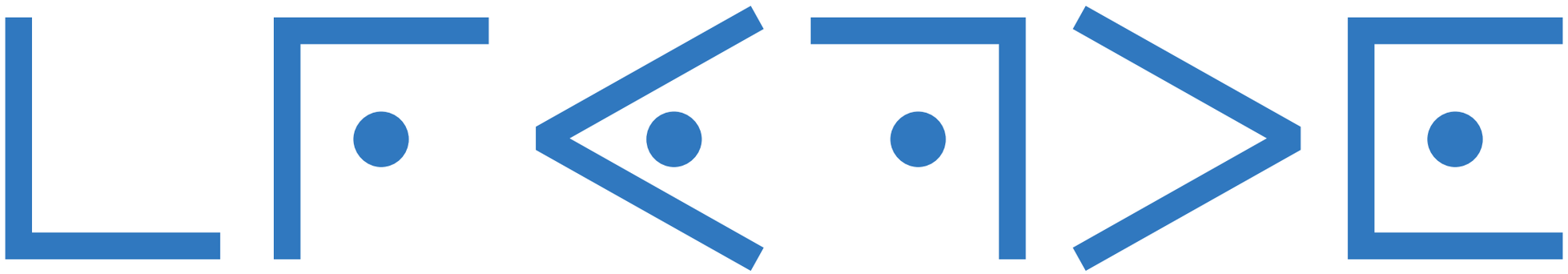
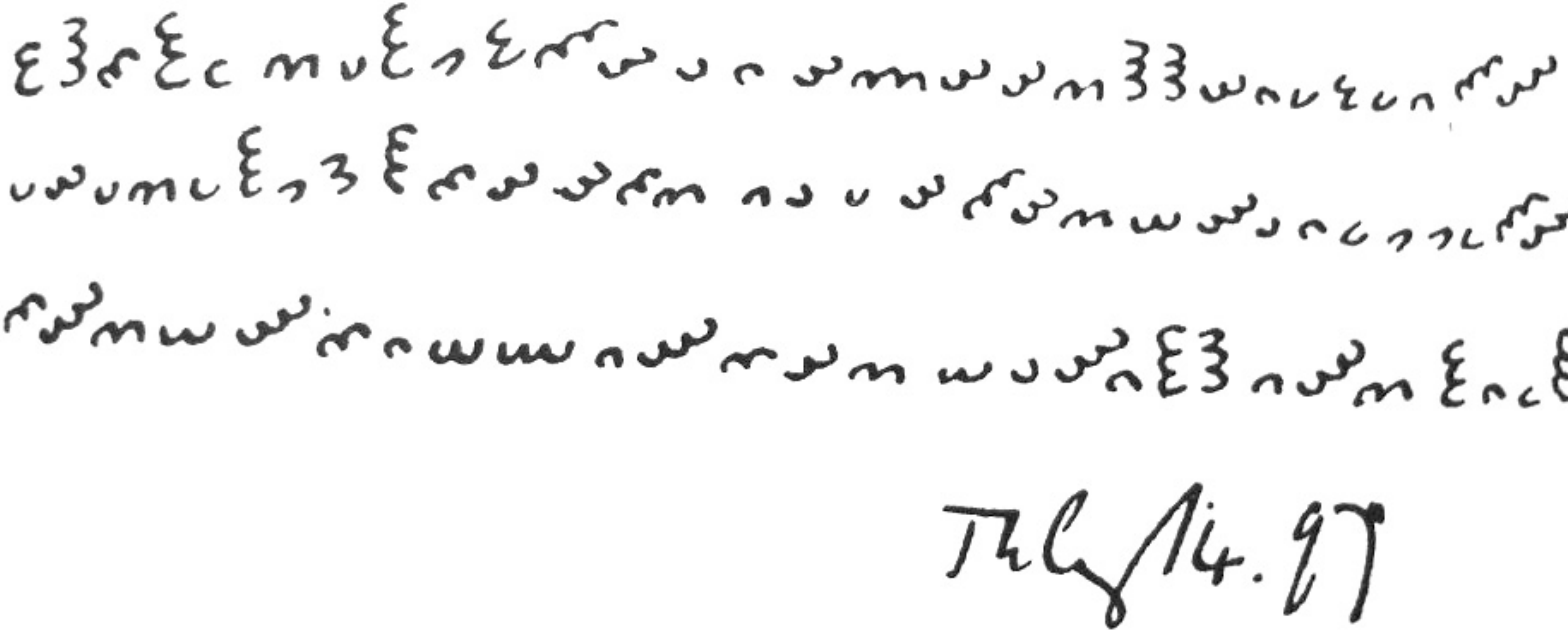


introduction

Nicolas Ollinger

M1 informatique — 2024/2025



Organisation

Cours	8 × 1h30 + 2h	N. Ollinger
TD	4 × 2h	Y. Boichut
TP	4 × 2h	Y. Boichut, N. Ollinger

Support de cours :

https://celene.univ-orleans.fr/course/view.php?id=12813

Prenez des notes pendant les cours !

