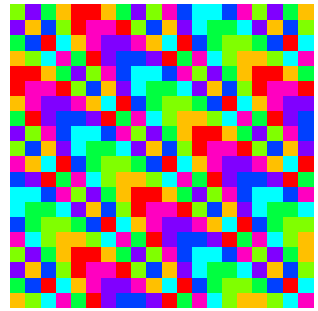
Mathématiques Discrètes (3)

Cryptosystèmes historiques

Michel Rigo
en co-titulariat avec Emilie Charlier

http://www.discmath.ulg.ac.be/

Année 2016–2017



CRYPTOGRAPHIE. N. F.

Art d'écrire en chiffres ou d'une façon secrète quelconque.

Ensemble des principes, méthodes et techniques dont l'application assure le chiffrement et le déchiffrement des données, afin d'en préserver la confidentialité et l'authenticité.

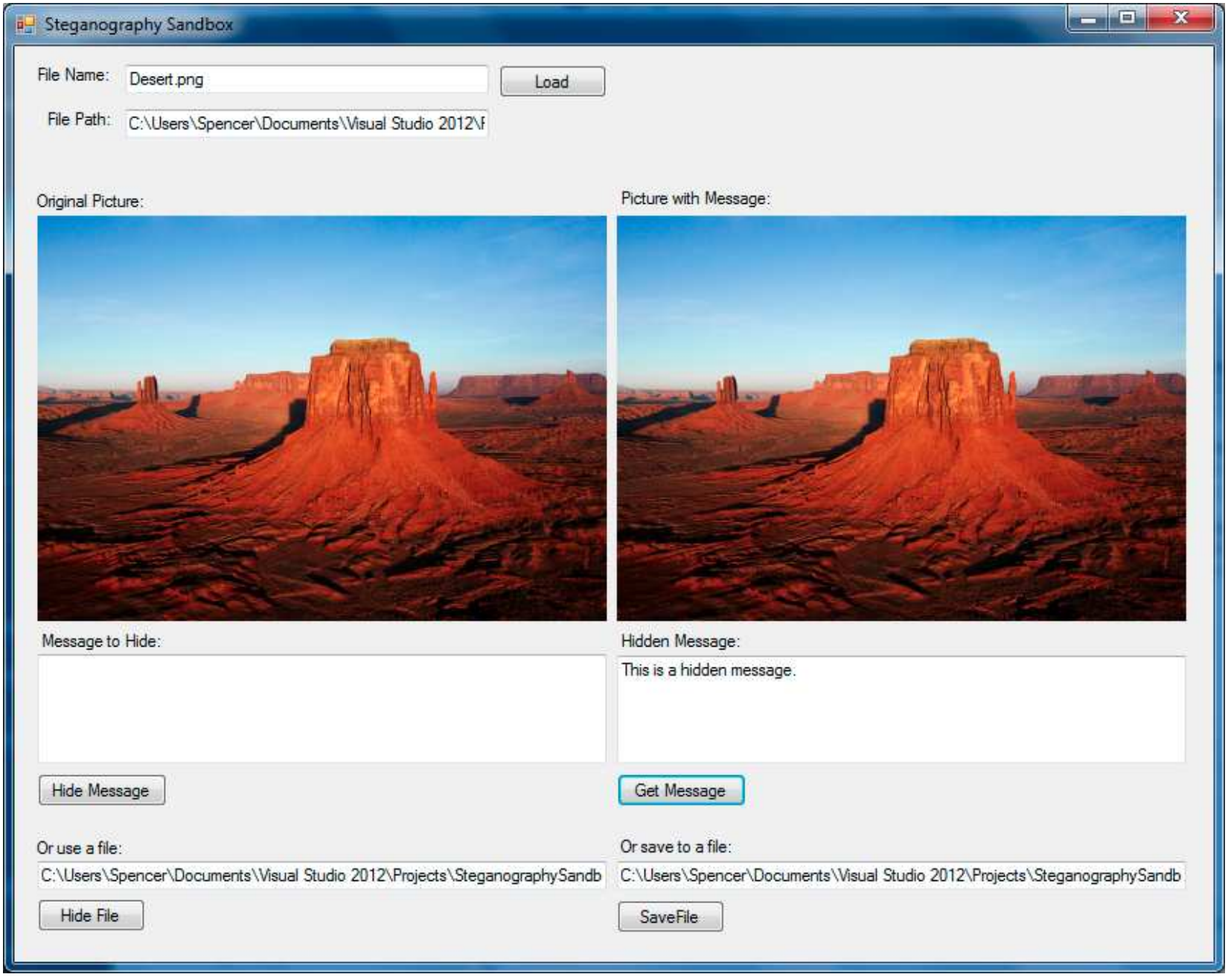
EXEMPLE

"Mon numéro de carte VISA est le 1234-3552-1209-7633"

↓

"XFHEBBCASKOIUUSBCKKQHDGGDDSJQQIEUEU"

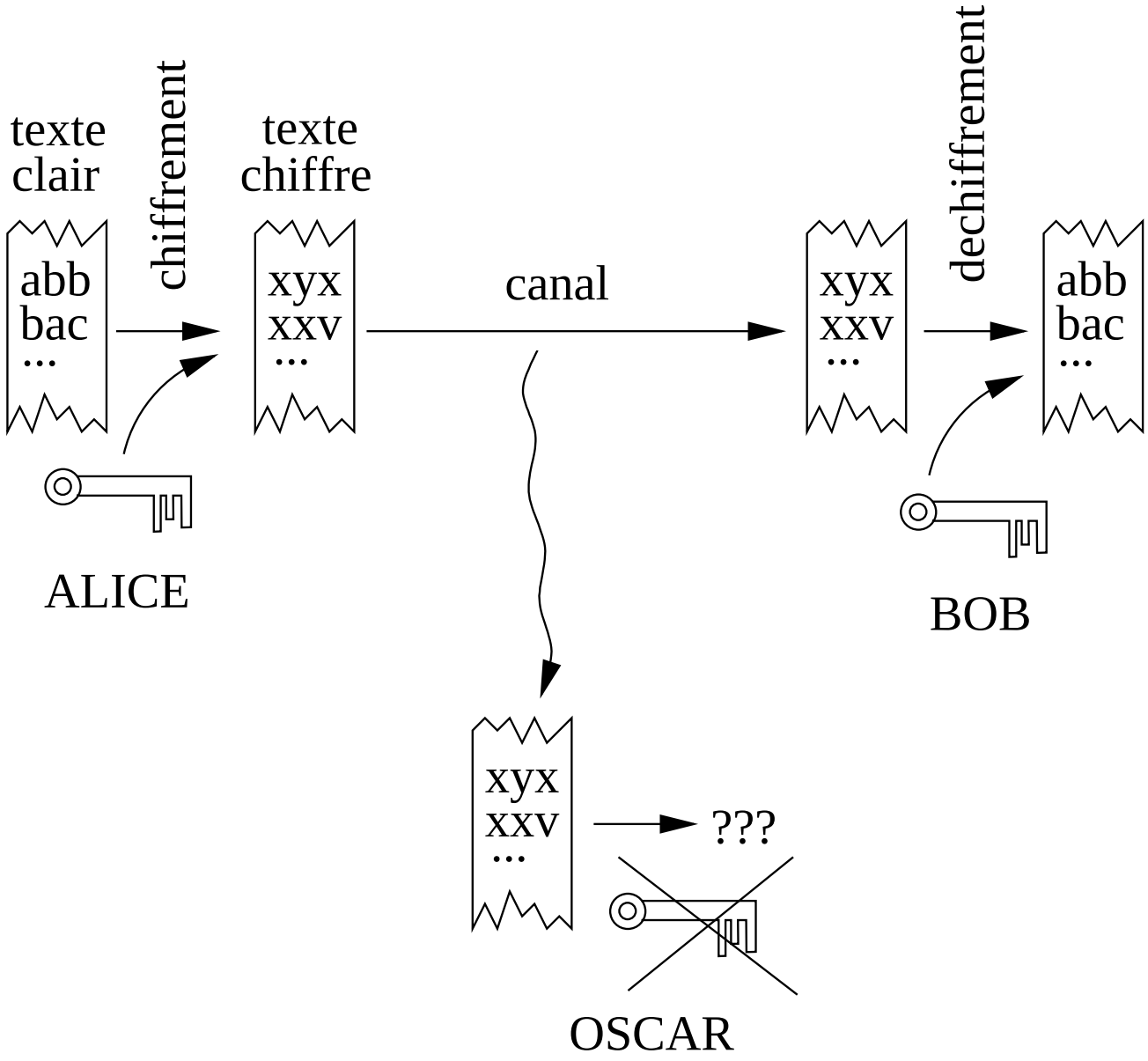
Scytale (image : wikipédia)


