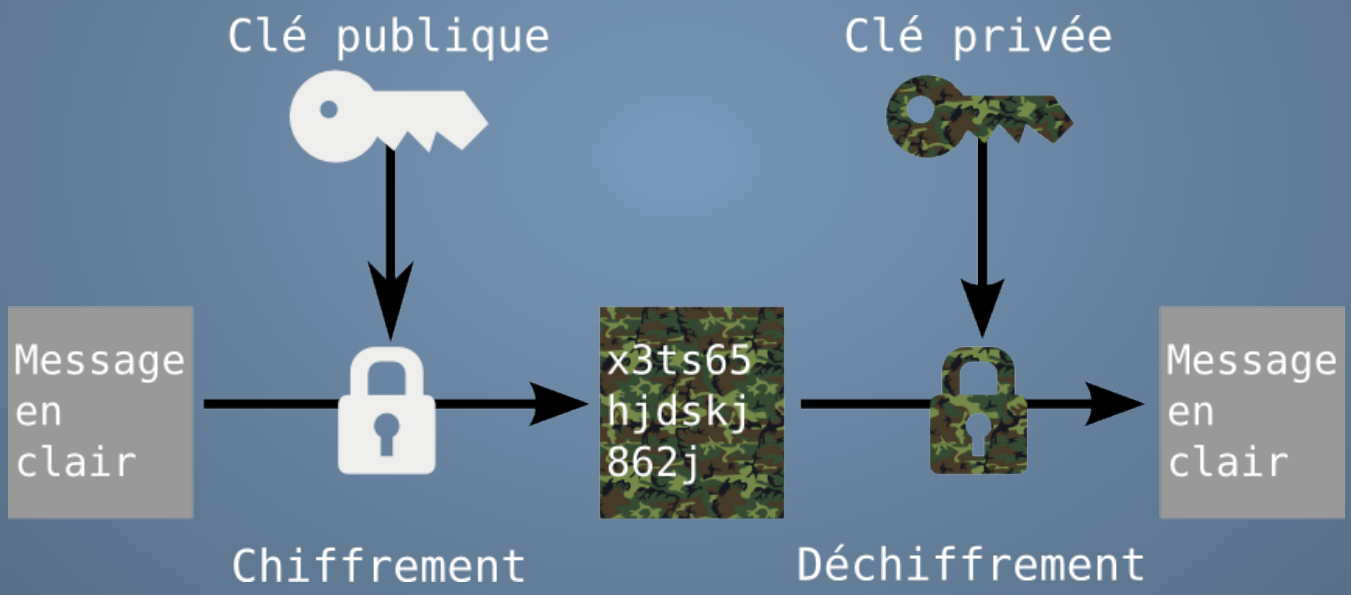
FIGURE: Les vecteurs d'initialisation doivent être unique !

L'informatique et la cryptographie moderne

- Le chiffrement symmétrique
- Le chiffrement asymmétrique

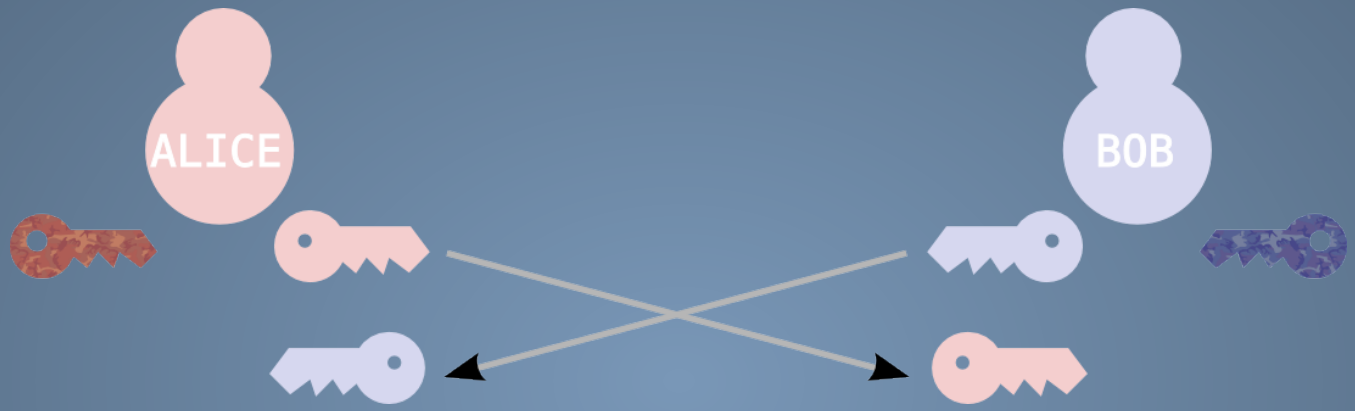
Chiffrement Asymétrique

- Une clé pour chiffrer et une autre pour déchiffrer
  - la clé pour **chiffrer** est **publique** et est distribuée
  - la clé pour **déchiffrer** est **privée** et est gardée secrète

