

# Histoire de la cryptographie de la première guerre mondiale à Internet

cryptographie +  
cryptanalyse = cryptologie

Prof. Jacques Savoy

Université de Neuchâtel



# Plan

- 1. Cryptographie classique**
2. La première guerre mondiale
3. La machine Enigma
4. Cryptographie à clés publiques (dès 1970)  
Applications à Internet / Web

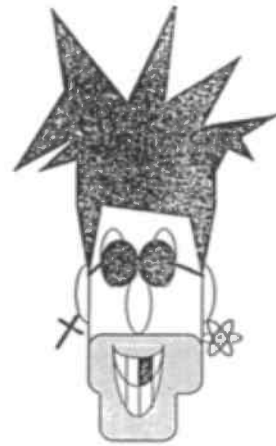
# Les besoins ...

1. Assurer une communication confidentielle  
(militaires, diplomates, amoureux, ...)

mais aussi ...

2. Authentifier une personne (carte crédit)
3. Signature (numérique, électronique)

# Le problème pour Anne et Bob

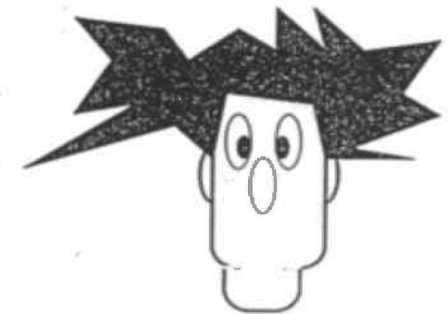


Charles

Anne



Bob



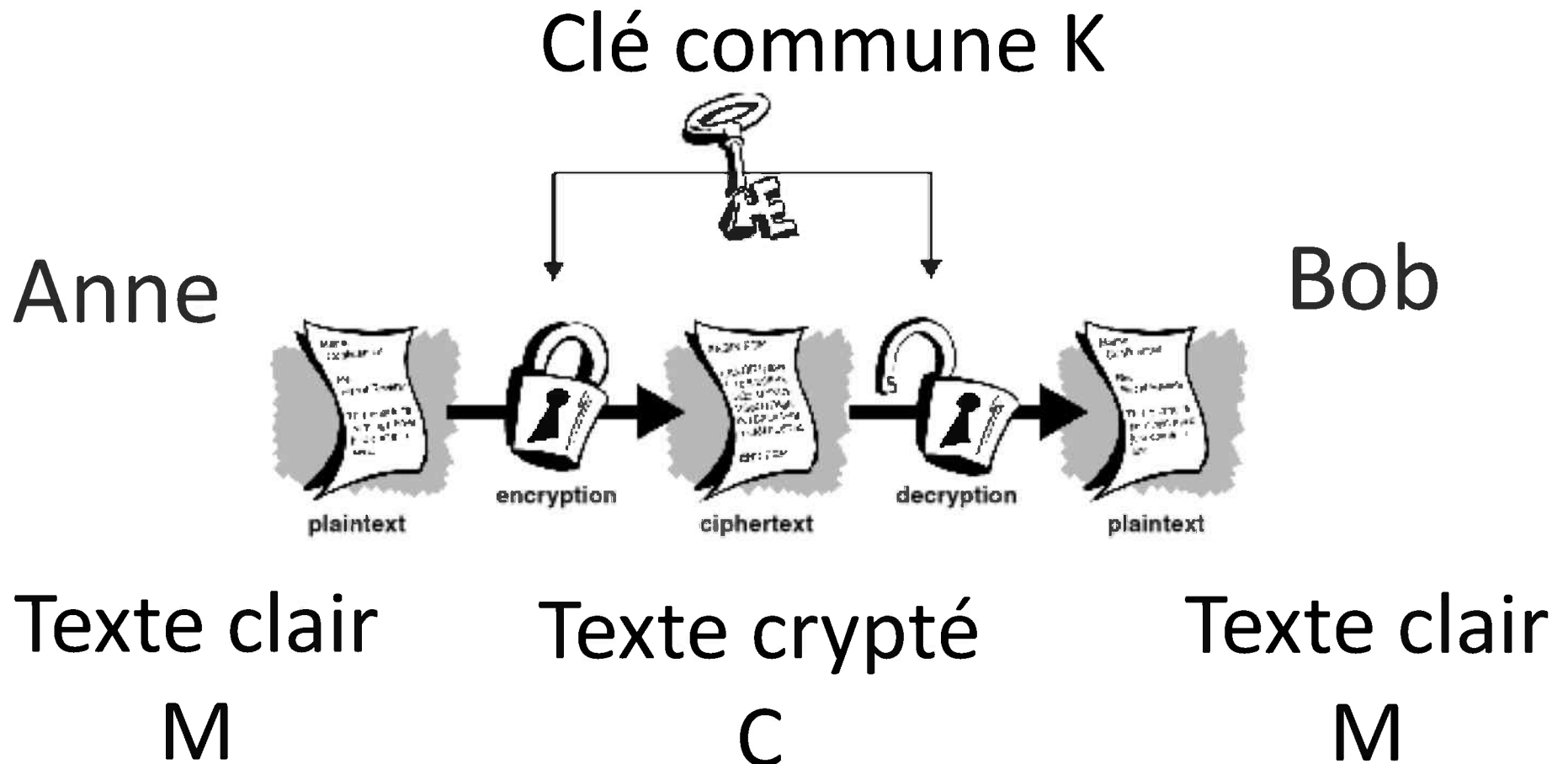
← ♀ + ♂ + || + Y ?

♀ + Y + Y + Y = ♀ ? →

← ♀ + Y + Y + ♂ = & !



# Cryptographie classique



# Techniques de cryptographie

Pour aider Anne et Bob, nous pouvons nous appuyer sur ...

1. Stéganographie (pas vraiment efficace)
2. Substitution
3. Transposition

# Stéganographie

Stéganographie

le message est dissimulé (encre invisible)

Par exemple

Dissimulation du n

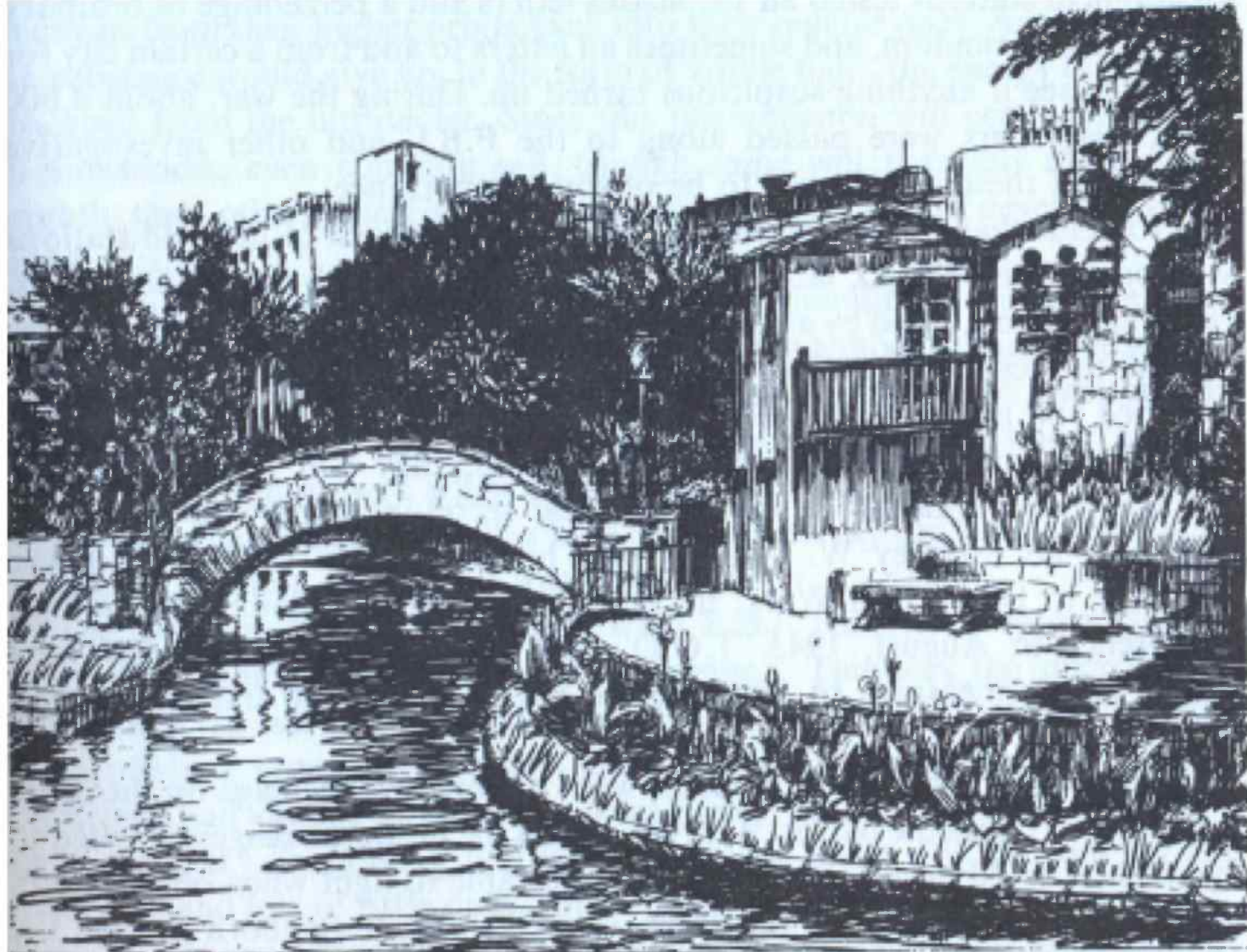
Dissimulation d'im



# Stéganographie

Le message est  
dissimulé dans  
un dessin

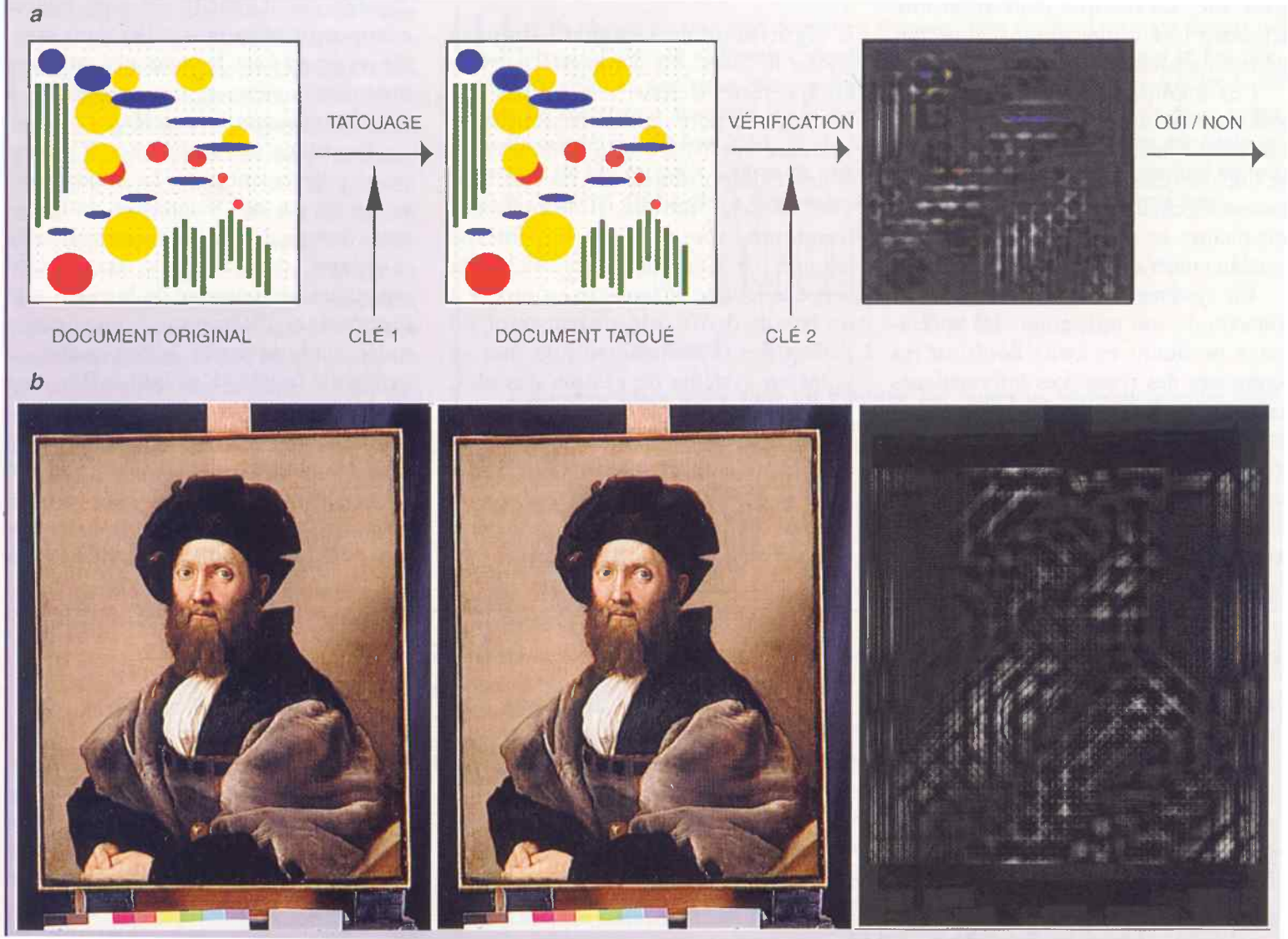
Journaux  
britanniques au  
XIXe siècle