Évaluation

Note finale = ⅓ **CC** + ⅔ **CT**

- **CT** : examen de 2h sur **Cours** + **TD** + **TP**
- **CC** : des éléments en mode CTF/SPRINT
- **Seconde session** sous forme d’un **CT** de 2h

Programmation en TP et SPRINT

La plupart des TP et le CC nécessitent l'emploi d'un langage pour *scripter* des calculs

Les TP sont écrits et documentés pour **Python**

Dans le langage choisi il faut savoir au moins :

- parcourir et modifier des chaînes et des fichiers
- manipuler et convertir vers et depuis des suites d'octets brutes, de l'UTF-8, des codages hexa, base64, ...
- extraire des sous-chaînes
- combiner des suites de bits à coup de XOR
- faire de l'arithmétique modulaire (+, *, puissance)
- utiliser une bibliothèque crypto complète et sérieuse : primitives usuelles (AES-CTR, SHA, RSA, DH, etc), entrées-sorties (formats PKCS, ASN.1, X509)

Internet Engineering Task Force (IETF)
Request for Comments: 7258
BCP: 188
Category: Best Current Practice
ISSN: 2070-1721

Pervasive Monitoring Is an Attack

Abstract

Pervasive monitoring is a technical attack that should be mitigated in the design of IETF protocols, where possible.

Status of This Memo

This memo documents an Internet Best Current Practi .

Cryptographie et sécurité

Étude des algorithmes et des protocoles permettant de préserver la confidentialité de l'information et de garantir son intégrité.

Trois scénarii **fil rouge** :

(1) Alice veut chiffrer des données pour assurer leur confidentialité

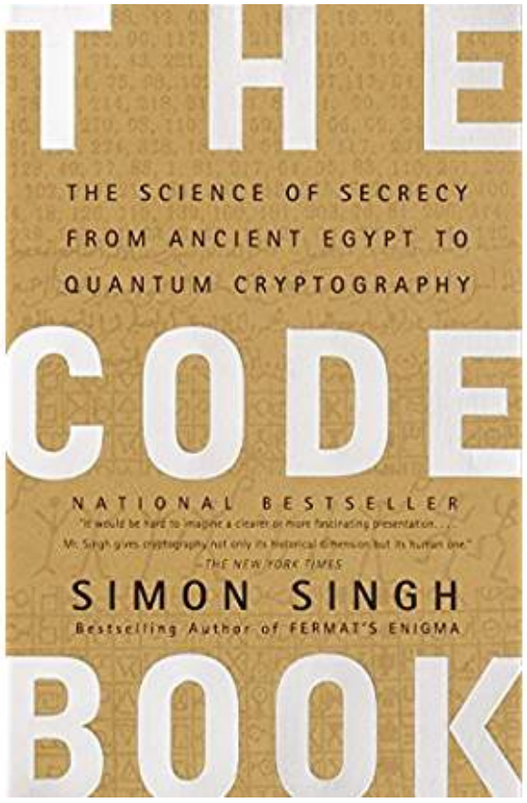
(2) Alice et Bob veulent établir un canal de communication secret à travers un réseau public