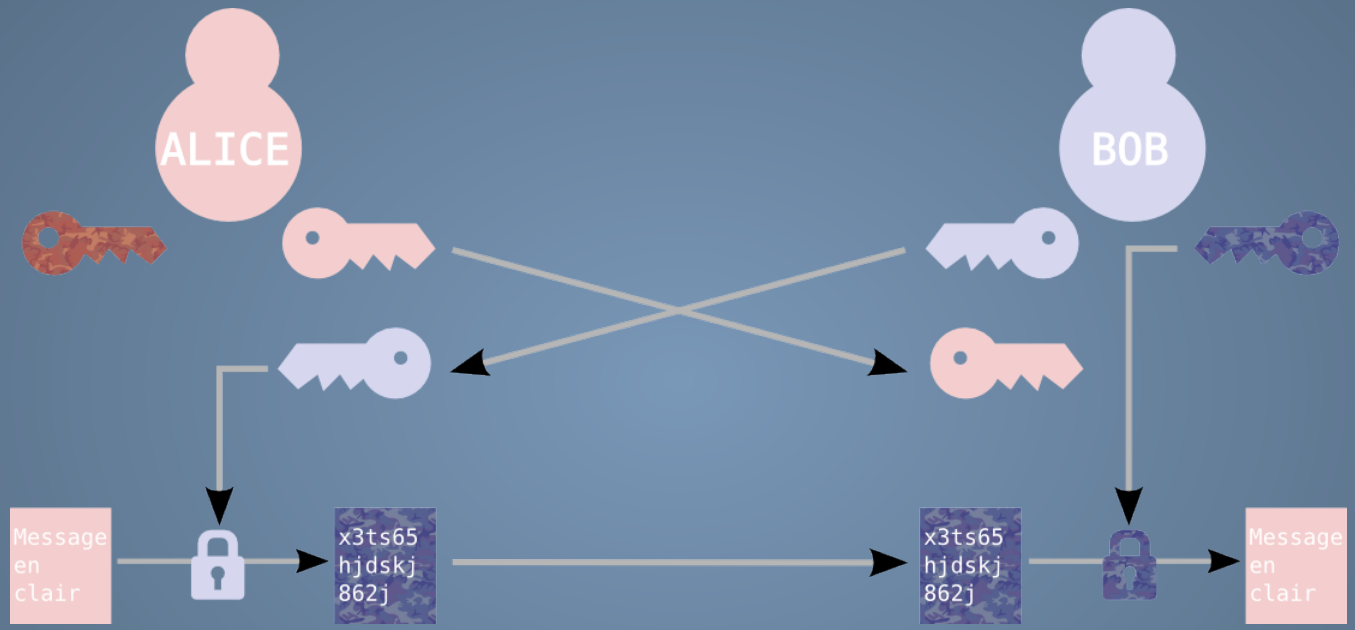


Chiffrement Asymétrique

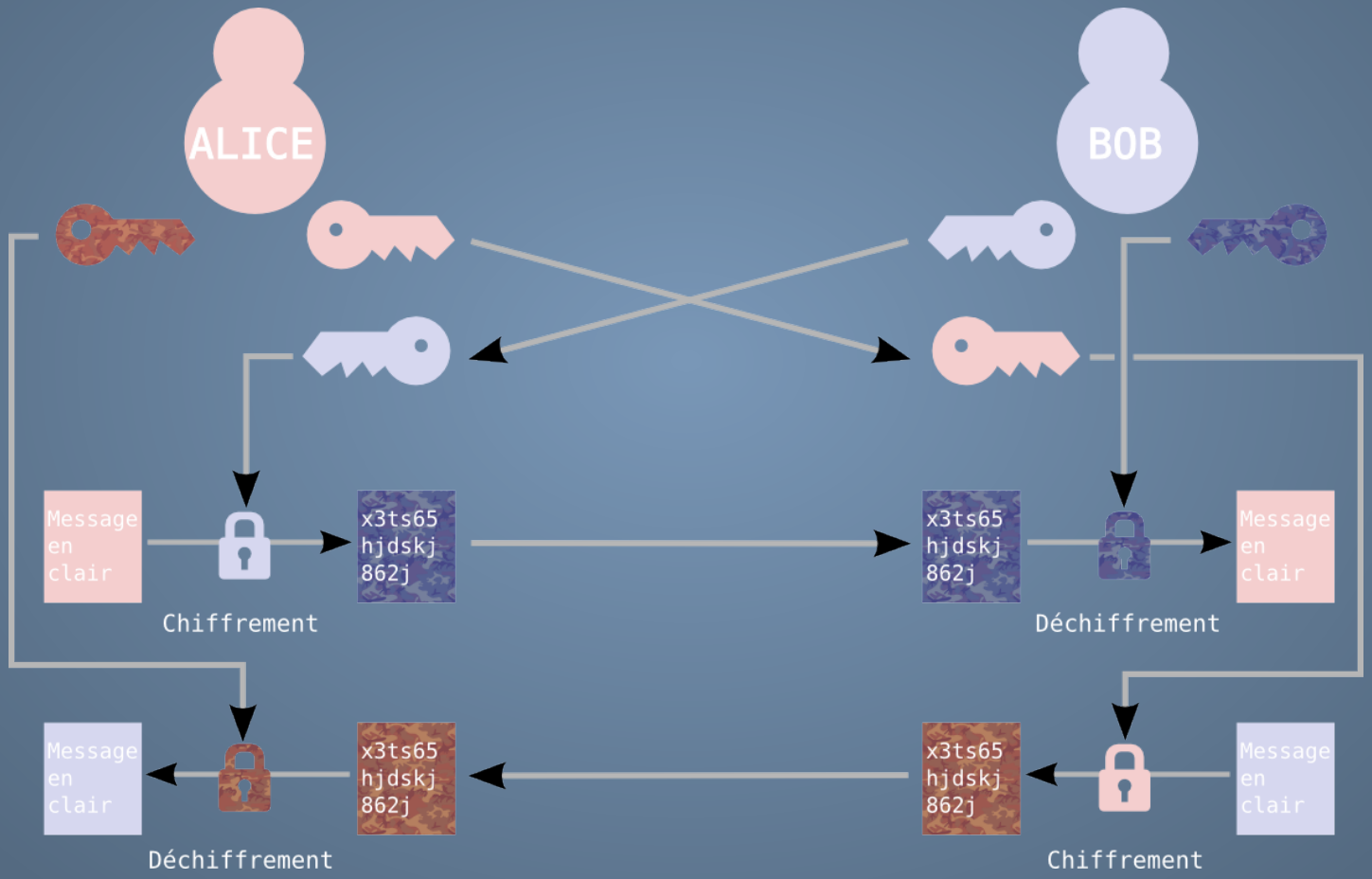
Chiffrement Asymétrique



Chiffrement Asymétrique



Chiffrement Asymétrique



Chiffrement Asymétrique : RSA

Le cryptosystème RSA

- Inventé en 1977 par Ron Rivest, Adi Shamir, and Leonard Adleman
- Clé de taille 1024 à 4096 bits

Principe	**Exemple**
1 : Trouver p et q premier entre eux	$p = 61$, $q = 53$
2 : Calculer $n = p * q$	$n = 61 * 53 = 3233$
3 : Calculer $\phi(n) = (p-1)(q-1)$	$\phi(n) = (61-1)(53-1) = 3120$
4 : Trouver $1 < e < \phi(n)$ premier avec $\phi(n)$	$e = 17$ premier avec 3120
5 : Calculez d tel que $d \equiv e^{-1} \mod \phi(n)$	$d = 2753$
• La clé publique est le couple (e, n) $c(m) = m^e \mod n$	$pub = (17, 3233)$ $c(m) = m^{17} \mod 3233$
• La clé privée est le couple (d, n) $m(c) = m^d \mod n$	$priv = (2753, 3233)$ $m(c) = m^{2753} \mod (3233)$

Le cryptosystème RSA

Robustesse

- Très difficile de factoriser un produit de nombre premier (très coûteux !)
- La meilleure cryptanalyse a réussi à cracker une seule clé de 768 bits (en plusieurs mois !)