Steganography Sandbox
File Name:
Desert.png
Load
File Path:
C:\Users\Spencer\Documents\Visual Studio 2012\F
Original Picture:
Picture with Message:
Message to Hide:
Hidden Message:
This is a hidden message.
Hide Message
Get Message
Or use a file:
C:\Users\Spencer\Documents\Visual Studio 2012\Projects\SteganographySandb
Or save to a file:
C:\Users\Spencer\Documents\Visual Studio 2012\Projects\SteganographySandb
Hide File
SaveFile

Applications

- Armée, gouvernement
- Banques, transactions bancaires, bancontact, ...
- Internet, paiement en ligne par carte de crédit, ...
- Vote électronique
- GSM (identification, code PIN)
- Télévision payante (à la carte)
- Signatures électroniques, recommandés électroniques, ...
- Mots de passe informatiques, ...

Les protagonistes...


texte
clair
chiffrement
texte
chiffre
canal
dechiffrement
abb
bac
...
xyx
xxv
...
xyx
xxv
...
abb
bac
...
ALICE
BOB
xyx
xxv
...
???
OSCAR

Système cryptographique

cryptosystème $(\mathcal{P}, \mathcal{C}, \mathcal{K})$

- $\mathcal{P}$ est l'ensemble fini des textes clairs possibles (plaintexts),
- $\mathcal{C}$ est l'ensemble fini des textes chiffrés possibles (ciphertexts),
- $\mathcal{K}$ est l'ensemble fini des clés possibles, appelé parfois espace des clés (keys),
- Pour tout $k \in \mathcal{K}$, il existe une fonction de chiffrement (encryption rule) e_k t.q.

$$e_k : \mathcal{P} \to \mathcal{C} : t \mapsto e_k(t)$$

et $\exists$ une fonction de déchiffrement (decryption rule) d_k t.q.

$$d_k : \mathcal{C} \to \mathcal{P} : t \mapsto d_k(t) \quad \text{et} \quad \forall t \in \mathcal{P},\ d_k(e_k(t)) = t.$$

Système cryptographique

Pour permettre le déchiffrage,
la fonction e_k doit être injective pour tout $k \in \mathcal{K}$.

Etape préalable au chiffrement

Codage = ensemble des conventions pour modifier le texte clair en un texte équivalent plus simple à traiter du point de vue cryptographique.

Exemple : chiffrement par décalage

$\mathcal{P} = \mathcal{C} = \mathcal{K} = \mathbb{Z}_{26}$. $\forall k \in \{0, \ldots, 25\}$,

$$e_k(x) = (x + k) \mod 26 \quad \text{et} \quad d_k(y) = (y - k) \mod 26.$$

suite $\mathbf{x} = x_1 x_2 \cdots x_\ell$, $x_i \in \mathcal{P}$ chiffrée avec e_k
($k \in \mathcal{K}$ choisi de commun accord entre A et B),

