

# Introduction à la cryptographie

---

Louiza Khati

3A  
Partie 1



# ANSSI



- Création juillet 2009
- Acteur majeur de la cyber sécurité en France
- Rôles :
  - Favorise le développement de la cyber sécurité en France
  - Apporte son expertise et son assistance aux administrations et aux industriels
  - Encadre et délivre des « visas de sécurité » (via CCN)
  - Forme les citoyens et entreprises (guides)
  - Etc.





# Laboratoire cryptographie

---

- Favorise la recherche dans ce domaine
- Echange sur les différents sujets auprès des acteurs internationaux
- Participe à la mise en place des bonnes pratiques crypto (guides)
- Apporte son expertise (certifications)

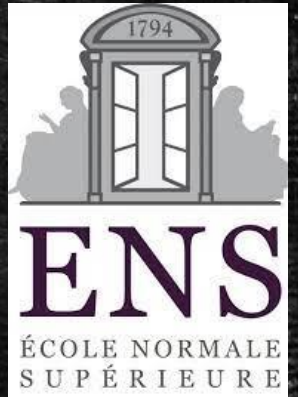




# Mon parcours

---

- 2009-2013 : Ecole d'ingénieur (double diplôme)
  - + Master recherche
- 2013-2017 : Evaluatrice cryptographie (CESTI)
- 2016-2019 : Thèse à l'ENS sur la cryptographie (symétrique)
- 2017-2020 : Experte au laboratoire Sécurité des composants (LSC)
- 2020 - : Experte au laboratoire cryptographie (LCR)
- 2017 - : Formatrice cryptographie (école/entreprise)

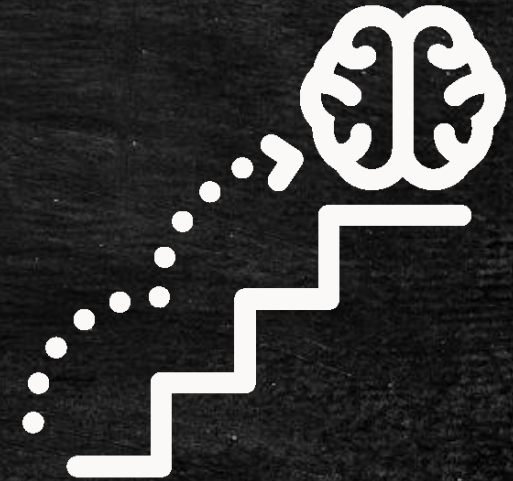




# Module cryptographie

---

- Introduction à la cryptographie
  - Cryptographie : domaine riche et complexe
- Objectifs :
  - Découvrir la cryptographie
  - Donner des intuitions
  - Connaître des exemples de constructions
  - Dépend de vous 😊
- Méthodes :
  - Cours + TD (contrôle continu)
  - Examen (1h)/semestre





# Ce cours

---

- Ne pas hésitez à poser des questions
  - Notions inconnues/floues
- Si c'est trop lent, trop rapide
- Répondre aux questions
  - Cours plus interactif → plus agréable!
  - Apprentissage plus rapide!
- Prendre des notes!!



A vous de jouer!




A bien connaitre!  
(aide à la révision seulement)



# Ce cours : Notation

---

- 1 Examen/semestre

- 1h avec un stylo seulement
- L'ensemble du cours (aide avec )

- Notation continue

- Exercices en cours
- TPs

- Remarque : toujours avoir son PC, stylo + feuilles!



A vous de jouer!



# Ce cours : Activités

---

- Chacun aura une fiche cartonnée
- Prendre soin de cette fiche !
  - Ne pas écrire dessus (ne pas l'abimer)
  - La rendre à la fin du cours !
- Mini-challenge à résoudre



A vous de jouer!



# La cryptographie

---

- « Science des écritures cachées »
- Grec ancien : « cruptos » (caché) et « graphein » (écriture)



- Objectif : garantir la « sécurité » des communications malgré la présence d'attaquants extérieurs



# La cryptologie

---

La cryptographie



Construire des primitives,  
des protocoles

La cryptanalyse



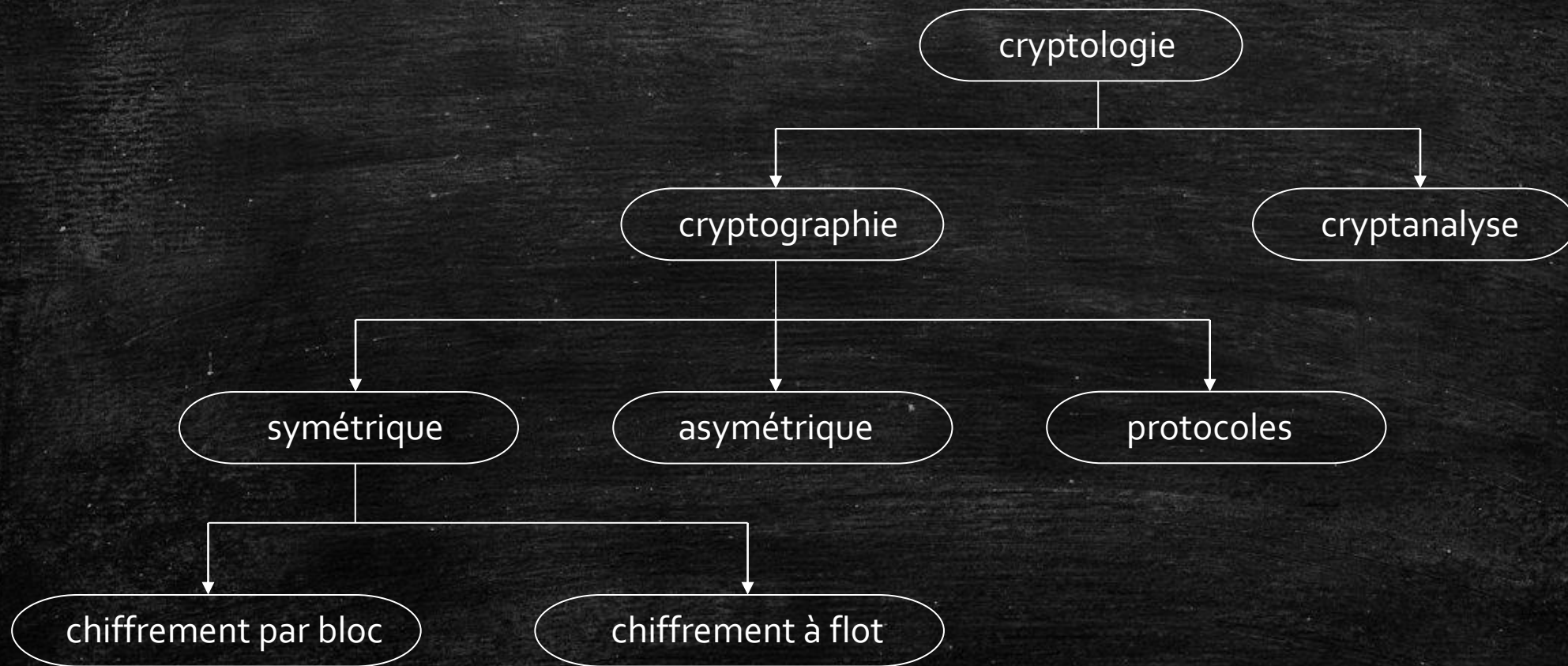
Mettre en évidence des  
faiblesses (« casser »)