Limitations

- Mécanisme de création des clés est long
- Chiffrement/Déchiffrement coûteux

Standards actuels

- RSA-OAEP
- RSASSA-PSS

Objectifs de sécurité

Confidentialité : Je veux des messages secrets

Intégrité : Je veux être sur que les données n'ont pas été modifiées

Fonctions de hashage : Intégrité

Une fonction de hashage

- permet de réduire un paquet de donnée de n'importe quelle taille en un paquet de donnée de taille fixe (le *hash*)
- une modification même mineure du paquet de donnée initial entraine un *hash* différent

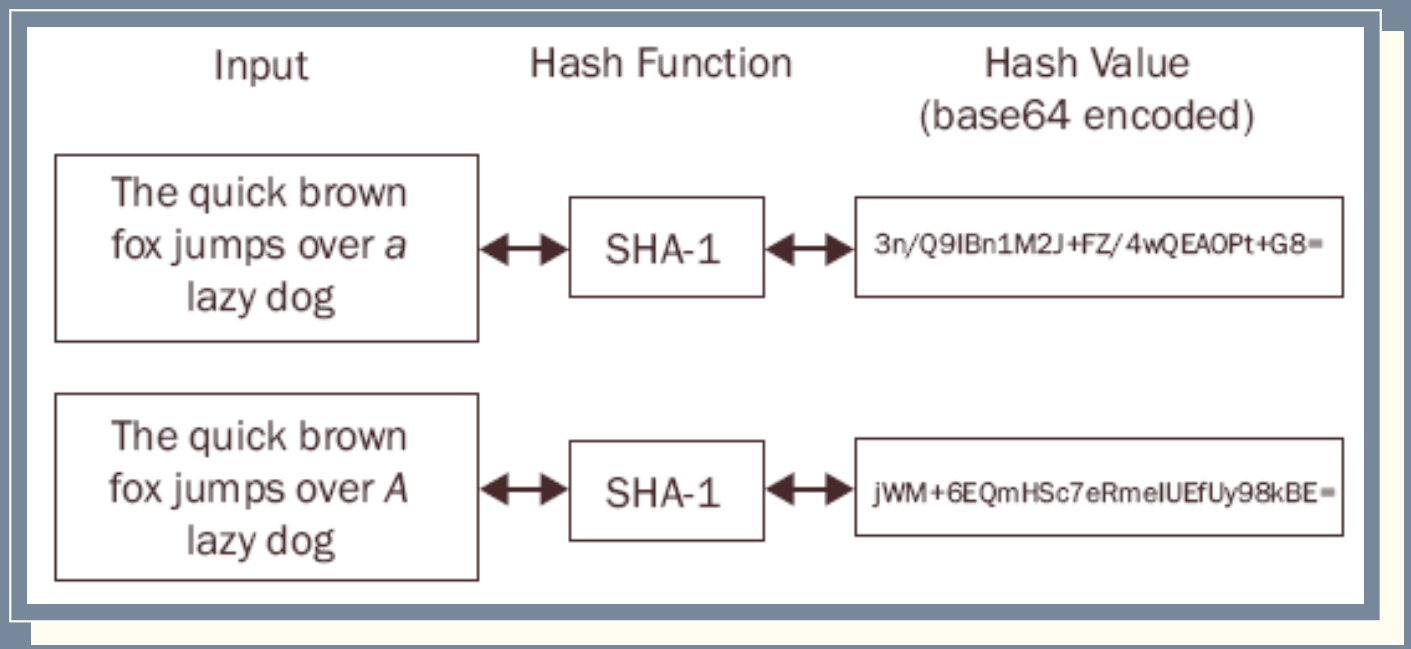


FIGURE: changement de hash après remplacement de 'a' par 'A'

Fonctions de hashage : propriétés

Les propriétés d'une bonne fonction de hashage :

1. La fonction doit être efficace
2. La fonction doit être publique
3. Il doit être difficile de trouver le message m à partir du *hash* $H(m)$
4. Il doit être difficile de trouver deux messages $m_1 \neq m_2$ tel que $H(m_1) = H(m_2)$

Quelques exemples :

1. md5sum
2. SHA

Fonction de hashage	SHA-1	SHA-224	SHA-256	SHA-384	SHA-512
Taille du *hash* (en bits)	160	224	256	384	512
Taille des données	$< 2^{64}$	$< 2^{64}$	$< 2^{64}$	$< 2^{128}$	$< 2^{128}$

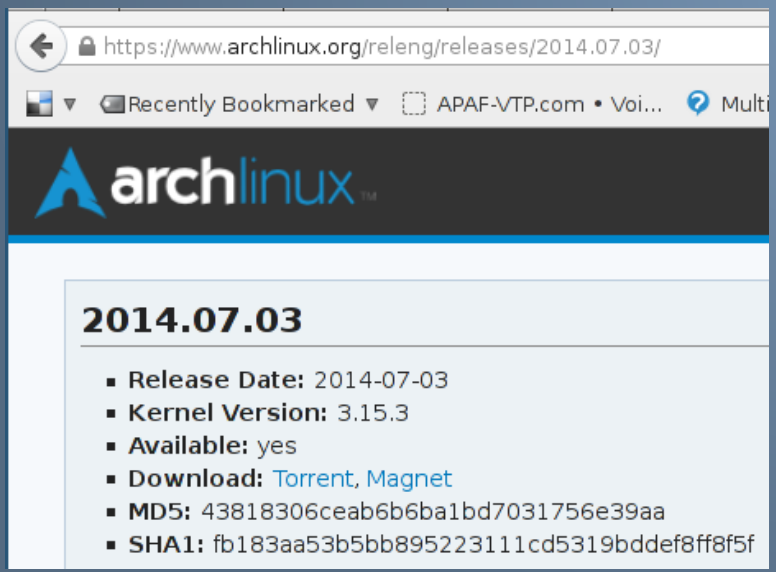
Fonctions de hashage : Applications

- Enregistrer des mots de passe dans une base de donnée

```
% cat /etc/pam.d/passwd
password  required  pam_unix.so sha256 shadow nullok

# cat /etc/shadow | grep root
root:$5$gNhcIicG$N/0aR2aBxlch3Qcy/ac/WHqswQyxwTY00RvvY2l:15783::::::
```

- Vérifier la bonne réception de données téléchargées




```
$ ls
archlinux-2014.07.03.iso

$ md5sum archlinux-2014.07.03.iso
43818306ceab6b6ba1bd7031756e39aa

$ sha1sum archlinux-2014.07.03.iso
fb183aa53b5bb895223111cd5319bddef8ff8f5f
```

Fonctions de hashage : Collisions

Il y a une collision si $m_1 \neq m_2$ mais que $H(m_1) = H(m_2)$

1. Peut il ne pas y avoir de collisions ? Il y a nécessairement des collisions puisque l'espace des *hash* possibles est plus petit que l'espace des messages possible.

2. Est-ce probable ? Paradoxe de la date d'anniversaire, quelle est la probabilité que au moins deux personnes parmis N aient le même anniversaire ? Il se trouve que c'est bien plus qu'on pourrait le croire.. en fait c'est pas vraiment un paradoxe, juste quelque chose de contre-intuitif