# Steganographie

Mais très utile  
sur les  
productions  
numériques  
(musique,  
video,  
images, etc.)



# Substitution

Jules César (guerre des Gaules)

1. Ecrire dans une langue étrangère
2. Substitution simple

A --> D  
B --> E  
C --> F  
...

VENI, VIDI, VICI →  
YHOL, YLGL, YLFL



# Substitution

Moyen simple. Sécuritaire ?

Encore utilisé entre 1880 et début du XXe siècle  
(Règle de St-Cyr)

Outil afin de simplifier le travail d'encryptage et de  
décryptage

ABCDEFGHIJKLMNOPQRSTUVWXYZ

abcdefghijklmnopqrstuvwxyz

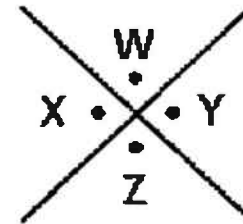
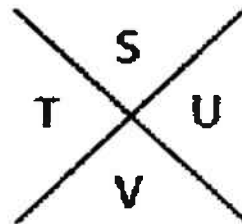
# Substitution


Substitution plus  
mystérieuse !

Pas des lettres  
mais des symboles

A	B	C
D	E	F
G	H	I

J	K	L
M	N	O
P	Q	R




a = 

b = 

:

:

z = 



# Autres exemples

Exemple: Charlemagne  
(800) et les émigrés  
royalistes français  
(1793)

a	𐌆	g	𐌈	n	𐌉	t	𐌊
b	𐌋	h	𐌌	o	𐌍	u	𐌎
c	𐌏	i	𐌐	p	𐌑	x	𐌒
d	𐌓	k	𐌔	q	𐌕	y	𐌖
e	𐌗	l	𐌘	r	𐌙	z	𐌚
f	𐌛	m	𐌜	s	𐌝	&	𐌞

## CHIFFRE DES ÉMIGRÉS

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	X	Y	Z
d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	x	y	z	a	b	c
22					26						30					34					38			
23					27						31					35					39			
24					28						32					36					40			
25					29						33					37					41			

ANJOU	aa	MARIGNY (Bernard de)	au
ARGENT	ab	MARINE	aw
ARRAS (Evêque d')	ac	NORMANDIE	ax
ARTOIS (Comte d')	ad	PARIS	ay
BERLIN	ae	PITT	az
BRETAGNE	af	POITOU	ba
CASTRIES (Maréchal de)	ag	RÉGENT (Monsieur le)	bb
CONDÉ (Prince de)	ah	REINE (La)	bc
ÉMIGRÉS	ai	ROI (Le feu)	bd
FLACHSLANDEN (Baron de)	ak	ROMANZOFF	be
GASTON	al	RUSSIE	bf
GRENVILLE (Lord)	am	SAINTONGE (La)	bg
HARCOURT (Duc d')	an	SERENT (Duc de)	bh
HECTOR (Comte d')	ao	SERENT (Vicomte de)	bi
HERMANN	ap	TOURS (Archevêque de)	bk
HERVILLY (Comte d')	aq	VAUGIRARD (de)	bl
JAUCOURT (Marquis de)	ar	VIENNE	bm
LONDRES (Cour de)	as	WORONZOFF	bn
LOUIS XVII	at		



# Substitution

Table des codes

Chaque mot (ou chaque mot important) est remplacé par un autre mot ou un symbole. Par exemple :

roi -> centre

argent -> tulipe

Espagne -> orange

France -> gourmand

**Le centre gourmand  
manque de tulipes.**

Mais changement de  
clés plus difficile !

# Substitution

Parue dans la presse autrichienne (1917)

« Suisse, 35 ans, tenu au courant des livres et correspondance, plusieurs années chef de service à Vienne, références de premier ordre. »

« 35<sup>e</sup> division partie de Vienne pour le front d'Italie »



# Principe de Kerchoffs (1883)

1. Système doit être indéchiffrable
2. La force ne doit pas résider dans l'algorithme de chiffrement (ou la machine)
3. La clé doit être simple à mémoriser, sans notes écrites, et facile à changer
4. Le système doit être portatif avec un seul opérateur
5. D'usage facile (pas de stress)
6. Applicable au télégraphe

# Principe de Kerchoffs (1883)

« Je ne connais qu'une manière de retarder une division de cavalerie. C'est de l'obliger à chiffrer.

Général français en 1937

« Nicht Amiens, Dunkerque; nicht Amiens, Dunkerque. »

(sur les ondes en mai 40)

# Sécurité

Substitution simple est-elle sécuritaire ?

Oui car le nombre de clés est très important.

26 choix pour la première,

25 pour la deuxième,

24 pour la troisième, ...

Soit au total  $26! = 26 \cdot 25 \cdot 24 \cdot \dots \cdot 2 =$

403 291 461 126 605 635 584 000 000

# Sécurité

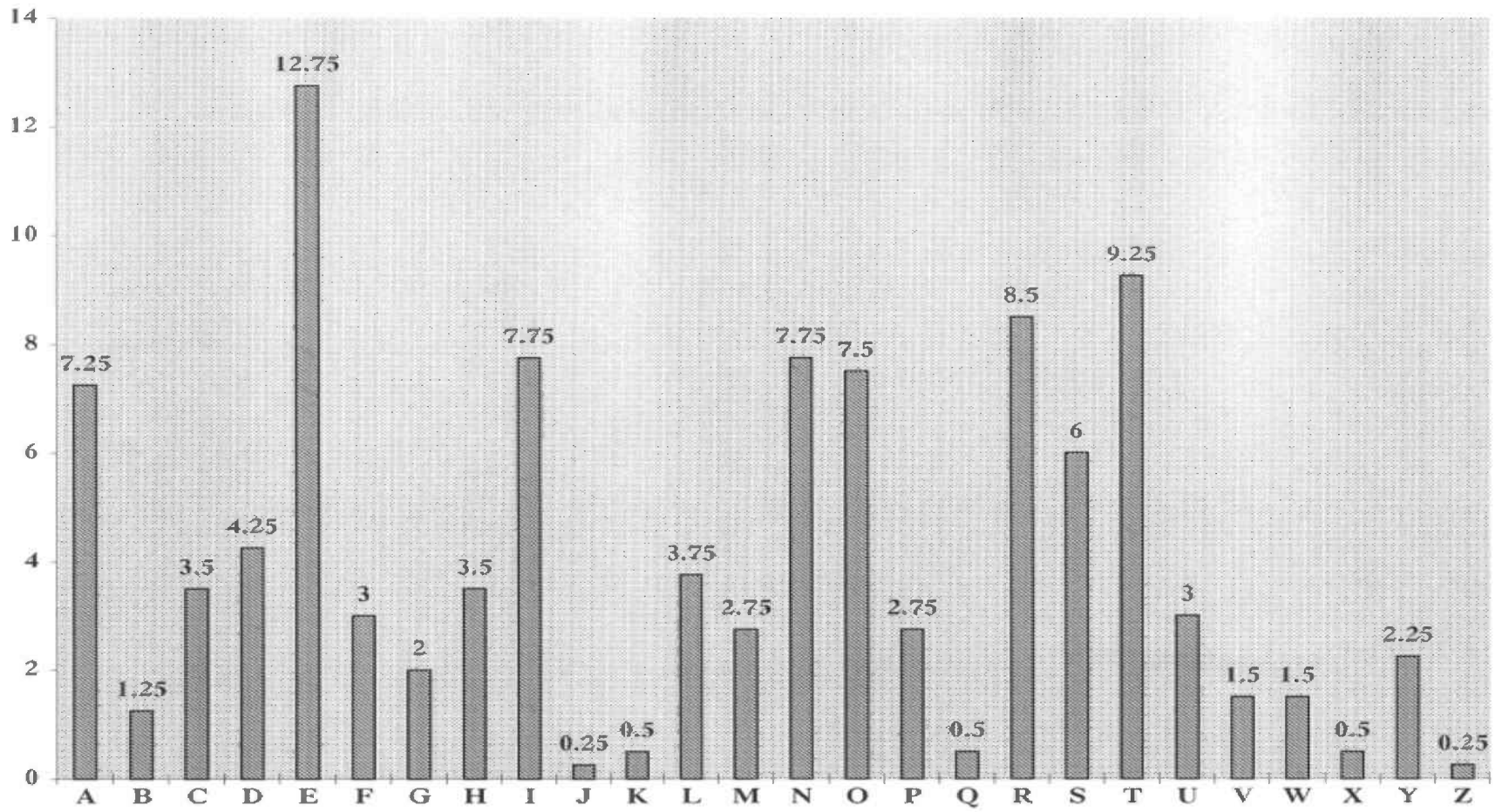
Attaque par l'analyse des fréquences

Al-Kindi IX<sup>e</sup> siècle

Toute langue naturelle comprend des régularités...