# La cryptologie

---

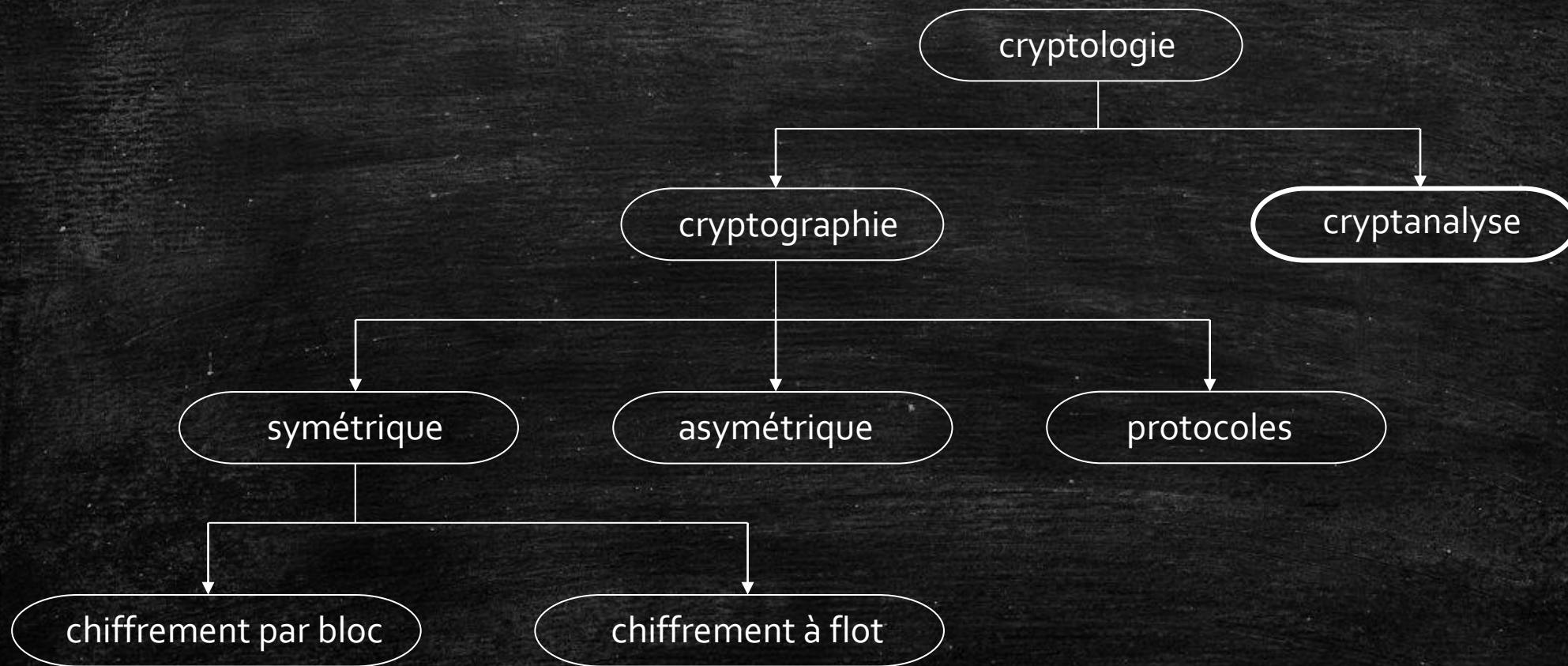


simplification !