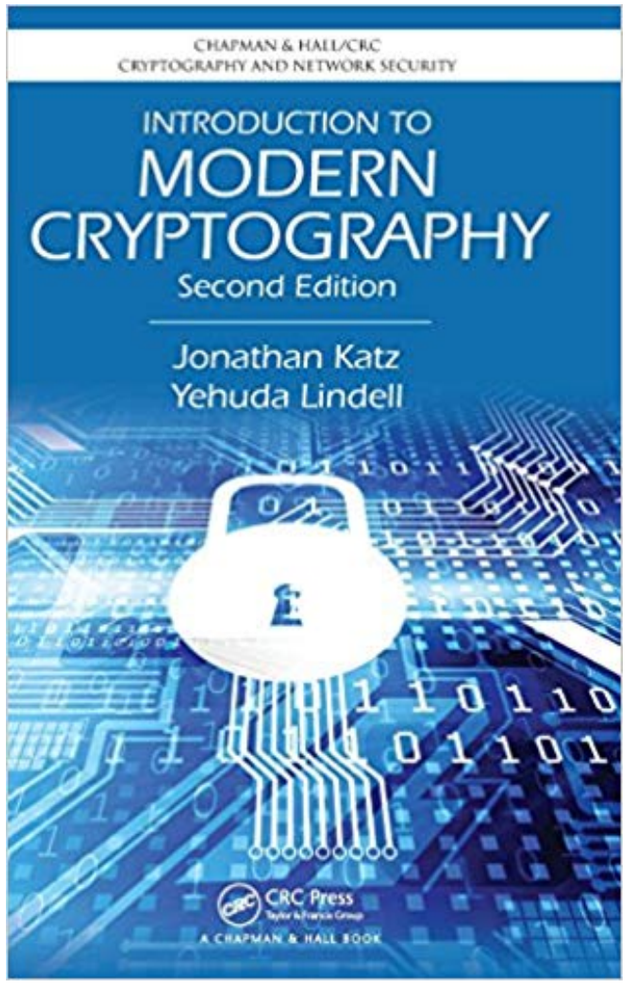
(3) Alice et Bob veulent échanger des messages électroniques signés et/ou chiffrés

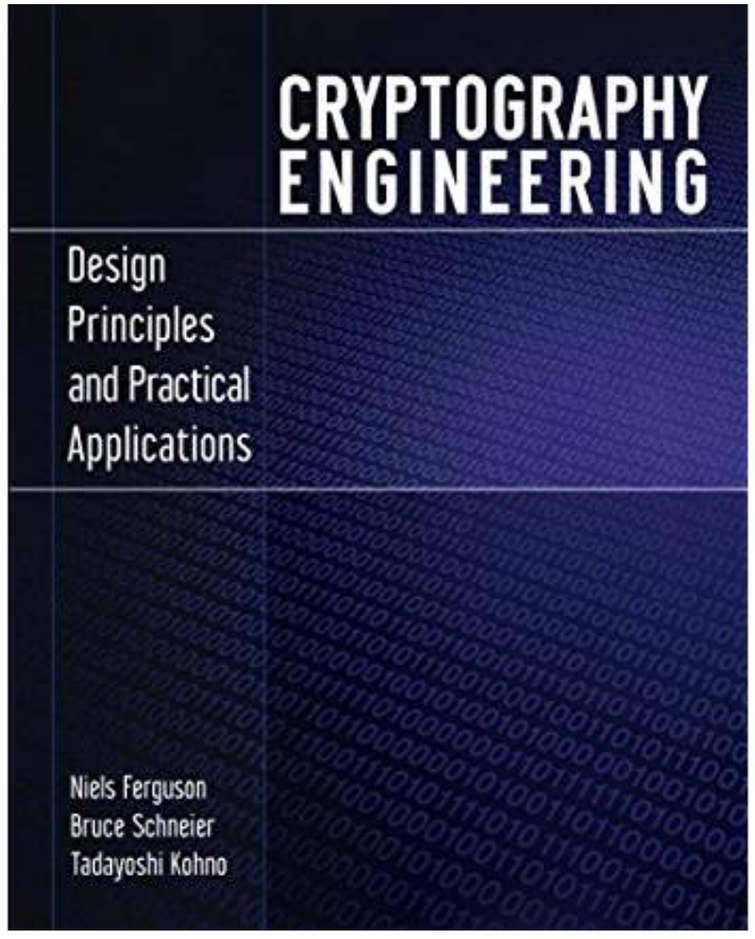
Au programme

1. éléments d'histoire de la cryptologie
2. notions fondamentales et formalisation
3. chiffrement symétrique par flot et par bloc
4. modes opératoires du chiffrement par bloc
5. protocoles, authentification, contrôle d'intégrité
6. hachage et génération de nombres pseudo-aléatoires
7. chiffrement asymétrique : DH, ElGamal
8. chiffrement asymétrique : RSA, courbes elliptiques
9. signature cryptographique, certificats, confiance