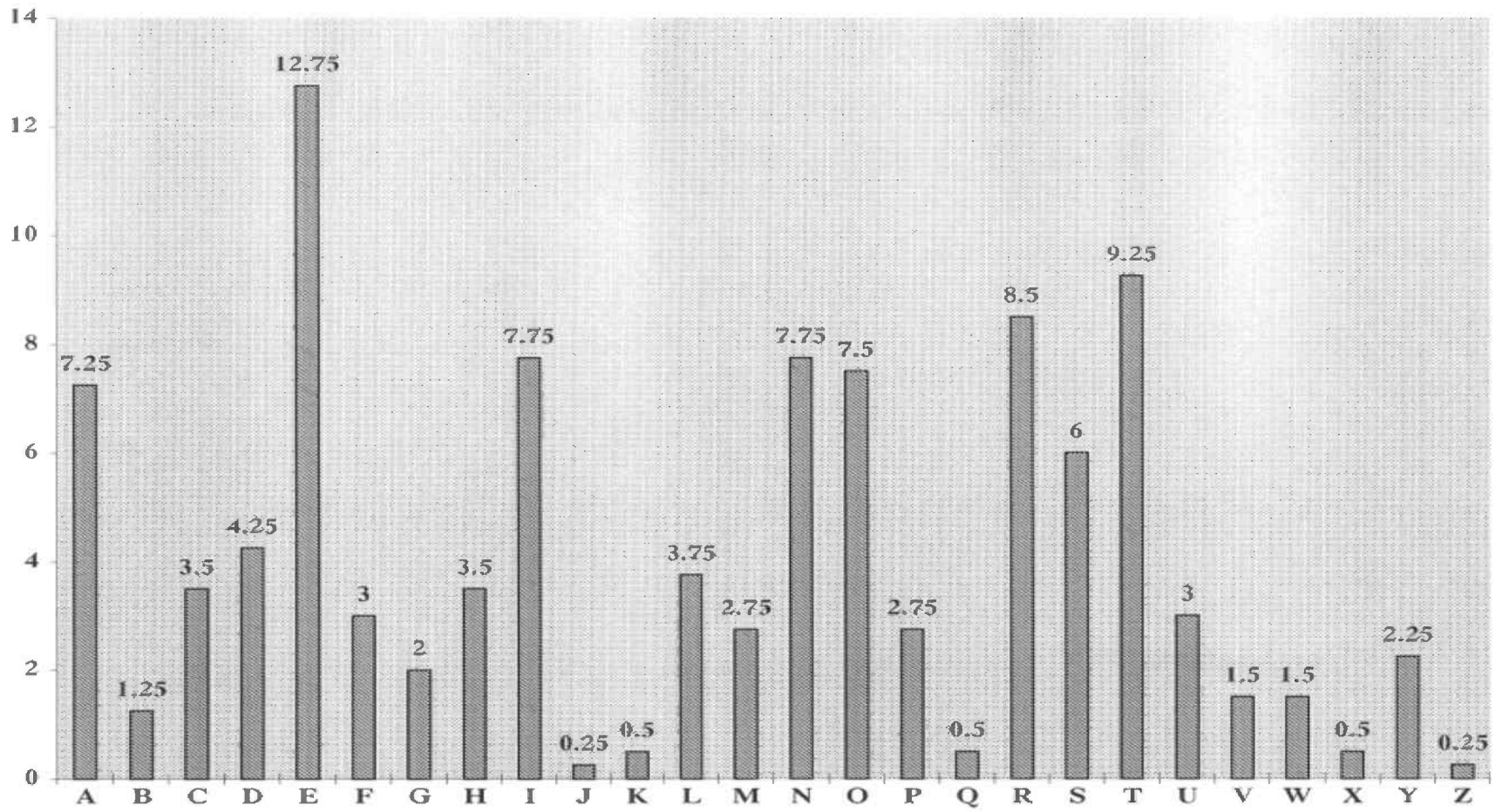
# Cryptanalyse

Attaque efficace par l'analyse des fréquences !



# Cryptanalyse

«uftu eft gsfrvfodft» à déchiffrer



# Cryptanalyse

Réponse «uftu eft gsfrvfodft»

**f** -> **e** (lettre la plus fréquente 5, donc e)

**u** -> **t** (lettre fréquente 2, donc t, r, n, o, i, a, s)

**t** -> **s** (lettre fréquente 2, donc r, n, o, i, a, s)

«test es gserveodes»

**e** -> **d** «test des gserveodes»

on essaie avec n, r, o, i, a ...

«test des frequences»

# Cryptanalyse

---

rang	mot	fréquence	fréq. rel.	fréq. cumul.
1	de	184'249	0.0576	0.0576
2	la	100'431	0.0314	0.0890
3	l	75'103	0.0235	0.1124
4	le	70'751	0.0221	0.1345
5	à	63'572	0.0199	0.1544
6	et	62'916	0.0197	0.1741
7	les	62'517	0.0195	0.1936
8	des	59'899	0.0187	0.2123
9	d	55'257	0.0173	0.2296
10	en	45'602	0.0143	0.2438



# Transposition

## Technique de la transposition

On ne remplace pas une lettre par une autre (ou un symbole) qui est toujours le même.

On perturbe l'ordre des lettres.

# Transposition

Dans ce cas, la lettre « a » sera chiffré par un « a » mais dans un désordre complet...

Le message à chiffrer « rendez-vous au port »  
On écrit le texte sous quatre colonnes (K=4)

1	2	3	4
<b>r</b>	<b>e</b>	<b>n</b>	<b>d</b>
<b>e</b>	<b>z</b>	<b>v</b>	<b>o</b>
<b>u</b>	<b>s</b>	<b>a</b>	<b>u</b>
<b>p</b>	<b>o</b>	<b>r</b>	<b>t</b>

# Transposition

1	2	3	4
<b>r</b>	<b>e</b>	<b>n</b>	<b>d</b>
<b>e</b>	<b>z</b>	<b>v</b>	<b>o</b>
<b>u</b>	<b>s</b>	<b>a</b>	<b>u</b>
<b>p</b>	<b>o</b>	<b>r</b>	<b>t</b>

Clé K pour émettre : 3 1 4 2

Première ligne : nvar

C = nvar reup dout ezso  
= nvarreupdoutezso

# Transposition

Par exemple, le Louchébem

On prend un mot (*fou*) et on applique les transformations suivantes :

1. la consonne du début va à la fin      fou -> ouf
2. placez un « L- » au début      Louf
3. ajoutez « -em » ou « -oque » à la fin. Loufoque

# Substitution polyalphabétique

Progrès notable avec Blaise de Vigenère (XVI<sup>e</sup> siècle)

Une lettre peut être représentée dans le texte chiffré par toutes les autres lettres, selon une clé de chiffrement (*polyalphabétique*)



# Substitution polyalphabétique

Pour la lettre « B » dans la clé, le décalage dans l'alphabet est de +1 (Modèle de J. César)

Si j'ai un « R » dans le texte clair et « B » dans la clé, j'ajoute +1 à « R » et je trouve « S »

Si j'ai un « E » dans le texte clair et « A » dans la clé, j'ajoute +0 à « E » et je trouve « E »

clair M =	R	E	N	A	I	S	S	A	N	C	E	...
clé K =	<b>B</b>	<b>A</b>	<b>C</b>	B	A	C	B	A	C	B	A	...
chiffrement C =	S	E	P	B	I	U	T	A	P	D	E	...

# En résumé

Comme solution pratique, on proposera d'utiliser les deux approches, soit

- la substitution (changer une lettre par une autre)
- la transposition (perturber l'ordre des lettres)

C'est l'état des connaissances au début du XX<sup>e</sup> siècle.

On admet que le chiffrement par substitution (*polyalphabétique*) est *sécuritaire, indéchiffrable*.

# Plan

1. Cryptographie classique
- 2. La première guerre mondiale**
3. La machine Enigma
4. Cryptographie à clés publiques (dès 1970)  
Applications à Internet / Web



# Première guerre mondiale

Contexte différent de la deuxième guerre mondiale (querelle de famille entre *Georges V*, *Nicolas II* et *Guillaume II*).

Pas de service de décryptage le 28/7/14 (sauf en France)



# Première guerre mondiale

La cryptographie devient une arme.

Peut-on faire quelque chose ?

1. On transmet en clair (armée russe) : progrès ?  
(ou sous le stress)
2. Analyse de trafic (doigté de l'opérateur)  
(expéditeur/destinataire/date/longueur/préambule)
3. Gestion des clés  
1914: changement trimestriel  
1918: quotidien

# Première guerre mondiale

Crypter les communications ?

1. Téléphone ?
2. Télégramme ? (1861-65)
3. Radio (1895) ?

Plusieurs réseaux / systèmes différents

1. Diplomates
2. Armée de terre
3. Marine
4. Espions



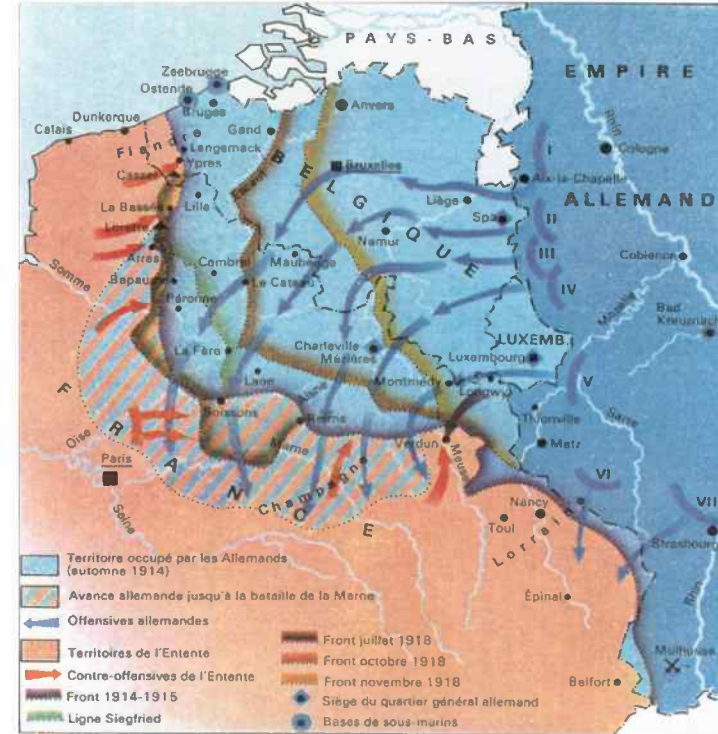
# Cryptanalyse, ses succès

Nov. 1916, Arthur Zimmermann,  
ministre des affaires étrangères

9 janvier, réunion au château  
de Pless.

Guerre navale totale dès le  
1 février 1917,

mais il faudrait éviter l'entrée en  
guerre des Etats-Unis qui vit sous  
la présidence Wilson.



# Cryptanalyse, ses succès

W. Wilson : (1916) « *Nous ne sommes pas en guerre, grâce à moi.* »

"All the News That's Fit to Print."

# The New York Times.

THE WEATHER  
Partly cloudy, colder tomorrow; overcast; strong west winds.  
For full weather report see Page 11.

VOL. LXVI...NO. 21,475.

NEW YORK, FRIDAY, NOVEMBER 10, 1916.—TWENTY-TWO PAGES.

ONE CENT In Greater New York, Jersey City and Newark. Elsewhere, TWO CENTS.

## WITH 272 ELECTORAL VOTES, WILSON WINS; GETS CALIFORNIA, NORTH DAKOTA, NEW MEXICO

**GERMANY FAVORS LEAGUE OF PEACE WITH CONDITION.**

**But Bethmann Hollweg Says the Entente Allies Must Renounce Their Annexation Schemes.**

**DENOUNCES "BRUTE FORCE"**

**Abolition of "Aggressive Coalitions" Put as First Step Toward International Harmony.**

**ANSWERS VISCOUNT GREY**

**Asserts That England Plunged Europe into War by Encouraging France and Russia.**

**Special Cable to THE NEW YORK TIMES.**  
BERLIN, Nov. 9.—Answering Viscount Grey, Chancellor of the Exchequer, in the course of his speech before the Main Committee of the Reichstag today said:  
"Germany is at all times ready to join..."

**Suffrage Amendment Defeated in Two States**

Woman suffrage amendments were evidently beaten in the two States that voted on the question last Tuesday. In South Dakota, with 290 precincts still to be heard from, the vote stood 52,934 for and 13,819 against the amendment.

**ASQUITH EXPOUNDS ESSENTIALS OF PEACE**

**Must Insure Security of Liberties of Europe, Free Future of World**

**TRADE OF NEUTRALS**

**German Talk of War Against It Called Fishy Fiction—Ready for Next Channel Raid.**

LONDON, Nov. 9.—The banquet of the new Lord Mayor of London, Sir William Henry Dunn, was given at the...

**WON'T CONCEDE WILSON VICTORY WITHOUT RECOUNT**

**Both Sides Should Be Anxious to Remove All Doubt. Willcox Says.**

**FOUR STATES IN QUESTION**

**New Hampshire, New Mexico.**

**WON'T CONCEDE WILSON VICTORY WITHOUT RECOUNT SHOW SUMMARY**

The Republican campaign managers will not concede the State of California to President Wilson until after the result of the official count of the vote which is scheduled to begin on Monday has been announced. And even then it is more than likely that if the result of the official canvass should give the...

