Sécurité des systèmes d'information

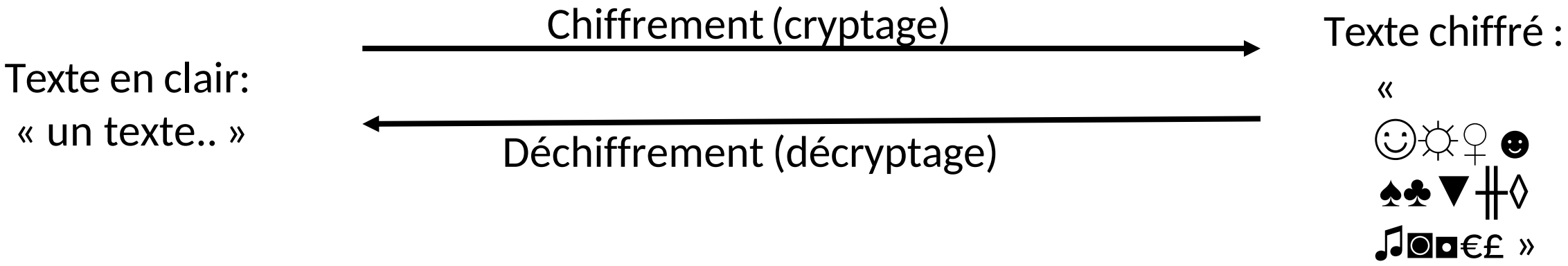
(initiation à la cryptographie)

Partie 1: C'est quoi la cryptographie?

université d'Alger 1 -
Benyoucef Benkhedda

Cryptographie

L’art de transformer une **information compréhensible** à une autre qui n’a **aucun sens**



