Histoire de la cryptographie de la première guerre mondiale à Internet

cryptographie +
cryptanalyse = cryptologie

Prof. Jacques Savoy
Université de Neuchâtel

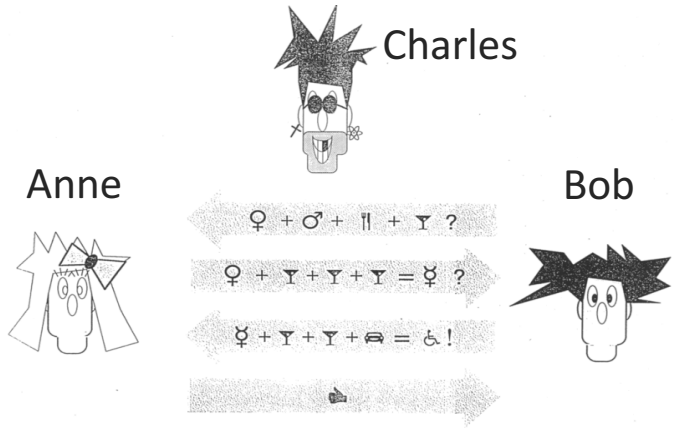
Plan

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

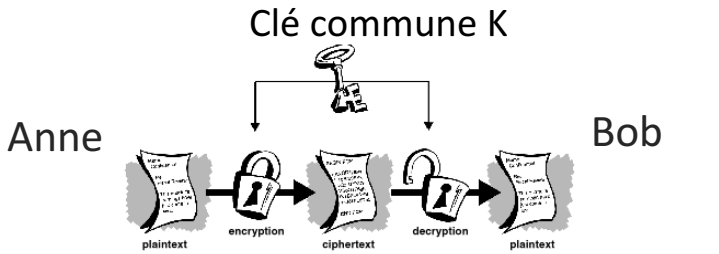
Les besoins …

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



Cryptographie classique



Texte clair
M

Texte crypté
C

Texte clair
M

Techniques de cryptographie

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

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

Stéganographie

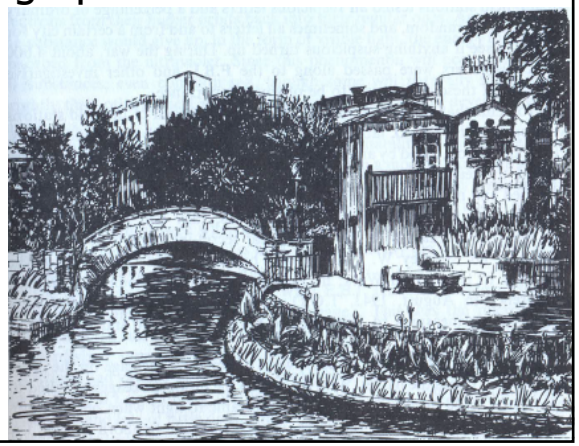
Stéganographie
le message est dissimulé (encre invisible)

Par exemple
Dissimulation du m
Dissimulation d'im

Stéganographie

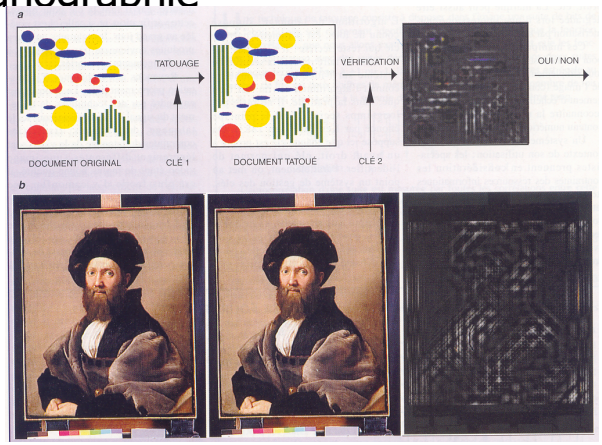
Le message est dissimulé dans un dessin

Journaux britanniques au XIXe siècle



Steganographie

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



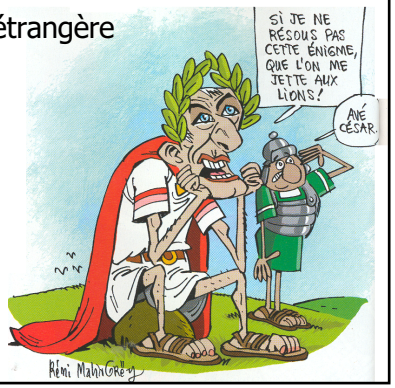
Substitution

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 ?