Fonctions de hashage : Paradoxe de la date d'anniversaire

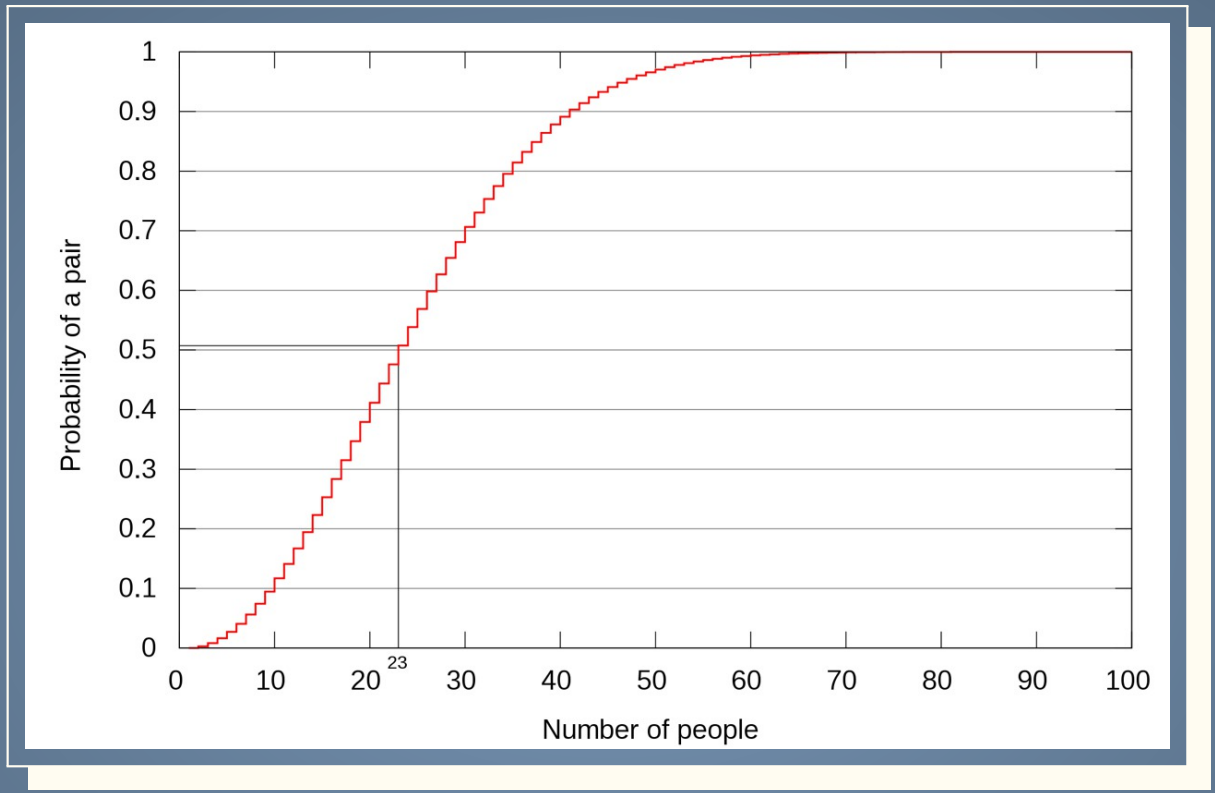


FIGURE: Probabilité de collision VS nombre de personnes

- Ce n'est pas la probabilité que quelqu'un qui rentre dans une pièce partage la même date d'anniversaire que quelqu'un d'autre
- C'est la probabilité que parmis toutes les paires de candidats possibles il y ait au moins une paire qui match

Limitation des fonctions de hashage

Limitation

- Le hash d'un message protège uniquement contre une modification accidentelle d'un message
- si un attaquant modifie le message, il peut très bien recalculer un hash pour ce nouveau message

Objectifs de sécurité

Confidentialité : Je veux des messages secrets
Intégrité : Je veux être sur que les données n'ont pas été modifiées
Authentification : Je veux savoir que je parle au bon correspondant

Message Authentication Code

- très similaire aux fonctions de hashage
- le MAC se base sur la donnée mais aussi sur un secret partagé
- protège contre la forge d'un message par un attaquant qui ne possède pas le secret

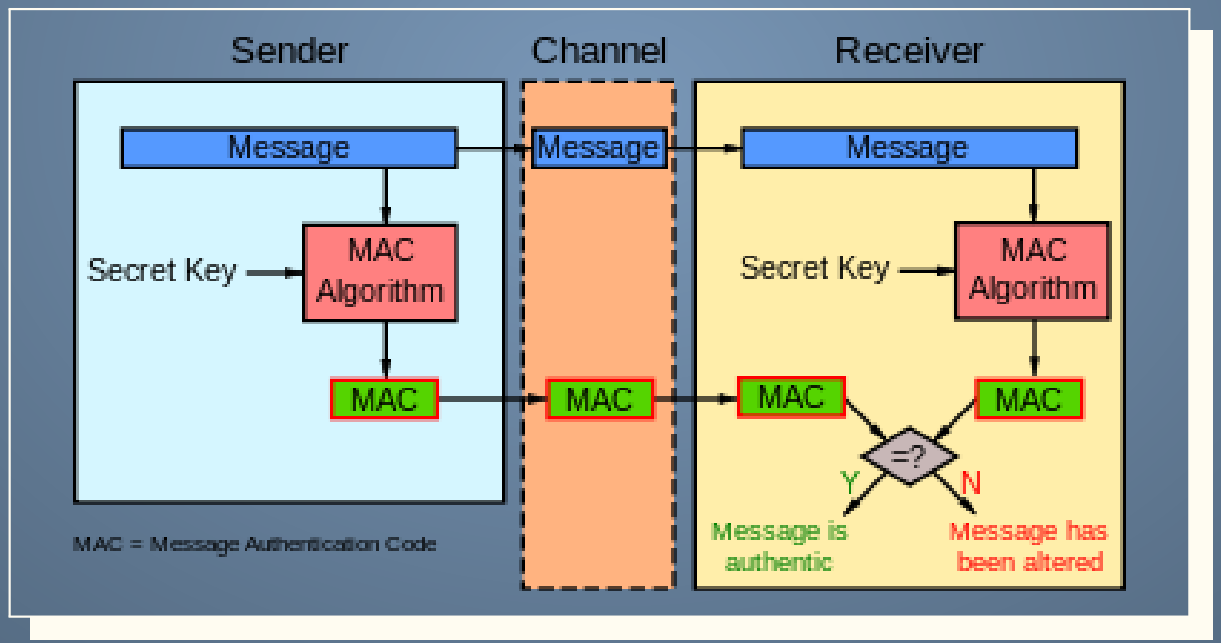
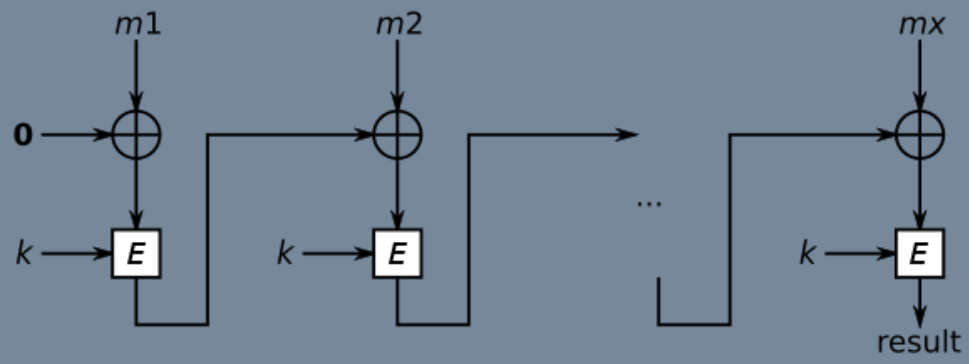


FIGURE: Schéma de principe d'un code d'authentification de message (source wikipedia)

Authentification : Message Authentication Code

Quelques Exemples

- HMAC : MAC calculé par fonction de hashage sur un message et un secret
  - HMAC-SHA1
  - HMAC-MD5
- CBC-MAC : MAC calculé pour un chiffrement par bloc en mode CBC



- OMAC, PMAC, etc.