Historique de la cryptographie

La cryptographie est utilisée depuis l'antiquité

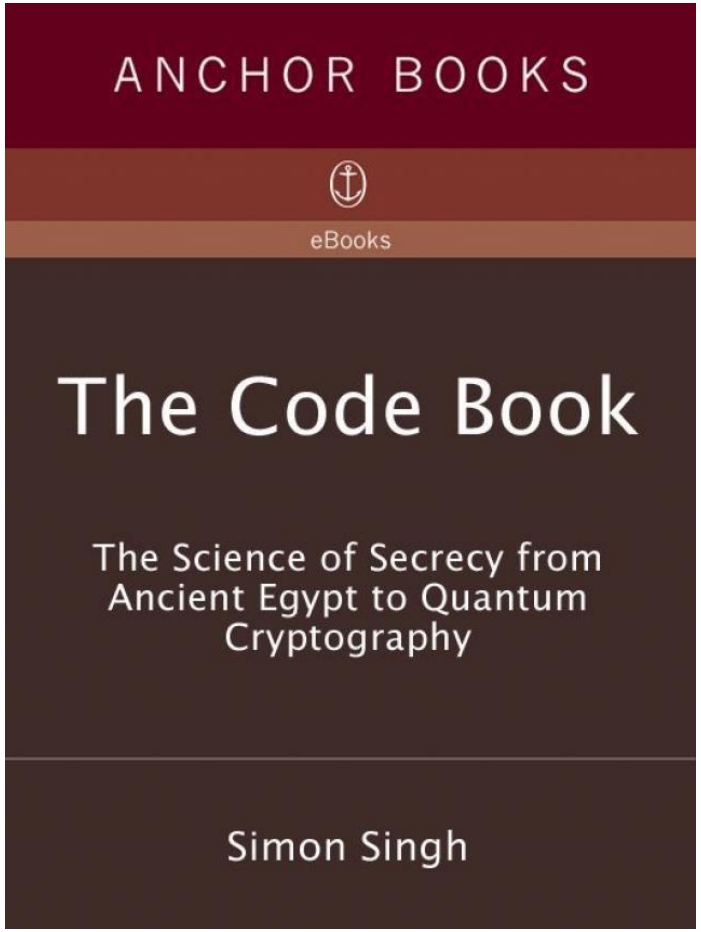
– Il y a 4000 ans par les égyptiens

- Cryptographie ancienne
  – Alphabet de la langue

    Ex: Français : 26 lettres

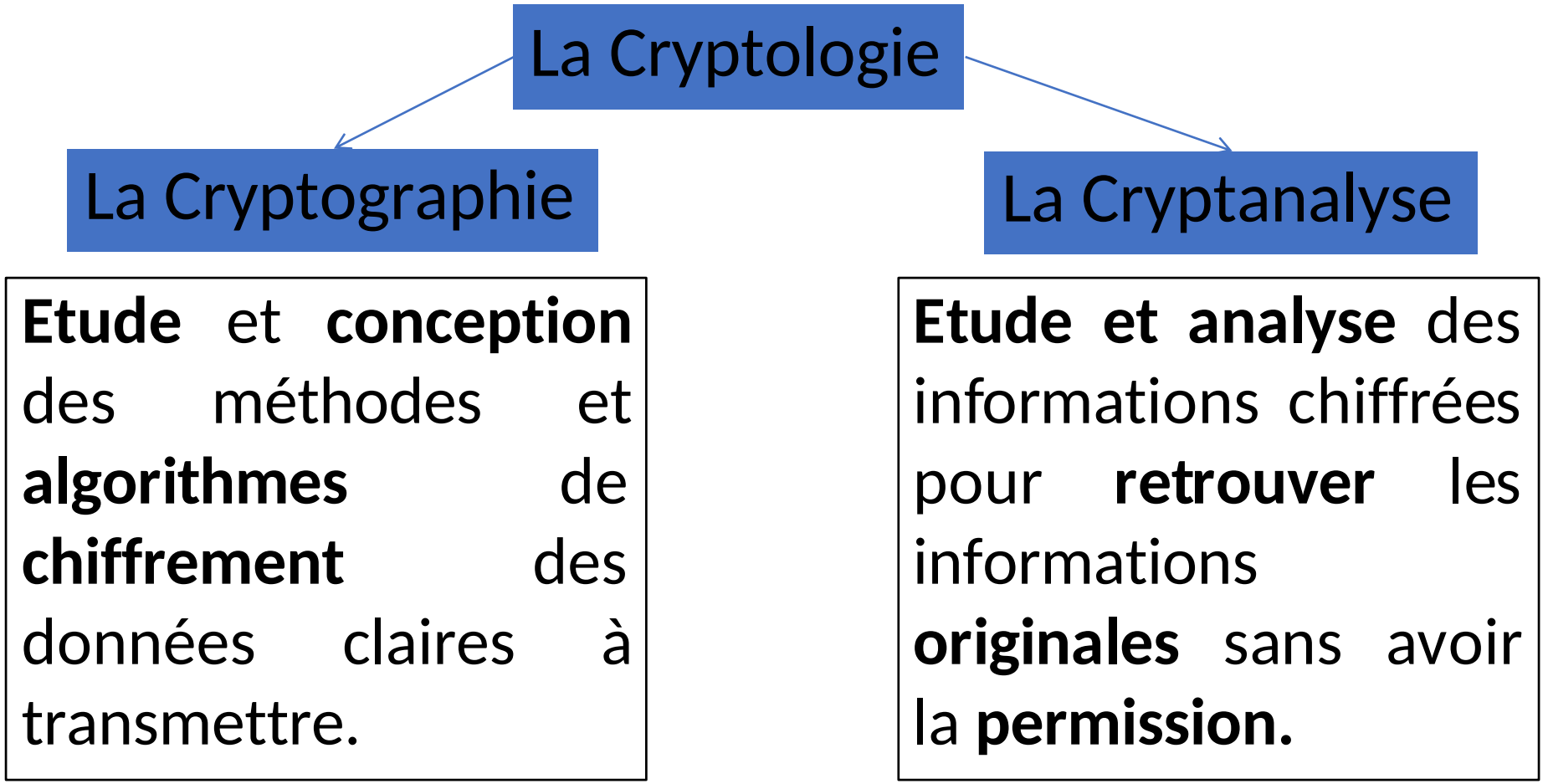
Chiffrement de César, de Vigénère, Scytale, Enigma,…

- Cryptographie moderne
  –L'apparition de l'informatique et prolifération des systèmes de communication
  – Alphabet = {0, 1}
  – Chiffrement symétrique et asymétrique



Terminologie

- La **cryptologie** peut être définie littéralement comme la *science du secret*. Elle se compose de deux grandes branches distinctes:



Terminologie

Symbole	Désignation
Pk	Clé publique
Sk	Clé secrète
m	Message claire
CT	Message chiffré
$ENC_k(m)$	Opération de chiffrement de message claire m en utilisant la clé k
$DEC_k(CT)$	Opération de déchiffrement de message chiffré CT en utilisant la clé k

Sécurité d'un crypto-système

- Un crypto-système est **sûr** (sécurisé) s'il garantit qu'**aucun** intervenant n'a la possibilité de posséder la **clef** de chiffrement ou de déchiffrer le message en un temps finie raisonnable.

- **La sécurité ne doit reposer que sur la clef de chiffrement, les algorithmes de chiffrement/déchiffrement sont supposés être connus par tout le monde.**

- En 1883, **August Kerckhoffs** publia les principes suivants de sécurité d'un crypto-système
  - **« La sécurité repose sur le secret de la clef en non sur le secret de l'algorithme »**
  - **« Le déchiffrement sans la clef doit être impossible »**
  - **« Trouver la clef à partir du couple (m,CT) doit être impossible en un temps raisonnable ».**

Types des crypto-systèmes

- On peut classer les algorithmes de cryptographie selon plusieurs critères :

Selon le mode d'utilisation de la clé :

- **Chiffrement symétrique** : la même clé est utilisée pour le chiffrement et le déchiffrement;
- **Chiffrement asymétrique**: deux clés sont utilisées , l'une pour chiffrer (clé publique) et l'autre pour déchiffrer (clé privée).

Selon le mode d'opération

- **Chiffrement par Bloc**: le texte en clair est divisé en blocs de tailles identiques
- **Chiffrementpar flot**: le texte est considéré comme un flot de bits (chiffrement par bits)

Cryptographie classique

- **Deux types:**
  - **Par substitution:** remplacement de chaque caractère du texte claire par un caractère de **l'alphabet**
  - **Par transposition:** remplacement de chaque caractère du texte claire par un caractère du **texte lui-même** (changement de position des caractères)

- **Chiffrement par substitution:** plusieurs exemples: chiffrement de César (année 100), chiffrement de Vigenère (année 1553) …etc.