Bibliographie



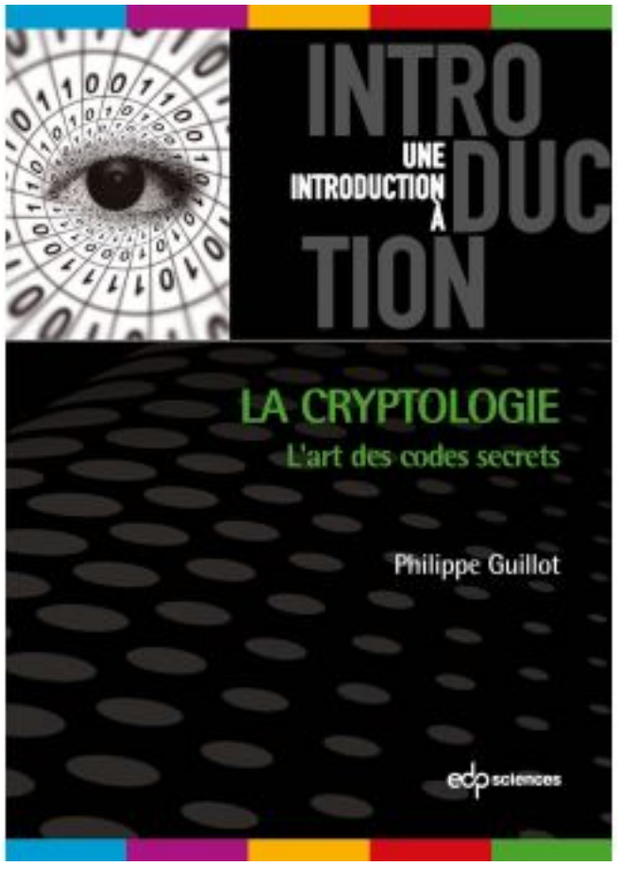


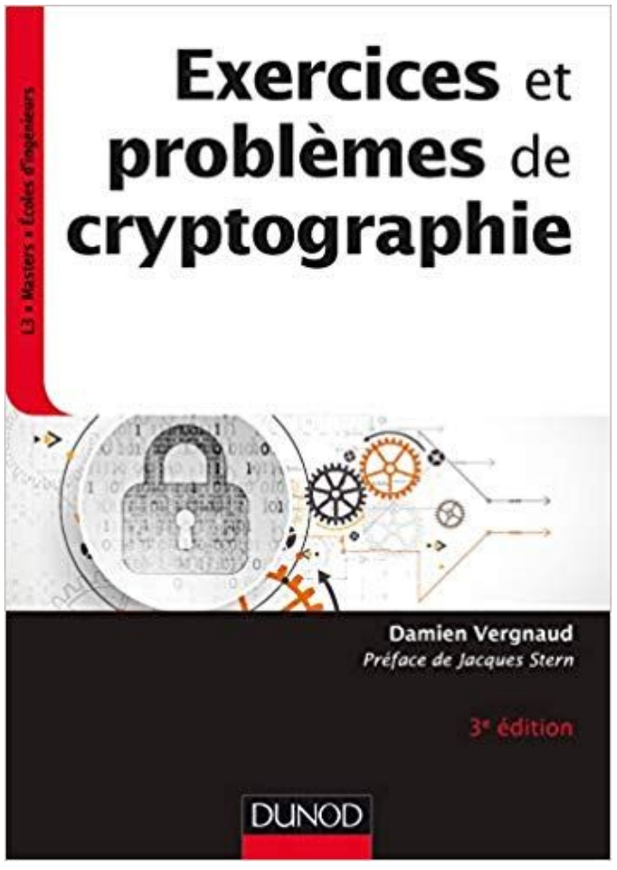


J. Katz et Y. Lindell. *Introduction to Modern Cryptography*, second edition.

N. Ferguson et al. *Cryptography Engineering*.

Bibliographie en français





Ph. Guillot. *Une introduction à la cryptologie*, EDP Sciences.

D. Vergnaud. *Exercices et problèmes de cryptographie*, 3e édition. DUNOD

ON DIT CHIFFRER, ET PAS CRYPTER. :-)

Aux temps anciens...

L'art de la dissimulation

Stéganographie

- ➡ *steganós* : étanche
- ➡ *graphein* : écriture

Déguiser un message dans un autre pour qu'il passe inaperçu.

-600 : Nabuchodonosor utilise des crânes

-480 : Démarate (Sparte) prévient son pays du projet d'invasion de Xerxès (Perse) à l'aide de tablettes de cire

1ier siècle av. J-C. : utilisation d'encre invisible

Échange épistolaire célèbre

« (...)
Quand je jure à vos pieds un éternel hommage
Voulez-vous qu'inconscient je change de langage
Vous avez su captiver les sentiments d'un coeur
Que pour adorer forma le Créateur.
Je vous aime et ma plume en délire.
Couche sur le papier ce que je n'ose dire.
Avec soin, de mes lignes, lisez les premiers mots
Vous saurez quel remède apporter à mes maux.
(...) »