Combiner Authentification et Chiffrement

- On peut combiner un message chiffré avec une MAC
  - AES-256-CTR + HMAC-SHA256
  - 3DES-CBC + CBC-MAC

- Comment les combiner ?

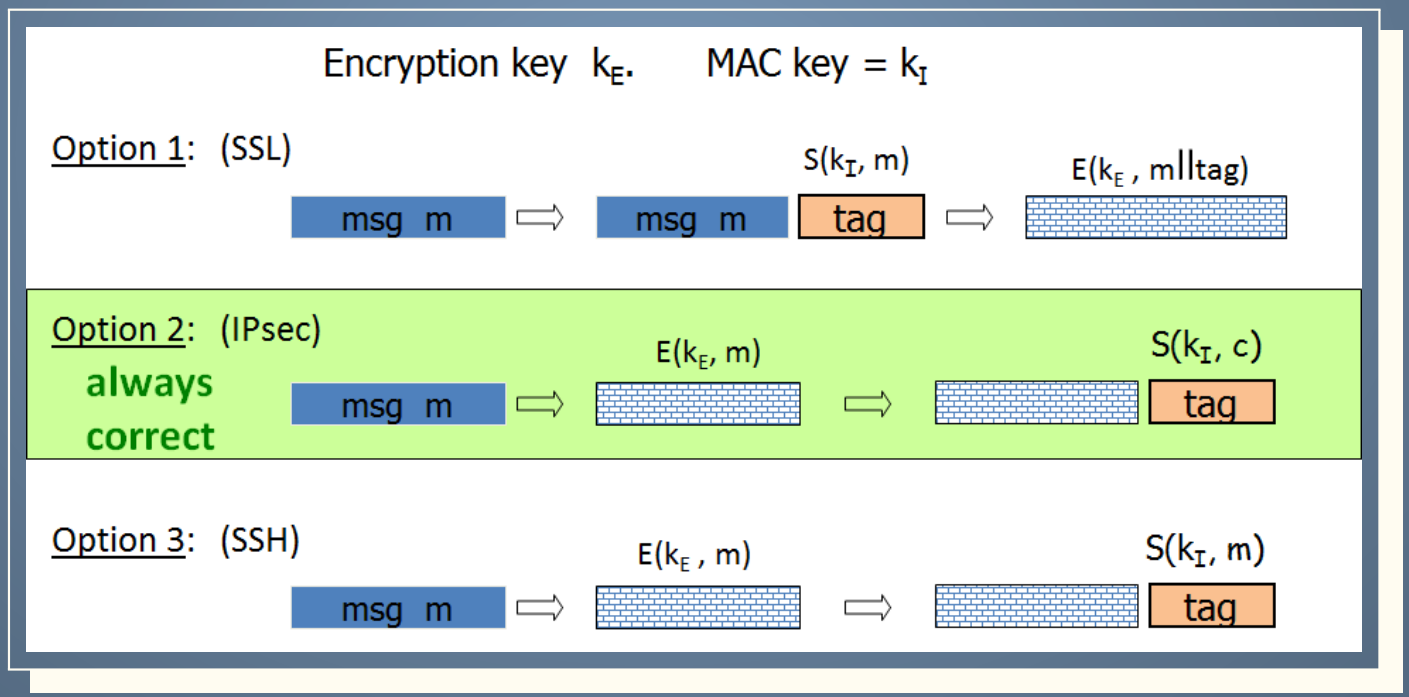


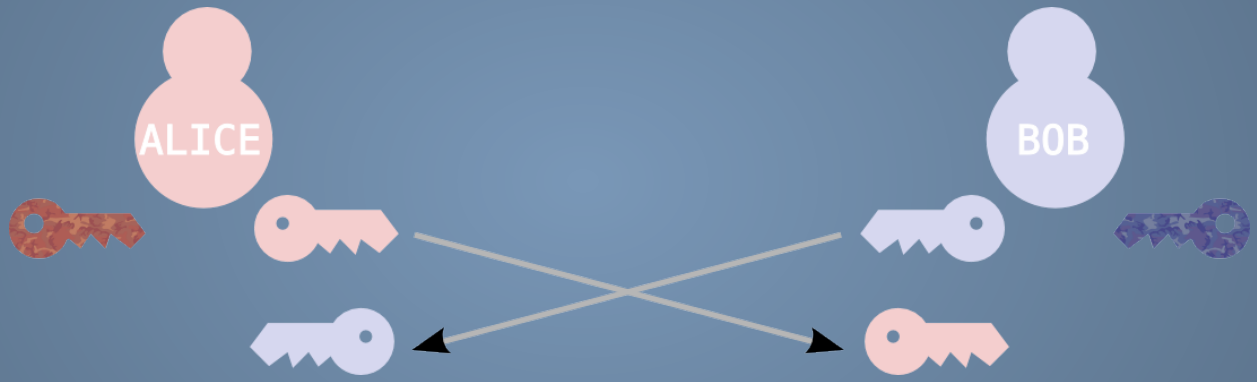
FIGURE: Chiffrer et ensuite MAC

Objectifs de sécurité

Confidentialité : Je veux des messages secrets
Intégrité : Je veux être sur que les données n'ont pas été modifiées
Authentification : Je veux vérifier que je parle au bon correspondant
Non-Répudiation : Je veux pouvoir Identifier un correspondant
i.e. Je peux prouver que je parlais bien avec lui et personne d'autre