- **Chiffrementpar transposition:** la scytale (400 av.)

Chiffrement de César

- C'est l'un des crypto-système les plus anciens.

- Il s'agit d'un décalage de l'alphabet par une nombre de cases prédéfinit (César a commencé par 3 cases). Le taux de décalage est la clé secrète
  - **Alphabet normale:** A, B, C,……,Z
  - **Alphabet décalée par 3:** D, E, F, ……,Z, A, B, C
  - Puis chaque lettre du texte claire doit être remplacée par le caractère correspondant dans l'alphabet décalée

- Mathématiquement parlant, le chiffrement de César consiste à remplacer le caractère du texte en prenant sa position dans **l'alphabet** par un autre qui est dans la position:

$$ENC_k(\text{caractère}) = (\text{position\_caractère\_alphabet} + k) \bmod \text{taille\_alphabet}$$

- Une faiblesse de ce système est d'essayer toutes les décalage possible (25 en français) jusqu'à arriver au bon choix

Substitution mono-alphabétique

- Vue cette faiblesse, une amélioration a été apportée en permutant les lettres de l'alphabet aléatoirement. Puis, chaque lettre est remplacée par une autre prédéfinie (table de correspondance) .

- Ce type de codage est appelé **substitution mono-alphabétique**. Le décodage devrait être plus difficile. Peut-on essayer tous les décodages possibles?

- Il y a en français 27!=10888869450418352160768000000 possibilités…

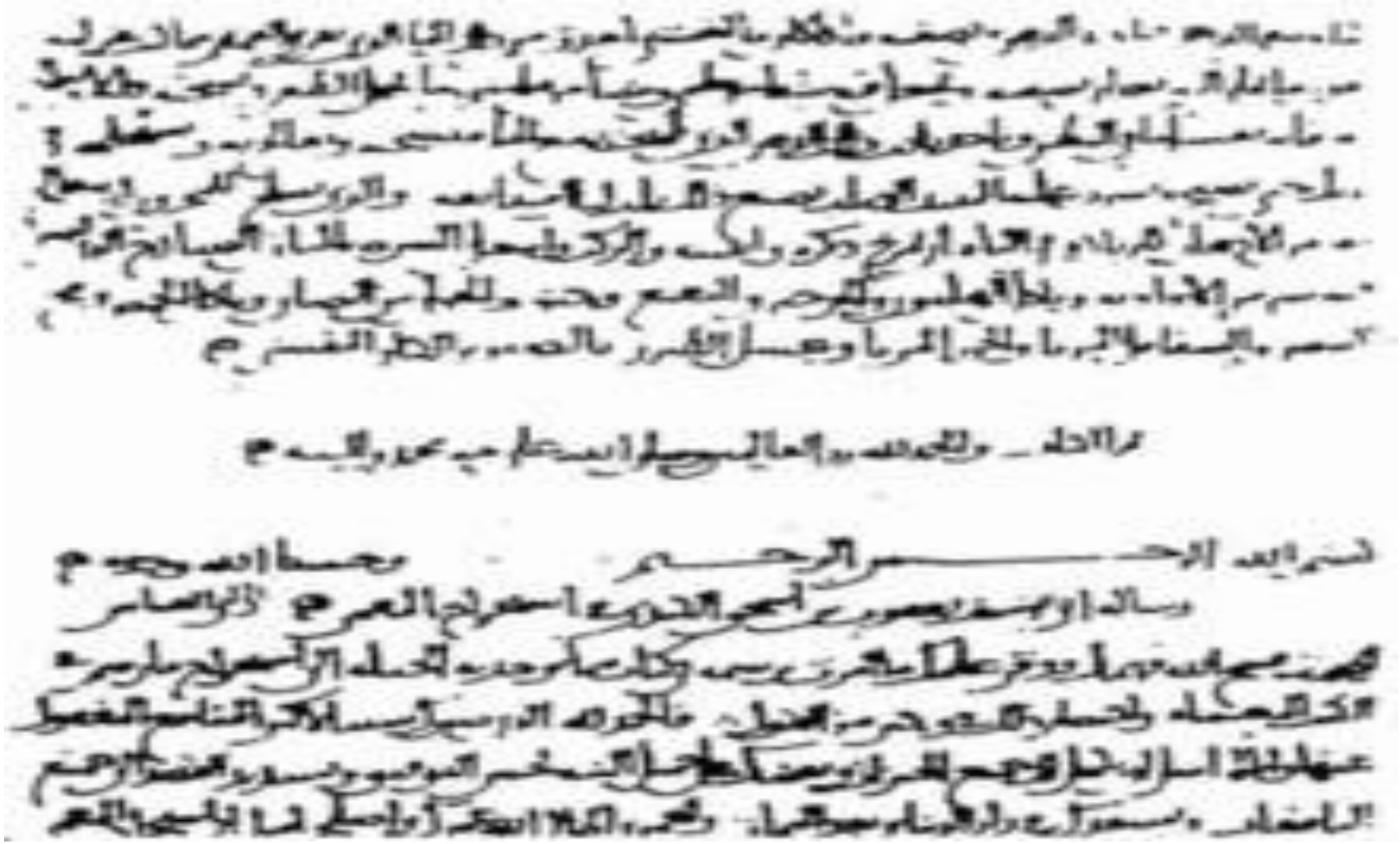
Substitution mono-alphabétique

- Le premier usage révélé de chiffrement par substitution dans un usage militaire est rapporté par Jules César dans **La guerre des Gaules**. César utilisait fréquemment ce type de chiffrement.