A transmet

$$\mathbf{y} = e_k(x_1) e_k(x_2) \cdots e_k(x_\ell).$$

Exemple : chiffrement par décalage

A veut transmettre le message "bonsoir", chaque lettre est remplacée par sa position dans l'alphabet $\Sigma = \{\mathtt{a}, \ldots, \mathtt{z}\}$

a	b	c	d	e	f	g	h	i	j	k	l	m	n
0	1	2	3	4	5	6	7	8	9	10	11	12	13

o	p	q	r	s	t	u	v	w	x	y	z
14	15	16	17	18	19	20	21	22	23	24	25

"bonsoir" est *codé* en "$\mathtt{x} = 1,14,13,18,14,8,17$".

codage : bijection entre l'alphabet Σ et $\{0, \ldots, 25\}$.

décodage : application inverse

Ne pas confondre : codage $\neq$ chiffrement.

Exemple : chiffrement par décalage

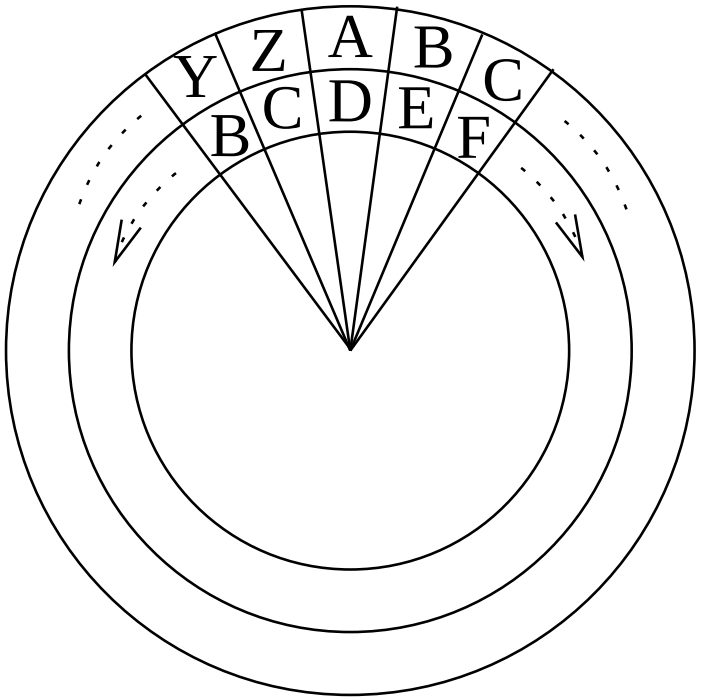
Fin de l'exemple...

Si la clé choisie est $k = 3$ (Jules César), alors

$$\begin{aligned}\mathbf{y} &= e_3(1)e_3(14)e_3(13)e_3(18)e_3(14)e_3(8)e_3(17)\\ &= 4, 17, 16, 21, 17, 11, 20.\end{aligned}$$

"`bonsoir`" $\longrightarrow$ "`erqvrlu`".

Exemple : chiffrement par décalage



Remarque

Cryptosystème peu sûr...

Exemple : chiffrement par décalage

2001 : l'odysée de l'espace, HAL

Principe de Kerckhoff

Cryptanalyse : ensemble des moyens et techniques mis en oeuvre pour retrouver le texte clair ou au moins une certaine information contenue dans celui-ci.

Hypothèses de travail

Le principe de Kerckhoff : *Oscar connaît le cryptosystème utilisé*.

La sécurité du système réside alors dans la protection de la clé k choisie par Alice et Bob.

Attaques

Types d'attaque dont dispose Oscar (par difficulté ↓)

- Texte chiffré connu : Oscar connaît uniquement un fragment de texte chiffré $\mathbf{y}$.
- Texte clair connu : Oscar connaît un texte clair $\mathbf{x}$ et le texte chiffré $\mathbf{y}$ correspondant.
- Texte clair choisi : Oscar a accès à une machine chiffrante. Il peut choisir un texte clair $\mathbf{x}$ et obtenir le texte chiffré $\mathbf{y}$ correspondant.
- Fonction de chiffrement connue : Oscar connaît précisément la fonction utilisée pour le chiffrement. Son but est alors de découvrir la fonction de déchiffrement. Situation typique des cryptosystèmes à clé publique.
- Texte chiffré choisi : Oscar a temporairement accès à une machine déchiffrante. Il peut choisir un texte chiffré $\mathbf{y}$ et obtenir le texte clair $\mathbf{x}$ correspondant.