d'Alfred de Musset à Georges Sand

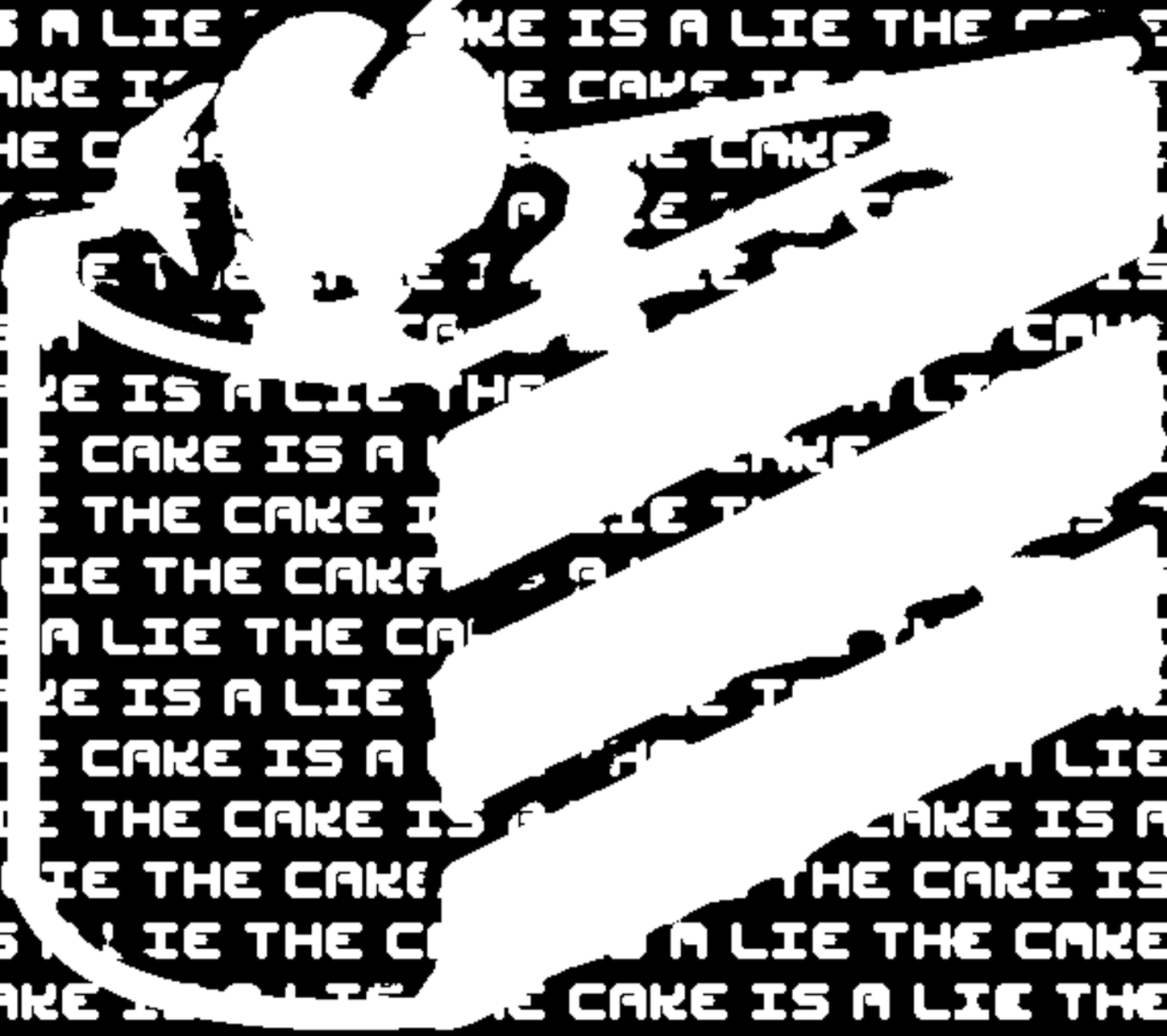
Échange épistolaire célèbre

« (...)
Cette indigne faveur que votre esprit réclame
Nuit à mes sentiments et répugne à mon âme
(...) »

réponse de Georges Sand

Un exemple plus moderne

- Dissimuler un message dans une image
- Chaque pixel code une couleur sur 24 bits
- Utiliser les bits de poids faible de chaque composante RVB pour coder des bits



Ici Londres ! Les Français parlent aux Français

Le Général a trois étoiles

Le coq est anémique

Les farfelus sont réunis

Fernande est amoureuse

Liou est très gentille

On reconstruit la maison de Georgette

Nous boirons bientôt le kirsch d’Alsace

Georges est tombé par terre

Antoine et Jacques sont deux copains

Codes

Un **code** est une table de correspondance (*clé*) fixée entre texte clair et unités correspondante du code secret.