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

- Ce sont les **Arabes** qui réussirent à **briser ce code** et qui inventèrent la cryptanalyse au 9ième siècle (**Al-Kindi**). La technique est appelée analyse des fréquences rédigée dans un traité intitulé ≪ *Manuscrit sur le déchiffrement des messages cryptographiques* ≫. (L'ouvrage fut découvert en 1987 dans une bibliothèque à Istanbul)

Substitution mono-alphabétique



Première page du *Manuscrit d'Al-Kindi sur le déchiffrement des messages cryptographiques*

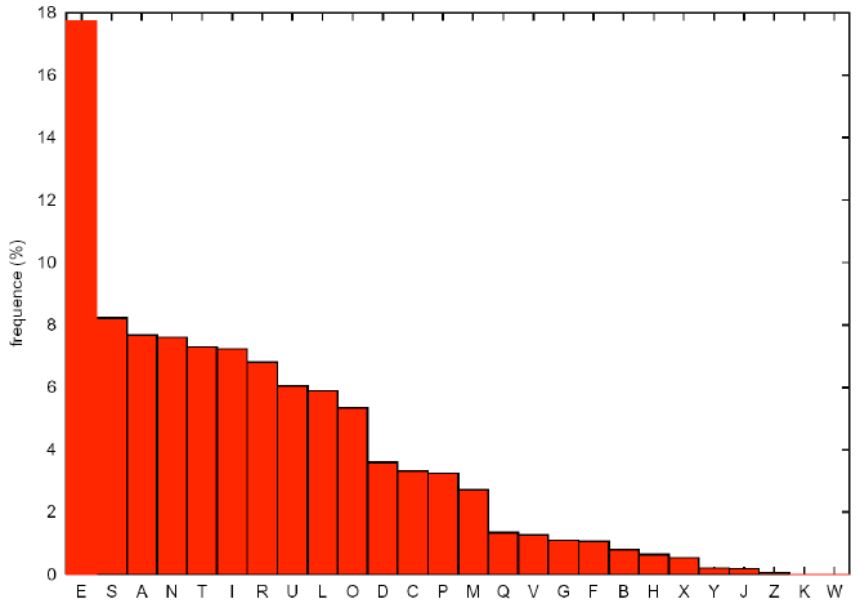
Substitution mono-alphabétique

- Par exemple soit le texte chiffré suivant:

nvxlbgi avxw n ctxnbw ubn dvttbn r bhxqacyb awbggbgi rbn cueciwv lcnibn vqnbcxz rbn tbwn hxq nxqlbgi qgrvubgin mvtacygvgn rb lvscyb ub gclqwb yuqnncgi nxw ubn yvxoowbn ctbwn c abqgb ubn vgi qun rbavnbn nxw ubn aucgmdbn hxb mbn wvqn rb u ckxw tcucrwvqin bi dvgibxz ucqnnbgi aqibxnbtbgi ubxwn ywcgrbn cqubn eucgmdbn mvttb rbn clqwvgn iwcqgbw c mvib r bxz mb lvscybxw cqub mvttb qu bni ycxmdb bi lbxub uxq gcyxbwb nq ebcx hx qu bni mvtqhxb bi ucqr u xg cycmb nvg ebm clbm xg ewxubyxbxub u cxiwb tqtb bg evqicgi u qgoqwtb hxq lvucqi ub avbib bni nbteuceub cx awqgmb rbn gxbbn hxq dcgib uc ibtabib bi nb wqi rb u cwmdbw bzqub nxw ub nvu cx tquqbx rbn dxbbn nbn cqubn rb ybcgi u btabmdbgi rb tcwmdbw

Substitution mono-alphabétique

- En utilisent les fréquences des lettres en français, on remarque que :



Dans le **chiffré :**

B	N	C	U	X	Q	G	I	W	V
18,7	9,91	7,78	6,90	6,72	6,37	5,84	5,84	5,30	4,60

En **français :**

E	S	A	N	T	I	R	U	L	O
17,8	8,23	7,68	7,61	7,30	7,23	6,81	6,05	5,89	5,34

Substitution mono-alphabétique

- On déduit donc que : B→E, N →S, C →A, ce qui donne :

svxlegi avxw s atxsew ues dvttes r ehxqaaye aweggegi res aueaiwvs lasies vqseaxz res tews hxq sxqlegi qgrvuegis mvtaaygvgs re lvsaye ue galqwe yuqssagi sxw ues yvxoowes atews a aeqge ues vgi qus reavses sxw ues auagmdes

hxe mes wvqs re u akxw tauarwvqis ei dvgiexz uaqssegi aqiexsetegi uexws ywagres aques euagmdes mvtte res alqwvgs iwaqgew a mvie r exz me lvsayexw aque mvtte qu esi yaxmde ei lexue uxq gayxewe sq eeax hx qu esi mvtqhxe ei uaqr u xg ayame svg eem alem xg ewxueyxexue u axiwe tqte eg evqiagi u qgoqwte hxq lvuaqi ue aveie esi seteuaeue ax awqgme res gxees hxq dagie ua ietaeie ei se wqi re u awmdew ezque sxw ue svu ax tquqex res dxees ses aques re yeagi u etaemdegi re tawmdew