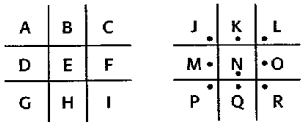
Encore utilisé entre 1880 et début du XXe siècle (Règle de St-Cyr)

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

Substitution

Substitution plus mystérieuse !

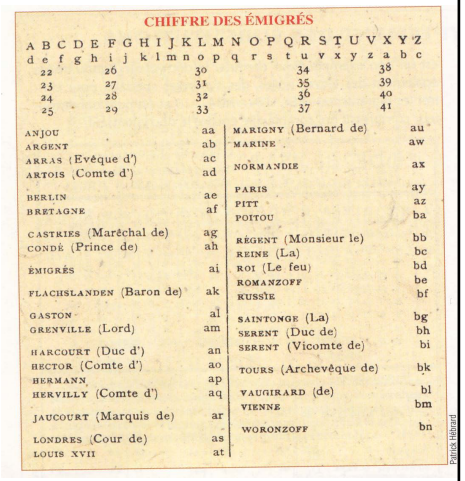
Pas des lettres mais des symboles



a = ⌟
b = ⌴
:
:
z = ^

Autres exemples

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



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		

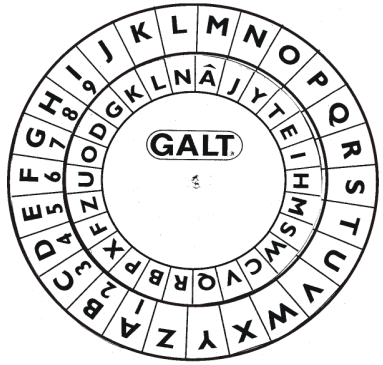
Patrick Hébrard

Substitution

Substitution plus complexe et rapide

(mécanique avec un disque de chiffrement)

Guerre de Sécession (1861-1865) et jusqu'en 1911



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. »

« 35e 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 $26! = 26 \cdot 25 \cdot 24 \cdot \ldots \cdot 2 =$
403 291 461 126 605 635 584 000 000