# La cryptologie

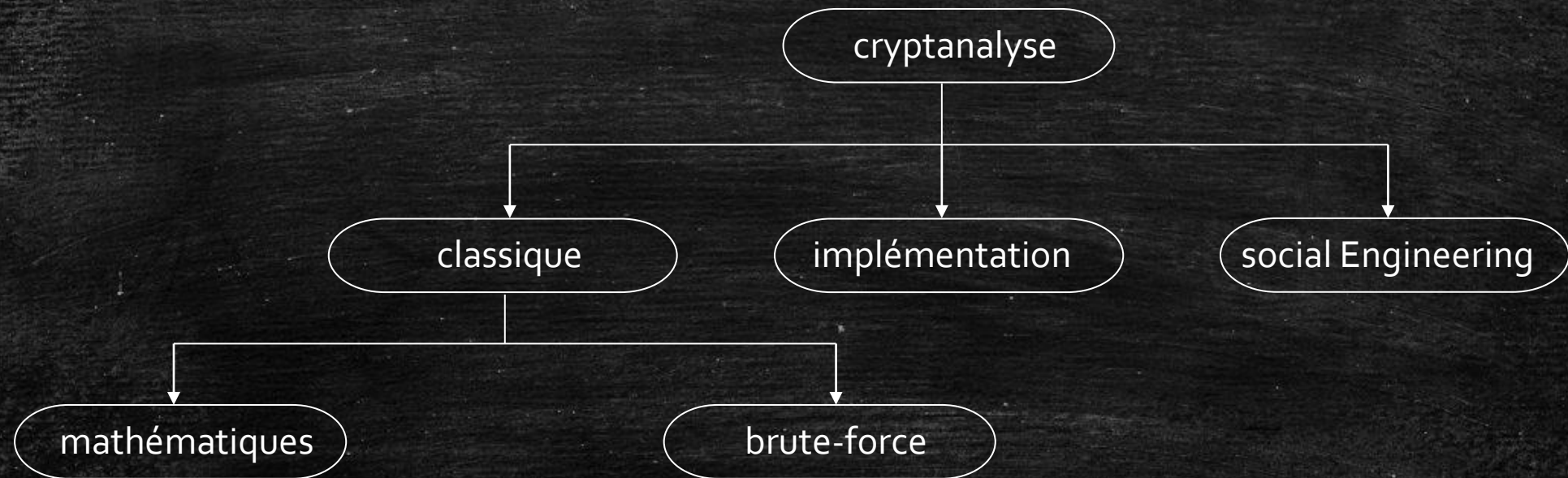
---





# La cryptanalyse

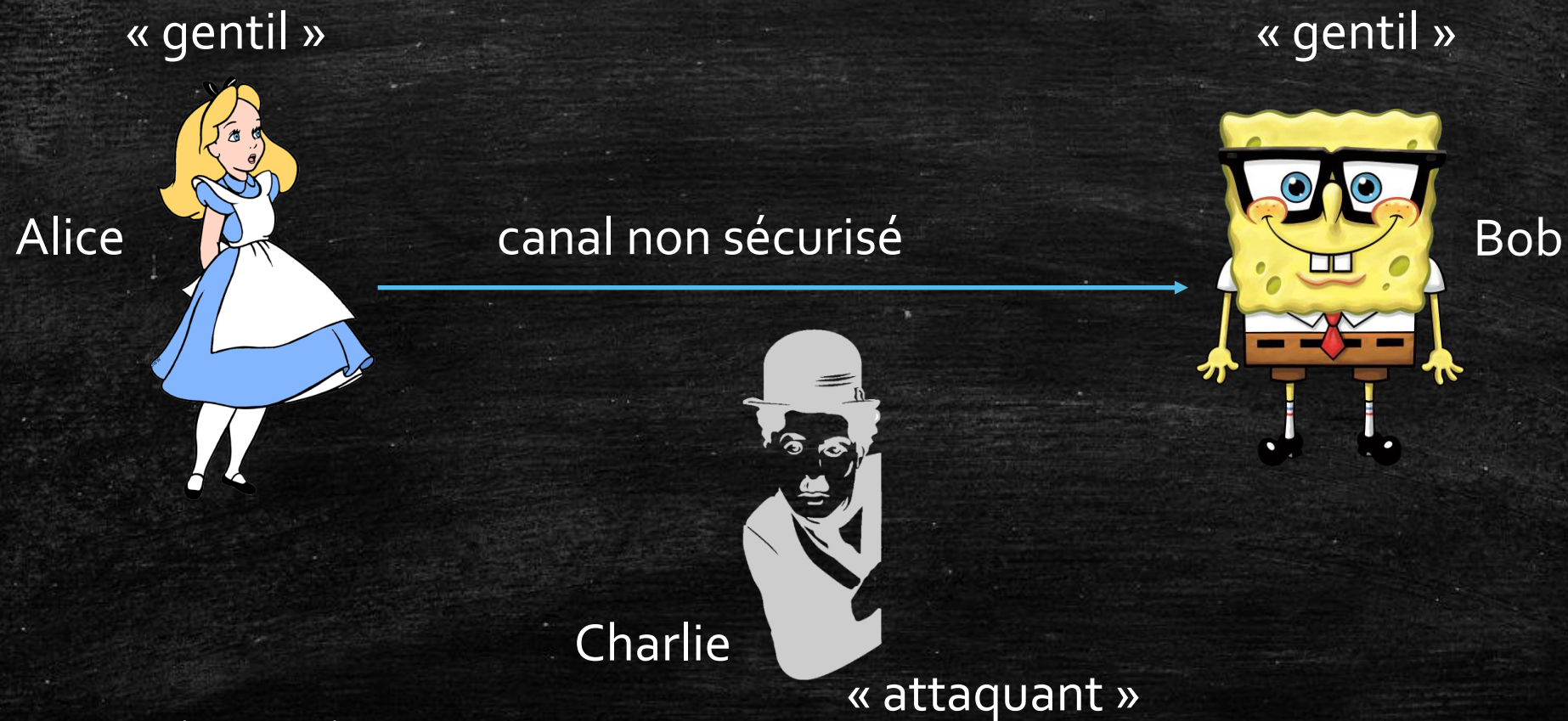
---





# Le scénario classique

---





# Les attaques

---

- « Oreille indiscreète » → écoute de flux
- Altération des données
- Répétition du message
- Retardement de la transmission
- Destruction du message
- Usurpation d'identité
- Répudiation du message
- Etc.