**Views of Wilson's Election Sent to Him by Wireless**

Special to The New York Times.  
ASSBURY PARK, N. J., Nov. 9.—To President Wilson aboard the yacht Mayflower, en route to Washington, Mead, the message was wirelessly shortly before midnight tonight by Secretary Tamm:  
"I am here surrounded by the loyal Democrats of old Manassah, and beg leave to send you our greeting and congratulations. The cause you have so nobly represented has at last triumphed, and we greet you, our hearts, our thoughts and our affections go to you."

**M'CORMICK JOYFUL**

Scene of growing jubilation at Democratic National headquarters here.

**WILSON AHEAD IN CALIFORNIA BY OVER 3,100**

**Republican Chairman Concedes State on Face of the Returns.**

**36 PRECINCTS ARE MISSING**

**These Cannot Change Result, Reached After Day of Great Political Tension.**

**FULL RECOUNT IS CERTAIN**

**Both Sides Carefully Watching the Canvass—Much Talk of a Split Vote.**

SAN FRANCISCO, Cal., Nov. 9.—California has given her electoral vote to Woodrow Wilson.  
The Republican Chairman, C. J. Rowell, admitted at 8:30 o'clock tonight that, barring some exceptional errors in the count, the President had carried the State.

**THE ELECTORAL VOTE**  
Total, 621 necessary to a election, 300.

State	WILSON	Votes	State	HUGHES	Votes
Alabama	12		Connecticut	7	
Arizona	3		Delaware	3	
Arkansas	9		Illinois	29	
California	11		Indiana	15	
Colorado	6		Iowa	13	
Florida	6		Maine	6	
Georgia	14		Massachusetts	18	
Idaho	6		Michigan	15	
Kansas	10		Minnesota	12	
Kentucky	13		(By 1,000 votes, 88 precincts missing.)		
Louisiana	10		New Hampshire	4	
Maryland	10		(By 121 votes, 23 precincts missing.)		
Massachusetts	10		New Jersey	14	
Mississippi	10		New York	45	
Missouri	18		Oregon	5	
Montana	4		Pennsylvania	138	
Nebraska	6		Rhode Island	5	
Nevada	5		South Dakota	5	
New Mexico	3		Vermont	4	
North Carolina	12		West Virginia	8	
North Dakota	5		Wisconsin	13	
Ohio	24				
Oklahoma	10				
South Carolina	9				
Tennessee	12				
Texas	20				
Utah	4				
Virginia	12				
Washington	7				
Wyoming	3				
<b>Total</b>	<b>272</b>		<b>Total</b>	<b>259</b>	

\*Vote by Unnamed Democratic Elector given to Hughes.  
†Substituted elector's name omitted from table; may give one vote to Wilson.  
‡If 10 States are classified as doubtful in the above table, under the close States the final returns are given.

**Hughes's Lead Is Up in Minnesota; Wilson Holds N. Dakota, New Mexico**

**CALIFORNIA DECIDES**

**Result Was in Doubt Till Republicans Gave It Up at 11:25 P. M.**

**MINNESOTA STILL CLOSE**

**Hughes's Lead Going Up There; Wilson Gains in Other Close States.**

**CONTESTS ARE PROMISED**

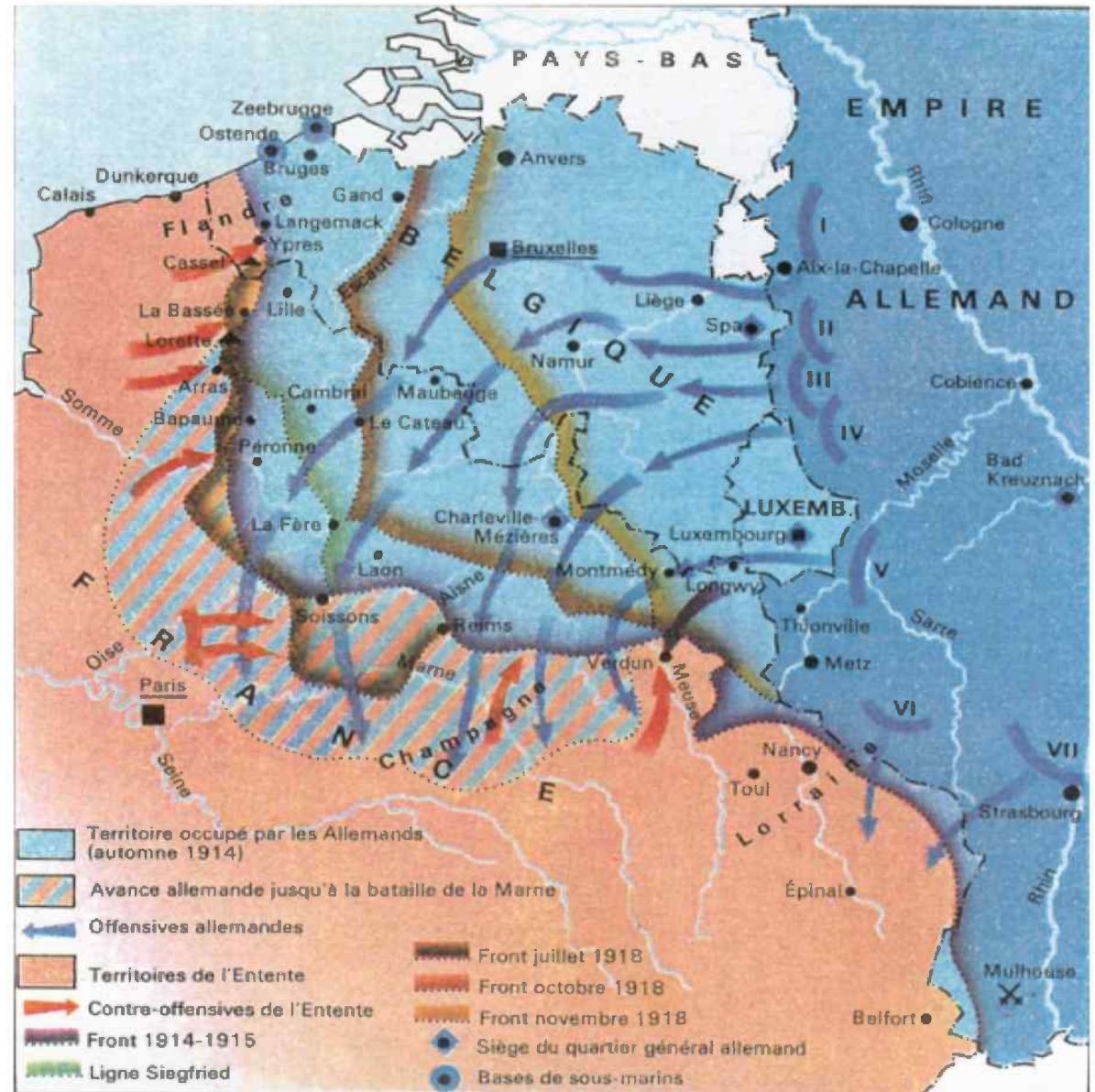
**Charges of Fraud Are Already Under Investigation in Some Districts.**

**ONE CITY PLAYS BIG PART**

# Cryptanalyse, ses succès

Situation sur le front en 1917

Comment empêcher ou retarder l'arrivée de troupes US ?



# Cryptanalyse, ses succès

Comment amener le Japon et le Mexique à déclarer la guerre aux Etats-Unis en même temps que l'Allemagne ?

Archives nationales, Washington, USA

<b>WESTERN UNION</b>	<b>TELEGRAM</b>	<b>15 110</b>	<b>35887</b>						
<small>NEWSPAPER EARLTON, PENNSYLVANIA</small>		<i>7060d</i>	<i>via Galveston</i>						
<b>GERMAN LEGATION</b>		<b>JAN 25 1917</b>							
<b>MEXICO CITY</b>									
130	13042	13401	8501	115	3528	418	17214	5491	11310
18147	18222	21560	10247	11518	23677	13605	5494	14936	
98092	5905	11311	10392	10371	0302	21290	5161	39695	
23571	17504	11209	18276	18101	0317	0228	17694	4473	
22284	22200	19452	21589	67893	5569	13918	8958	12137	
1333	4725	4458	5905	17165	13851	4458	17149	14471	6700
13850	12224	8929	14991	7382	15857	67895	14218	36477	
5870	17553	87893	5870	5454	16102	15217	22801	17138	
21001	17388	7440	23638	18222	0719	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	7032	7367	6926	52262	11267
21100	21272	9346	9559	22464	15874	18502	18500	15857	
2188	5376	7381	98092	16127	13466	9350	9220	76036	14219
5144	2831	17920	11347	17142	11264	7667	7762	15099	9110
10482	97556	3589	3670						
<b>Charge German Embassy,</b>		<b>BERNSTORFF,</b>							

# Cryptanalyse, ses succès

17 janvier, interception du télégramme par les Britanniques

23 février, l'ambassadeur américain à Londres reçoit le télégramme Zimmerman décrypté

27 février les Etats-Unis sont au courant des intentions allemandes



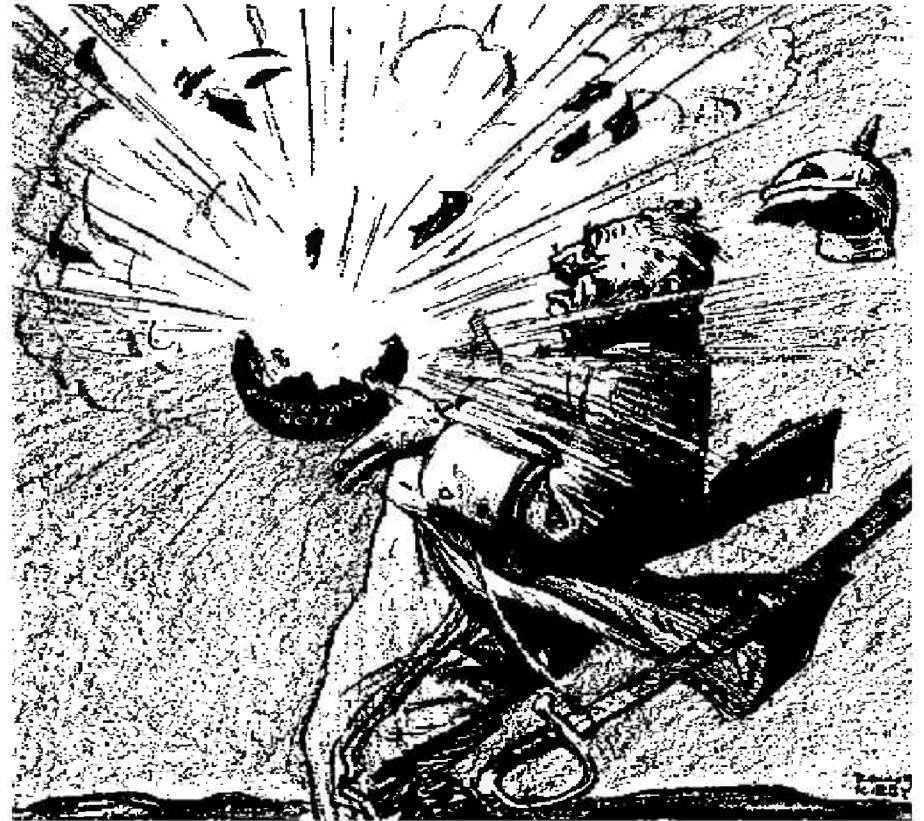


# Cryptanalyse, ses succès

Le télégramme intercepté est-il authentique ?

La réponse arrive le 2 mars 1917

Le 2 avril, la déclaration de guerre est adoptée par le Congrès



# Plan

1. Cryptographie classique
2. La première guerre mondiale
- 3. La machine Enigma**
4. Cryptographie à clés publiques (dès 1970)  
Applications à Internet / Web

# *The World Crisis (1923)*

Au début de septembre 1914, le croiseur léger allemand *Magdeburg* fit naufrage dans la Baltique. Le corps de l'un des sous-officiers allemands fut repêché par les Russes quelques heures plus tard et, serrés contre sa poitrine ... étaient le chiffre et le livre des signaux de l'armée allemande... l'amirauté russe avait été capable de décoder au moins certaines parties des messages de la *Kriegsmarine*. Les Russes jugèrent que, en tant que première puissance navale, l'Amirauté britannique se devait d'avoir ces livres...