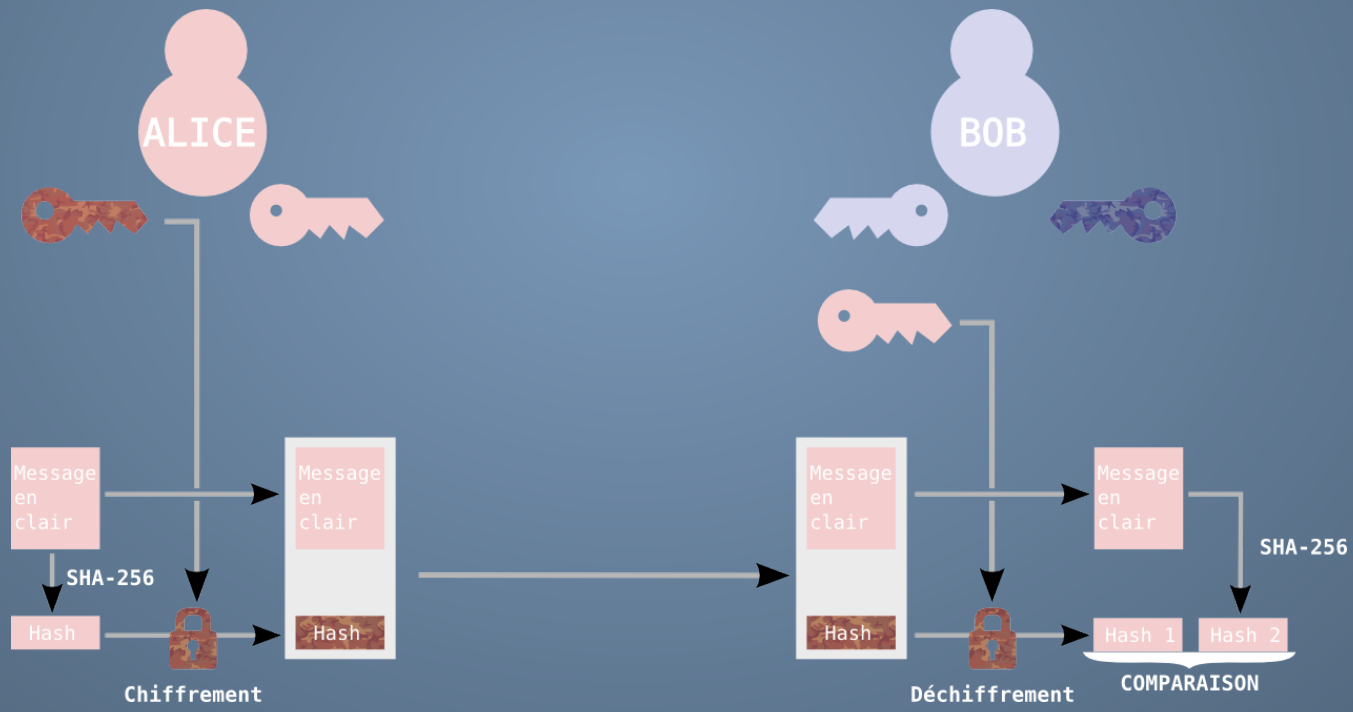
Non-répudiation : signature

- Possible grâce au chiffrement asymétrique
  - Cryptographie symétrique : n'importe qui possédant la clé peut envoyer des messages (pas de non-répudiation)
  - Cryptographie asymétrique : une paire de clé par correspondant
- Signature Numérique



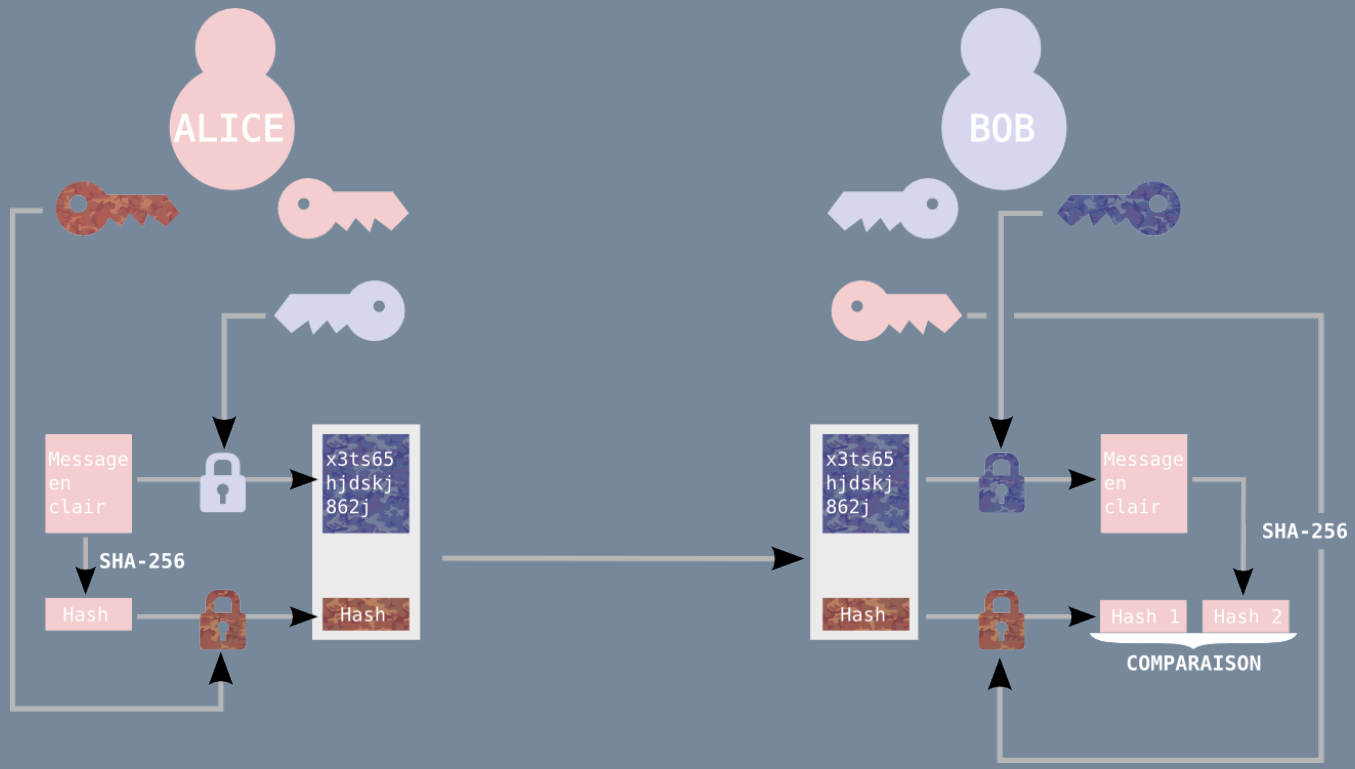
Non-répudiation : signature

- Possible grâce au chiffrement asymétrique
  - Cryptographie symétrique : n'importe qui possédant la clé peut envoyer des messages (pas de non-répudiation)
  - Cryptographie asymétrique : une paire de clé par correspondant
- Signature Numérique



Combiner Signature et Chiffrement : Un système parfait ?

Confidentialité, Intégrité, Authenticité et Non-répudiation



Objectifs de sécurité

Confidentialité : Je veux des messages secrets
Intégrité : Je veux être sur que les données n'ont pas été modifiées
Authentification : Je veux vérifier que je parle au bon correspondant
Non-Répudiation Je veux pouvoir Identifier un correspondant

Objectifs	Hash	MAC	Signature
Intégrité	Oui	Oui	Oui
Authenticité	Non	Oui	Oui
Non-répudiation	Non	Non	Oui
Type de clé	–	Symétrique	asymétrique

Est-ce que cela suffit ?