Canal non sécurisé

---

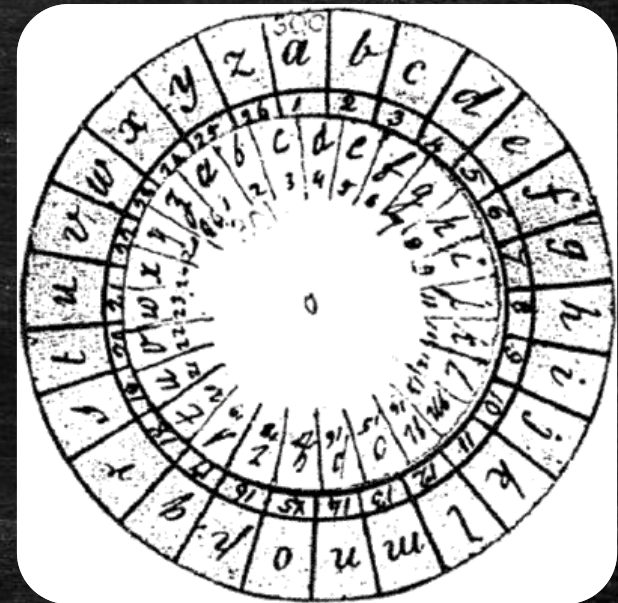


Charlie



# Un peu d'histoire : Cryptographie

- Très vieille discipline
- Jeux de symboles/lettres
- Avant le 20<sup>ème</sup> siècle
  - Systèmes très simples à utiliser
  - Chiffrement manuel



Cryptographe de weatstone



# Stéganographie

---

- Définition : Principe de cacher un message

- Exemples :





# Stéganographie

---

- Définition : Principe de cacher un message
- Exemples :
  - Ecriture sur le cuir chevelu
  - Tablette de cire
  - Encre invisible : jus de citron, lait, vinaigre
  - Abbé Jean de Trithème (une lettre = morceaux de phrase)
  - Cacher un message dans une image





# Stéganographie

---

- Auguste Mangeot publia dans *Le Monde musical* le sonnet suivant qu'il trouvait admirable bien qu'adressé par un correspondant anonyme :

Musique, tu me fus un palais enchanté  
Au seuil duquel menaient d'insignes avenues  
Nuit et jour, des vitraux aux flammes continues,  
Glissait une adorable et vibrante clarté.  
Et des chœurs alternant, - dames de volupté,  
Oréades, ondins, faunes, prêtresses nues, -  
Toute la joie ardente essorait vers les nues,  
Et toute la langueur et toute la beauté.  
Sur un seul vous de moi, désir chaste ou lyrique,  
Ta fertile magie a toujours, ô musique :  
Bercé mon tendre songe ou mon brillant désir.  
Et quand viendra l'instant ténébreux et suprême,  
Tu sauras me donner le bonheur de mourir,  
En refermant les bras sur le Rêve que j'aime !





# Stéganographie

---

- Auguste Mangeot publia dans *Le Monde musical* le sonnet suivant qu'il trouvait admirable bien qu'adressé par un correspondant anonyme :

Musique, tu me fus un palais enchanté  
Au seuil duquel menaient d'insignes avenues  
Nuit et jour, des vitraux aux flammes continues,  
Glissait une adorable et vibrante clarté.  
Et des chœurs alternant, - dames de volupté,  
Oréades, ondins, faunes, prêtresses nues, -  
Toute la joie ardente essorait vers les nues,  
Et toute la langueur et toute la beauté.  
Sur un seul vou de moi, désir chaste ou lyrique,  
Ta fertile magie a toujours, ô musique :  
Bercé mon tendre songe ou mon brillant désir.  
Et quand viendra l'instant ténébreux et suprême,  
Tu sauras me donner le bonheur de mourir,  
En refermant les bras sur le Rêve que j'aime !

Acrostiche!



# Notion de sécurité : Confidentialité

---

**Protéger le contenu** des informations sauvegardées ou transmises sur un réseau





# Notion de sécurité : Intégrité ou authenticité de la donnée

---

S'assurer de la **non-modification** d'un message, accidentelle ou intentionnelle.





# Notion de sécurité : Authentification (de la personne)

---

S'assurer de la **provenance** d'un message et de **l'authenticité de son émetteur**.





# Notion de sécurité : Non-répudiation

---





# Repères historiques

---

- **Age artisanal** (→1900)
  - Systèmes de substitutions et permutations basiques
  - Faisable avec un crayon et du papier
- **Age technique** (1900 →1970)
  - Substitutions et permutations utilisant des machines mécaniques ou électromécaniques (guerres mondiales)
- **Age paradoxal** (→ aujourd'hui)
  - Nouveaux mécanismes répondant à des questions à priori hors d'atteinte



# Repères historiques

---

- **Age artisanal** (→1900)
  - Systèmes de substitutions et permutations basiques
  - Faisable avec un crayon et du papier
- **Age technique** (1900 →1970)
  - Substitutions et permutations utilisant des machines mécaniques ou électromécaniques (guerres mondiales)
- **Age paradoxal** (→ aujourd'hui)
  - Nouveaux mécanismes répondant à des questions à priori hors d'atteinte



# Chiffrement par transposition

Consiste à **changer l'ordre** des lettres

- Ne modifie pas la fréquence des lettres du texte
- Exemple : le Scytale ou « bâton de Plutarque »
  - Chiffrer :
    - Enrouler la ceinture autour du bâton
    - Écrire une lettre sur chaque circonvolution
  - Déchiffrer :
    - Avoir un bâton identique
    - Enrouler la ceinture autour du bâton et lire

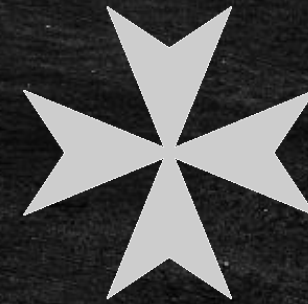
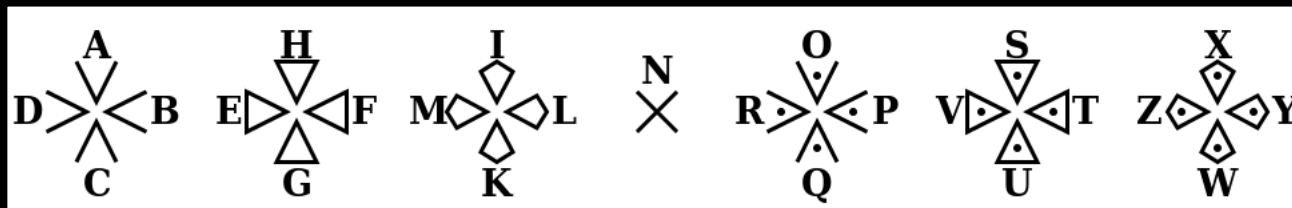




# Chiffrement par substitution

**Remplacer** chaque lettre de l'alphabet d'un message par un symbole (chiffre, lettre, dessin...)

- Exemple : Chiffre des templiers (ou le chiffre de Corneille Agrippa)
  - Remplacer chaque lettre de l'alphabet d'un message par un symbole (chiffre, lettre, dessin...)