# Enigma (1925 - 1945 ...)

Machine de chiffrement des Allemands pour les relations diplomatiques puis pour l'armée.

Scherbius (fondé en 1918, armée : 1925)  
(similaire aux Etats-Unis, Hollande, Angleterre)

- Mécanique (vitesse)
- Changement facile de clés
- Chiffrement par cascades de substitutions (casser toute régularité de la langue)
- Confiance absolue en son inviolabilité.

# Enigma (1925 - 1945 ...)

Composantes

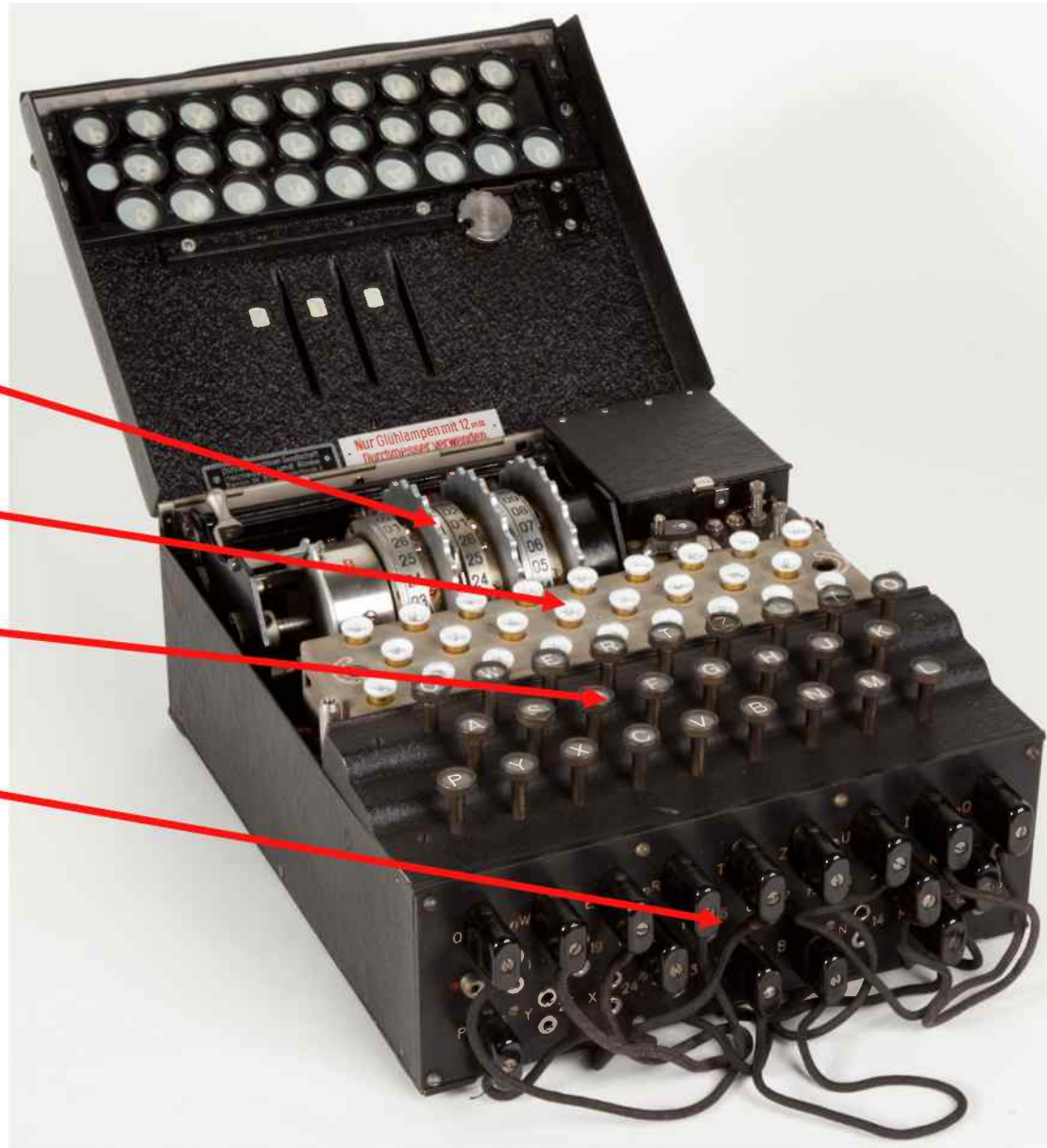
Trois rotors (substitution, 26 lettres)

Panneau lumineux

Clavier

Panneau de connections frontal

Il est prévu que la sécurité du système de cryptage soit préservée même si l'ennemi a une machine à sa disposition



# Enigma (1925 - 1945 ...)

Changement quotidien des clés sur une machine Enigma

- Connections avant : A-L, P-R, T-D, B-W, K-F, O-Y
- Brouilleur : 2 – 3 - 1
- Orientation du brouilleur : Q – C – W



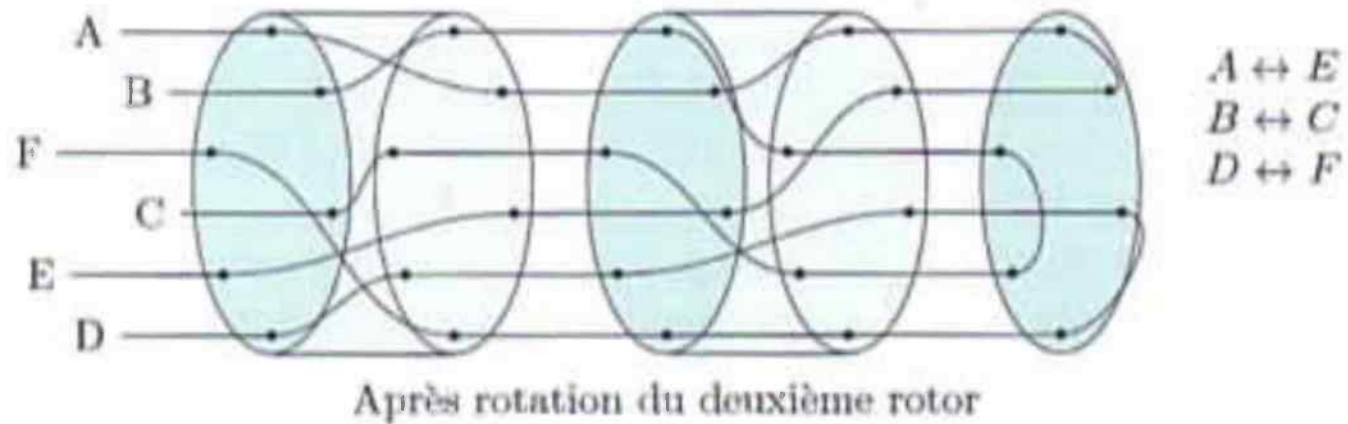
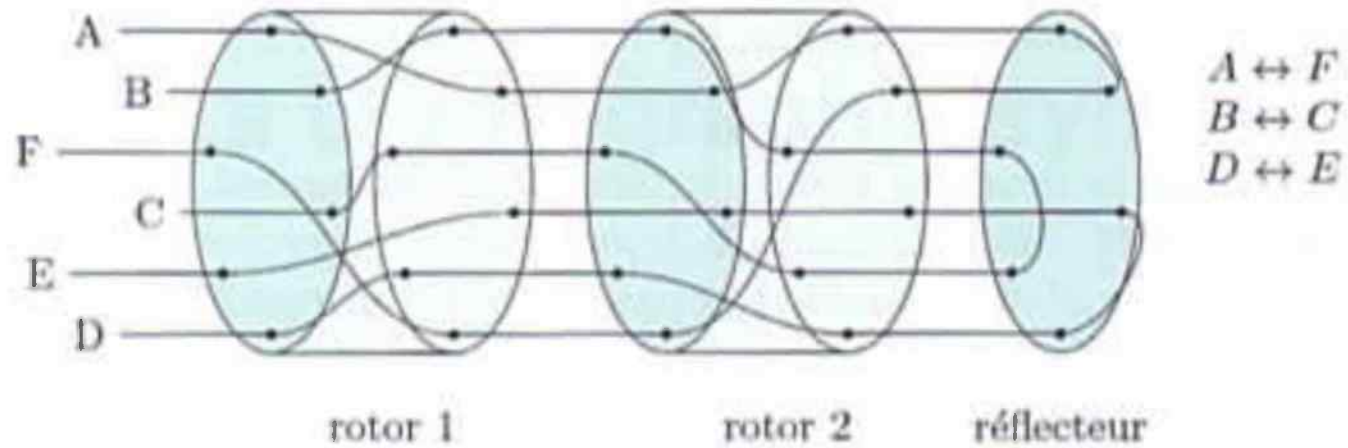
Nombre de clés

$26 \times 26 \times 26 \times 6 \times 100 \times 391 \times 791 \times 500 = 10^{16} = 10\,000\,000\,000\,000\,000$

Et durant le même jour, clé de session (une clé par message) :  
changement de position de l'orientation du brouilleur

PGHPGH -> KIVBJE

# Enigma (1925 - 1945 ...)



# A l'attaque d'Enigma

Trahison de Schmidt (8 nov. 1931) vente de documents à l'agent français Rex

France renonce...



Pologne : Marian Rejewski (1905-1980)

- Construire une réplique de la machine (en partie depuis la machine commerciale)
- Déchiffrement via l'émission de la clé de session en double (PGHPPGH -> KIVBJE)  
Lien entre P -> K et P -> B (+ 3 mouvements)



# A l'attaque d'Enigma

24 juillet 1939 : les Polonais donnent une machine Enigma aux Français et Anglais

1 septembre 1939 : début de la 2<sup>e</sup> guerre mondiale

Room 40 -> Bletchley : Plus de ressources

1. Les trois lettres clef ne sont pas toujours aléatoires (clavier)
2. Le rotor ne peut pas être à la même place deux jours de suite
3. Connections : pas entre lettres consécutives (S->T)

# Position des brouilleurs

3

5 rotors

123	124	125	134	135	142	143	145	152	153
132	154	214	215	234	235	241	243	245	251
213	253	254	314	315	324	325	341	342	345
231	351	352	354	412	413	415	421	423	425
312	431	432	435	451	452	453	512	513	514
321	521	523	524	531	532	534	541	542	543

3 rotors -> 6 possibilités

5 rotors -> 60 possibilités

# Position des brouilleurs

123

Cinq rotors

		214	215	234	235	241		245	251
		254	314	315		325	341	342	345
231	351	352	354	412		415			425
312	431	432	435	451	452		512		514
	521			531	532	534	541	542	