Le sous-marin est attendu à ➟ Jean

10 heures ➟ est là

12 heures ➟ n'est pas là

Peu pratique : taille de clé, structure du texte, caractère statique de la table.

Chiffres

Un algorithme de chiffrement permet de transmettre n'importe quel message (historiquement textes, de nos jours bits donc textes, fichiers, images, binaires, *etc*)

$$C = E(K, M)$$

$$M = D(K, C)$$

Naissance de la cryptographie

Cryptographie

- ➡ *kruptos* : caché
- ➡ *graphein* : écriture

-400 : les scytales spartiates
-100 : chiffre de césar, décalage alphabétique
1580 : Marie Stuart, chiffre par substitution
1586 : *Traité des chiffres*, chiffre de Vigenère
1918 : Enigma, mécanisation
1976 : cryptographie asymétrique
20xx : cryptographie post-quantique

KEISER
SVAR

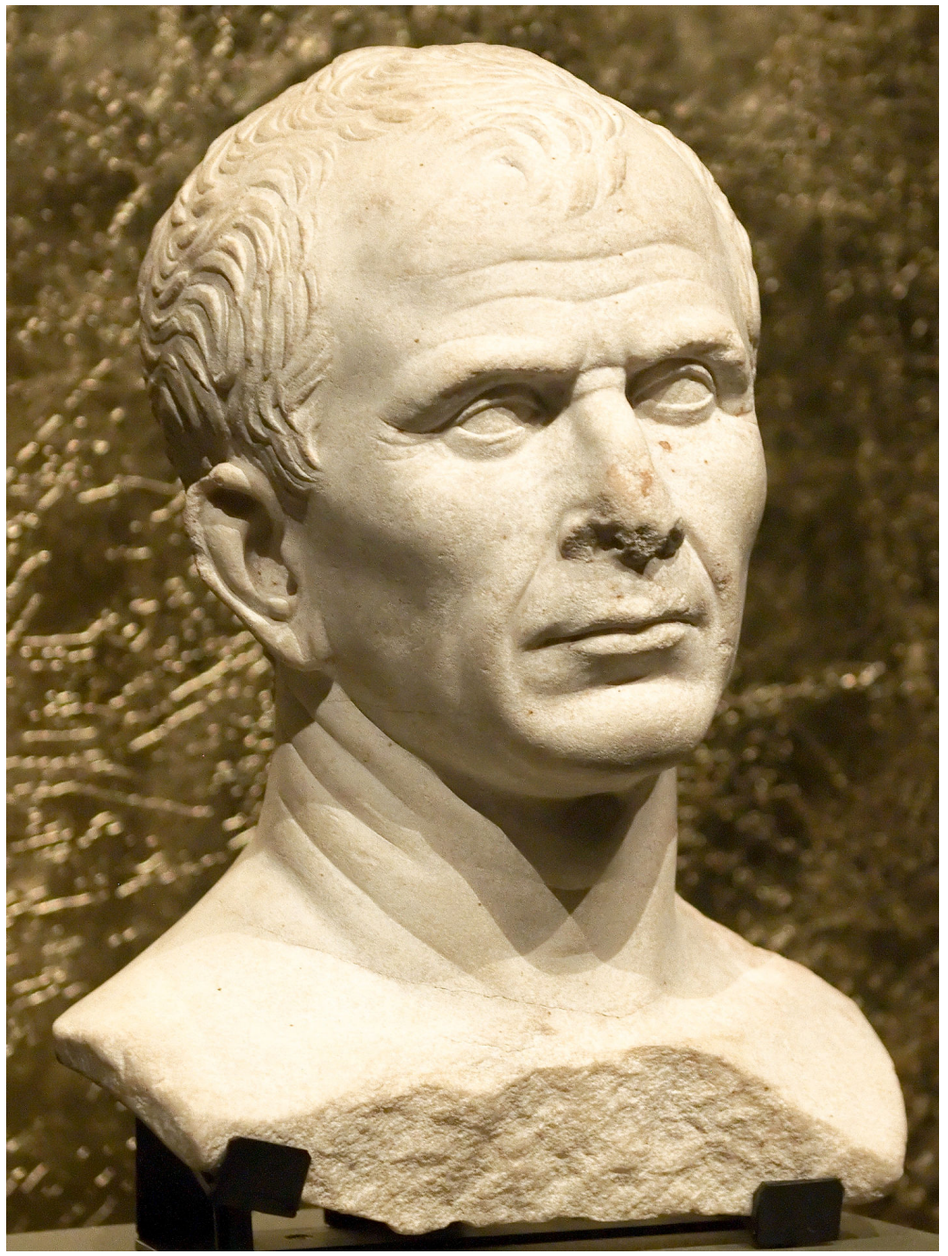
Chiffre de César

Utilisé par Jules César pour sa correspondance secrète.