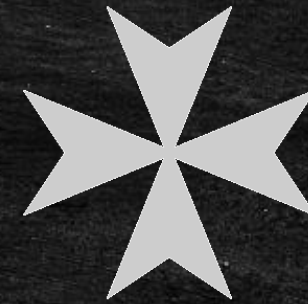
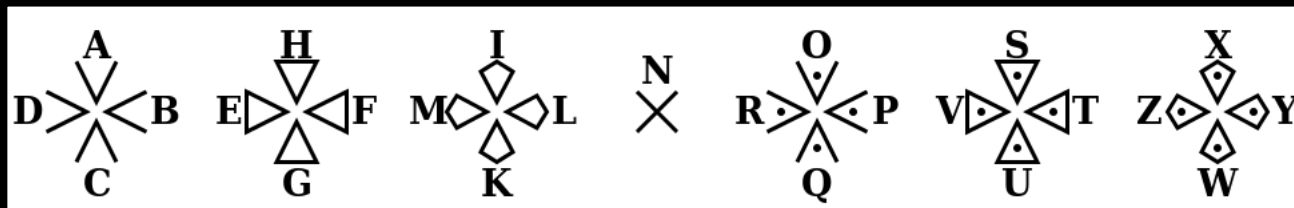




# Chiffrement par substitution

**Remplacer** chaque lettre de l'alphabet d'un message par un symbole (chiffre, lettre, dessin...)

- Exemple : Chiffre des templiers (ou le chiffre de Corneille Agrippa)
  - Remplacer chaque lettre de l'alphabet d'un message par un symbole (chiffre, lettre, dessin...)

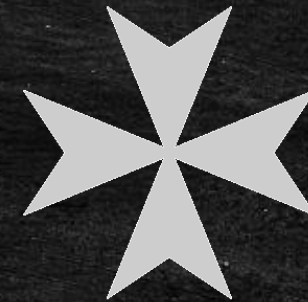
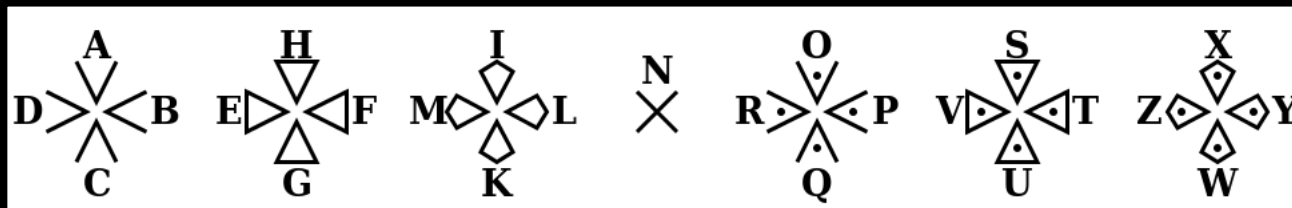




# Chiffrement par substitution

A vous de jouer

Lever la main pour annoncer votre mot en clair!





# Chiffrement par substitution

- Chiffrement **mono-alphabétique**
  - Une lettre en clair est remplacée par une autre lettre
- Chiffrement de César
  - Décalage des positions des lettres
  - Décalage = 3 (César)

Texte clair

Demandez le retrait des troupes



Texte chiffré

Ghpdq ghcoh uhwud lwghv wurxs hv



*Utilisé par César  
d'après Suétone  
(50 avant JC)*





# Chiffrement par substitution

- Chiffrement **mono-alphabétique**
  - Une lettre en clair est remplacée par une unique symbole
- Chiffrement de César
  - Décalage des positions des lettres
  - Décalage = 3 (César)

**A vous de jouer**

**Lever la main pour annoncer votre mot en clair!**



*Utilisé par César  
d'après Suétone  
(50 avant JC)*





# Chiffrement par substitution

---

- Substitution générale

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



# Chiffrement par substitution

---

- Substitution générale

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

Substitution devient ?





# Chiffrement par substitution

---

- Substitution générale

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

Substitution devient Lwzlmomowmogf

Clé ?





# Sécurité

---

- Comment casser un chiffrement mono-alphabétique ?
- Différentes attaques possibles
  - Attaque par recherche exhaustive (« brut force ») : tester toutes les possibilités !
- Dans le cas de la substitution mono-alphabétique :





# Sécurité

---

- Comment casser un chiffrement mono-alphabétique ?
- Différentes attaques possibles
  - Attaque par recherche exhaustive (« brut force ») : tester toutes les possibilités !
- Dans le cas de la substitution mono-alphabétique :
  - Lettre « a » : 26 possibilités
  - Lettre « b » : 25 possibilités
  - Lettre « c » : 24 possibilités
  - ...
  - Lettre « y » : 2 possibilités
  - Lettre « z » : 1 possibilité



# Sécurité

---

- Comment casser un chiffrement mono-alphabétique ?
- Différentes attaques possibles
  - Attaque par recherche exhaustive (« brut force ») : tester toutes les possibilités !
- Dans le cas de la substitution mono-alphabétique :
  - Lettre « a » : 26 possibilités
  - Lettre « b » : 25 possibilités
  - Lettre « c » : 24 possibilités
  - ...
  - Lettre « y » : 2 possibilités
  - Lettre « z » : 1 possibilité

$$26! = 26 \times 25 \times 24 \times \dots \times 1$$

Soit

403 291 461 126 605 635 584 000 000

permutations possibles !