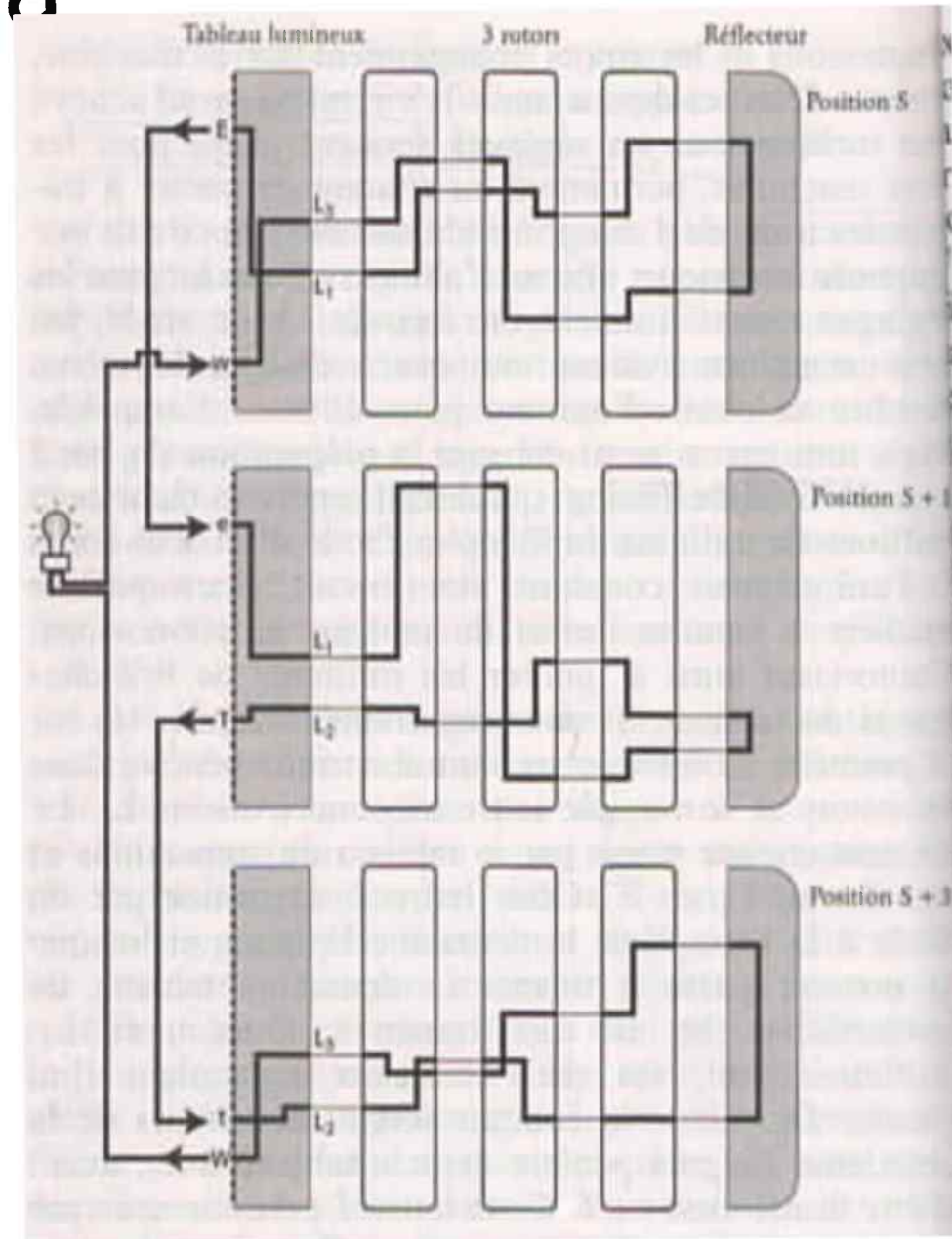
3 rotors -> 2 possibilités

5 rotors -> 33 possibilités

# A l'attaque d'Enigma

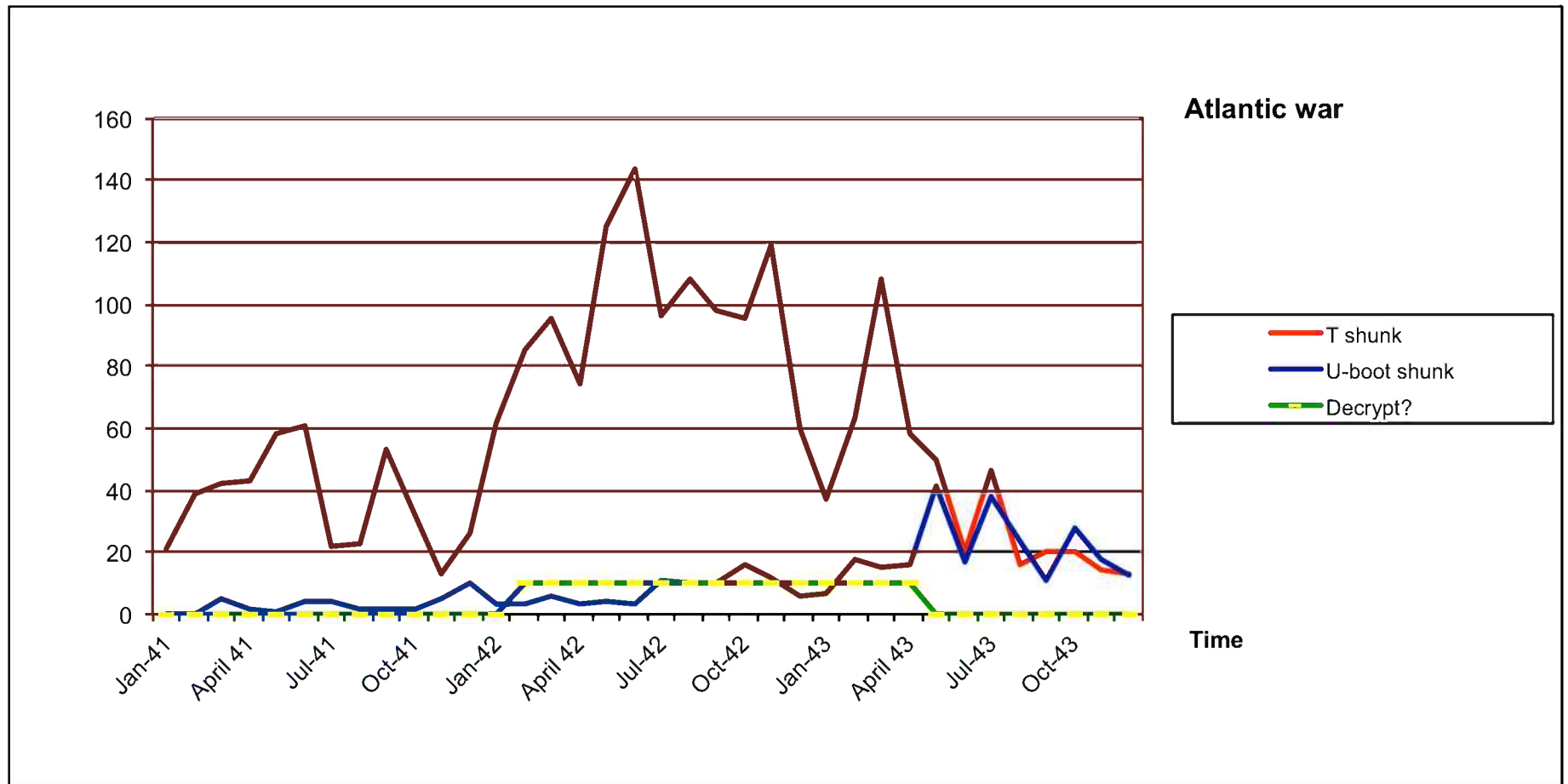
Turing (1912-1954)

1. Predire le contenu (météo)
2. Style rigide des messages
3. Cycles de Rejewski  
S : w -> E  
S+1 : e -> T  
S+2 : t -> W
4. Relié trois Enigma (bombe)



# Déchiffrer Enigma

Succès si l'on peut déchiffrer...



# La guerre dans le Pacifique

1928 : « Un gentleman ne lit pas le courrier d'autrui »

Déchiffrement des messages japonais par les américains : possible

Pour les Japonais :

1. Le Japonais est une langue trop complexe  
コソボ紛争におけるNATOの攻撃と
2. Impossible de décrypter. Preuve : échec dans le décryptage des messages américains (mais pas ceux de l'US Air Force)

# La guerre dans le Pacifique

7 dec. 1941 : L'attaque de Pearl Harbor (2 403 tués)

Le service de décryptage savait l'imminence de l'attaque (mais pas la localisation)



# Amiral Yamamoto

Printemps 1943 : Amiral Yamamoto prépare une contre-offensive (perte de Guadalcanal)

Inspection des troupes (18 avril) dans les îles Salomon

13 avril : itinéraire de Yamamoto diffusé  
cryptogramme intercepté  
multiplicité des destinataires

Interception : Oui ou non?

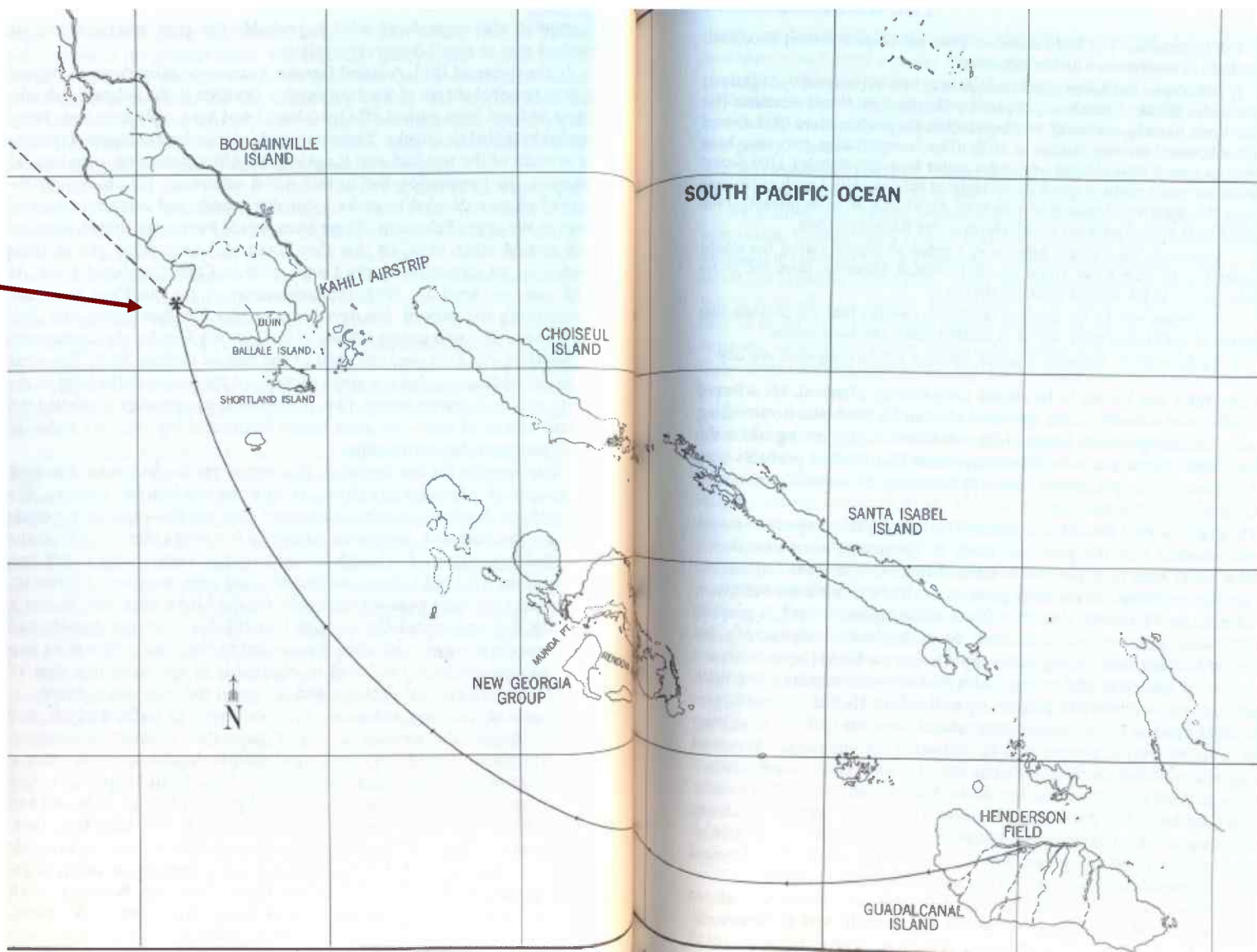


# Amiral Yamamoto

Interception  
18 P38  
Lightning



21 mai:  
annonce de  
la mort de  
Yamamoto



ETRANGER

03.09.16 09:37

Les USA ont piraté l'Elysée en 2012  
 Les services américains ont piraté les ordinateurs des collaborateurs de la présidence française. L'intrusion avait été repérée par l'Elysée durant l'entre-deux-tours de l'élection présidentielle de 2012. Elle a été confirmée par un ancien directeur de la DGSE.