Implémentation

```
In[1]:= Characters["bonjour"]

Out[1]= {b, o, n, j, o, u, r}

In[2]:= StringJoin[{"a", "b", "c"}]

Out[2]= abc

In[3]:= Map[Sqrt[#] &, {4, 2, 9}]

Out[3]= {2, √2, 3}
```

Implémentation

code / decode

```
alphabet = {" ", "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", ",", ".", "'", ":", "?"};

code[mot_] := Map[Position[alphabet, #][[1, 1]] - 1 &, Characters[mot]]

texteclair = "le jour de ses onze ans, harry potter, un orphelin eleve par un
    oncle et une tante qui le detestent, voit son existence bouleversee.";

codetxclair = code[texteclair]

{12, 5, 0, 10, 15, 21, 18, 0, 4, 5, 0, 19, 5, 19, 0, 15, 14, 26, 5, 0, 1, 14, 19, 27, 0, 8, 1,
 18, 18, 25, 0, 16, 15, 20, 20, 5, 18, 27, 0, 21, 14, 0, 15, 18, 16, 8, 5, 12, 9, 14, 0, 5,
 12, 5, 22, 5, 0, 16, 1, 18, 0, 21, 14, 0, 15, 14, 3, 12, 5, 0, 5, 20, 0, 21, 14, 5, 0, 20, 1,
 14, 20, 5, 0, 17, 21, 9, 0, 12, 5, 0, 4, 5, 20, 5, 19, 20, 5, 14, 20, 27, 0, 22, 15, 9, 20, 0,
 19, 15, 14, 0, 5, 24, 9, 19, 20, 5, 14, 3, 5, 0, 2, 15, 21, 12, 5, 22, 5, 18, 19, 5, 5, 28}

decode[liste_] := StringJoin[Table[alphabet[[liste[[i]] + 1]], {i, 1, Length[liste]}]]

decode[codetxclair]

le jour de ses onze ans, harry potter, un orphelin eleve par un
  oncle et une tante qui le detestent, voit son existence bouleversee.
```

Implémentation

```
cesar[n_] := Mod[n + 3, 32]

codetxchiffre = cesar[codetxclair]

{15, 8, 3, 13, 18, 24, 21, 3, 7, 8, 3, 22, 8, 22, 3, 18, 17, 29, 8, 3, 4, 17,
 22, 30, 3, 11, 4, 21, 21, 28, 3, 19, 18, 23, 23, 8, 21, 30, 3, 24, 17, 3, 18,
 21, 19, 11, 8, 15, 12, 17, 3, 8, 15, 8, 25, 8, 3, 19, 4, 21, 3, 24, 17, 3, 18,
 17, 6, 15, 8, 3, 8, 23, 3, 24, 17, 8, 3, 23, 4, 17, 23, 8, 3, 20, 24, 12, 3, 15,
 8, 3, 7, 8, 23, 8, 22, 23, 8, 17, 23, 30, 3, 25, 18, 12, 23, 3, 22, 18, 17, 3,
 8, 27, 12, 22, 23, 8, 17, 6, 8, 3, 5, 18, 24, 15, 8, 25, 8, 21, 22, 8, 8, 31}

txchiffre = decode[codetxchiffre]

ohcmrxucghcvhvcrq'hcdqv:ckduu.csrwwhu:
  cxqcruskholqchohyhcsducxqcrqfohchwcxqhcwdqwhctxlcohcghwhvwhqw:
  cyrlwcvrqch,lvwhqfhcerxohyhuvhh?
```