Objectifs de sécurité

Confidentialité :	Je veux des messages secrets
Intégrité :	Je veux être sur que les données n'ont pas été modifiées
Authentification :	Je veux vérifier que je parle au bon correspondant
Non-Répudiation :	Je veux pouvoir Identifier un correspondant
Clé de session :	Une clef de chiffrement différente pour chaque message
Échange de clé :	S'accorder avec la correspondance sur les clés à utiliser

Clé de session

Méthode RSA

1. Générer aléatoirement la clé de session
2. La chiffrer avec la clé publique du destinataire
3. Signer la donnée chiffrée avec la clé privée de l'émetteur
4. Goto 1

Clé de session

Méthode RSA

1. Générer aléatoirement la clé de session
2. La chiffrer avec la clé publique du destinataire
3. Signer la donnée chiffrée avec la clé privée de l'émetteur
4. Goto 1

Problème

- Si un jour ma clé privée est découverte et que mes communications étaient enregistrées (coucou la NSA), on peut déchiffrer les clés de session et donc le contenu des messages de la session

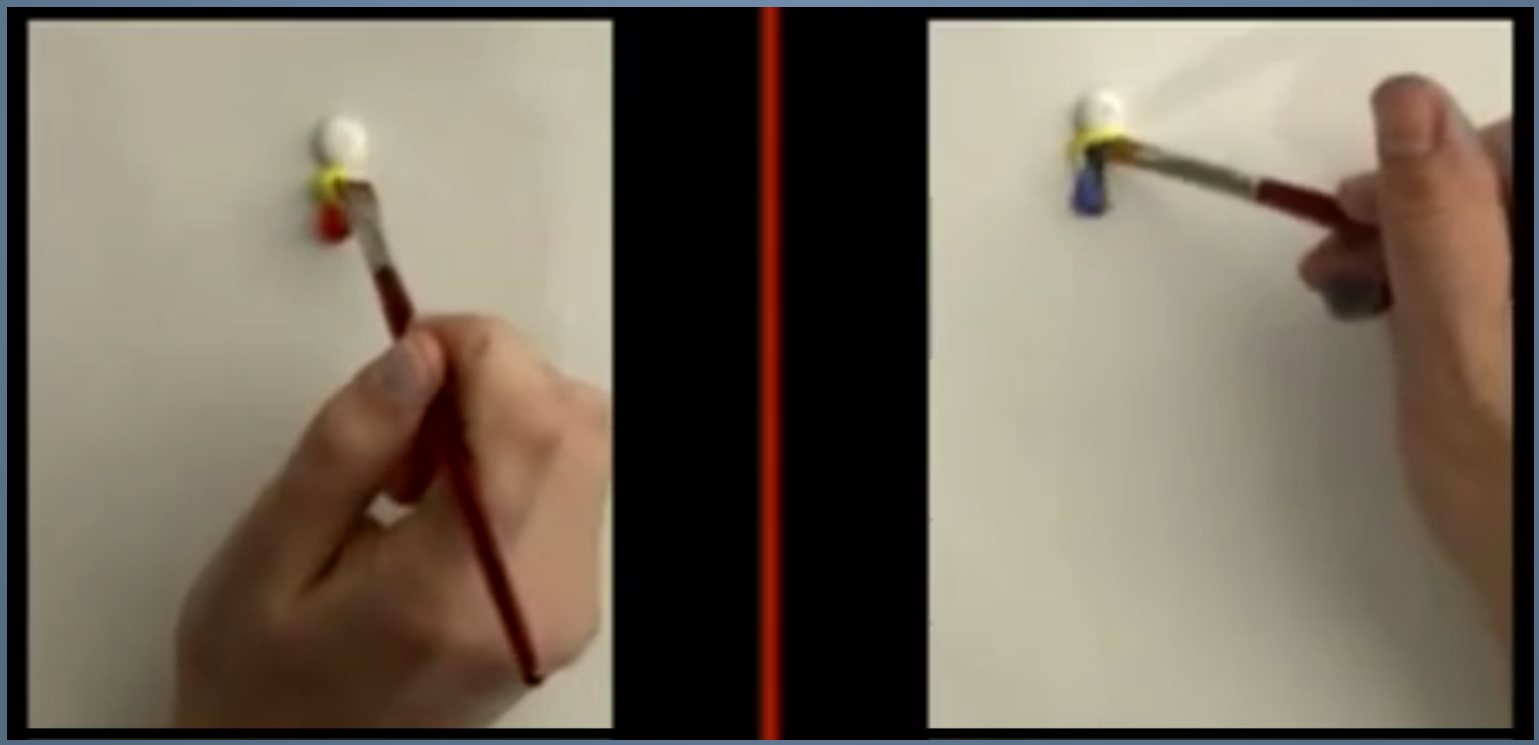
Objectifs de sécurité

Confidentialité :	Je veux des messages secrets
Intégrité :	Je veux être sur que les données n'ont pas été modifiées
Authentification :	Je veux vérifier que je parle au bon correspondant
Non-Répudiation :	Je veux pouvoir Identifier un correspondant
Perfect Forward Secrecy :	La compromission de la clé privée ne compromet pas les clés de sessions

Perfect Forward Secrecy

Diffie Hellman

- Permet à deux correspondants de se mettre d'accord sur un même nombre sans qu'une troisième personne ne puisse découvrir le nombre, même en ayant écouté tout les échanges



Perfect Forward Secrecy

Off-the-record

- Chiffrement pour les communications instantannées (irc, jabber, google talk, etc.)
- L'objectif est de fournir un système qui imite une réelle conversation orale privée
- utilise une combinaison de Diffie-Hellman, AES et SHA1
  - Chiffrement symétrique AES pour envoyer les messages de façon confidentiel
  - Authentification par secret partagé (comparaison d'empreinte)
  - SHA1 pour assurer l'intégrité de la communication
  - La clé AES change à chaque message grâce à Diffie Hellman assurant une forward secrecy
- Les messages ne sont pas signé et donc OTR permet une deniable authentication (cela s'oppose à la non-répudiation)
- se présente sous la forme d'un plugin pour pidgin/jabber

Objectifs de sécurité

Confidentialité :	Je veux des messages secrets
Intégrité :	Je veux être sur que les données n'ont pas été modifiées
Authentification :	Je veux vérifier que je parle au bon correspondant
Non-Répudiation :	Je veux pouvoir Identifier un correspondant
Perfect Forward Secrecy :	La compromission de la clé privée ne compromet pas les clés de sessions
deniable authentication :	Je peux nier avoir eu cette conversation
asynchrone forward secrecy :	forward secrecy avec une communication asynchrone

Asynchrone Forward Secrecy

Axolotl Ratchet

- Système récent développé par Whisper System pour **TextSecure** (Chiffrage SMS)
- forward secrecy dans un environnement asynchrone (Mail, SMS, etc.)
- Diffie Hellman utilisé dans un mode "envoyer/recevoir" au lieu de "diffuser/recevoir/envoyer".