Le Monde révèle samedi que Bernard Barbier, ancien directeur technique du service de renseignement extérieur français (DGSE), a assuré que les USA se trouvaient derrière un piratage de l'Elysée durant le mandat de N.Sarkozy.

Cette information - "passée complètement inaperçue" selon le quotidien français - a été révélée lors d'une conférence enregistrée et mise en ligne sur YouTube le 18 juin dernier.

?



Associateur suisse Walter Stucki.

STR/KeyStone



A peine les espions américains eurent-ils craqué les codes suisses qu'ils en firent un usage intensif

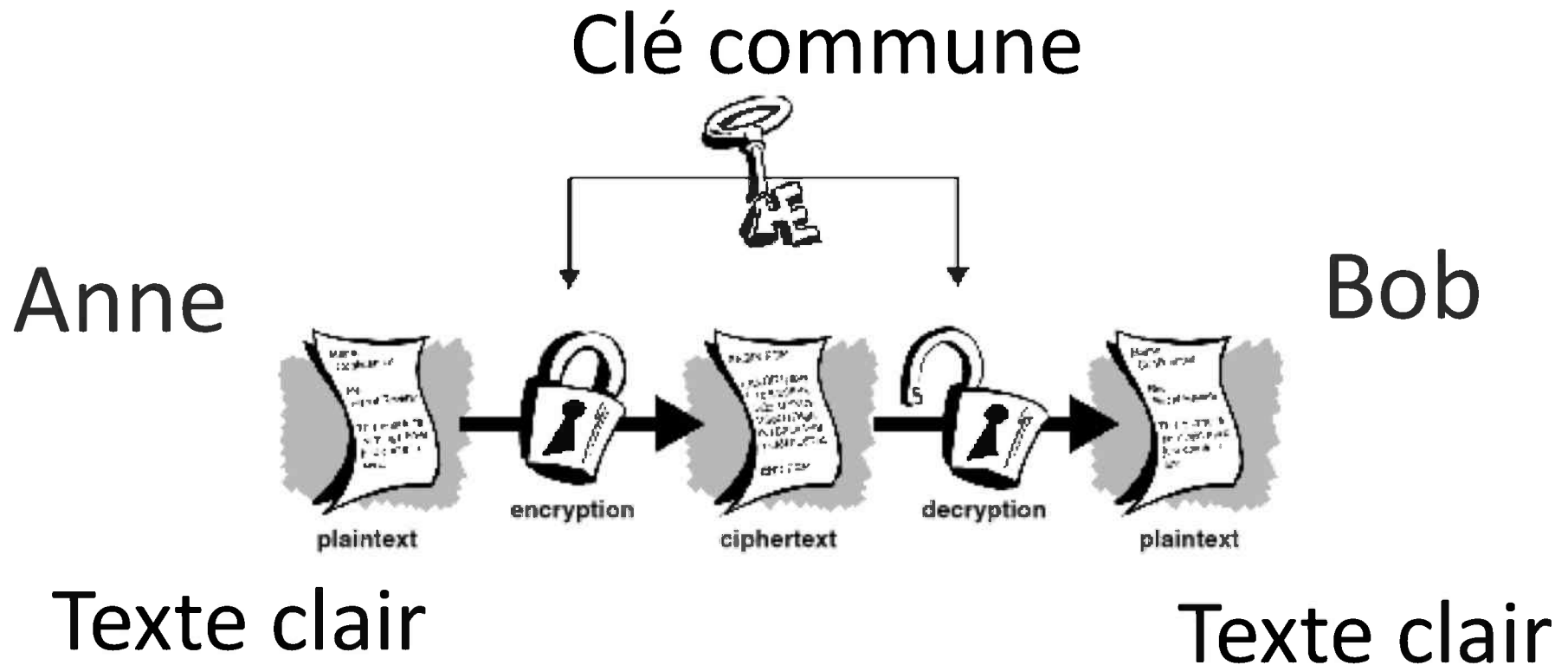


Crypto Museum

# Plan

1. Cryptographie classique
2. La première guerre mondiale
3. La machine Enigma
- 4. Cryptographie à clés publiques (1970)**  
Applications à Internet / Web

# Limite de la cryptographie classique



Comment partager un secret  
entre le client  
et le vendeur ?



Parler en clair ?  
Toujours passer par un  
intermédiaire ...

Impossible ?

# A clés publiques

Avec Internet

Echange d'information confidentielle  
(numéro de carte de crédit)

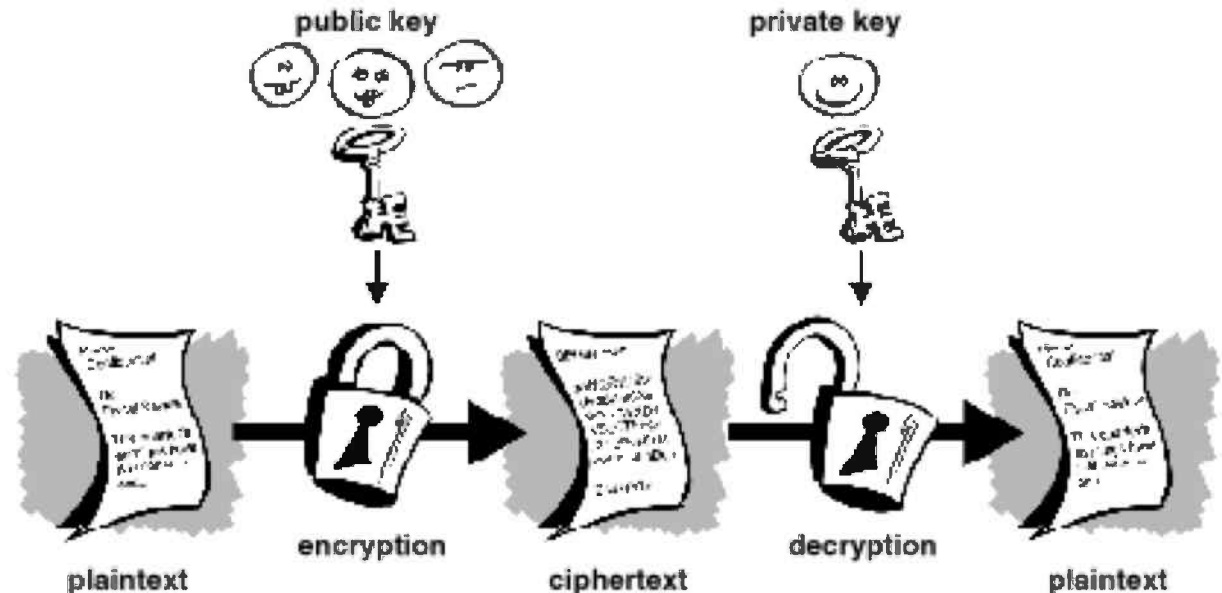
Signature électronique (authentifier)  
et cela sans se connaître (banque, vote, ...)

# Cryptographie classique et cryptographie à clés publiques

Classique : une seule clé

La solution moderne :

Deux clés :  
une privée  
une publique



# A clés publiques

Principes :

On utilise une clé pour chiffrer et l'autre clé pour déchiffrer le message.

Il n'y a pas de moyen « facile » pour déterminer la valeur d'une clé même lorsque l'on connaît l'autre.



# A clés publiques

Exemple :

Si l'on trouve 81 et que la fonction était « mettre au carré » soit  $f(x) = x^2$  alors, avec la racine carrée, je retrouve le  $x$  de départ, soit 9 dans notre exemple.

Mais parfois les choses sont plus compliquées ...

Par analogie

Les espions et les gardes-frontières ...

# A clés publiques

Par une opération dont l'inverse s'avère « difficile »

Garde-frontière :

Prendre le nombre, le mettre au carré, puis les trois chiffres du centre doivent être « 872 »

Espion :

Le nombre : 2 547

# A clés publiques

Application :

$$2\ 547 \times 2\ 547 = 6\ 487\ 209 = 64\ \mathbf{872}\ 09$$

Les deux chiffres au centre « 872 »

-> on peut passer

mais si on connaît seulement « 872 »,  
il faut essayer tous les nombres  
possibles...

# A clés publiques

Chez Anne :

Elle utilise sa clé privée

Puis la clé publique de Bob

Chez Bob :

La clé privée de Bob

Puis la clé publique de  
Anne

# A clés publiques

Chez Anne :

Elle utilise sa clé privée

Puis la clé publique de Bob

Chez Bob :

La clé privée de Bob

Puis la clé publique de  
Anne

Pourquoi est-on certain que le message vient  
bien de Anne ?

# A clés publiques

Facile ? Alors décomposer la valeur de  $n$  suivante ...

$n =$  114 381 625 757 888 867 669 235 779 976 146 612 010  
218 296 721 242 362 562 561 842 935 706 935 245 733 897  
830 597 123 563 958 705 058 989 075 147 599 290 026 879  
543 541

$p =$  32 769 132 993 266 709 549 961 988 190 834 461 413  
177 642 967 992 942 539 798 288 533

$q =$  3 490 529 510 847 650 949 147 849 619 903 898 133 417  
764 638 493 387 843 990 820 577

# Applications à Internet

Sur Internet, on « surfe » via le protocole HTTP (HyperText Transfer Protocol) mais tout le monde peut écouter...

Encryptage de votre numéro de carte de crédit (HTTPS (SSL)). But : se créer une clé (de session)

Signature électronique (Vote électronique)

Bitcoin

# Achat en ligne

Amazon.fr: la guerre des codes secrets: Livres

http://www.amazon.fr/s/ref=nb\_sb\_noss?\_\_mk\_fr\_FR=ÅMÅZÕÑ&url=search-alias%3Dstripbooks&field=... Google

Apple Yahoo! Google Maps YouTube Wikipedia Popular News (684)

**amazon.fr** Chez Jacques | Promotions | Chèques-cadeaux | Vendre | Aide

VENTE PRIVÉE **MODE -40%**

Parcourir les boutiques

Rechercher Livres en français la guerre des codes secrets Go

Bonjour Jacques  
Votre compte

Panier

Livres Recherche détaillée Nos rubriques Meilleures ventes Précommandes Livres anglais et étrangers Promotions Livres d'occasion Amazon Rachète

**Nouveautés**  
Dans les 3 mois à venir (1)

**Boutique**  
Toutes les boutiques

**Livres**  
Informatique et Internet (1)  
Histoire (6)  
Littérature (4)  
Religions et Spiritualités (1)  
Sciences, Techniques et Médecine (3)  
Sciences humaines (8)  
Actu, Politique et Société (6)  
Études supérieures (6)  
Entreprise et Bourse (2)  
Droit (1)