Sécurité

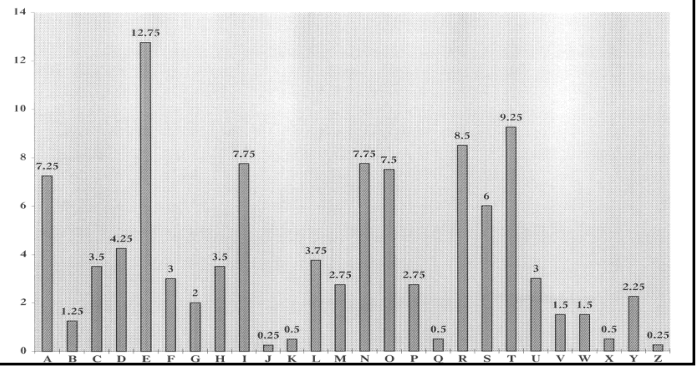
Attaque par l'analyse des fréquences

Al-Kindi IX^{e} siècle

Toute langue naturelle comprend des régularités…

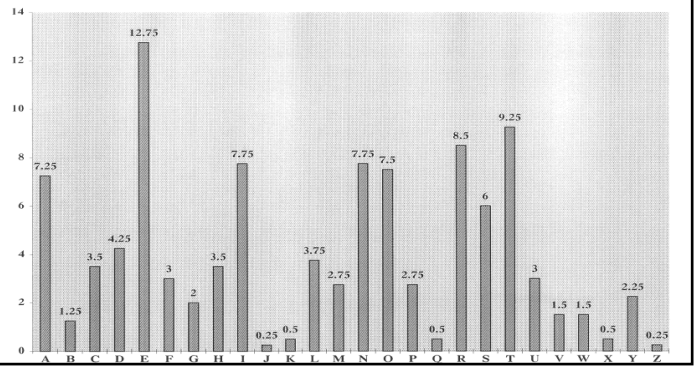
Cryptanalyse

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 ees 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
r	**e**	**n**	**d**
e	**z**	**v**	**o**
u	**s**	**a**	**u**
p	**o**	**r**	**t**

Transposition

1	2	3	4
r	**e**	**n**	**d**
e	**z**	**v**	**o**
u	**s**	**a**	**u**
p	**o**	**r**	**t**

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 — `L`ouf
3. ajoutez « -`em` » ou « -`oque` » à la fin. — `L`ouf`oque`

Substitution polyalphabétique

Progrès notable avec Blaise de Vigenère (XVIe 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**	**A**	**C**	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^{e} 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

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

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

GERMANY FAVORS LEAGUE OF PEACE WITH CONDITION.

WON'T CONCEDE WILSON VICTORY WITHOUT RECOUNT

WILSON AHEAD IN CALIFORNIA BY OVER 3,100

THE ELECTORAL VOTE.

CALIFORNIA DECIDES

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

MINNESOTA STILL CLOSE

ASQUITH EXPOUNDS ESSENTIALS OF PEACE

M'CORMICK JOYFUL

WON'T CONCEDE WILSON VICTORY WIHOUT RECOUNT

SHOW SUMMARY

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

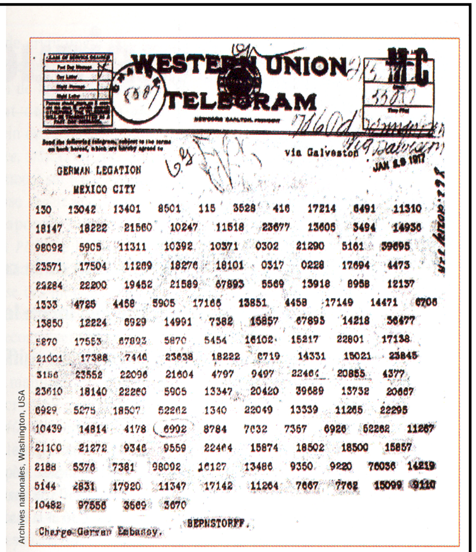
Cryptanalyse, ses succès

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 a déclarer la guerre aux Etats-Unis en même temps que l'Allemagne ?



WESTERN UNION TELEGRAM

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
22284 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.

Archives nationales, Washington, USA

Cryptanalyse, ses succès

17 janvier, interception du télégramme par les Britanniqu

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

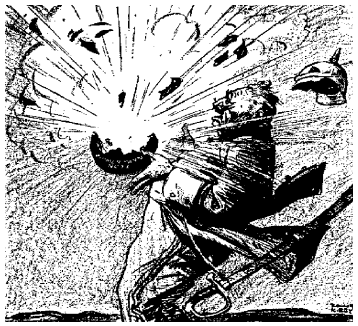
27 février les Etats-Unis sont au courant des intentions allemandes

Cryptanalyse, ses succès

Le télégramme intercepté est-il authentique ?

La réponse arrive le 2 mars 1917

Le 2 avril, la déclaration de guerre est adopté 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

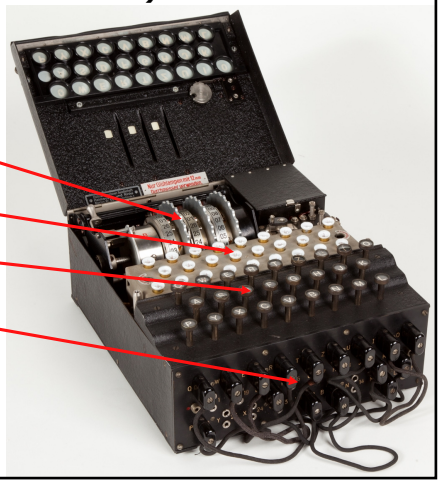
Trois rotors (substitution, 26 lettres)