$\approx 2^{88}$  opérations



# Ordres de grandeur

---

- Combien d'opérations peut effectuer un ou plusieurs ordinateurs en un temps fini
  - Ordinateur cadencé à 1 Ghz effectue  $2^{30}$  opérations élémentaires en 1 seconde.
- Que représente  $2^{80}$  opérations ?

A vous de faire le calcul : PC autorisé  
Lever la main quand vous trouvez





# Ordres de grandeur

---

- Combien d'opérations peut effectuer un ou plusieurs ordinateurs en un temps fini
  - Ordinateur cadencé à 1 Ghz effectue  $2^{30}$  opérations élémentaires en 1 seconde.
- Que représente  $2^{80}$  opérations ?
  - $2^{88} \approx 10^{10}$  années à 1 Ghz = nombres d'opérations qu'aurait pu effectuer un ordinateur depuis le début de l'univers...
  - $2^{80} > 10^7$  années à 1Ghz

**On peut effectuer  $2^{62}$  opérations mais  $2^{80}$  n'est pas atteignable en temps raisonnable (moins de 150 ans)**



# Sécurité : Chiffrement mono-alphabétique

---

- Attaque simple
  - Tester toutes les permutations possibles → attaque par force brute

Un peu long ...



- Attaque plus intelligente ?



# Sécurité : Chiffrement mono-alphabétique

- Attaque simple

- Tester toutes les permutations possibles → attaque par force brute



Un peu long ...



- Analyse **fréquentielle** des lettres de l'alphabet

- Un lettre dans le message clair = une lettre dans le message chiffré
- Nombre d'occurrence de chaque lettre est facilement calculé!



# Analyse de fréquence

nvxlbgi avxw n ctnxbw ubn dvttbn r bhxqacyb  
awbggbgi rbn cueciwn lcnibn vqnbcxz rbn tbwn  
hxq nxqlbgi qgrvubgin mvtacygvgn rb lvscyb  
ub gclqwb yuqnncgi nxw ubn yvxooown ctbwn  
c abqgb ubn vgi qun rbavnb nxbw ubn aucgmdbn  
hxb mbn wvqn rb u ckxw tcucrwwqin 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

Fréquences  
en français

E : 17,8
S : 8,23
A : 7,68

Fréquences  
dans le chiffré

B : 18,7
N : 9,91
C : 7,78

B	→	E
N	→	S
C	→	A



# Analyse de fréquence

nvxlegi avxw n ctxnew uen dvttten r ehxqacye  
aweggegi ren cuceiwvn lcnien vqneecxz ren tewn  
hxq nxqlégi qgrvuegin mvtacygvgn re lvscye  
ue gclqwe yuqnncgi nxw uen yvxooowen ctewn  
c aeqge uen vgi qun reavnen nxw uen aucgmnden  
hxe men wvqn re u ckxw tcucrwwqin ei dvgiexz  
ucqnnegi aqieynetegi uexwn ywcgren cquen eucgmnden  
mvtte ren clqwvgn iwcqgew c mvie r exz  
me lvscyexw cque mvtte qu eni ycxmde ei lexue  
uxq gcyxewe nq eecx hx qu eni mvtqhxe ei ucqr  
u xg cycme nvg eem clem xg ewxueyxexue  
u cxiwe tqte eg evqicgi u qgoqwte hxq lvucqi  
ue aveie eni neteuceue cx awqgme ren gxeen  
hxq dcgie uc ietaeie ei ne wqi re u cwmdew  
ezque nxw ue nvu cx tquqex ren dxeen  
nen cquen re yecgi u etaemdegi re tcwmdew

Fréquences  
en français

E : 17,8
S : 8,23
A : 7,68

Fréquences  
dans le chiffré

B : 18,7
N : 9,91
C : 7,78

B	→	E
N	→	S
C	→	A



# Analyse de fréquence

svxlegi avxw s ctxsew ues dvtttes r ehxqacye  
aweggegi res cueciwws lcsies vqsecxz res tewws  
hxq sxqlegi qgrvuegis mvtacygvgs re lvscye  
ue gclqwe yuqsscgi sxw ues yvxooowes ctews  
c aeqge ues vgi qus reavses sxw ues aucgmde  
hxe mes wvqs re u ckxw tcucrwwqis ei dvgiexz  
ucqsségi aqie~~x~~setegi uexws ywcgres cques eucgmde  
mvtte res clqwvgs iwcqgew c mvie r exz  
me lvscyexw cque mvtte qu esi ycxmde ei lexue  
uxq gcyxewe sq eecx hx qu esi mvtqhxe ei ucqr  
u xg cycme svg eem clem xg ewxueyxexue  
u cxiwe tqte eg evqicgi u qgoqwte hxq lvucqi  
ue aveie esi seteu~~ce~~ue cx awqgme res gxees  
hxq d~~c~~gie uc ietaeie ei se wqi re u cwmdew  
ezque sxw ue svu cx tq~~u~~qex res dxees  
ses cques re yecgi u etaemdegi re tcwmdew

Fréquences  
en français

E : 17,8
S : 8,23
A : 7,68

Fréquences  
dans le chiffré

B : 18,7
N : 9,91
C : 7,78

B	→	E
N	→	S
C	→	A



# Analyse de fréquence

svxlegi avxw s atxsew ues dvtttes r ehxqaaye  
aweggegi res aueaiwvs lasies vqseaxz res tewws  
hxq sxqlegi qgrvuegis mvtaaygvgs re lvsaye  
ue galqwe yuqssagi sxw ues yvxooowes atews  
a aeqqe 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 iwaqqew 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

Fréquences  
en français

E : 17,8
S : 8,23
A : 7,68

Fréquences  
dans le chiffré

B : 18,7
N : 9,91
C : 7,78

B	→	E
N	→	S
C	→	A



# Analyse de fréquence

svxlegi avxw s atxsew ues dvtttes r ehxqaaye  
aweggegi res aueaiwvs lasies vqseaxz res tew  
hxq sxqlegi qgrvuegis mvtaaygvgs re lvsaye  
ue galqwe yuqssagi sxw ues yvxooowes atews  
a aeqqe 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 iwaqqew 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