Substitution mono-alphabétique

•On peut utiliser ensuite les statistiques sur le bigrammes:

Bigrammes les plus fréquents dans le chiffré :

ES	UE	GI	RE	EG	EX	IE	SE	QU	TE	UA	EW	AG	AQ	HX
25	17	13	12	9	8	8	8	8	8	8	7	7	7	7

Bigrammes les plus fréquents en français :

ES	LE	EN	DE	RE	NT	ON	ER	TE	SE	ET	EL	QU	AN	NE	OU	AI

•On peut déduire que : U→ L, R → D , G → N , Q → I

Bigrammes les plus fréquents dans le chiffré (après subst.):

ES	LE	NI	DE	EN	EX	IE	SE	IL	TE	LA	EW	AN	AI	HX
25	17	13	12	9	8	8	8	8	8	8	7	7	7	7

• On peut déduire que: I →T

Substitution mono-alphabétique

- Le texte chiffré devient après substitution :

svxlent avxw s atxsew les dvttes d ehxiaaye awennent des aleatwvs lastes viseaxz des tews hxi sxilent indvlents mvtaaynvns de lvsaye le naliwe ylissant sxw les yvxoowes atews a aeine les vnt ils deavses sxw les alanmdes hxe mes wvis de l akxw taladwvits et dvntexz laissent aitexsetent lexws ywandes ailes elanmdes mvtte des aliwvns twainew a mvte d exz me lvsayexw aile mvtte il est yaxmde et lexle lxi nayxewe si eeax hx il est mvtihxe et laid l xn ayame svn eem alem xn ewxleyxexle l axtwe tite en evitant l inoiwte hxi lvlait le avete est setelaele ax awinme des nxees hxi dante la tetaete et se wit de l awmdew ezile sxw le svl ax tiliex des dxees ses ailes de yeant
l etaemdent de tawmdew

- Quelque mots apparaissent :

indvlent, vnt (V → O); oiseaxz (X → U, Z → X); a aeine (A → P) ; leuws (W → R); taladroits (T → M); yrandes (Y → G)

Substitution mono-alphabétique

- Le texte devient donc:

soulent pour s amuser les dommes d ehuipage prennent des aleatros lastes oiseaux des mers hui suilent indolents mompagnons de losage le nalire glissant sur les gouoores amers a peine les ont-ils deposes sur les planmdes hue mes rois de l akur maladroits et donteux laissent piteusement leurs grandes
ailes elanmdes momme des alirons trainer a mote d eux me losageur aile momme il est gaumde et leule lui naguere si eeau hu il est momihue et laid l un agame son eem alem un erulegueule l autre mime en eoitant l inoirme hui lolait le poete est semelaele au prinme des nuees hui dante la tempete et se rit de l armder exile sur le sol au milieu des duees ses ailes de geant l empemdent de marmder

- On peut facilement continuer le processus et trouver le texte complet (ex: L → V, D → H,h → Q…..)

Chiffrement de Vigenère

- Au 16ième siècle, on brisait les codes de façon routinière. La balle était dans le camp des cryptographes. **Blaise de Vigenère** (1523-1596), inventa un code simple et subtile. Il s'agit d'une amélioration du chiffre par décalage.

- Vigenère est le premier à avoir introduit la notion de **clé**, on choisit un **mot de code** on l'utilise pour chiffrer. Il est répété autant de fois que la taille du texte clair, ensuite chaque lettre du texte est décalée en fonction de la valeur numérique correspondant au symbole de la clé associée.

- Exemple :clé=ALAIN={1,12,1,9,14}

LE_CODE_DE_VIGENERE_EST_IL_INDECHIFFRABLE **(41 symbole)**

ALAINALAINALAINALAINALAINALAINALAINALAINALAINA **(41 symbole)**

MQALBEQAMSAGJPSOQSNNFDUIWMLJWRFOIRTGCBKZF **(41 symbole)**

le Carré de Vigenère

	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

Chiffrement de Vigenère

- Mathématiquement, on considère que les lettres de l'alphabet sont numérotées de 0 à 25 (A=0, B=1 …). La transformationlettre par lettre se formalise simplement par :

$$\text{Chiffré}[i] = (\text{Texte}[i] + \text{Clé}[i]) \textbf{ modulo } 26$$

- Le chiffre de Vigenère est-il indéchiffrable?

- Les **cryptanalystes** furent déjoués pendant près de 3 siècles par le chiffre de **Vigenère** jusqu'au 19ième siècle lorsque **Charles Babbage** réussit à le briser.