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

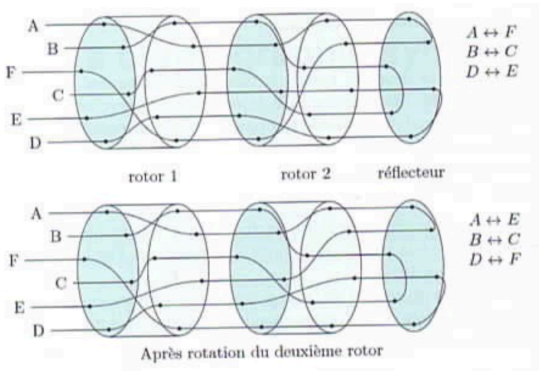
- Connections avant : A-L, P-R, T-D, B-W, K-F, O-Y
- Brouilleur : 2 – 3 - 1
- Orientation du brouilleur : Q – C – W

Nombre de clés

26x26x26x 6 x 100 391 791 500 = 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 (PGHPGH -> 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 2e 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	

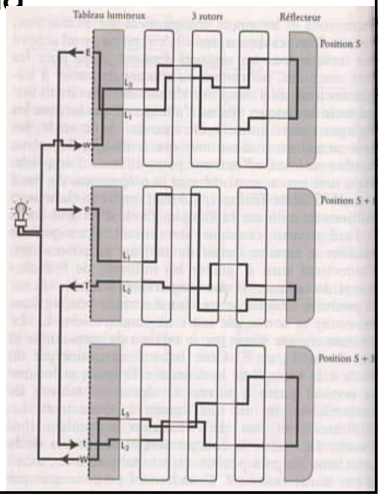
3 rotors -> 2 possibilités

5 rotors -> 33 possibilités

A l'attaque d'Enigma

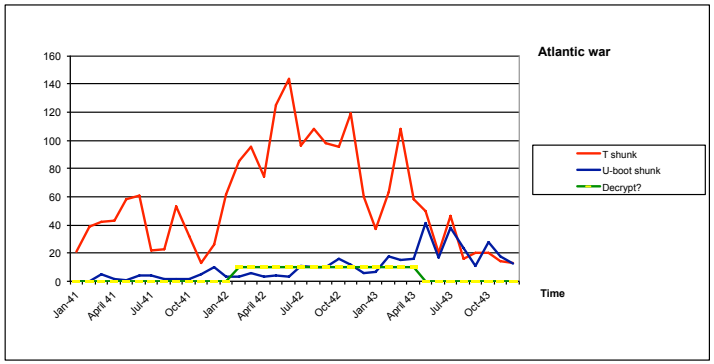
Turing (1912-1954)

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

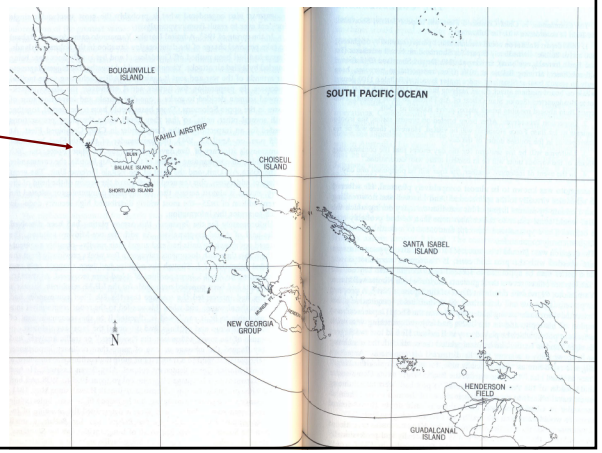
13 avril : itinéraire de Yamamoto diffusé
cryptogramme intercepté
multiplicité des destinataires

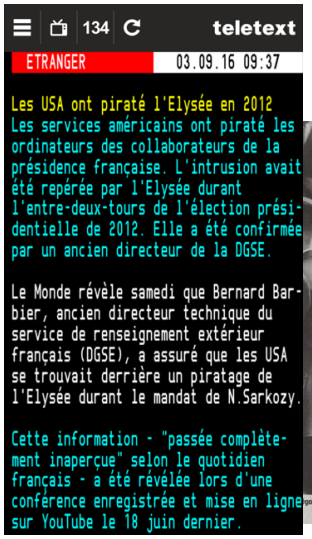
Interception : Oui ou non?