Bigrammes  
fréquents

ES	LE
EN	DE
AI	TE

Bigrammes  
dans le chiffré

ES	: 25
UE	: 17
RE	: 12
EG	: 9
AQ	: 7

U	→	L
R	→	D
G	→	N
Q	→	I



# Analyse de fréquence

svxleni avxw s atxsew les dvtttes d ehxiaaye  
awenneni des aleaiwvs lasies viseaxz des teww  
hxi sxleni indvlenis mvtaaynvns de lvsaye  
le naliwe ylissani sxw les yvxooowes atews  
a aeine les vni ils deavses sxw les alanmdes  
hxe mes wvis de l akxw taladwviis ei dvniexz  
laissenai aiiexseteni lexws ywandes ailes elanmdes  
mvtte des aliwvns iwainew a mvie d exz  
me lvsayexw aile mvtte il esi yaxmde ei lexle  
lxi nayxewe si eeax hx il esi mvtihxe ei laid  
l xn ayame svn eem alem xn ewxleyxexle  
l axiwe tite en eviiani l inoiwte hxi lviiai  
le aveie esi setelaele ax awinme des nxees  
hxi danie la ietaeie ei se wii de l awmdew  
ezile sxw le svi ax tiliex des dxees  
ses ailes de yeani l etaemdeni de tawmdew

Bigrammes  
fréquents

ES	LE
EN	DE
AI	TE

Bigrammes  
dans le chiffré

ES	: 25
UE	: 17
RE	: 12
EG	: 9
AQ	: 7

U	→	L
R	→	D
G	→	N
Q	→	I



# Analyse de fréquence

svxleni avxw s atxsew les dvtttes d ehxiaaye  
awenneni des aleaiwvs lasies viseaxz des teww  
hxi sxleni indvlenis mvtaaynvns de lvsaye  
le naliwe ylissani sxw les yvxooowes atews  
a aeine les vni ils deavses sxw les alanmdes  
hxe mes wvis de l akxw taladwviis ei dvniexz  
laisseni aiiexseteni lexws ywandes ailes elanmdes  
mvtte des aliwvns iwainew a mvie d exz  
me lvsayexw aile mvtte il esi yaxmde ei lexle  
lxi nayxewe si eeax hx il esi mvtihxe ei laid  
l xn ayame svn eem alem xn ewxleyxexle  
l axiwe tite en eviiani l inoiwte hxi lvlaii  
le aveie esi setelaele ax awinme des nxees  
hxi daniel la ietaeie ei se wii de l awmdew  
ezile sxw le svl ax tiliex des dxees  
ses ailes de yeani l etaemdeni de tawmdew

Bigrammes  
fréquents

ES LE  
EN DE  
AI TE

Bigrammes  
dans le chiffré

IE : 8

I → T



# Analyse de fréquence

svxlent avxw s atxsew les dvtttes d ehxtaaye  
awennent des aleatwvs lastes viseaxz des teww  
hxi sxileni indvlents mvtaaynvns de lvsaye  
le naliwe yllissant sxw les yvxooowes atews  
a aeine les vnt ils deavses sxw les alanmdes  
hxe mes wvis de l akxw taladwvits et dvntexz  
laissent aitéxsetent 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 mvthxe 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

Bigrammes  
fréquents

ES LE  
EN DE  
AI TE

Bigrammes  
dans le chiffré

IE : 8

I → T



# Analyse de fréquence

soxlent aoxw s atxsew les dottes d ehxtaaye  
awennent des aleatwos lastes oiseaxz des teww  
hxi sxileni indolents motaaynons de losaye  
le naliwe yllissant sxw les yoxoowes atews  
a aeine les ont ils deaoses sxw les alanmdes  
hxe mes wois de l akxw taladwoits et dontexz  
laissent aïtexsetent lexws ywandes ailes elanmdes  
motte des aliwons twainew a mote d exz  
me losayexw aile motte il est yaxmde et lexle  
lxi nayxewe si eeax hx il est motihxe et laid  
l xn ayame son eem alem xn ewxleyxexle  
l axtwe tite en eoïtant l inoiwte hxi lolait  
le aoete est setelaele ax awinme des nxees  
hxi dante la tetaete et se wit de l awmdew  
ezile sxw le sol ax tiliex des dxees  
ses ailes de yeant l etaemdent de tawmdew

## Mots dans le chiffré

indvlents

V → Q

oiseaxz

X → U  
Z → X

leuws

W → R



# Analyse de fréquence

soulent aouw s atusew les dottes d ehutaaye  
awennent des aleatwos lastes oiseaux des teww  
hui suileni indolents motaaynons de losaye  
le naliwe yllissant suw les youoowes atews  
a aeine les ont ils deaoses suw les alanmdes  
hue mes wois de l akuw taladwoits et donteuw  
laissent aiteusetent leuws ywandes ailes elanmdes  
motte des aliwons twainew a mote d euz  
me losayeuw aile motte il est yaumde et leule  
lui nayuewe si eeau hu il est motihue et laid  
l un ayame son eem alem un ewuleyueule  
l autwe tite en eoitant l inoiwte hui lolait  
le aoete est setelaele au awinme des nuees  
hui dante la tetaete et se wit de l awmdew  
ezile suw le sol au tilieu des duees  
ses ailes de yeant l etaemdent de tawmdew

## Mots dans le chiffré

indvlents

V	→	O
---	---	---

oiseaxz

X	→	U
Z	→	X

leuws

W	→	R
---	---	---



# Analyse de fréquence

soulent aour s atuser les dottes d ehutaaye  
arennent des aleatros lastes oiseaux des ters  
hui suileni indolents motaaynons de losaye  
le nalire ylissant sur les youoores aters  
a aeine les ont ils deaoses sur les alanmdes  
hue mes rois de l akur taladroits et donteux  
laissent aiteusetent leurs yrandes ailes elanmdes  
motte des alirons trainer a mote d eux  
me losayeur aile motte il est yaumde et leule  
lui nayuere si eeau hu il est motihue et laid  
l un ayame son eem alem un eruleyueule  
l autre tite en eoitant l inoirt hui lolait  
le aoete est setelaele au arinme des nuees  
hui dante la tetaete et se rit de l armder  
exile sur le sol au tilieu des duees  
ses ailes de yeant l etaemdent de tarmder

## Mots dans le chiffré

indv~~l~~ents

V → O

oisea~~x~~z

X → U  
Z → X

leu~~w~~s

W → R



# Analyse de fréquence

---

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;  
Exilé sur le sol au milieu des huées,  
Ses ailes de géant l'empêchent de marcher.