**Livres > "la guerre des codes secrets"**

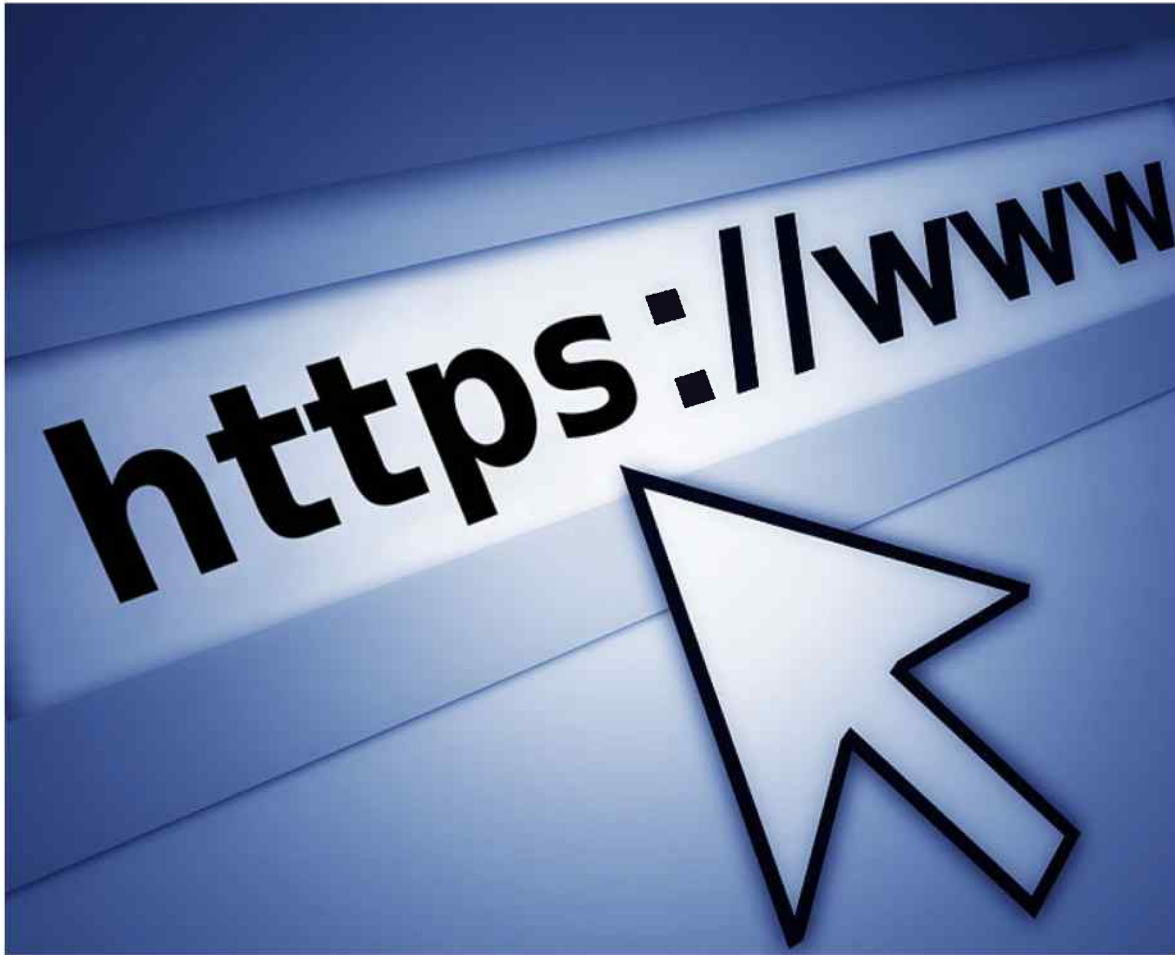
q5 Y! et al

Résultats 1 - 16 sur 27 Trier par Pertinence

 **La guerre des codes secrets** de Kahn (20 janvier 1992)  
**EUR 34,00** d'occasion (2 offres)



# Achat en ligne avec **https**



# Achat en ligne avec https

Vos commandes

https://www.amazon.fr/gp/css/order-history?ie=UTF8&ref\_=ya\_\_57b\_css&openid.assoc\_handle=fran

amazon.fr

Chez Jacques | Promotions | Chèques-cadeaux | Vendre | Aide

VENTE PRIVÉE **MODE -40%**

Parcourir les boutiques

Rechercher

Toutes nos boutiques

Go

Bonjour **Jacques**  
Votre compte

Panier

Amazon.fr

Meilleures ventes

Promotions

Listes d'envies

Chèques-cadeaux

Economisez en vous abonnant

Options de livraison

Vendez !

Votre compte > Vos commandes

Liste des commandes par date

Commandes en cours

Recherchez vos commandes :

Titre, boutique, destinataire...

Go

Date :

Commandes passées dans les 30 derniers jours

Go

1 commande passée dans les 30 derniers jours

Page : 1 sur 1

COMMANDE PASSÉE

**2 janvier 2013**

Détails des commandes | Version

Imprimable

N° DE COMMANDE

403-3190724-2373922

DESTINATAIRE Jacques Savoy

TOTAL EUR 30,99

DATE DE LIVRAISON PRÉVUE **mercredi 9 janvier 2013 - vendredi 18 janvier 2013**

**Expédié**

Suivi non disponible. Pourquoi ?



**La guerre des codes secrets**

Kahn

Vendu par : Art et Histoire d'Europe (profil vendeur)

Actions disponibles

Contactez le vendeur

Envoyer/Afficher la réclamation

Retourner un article

Évaluer un vendeur

# Principe de https



# Principes https



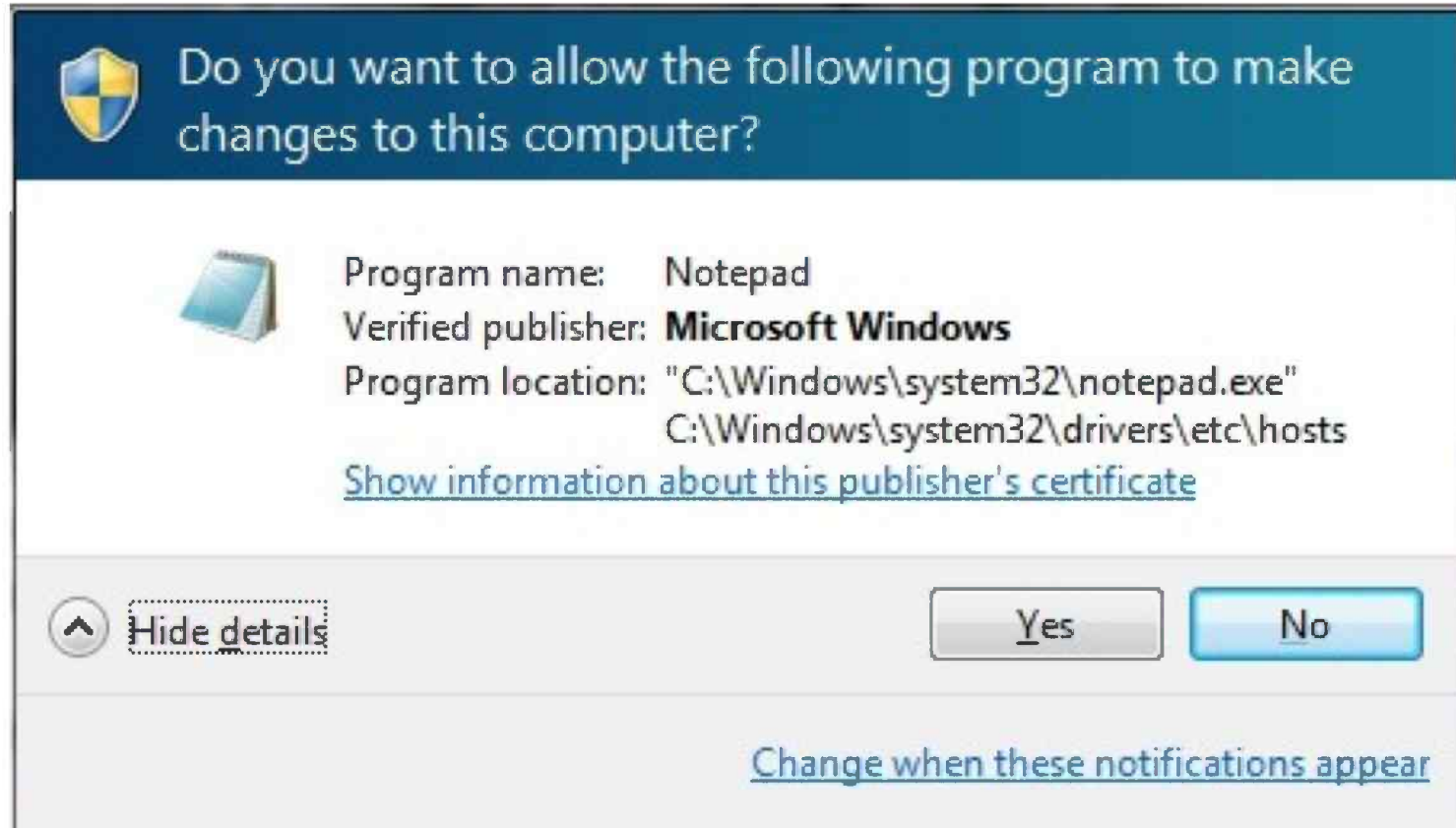
Certificats

VeriSign  
Microsoft



# Signature numérique

Authentifier l'auteur  
d'un logiciel

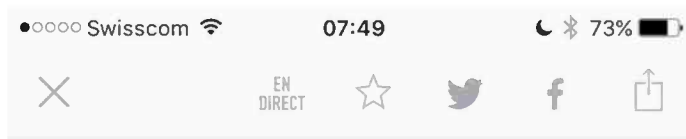


# Signature numérique

Un logiciel douteux!



# Dernières nouvelles ...



## Comment la NSA a espionné un militant pro-démocratie pour le compte de la Nouvelle-Zélande

Le 16 août 2016 à 19h45

Pour la première fois, l'identité d'une cible de PRISM, le programme de surveillance américain dévoilé par Edward Snowden, a été rendue publique.



Le siège de la NSA. | Reuters

**T**'existence de Prism, le programme de



News  
Etats-Unis Il y a 4h

## Yahoo! a espionné ses clients pour les autorités



Siège de Yahoo, à Sunnyvale en Californie (Etats-Unis).

photo: Keystone

**Selon des ex-employés, la société a obéi aux directives de la NSA.**

Yahoo! a secrètement conçu l'an dernier un logiciel lui permettant de rechercher des données précises à la demande des services de sécurité américains dans l'ensemble des

# Dernières nouvelles ...

Swisscom 4G 17:15 67%

News

E-extorsion Il y a 3h

## Indépendants aussi visés par les racketteurs du Net

Le patron d'un magasin en ligne alémanique a été contacté le week-end dernier par des hackers, qui menaçaient de détruire sa base de données clients s'il ne payait pas.

«Nous sommes Armada Collective. Nous sommes en possession de votre base de données.» Le sang du propriétaire d'une boutique en ligne alémanique n'a fait qu'un tour, le week-end dernier, quand il a ouvert sa boîte e-mail. Un collectif de hackers le priait de leur verser 2,85 bitcoins (environ 2800 francs) ou toutes ses données clients seraient effacées. Pour prouver qu'ils ne plaisantaient pas, les pirates ont envoyé la copie d'une entrée de la base de données. Ils ont même expliqué qu'il pouvait acheter des bitcoins aux distributeurs CFF.

PUBLICITÉ

Tradez FX

Swisscom 14:25 43%

News

Espagne Il y a 1h

## Réseau international de cyberpirates démantelé



L'enquête avait débuté fin 2014.

### Des perquisitions en Espagne et au Royaume-Uni ont conduit à l'arrestation de 44 personnes.

La police espagnole a annoncé vendredi le démantèlement d'un réseau international piratant les messageries électroniques de chefs d'entreprises pour leur soutirer des centaines de milliers d'euros au bénéfice de

Swisscom 19:45 94%

News

Russie Il y a 33'

## Des hackers volent plus de 30 millions à la banque



La banque centrale de Russie.

Photo: AFP

### Des pirates informatiques ont attaqué l'institution publique et ont puisé de l'argent dans les comptes.

Des pirates informatiques ont volé plus de deux milliards de roubles (31,3 millions de francs) sur des comptes ouverts à la banque



# Quelques précautions...

- Aucune institution financière ne vous demandera un mot de passe ou une identité en claire via le courriel  
Même si le logo apparaîtrait et qu'il est parfait...
- Ne jamais ouvrir un fichier Word ou Excel attaché à un courriel.
- Ne jamais se rendre sur un site que l'on vous propose depuis un courriel douteux.
- Attention aux clés USB  
(pour ceux qui veulent une plus grande protection)

# Histoire de la cryptographie de la première guerre à Internet

Prof. Jacques Savoy  
Université de Neuchâtel