Amiral Yamamoto

Interception 18 P38 Lightning

21 mai: annonce de la mort de Yamamoto



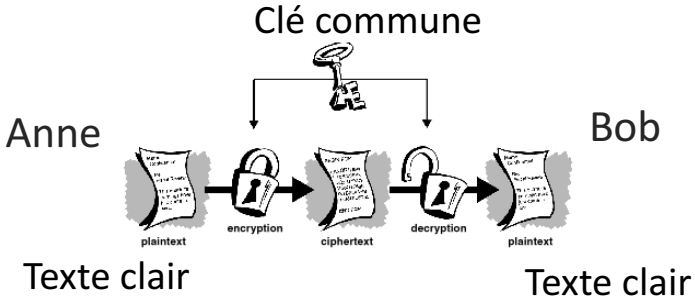


?

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

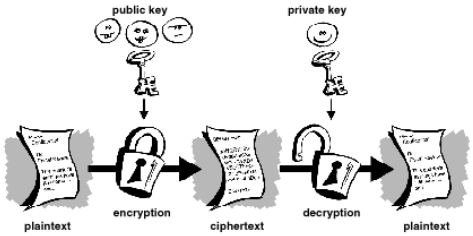
Echange d'information confidentielle
(numéro de carte de crédit)
Signature électronique (authentifier)
et cela sans se connaître (banque, vote, …)

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 x 2 547 = 6 487 209 = 64 **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

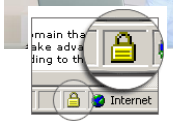
Achat enligne

Achat enligne avec **https**

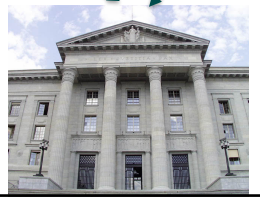
Achat enligne avec https

Principe de https

Principes https



Certificats



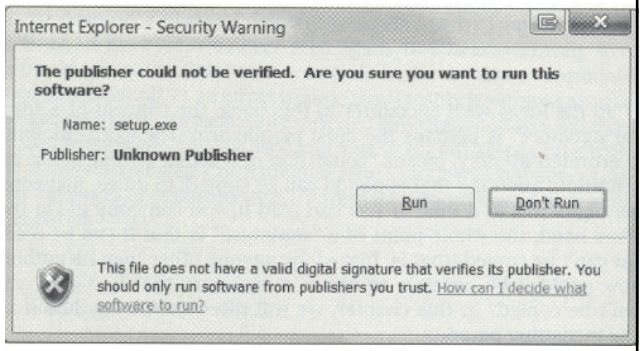
VeriSign
Microsoft

Signature numérique

Authentifier l'auteur
d'un logiciel

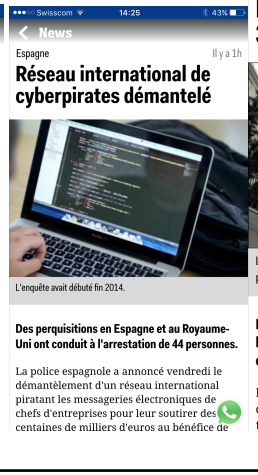
Signature numérique

Un logiciel douteux!



Dernières nouvelles ...

Dernières nouvelles ...



Quelques précautions…

- Aucune institution financière ne vous demandera un mot de passe ou une identité en claire via le courriel
  Même si le logo apparaît 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 mondiale à Internet

Simon SINGH

Histoire des codes secrets

Livre de Poche

Prof. Jacques Savoy

Université de Neuchâtel