Chaque lettre du texte est remplacée par celle qui se trouve trois lettres plus loin dans l'alphabet.

A ➡ D, B ➡ E, C ➡ F, ..., Z ➡ C

WX TXRTXH ILOL



Chiffrement par décalage

C'est un chiffre de César avec un autre décalage qui constitue la clé secrète.

Permutation circulaire de l'ensemble des lettres de l'alphabet.

```
ABCDEFGHIJKLMNOPQRSTUVWXYZ
NOPQRSTUVWXYZABCDEFGHIJKLM
```

Ainsi K=3 est le chiffre de César et K=13 est le ROT13 populaire parmis les utilisateurs d'UNIX

Programmation

Algorithme

- On numérote les lettres de 0 à 25
- On choisit une clé $K \in \{1, \ldots, 25\}$
- Pour une lettre $x \in \{0, \ldots, 25\}$

$$E(K, x) = (x + K)_{/26}$$

Exemple

Chiffre du message ZORRO avec $K = 3$

- $E(3, Z) = E(3, 25) = (25 + 3)_{/26} = 28_{/26} = 2 = C$
- $E(3, O) = E(3, 14) = (14 + 3)_{/26} = 17_{/26} = 17 = R$
- $E(3, R) = E(3, 17) = (17 + 3)_{/26} = 20_{/26} = 20 = U$

$$ZORRO \rightarrow CRUUR$$

Pause exercice

Déchiffrer le message suivant sachant qu'il a été chiffré avec un décalage de 12 :

OQEF QZRA DSQM ZFCG

AZPH UQZF RADS QDAZ

Chiffrement par substitution

Généralise le chiffrement par décalage à un chiffrement monoalphabétique arbitraire en autorisant n'importe quelle substitution.

Problème : la clé prend de la place, c'est la permutation complète de l'alphabet.

Chiffrement par substitution

Construction de clé à partir d'un mot de passe

- Etablir une clé (ex : *securite*)
- Supprimer les lettres doubles (ex : *securite* $\rightarrow$ *securit*)
- Faire correspondre les premières lettres de l'alphabet aux lettres de la clé
- Complèter la table en reprenant l'alphabet à partir de la dernière lettre de la clé nettoyée et en supprimant les lettres présentes dans la clé

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

Q	R	S	T	U	V	W	X	Y	Z
G	H	J	K	L	M	N	O	P	Q

Faiblesses du chiffrement par substitution

- Toutes les occurences d'une même lettre est chiffrée de la même manière
- Par conséquent, même chose pour tout groupe de lettres

Une simple analyse des fréquences des lettres casse un chiffrement par substitution

Lettre	Fréquence	Lettre	Fréquence
A	8.25	N	7.25
B	1.25	O	5.75
C	3.25	P	3.75
D	3.75	Q	1.25
E	17.75	R	7.25
F	1.25	S	8.25
G	1.25	T	7.25
H	1.25	U	6.25
I	7.25	V	1.75
J	0.75	W	0
K	0	X	0
L	5.75	Y	0.75
M	3.25	Z	0

Chiffrement polyalphabétique

But : Masquer autant que possible la structure du texte clair i.e. répétitions

- de caractères
- de petits groupes de caractères

Une approche est d'appliquer un décalage fonction de la position du caractère dans le texte

Chiffre de Vigenère

Substitutions alphabétiques multiples par décalage

- On choisit un mot clé
- Le rang de chaque lettre de la clé définit un décalage à appliquer

Exemple

Chiffrer le texte NOUSSOMMESDECOUVERTS avec le carré de Vigenère avec comme clé DECEPTION

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	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	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	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	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
...																									
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
...																									
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	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	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
...																									
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

Texte clair	N	O	U	S	S	O	M	M	E	S	D	E	C	O	U	V	E	R	T	S
Clé répétée	D	E	C	E	P	T	I	O	N	D	E	C	E	P	T	I	O	N	D	E
Texte chiffré	Q	S	W	W	H	H	U	A	R	V	H	G	G	D	N	D	S	E	W	W

Programmation

- $toInt : \ A \ldots Z \mapsto 0 \ldots 25$
- $toLetter : \ 0 \ldots 25 \mapsto A \ldots Z$
- $message, cle, chiffre : \ String$

Algorithme

vigenere(message,cle) =
Debut
    Pour $i := 0$ à $message.size()$ faire
        $chiffre[i] := toLetter((toInt(cle[i_{/cle.size()}]) + toInt(message[i]))_{/26})$
    FinPour
    retourne *chiffre*
Fin

M :	N	O	U	S	S	O	M	M	E	S	D	E	...
	13	14	20	18	18	14	12	12	4	18	3	4	...
K :	D	E	C	E	P	T	I	O	N	D	E	C	...
	3	4	2	4	15	19	8	14	13	3	4	2	...
	16	18	22	22	33	33	20	26	17	21	7	6	...
/26	16	18	22	22	7	7	20	0	17	21	7	6	...
C :	Q	S	W	W	H	H	U	A	R	V	H	G	...