- La technique est relativement simple: la première étape consiste à déterminer **la longueur de la clé**. Une fois déterminée , elle servira à **décomposer** le texte chiffré en un ensemble de ***l* suites** de caractères pour une taille l de la clé.

- Chaque suite i parmi les l suites est ensuite **analysée** par la méthode **d'analyse fréquentielle** (d'Al-Kindi) car chaque suite correspond à un chiffrement **mono-alphabétique** par un caractère de la clé.

- La clé est donc déduite en ***l* étapes.**

Chiffrement de Vigenère

- Exemple : soit le texte chiffré suivant:

```
KQOWE FVJPU JUUNU KGLME KJINM WUXFQ MKJBG WRLFN FGHUD WUUMB SVLPS NCMUE KQCTE SWREE
KOYSS IWCTU AXYOT APXPL WPNTC GOJBG FQHTD WXIZA YGFFN SXCSE YNCTS SPNTU JNYTG GWZGR
WUUNE JUUQE APYME KQHUI DUXFP GUYTS MTFFS HNUOC ZGMRU WEYTR GKMEE DCTVR ECFBD JQCUS
WVBPN LGOYL SKMTE FVJJT WWMFM WPNME MTMHR SPXFS SKFFS TNUOC ZGMDO EOYEE KCPJR GPMUR
SKHFR SEIUE VGOYC WXIZA YGOSA ANYDO EOYJL WUNHA MEBFE LXYVL WNOJN SIOFR WUCCE SWKVI
DGMUC GOCRU WGNMA AFFVN SIUDE KQHCE UCPFC MPVSU DGAVE MNYMA MVLFM AOYFN TQCUA FVFJN
XKLNE IWCWO DCCUL WRIFT WGMUS WOVMA TNYBU HTCOC WFYTN MGYTQ MKBBN LGFBT WOJFT WGNTE
JKNEE DCLDH WTVBU VGFBI JG
```

- Phase 1: trouvé la taille de la clé : Soulignez les répétitions de 3 caractères ou plus :

```
KQOWE FVJPU JUUNU KGLME KJINM WUXFQ MKJBG WRLFN FGHUD WUUMB SVLPS NCMUE KQCTE SWREE
KOYSS IWCTU AXYOT APXPL WPNTC GOJBG FQHTD WXIZA YGFFN SXCSE YNCTS SPNTU JNYTG GWZGR
WUUNE JUUQE APYME KQHUI DUXFP GUYTS MTFFS HNUOC ZGMRU WEYTR GKMEE DCTVR ECFBD JQCUS
WVBPN LGOYL SKMTE FVJJT WWMFM WPNME MTMHR SPXFS SKFFS TNUOC ZGMDO EOYEE KCPJR GPMUR
SKHFR SEIUE VGOYC WXIZA YGOSA ANYDO EOYJL WUNHA MEBFE LXYVL WNOJN SIOFR WUCCE SWKVI
DGMUC GOCRU WGNMA AFFVN SIUDE KQHCE UCPFC MPVSU DGAVE MNYMA MVLFM AOYFN TQCUA FVFJN
XKLNE IWCWO DCCUL WRIFT WGMUS WOVMA TNYBU HTCOC WFYTN MGYTQ MKBBN LGFBT WOJFT WGNTE
JKNEE DCLDH WTVBU VGFBI JG
```

Chiffrement de Vigenère

- Ces séquences redondantes peuvent se produire par deux causes :
  - Soit la **même séquence** de lettres du texte clair a été chiffrée avec la **même partie** de la clef ;
  - Soit deux suites de lettres **différentes** dans le texte clair auraient (possibilité faible) par **pure coïncidence** engendré la même suite dans le texte chiffré.
- Pour chaque répétition, mesurer la période

Séquence répétée	Distance
WUU	95
EEK	200
WXIZAYG	190
NUOCZGM	80
DOEOY	45
GMU	90

Chiffrement de Vigenère

- Les **distances** entre les **occurrences** doivent être des **diviseurs de la taille de la clé**, donc pour chaque période, décomposer en **facteurs premiers** et regarder quel **facteur est commun** a tous :

		Longueurs de clef possibles			
Séquence répétée	Espace de 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 est ici longue de **5 caractères**.

Chiffrement de Vigenère

- Les lettres du texte sont ensuite classées en 5 **groupes**:
  -la 1ère, la 6ème, … dans le premier groupe
  -la 2ème, la 7ème, … dans le deuxième groupe
  -la 3ème, la 8ème, dans le troisième groupe
  - …