Objectifs de sécurité

Confidentialité :	Je veux des messages secrets
Intégrité :	Je veux être sur que les données n'ont pas été modifiées
Authentification :	Je veux vérifier que je parle au bon correspondant
Non-Répudiation :	Je veux pouvoir Identifier un correspondant
Perfect Forward Secrecy :	La compromission de la clé privée ne compromet pas les clés de sessions
deniable authentication :	Je peux nier avoir eu cette conversation
asynchrone forward secrecy :	forward secrecy avec une communication asynchrone
données locales :	Les données locales sont elles aussi confidentielles

Données Locales

- Chiffrage du disque dur
  - TrueCrypt ? !
  - Luks
- Chiffrage des fichiers
  - GnuPG
  - OpenSSL
- Chiffrage d'une base de donnée
  - SQLCipher (256-bit AES, chiffrement transparent)

Objectifs de sécurité

Confidentialité :	Je veux des messages secrets
Intégrité :	Je veux être sur que les données n'ont pas été modifiées
Authentification :	Je veux vérifier que je parle au bon correspondant
Non-Répudiation :	Je veux pouvoir Identifier un correspondant
Perfect Forward Secrecy :	La compromission de la clé privée ne compromet pas les clés de sessions
deniable authentication :	Je peux nier avoir eu cette conversation
asynchrone forward secrecy :	forward secrecy avec une communication asynchrone
données locales :	Les données locales sont elles aussi confidentielles
Stockage des clés :	Ne pas stocker les clés en clairs

Problème de stockage des clés : Les générer par mot de passe ?

Key Derivation Function

- Algorithme conçu pour générer une clé à partir d'un mot de passe
- Conçu pour s'exécuter lentement afin de déjouer les attaques par brute-force

Quelques KDF

- PBKDF2 (Password-Based Key Derivation Function 2)
  - c'est juste un hash qui tourne en boucle
  - `DK = PBKDF2(Hash, Password, Salt, iterations, desiredOutputLen)`
  - Exemple : WPA2 utilise `DK = PBKDF2(HMAC-SHA1, passphrase, ssid, 4096, 256)`
- scrypt
  - consomme beaucoup de mémoire pour s'exécuter
- Password Hashing Competition
  - chercher des nouveaux KDFs
  - résultats fin 2015

Objectifs de sécurité

Confidentialité :	Je veux des messages secrets
Intégrité :	Je veux être sur que les données n'ont pas été modifiées
Authentification :	Je veux vérifier que je parle au bon correspondant
Non-Répudiation :	Je veux pouvoir Identifier un correspondant
Perfect Forward Secrecy :	La compromission de la clé privée ne compromet pas les clés de sessions
deniable authentication :	Je peux nier avoir eu cette conversation
asynchrone forward secrecy :	forward secrecy avec une communication asynchrone
données locales :	Les données locales sont elles aussi confidentielles
Stockage des clés :	Ne pas stocker les clés en clairs
Usabilité :	Comment échanger des clés ?

Échanger des clés : Les Key Signing Party

FIGURE: une key-signing-party à Berlin

FIGURE: vérifier une clé peut être fastidieux

Échanger des clés : Les Fingerprint

- Une clé est trop fastidieux à vérifier
- On compare plutôt le fingerprint de la clé
- Fingerprint est un hash de la clé (MD5, SHA-256, etc.)

FIGURE: fingerprint de OTR

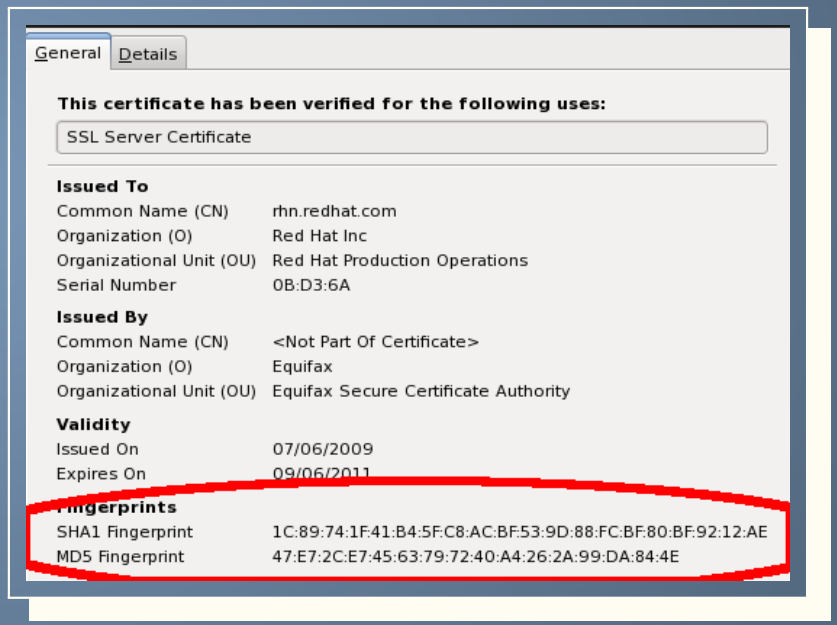


FIGURE: fingerprint d'un certificat SSL (Firefox)

Échanger des clés : Les Fingerprint visuels

```
# ssh blah@10.0.1.2
The authenticity of host '10.0.1.2 (10.0.1.2)' can't be established.
RSA key fingerprint is 59:dd:fb:b3:6f:b1:85:30:0a:c2:01:d6:4a:fa:09:19.
+--[ RSA 2048]----+
|    oo           |
|  E.. o    . .   |
|   = o .  . . .  |
|  + . o .o  o  . |
|   o . .S. . o.. |
|    o     .   .o.|
|               .=|
|               .+|
|              oo|
+-----------------+
Are you sure you want to continue connecting (yes/no)?
```

FIGURE: fingerprint visuel de Shs

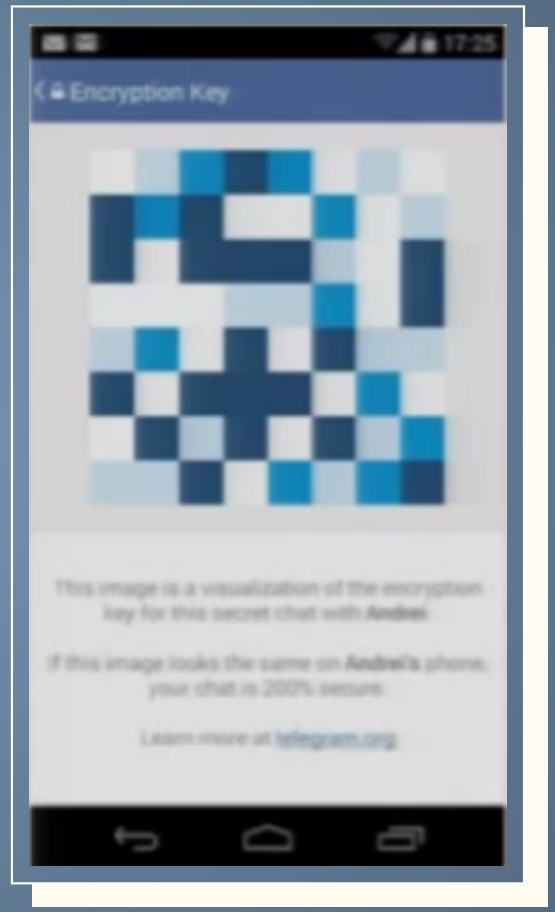


FIGURE: fingerprint pour Telegram (Android APP)