Pause exercice

Déchiffrer le message suivant sachant qu'il a été chiffré avec la clé **`GLADOS`** :

```
ZSEU SAYY OFOC K
```

Chiffrement par xor

$\oplus$ ou *ou-exclusif*

- $1 \oplus 0 = 1$
- $0 \oplus 1 = 1$
- $0 \oplus 0 = 0$
- $1 \oplus 1 = 0$

Chiffrement

1. Une clé K binaire de taille k
2. Une donnée M binaire
3. Découpage de M en blocs de taille k : $m_1, \ldots, m_n$
4. Application de $\oplus$ entre chaque bloc et la clé K

Cryptanalyse

Cryptanalyse

L'objectif de la cryptanalyse est de trouver des algorithmes d'attaque qui permettent de reconstituer l'information sans connaître la clé.

Ou bien en déchiffrant le message en clair

Ou bien en recalculant la clé secrète

Différents types d'attaques

- *Attaque à texte chiffré seul* : Le cryptanalyste dispose uniquement des textes chiffrés de plusieurs messages
- *Attaque à texte clair connu* : textes clairs plus chiffrements. Trouver la clé
- *Attaque à texte clair choisi statique* : Le cryptanalyste peut choisir les textes clairs
- *Attaque à texte clair choisi dynamique* : Le cryptanalyste adapte ses choix en fonction des textes chiffrés précédents
- *Attaques exhaustives ou à force brute* : Essai de toutes les clés possibles

Chiffrement par décalage

- Le texte chiffré EF donne 26 textes clairs possibles
- AB, BC, CD, DE, EF, FG, GH, HI, IJ, JK, KL, LM, MN, NO, OP, PQ, QR, RS, ST, TU, UV, VW, WX, XY, YZ
- Si c'est un mot de deux lettres en français, alors il existe deux clés possibles : $K = 25$ et $K = 11$
- Déchiffrez le message suivant : ZYF A CRYGR NYQ RPMN BSP KYGQ AY TY BCTCLGP SL NCS NJSQ AMKNJGOSC

Cryptanalyse statique

- Attaque à texte chiffré seul
- Corrélation éventuelle entre les propriétés statistiques du texte clair et celles du texte chiffré
- Utilisation de tables de fréquences comme nous l'avons vu précédemment

Lettre	Fréquence	Lettre	Fréquence
A	8.25	N	7.25
B	1.25	O	5.75
C	3.25	P	3.75
D	3.75	Q	1.25
E	17.75	R	7.25
F	1.25	S	8.25
G	1.25	T	7.25
H	1.25	U	6.25
I	7.25	V	1.75
J	0.75	W	0
K	0	X	0
L	5.75	Y	0.75
M	3.25	Z	0

Cryptanalyse statique

- Attaque à texte chiffré seul
- Corrélation éventuelle entre les propriétés statistiques du texte clair et celles du texte chiffré
- Utilisation de tables de fréquences comme nous l'avons vu précédemment

ES	305	TE	163	OU	118	EC	100	EU	89	EP	82
LE	246	SE	155	AI	117	TI	98	UR	88	ND	80
EN	242	ET	143	EM	113	CE	98	CO	87	NS	79
DE	215	EL	141	IT	112	ED	96	AR	86	PA	78
RE	209	QU	134	ME	104	IE	94	TR	86	US	76
NT	197	AN	130	IS	103	RA	92	UE	85	SA	75
ON	164	NE	124	LA	101	IN	90	TA	85	SS	73
ER	163										

Indice de coïncidence

- 1920 : William F. Friedman
- Permet de déterminer
  - s'il s'agit d'un chiffrement mono-alphabétique ou poly-alphabétique
  - la longueur probable de la clé
- Calcul de l'indice de coincïdence
- En français, l'indice de coincïdence est d'environ 0.0746

$$IC = \sum_{l=A}^{l=Z} \frac{n_l(n_l - 1)}{n(n-1)}$$