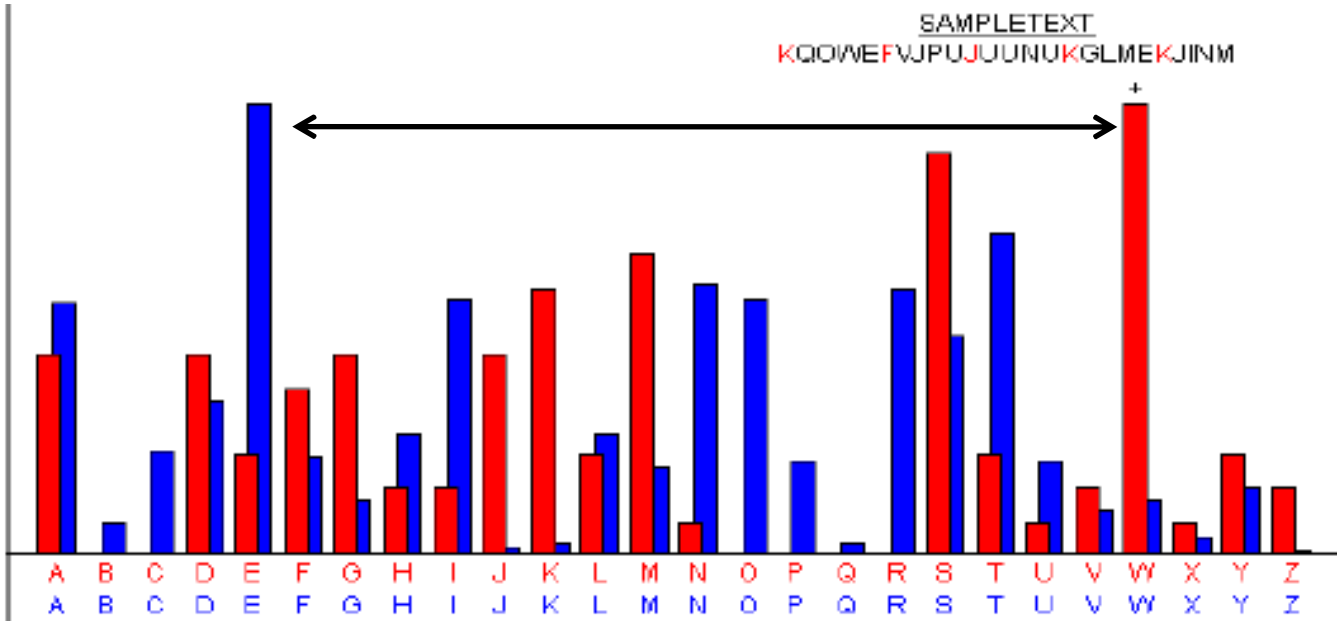
- Puis chaque groupe est ensuite **analysé** selon la méthode d' Al-Kindi, c'est à dire selon une analyse statistique.

- L'analyse statistique permettra de déduire le caractère le **plus fréquent** du texte **chiffré** qui correspondra au caractère le **plus fréquent** de la langue **française** (faire correspondre les deux histogrammes). Ceci va permettre de déduire la première lettre de la clé .

- Le processus et répété sur les autres groupes pour déduire le reste de la clé.

Chiffrement de Vigenère

- En rouge, l'analyse de fréquence du 1ièr groupe, en bleu le diagramme de fréquence des lettres en français.
- On voit que la lettre **W** du groupe correspond a la lettre **E** du français



- Avec **W** = 23 et **E** = 5, on trouve 23 – 5 + 1= 19 donc la première lettre de la clé est **S**.

Chiffrement de Vigenère

- Le même processus est répété pour trouver les autre lettres de la clé en analysent les groupes 2,3,4 et 5.

- La clé trouvée est **SCUBA**,en déchiffrant le texte on trouve:

```
SOUVE NTPOU RSAMU SERLE SHOMM ESDEQ UIPAG EPREN NENTD ESALB ATROS VASTE SOISE AUXDE SMERS
QUISU IVENT INDOL ENTSC OMPAG NONSD EVOYA GELEN AVIRE GLISS ANTSU RLESG OUFFR ESAME RSAPE
INELE SONTI LSDEP OSESS URLES PLANC HESQU ECESR OISDE LAZUR MALAD ROITS ETHON TEUXL AISSE
NTPIT EUSEM ENTLE URSGR ANDES AILES BLANC HESCO MMEDE SAVIR ONSTR AINER ACOTE DEUXC EVOYA
GEURA ILECO MMEIL ESTGA UCHEE TVEUL ELUIN AGUER ESIBE AUQUI LESTC OMIQU EETLA IDLUN AGACE
SONBE CAVEC UNBRU LEGUE ULELA UTREM IMEEN BOITA NTLIN FIRME QUIVO LAITL EPOET EESTS EMBLA
BLEAU PRINC EDESN UEESQ UIHAN TELAT EMPET EETSE RITDE LARCH ERBAU DELAI RE
```

« Souvent pour s'amuser les hommes d'équipage prennent des albatros, vastes oiseaux des mers, qui suivent, indolents compagnons de voyage, le navire glissant sur les gouffres amers.
A peine les ont-ils déposés sur les planches que ces rois de l'azur, maladroits et honteux, laissent piteusement leurs grandes ailes blanches, comme des avirons, traîner à côté d'eux.
Ce voyageur ailé, comme il est gauche et veule, lui naguère si beau, qu'il est comique et laid.
L'un agace son bec avec un brûle-gueule, l'autre mime en boitant l'infirme qui volait.
Le poète est semblable au prince des nuées, qui hante la tempête et se rit de l'archer.
Charles Baudelaire »