Charles Baudelaire (Les fleurs du mal)



# Chiffrement de Vigenère (1586 - 1863)

- Substitution **poly-alphabétique**
  - Une lettre clair peut être chiffré par différentes lettres
- La clé est la répétition d'un mot (CHIPS)
- La lettre chiffrée : croisement clé/message

Texte

	A	B	C	D	E	F	G	H	I	J	K	L	M	N
A	A	B	C	D	E	F	G	H	I	J	K	L	M	N
B	B	C	D	E	F	G	H	I	J	K	L	M	N	O
C	C	D	E	F	G	H	I	J	K	L	M	N	O	P
D	D	E	F	G	H	I	J	K	L	M	N	O	P	Q
E	E	F	G	H	I	J	K	L	M	N	O	P	Q	R
F	F	G	H	I	J	K	L	M	N	O	P	Q	R	S
G	G	H	I	J	K	L	M	N	O	P	Q	R	S	T
H	H	I	J	K	L	M	N	O	P	Q	R	S	T	U
I	I	J	K	L	M	N	O	P	Q	R	S	T	U	V
J	J	K	L	M	N	O	P	Q	R	S	T	U	V	W
K	K	L	M	N	O	P	Q	R	S	T	U	V	W	X
L	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y

Message I L E S T C A C H E A P A R I S

clé C H I P S C H I P S C H I P S C

chiffré K

clé



# Vigenère : exemple

I L E S T C A C H E A P A R I S

C H I P S C H I P S C H I P S C

chiffré K



	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



# Vigenère : exemple

I L E S T C A C H E A P A R I S

C H i P S C H i P S C H i P S C

chiffré K S M H L E H K W W C W I G A U

	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



# Vigenère : exemple

A vous de jouer!

Lever la main pour annoncer  
votre mot en clair!

Pas de PC!



Le secret est : DYNA

	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



# Vigenère : exemple

I L E S T C A C H E A P A R I S

C H I P S C H I P S C H I P S C

chiffré K S M H L E H K W W C W I G A U


Limite ?



	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 : limite

- La clé est répétée
- Vers le chiffrement de Vernam
- Rappels sur l'opérateur « ou exclusif » : opérateur binaire 
  - Calculs très rapides
  - Opérations :
    - $a \text{ xor } b = b \text{ xor } a$
    - $a \text{ xor } a = 0$
    - $a \text{ xor } 0 = a$
    - $a \text{ xor } b = c \rightarrow c \text{ xor } a = b$
  - Permet de « masquer » une valeur

	0	1
0	0	1
1	1	0



# Chiffrement de Vigenère

---

- Chiffrement de Vernam, masque jetable
- Clé binaire générée aléatoirement  $K = b'011101100'$  (usage unique)
- Taille de la clé = taille du message

Message      1 0 1 0 0 1 0 1 1 1 0 1



Clé            0 1 1 1 0 1 1 0 0 1 0 0

---

Chiffré





# Chiffrement de Vigenère

---

- Chiffrement de Vernam, Masque jetable
- Clé binaire générée aléatoirement  $K = b'011101100'$  (usage unique)
- Taille de la clé = taille du message

Message      1 0 1 0 0 1 0 1 1 1 0 1



Clé            0 1 1 1 0 1 1 0 0 1 0 0

---

Chiffré       1 1 0 1 0 0 1 1 1 0 0 1

Différence avec Vigenère ?





# Chiffrement de Vigenère

---

- Chiffrement de Vernam, Masque jetable
- Clé binaire générée aléatoirement  $K = b'011101100'$  (usage unique)
- Taille de la clé = taille du message

Message      1 0 1 0 0 1 0 1 1 1 0 1



Clé            0 1 1 1 0 1 1 0 0 1 0 0

---

Chiffré       1 1 0 1 0 0 1 1 1 0 0 1

Encodage : ASCII

Secret : « LE BUT DE NOTRE VIE EST  
D ETRE HEUREUSES »

(sans espace)





# Chiffrement de Vigenère

---

- Chiffrement de Vernam, Masque jetable
- Clé binaire générée aléatoirement  $K = b'011101100'$  (usage unique)
- Taille de la clé = taille du message

Message      1 0 1 0 0 1 0 1 1 1 0 1



Clé            0 1 1 1 0 1 1 0 0 1 0 0

---

Chiffré       1 1 0 1 0 0 1 1 1 0 0 1

Différence avec Vigenère ?  
Faiblesse ?





# Chiffre de Vernam (1917)

---

- Masque jetable
- Clé binaire générée aléatoirement  $K = b'011101100'$  (usage unique)
- Taille de la clé = taille du message
- Sécurité **inconditionnelle** :
  - Peu importe la capacité de calcul, incassable si
    - la clé est secrète et aléatoire
    - La clé est à usage unique
    - Taille de la clé = taille du message
- Limite ?





# Chiffre de Vernam (1917)

---

- Masque jetable
- Clé binaire générée aléatoirement  $K = b'o11101100'$  (usage unique)
- Taille de la clé = taille du message
- Sécurité **inconditionnelle** :
  - Peu importe la capacité de calcul, incassable si
    - la clé est secrète et aléatoire
    - La clé est à usage unique
    - Taille de la clé = taille du message
- Limite : inutilisable en pratique