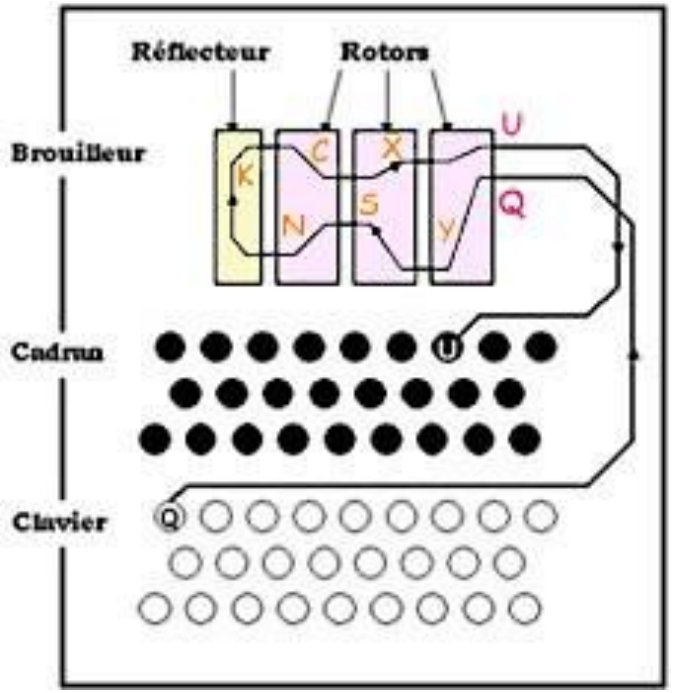
La Machine ENIGMA

- La cryptologie a joué un rôle **décisif** pendant la Seconde Guerre mondiale. Les exploits des alliés en matière de cryptologie auraient permis d'écourter la guerre. **Churchill** citait la cryptographie comme l'un des facteurs clefs de la victoire.

- La guerre a permis une grande évolution de l'art de la cryptographie. Plusieurs techniques ont été élaborées, dont la plus fameuse est la machine **ENIGMA**.

- C'est une machine conçue par les allemands pour chiffrer leurs messages. Cette machine peut être considérée comme la **première machine électromagnétique** traitant de l'information. Elle a permis de lancer l'informatique après la guerre à travers les travaux d'Alain Turing.

La Machine ENIGMA



La Machine ENIGMA

- Brièvement, la machine **Enigma** chiffre les informations en réalisant le passage d'un **courant électrique** à travers une série de composants.

- Le courant est transmis en pressant une **lettre** sur le clavier. Après sa traversée dans un réseau **complexe** de fils, une **lampe indique la lettre chiffrée**. Le premier composant est une série de roues adjacentes, appelées « **rotors** », qui contiennent les fils électriques utilisés pour coder le message. Les rotors tournent, variant la configuration complexe du réseau chaque fois qu'une lettre est tapée. La machine Enigma utilise habituellement une autre roue, nommée « **réflecteur** », et un composant, appelé **pupitre de connexion**, permettant de complexifier encore plus le processus de chiffrement.

La Machine ENIGMA

- La première version d'ENIGMA était utilisée comme suit:

  - Agencement des 3 rotors:123, 132, 213, 231, 312, 321 (6 possibilités).
  - Position des trois rotors, 3 lettres.(26x26x26=17 576 possibilités).
  - Connexionsdes fiches (26 connexions). 100 391 791 500 possibilités.
  - Nombre total de clefs:

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

10 million de milliard de possibilités…

  - Tout tentative de casser la machine sans avoir la clé semble quasi impossible!

La Machine ENIGMA

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

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

- Peu après, la Pologne fut prise par les Allemands et le bureau de chiffrement anglais récupéra les travaux de Rejewski, dans le plus grand secret.

- Un étudiant s'amusa un jour à programmer en langage C la simulation du fonctionnement d'une machine **Enigma**. Ce programme fut inclus dans les distributions **UNIX** sous le nom de **crypt** (utilisable comme une commande UNIX).

La Machine ENIGMA

- Plusieurs autres codes ont vu le jour pendant la guerre mondiale :
  - Code ADFGVX: utilisé par les allemands, c'est une amélioration du carré de polybe;
  - Code UBCHI: utilisé aussi par les allemands;
  - Le code de lorenz: le premier chiffrement par flot;
  - …….

- Avec l'avancement des sciences **mathématiques**, les algorithmes de cryptographie deviennent de plus en plus **complexes** et **robustes**.

- Deux exemples simples de chiffrements qui utilisent des transformations mathématiques sont:
  - Le chiffrement de **Hill** (1929)
  - Le chiffrement affine.

Cryptographie moderne

- D'un autre coté, dès 1977, D.Rivest, A.Shamir et L.Adleman proposent un nouvel principe, celui de la **cryptographie asymétrique** avec leur algorithme **RSA**, basé sur les nombres **premiers** et l'exponentiation modulaire.

- Une version améliorée du RSA : Le **PGP** est proposé par **Philip Zimmermann** en 1991 pour être utilisé à grande échelle et sur des machines personnelles. Elle demeure un standard fiable jusqu'à nos jours.

- En 1994, **Taher ElGamel** a publié un nouveau standard asymétrique connu sous le nom « algorithme d'**ElGamel** » utilisant le problème du **logarithme discret**. Il est considéré actuellement comme un standard comparable à RSA.

- Ce qu'on va voir dans la suite de ce chapitre