Implémentation

Cryptanalyse ?

```
In[17]:= Count[{1, 2, 1, 1, 2}, 1]

Out[17]= 3

In[22]:= Count[Characters[texteclair], "e"]

Out[22]= 24

In[19]:= Map[Count[codetxclair, #] &, Table[i, {i, 0, 31}]]

Out[19]= {23, 4, 1, 2, 2, 24, 0, 0, 2, 4, 1, 0, 6, 0,
          11, 8, 3, 1, 7, 7, 10, 6, 3, 0, 1, 1, 1, 3, 1, 0, 0, 0}

In[18]:= Map[Count[codetxchiffre, #] &, Table[i, {i, 0, 31}]]

Out[18]= {0, 0, 0, 23, 4, 1, 2, 2, 24, 0, 0, 2, 4, 1,
          0, 6, 0, 11, 8, 3, 1, 7, 7, 10, 6, 3, 0, 1, 1, 1, 3, 1}
```

Fréquence d'apparition

fréquences d'apparition des différentes lettres apparaissant dans les textes écrits en français.

lettre	%
e	15,87
a	9,42
i	8,41
s	7,90
t	7,26
n	7,15
r	6,46
u	6,24
l	5,34

Codage par blocs

Unité fondamentale pour réaliser le codage d'une chaîne, non pas une lettre, mais un bloc de m lettres consécutives.

Un bloc $t_1 \cdots t_m$ de $m \geq 1$ entiers consécutifs < 32, représente un nombre n écrit en base 32 :

$$n = \sum_{j=1}^{m} t_j \, 32^{m-j}.$$

Bloc de longueur m représente un nombre $0 \leq n \leq 32^m - 1$.

$\mathcal{P} = \mathcal{C} = \mathbb{Z}_{32^m}$ et non plus $\mathbb{Z}_{32}$.

Codage par blocs

Utiliser un codage dans lequel on considère des blocs de m éléments augmente la sécurité du cryptosystème.

Sur notre exemple, $\mathcal{K} = \mathbb{Z}_{32}$ passe à $\mathcal{K} = \mathbb{Z}_{32^m}$.

Puisque le nombre de clés augmente, une recherche exhaustive menée par Oscar prend beaucoup plus de temps

si $m = 5$, $32^5 \simeq 33 \times 10^6$ et en testant 1000 clés/seconde, un peu plus de 9 heures pour parcourir l'espace des clés.

Codage par blocs

Si nous découpons le texte clair en tronçons de longueur m, il faudrait que ce texte soit de longueur divisible par m.

S'il ne l'était pas, on ajouterait au préalable des symboles à la fin du texte pour que sa longueur soit divisible par m.

Attention

Faille possible de sécurité !

Implémentation

```
ajout[liste_, m_] := PadRight[liste, Length[liste] + Mod[-Length[liste], m]]

codetxclair = ajout[codetxclair, 5]

{12, 5, 0, 10, 15, 21, 18, 0, 4, 5, 0, 19, 5, 19, 0, 15, 14, 26, 5, 0, 1, 14,
 19, 27, 0, 8, 1, 18, 18, 25, 0, 16, 15, 20, 20, 5, 18, 27, 0, 21, 14, 0, 15, 18,
 16, 8, 5, 12, 9, 14, 0, 5, 12, 5, 22, 5, 0, 16, 1, 18, 0, 21, 14, 0, 15, 14, 3,
 12, 5, 0, 5, 20, 0, 21, 14, 5, 0, 20, 1, 14, 20, 5, 0, 17, 21, 9, 0, 12, 5, 0,
 4, 5, 20, 5, 19, 20, 5, 14, 20, 27, 0, 22, 15, 9, 20, 0, 19, 15, 14, 0, 5, 24,
 9, 19, 20, 5, 14, 3, 5, 0, 2, 15, 21, 12, 5, 22, 5, 18, 19, 5, 5, 28, 0, 0, 0}

codebloc[liste_, m_] := Map[FromDigits[#, 32] &, Partition[liste, m]]

codetxclair = codebloc[codetxclair, 5]

{12747087, 22610053, 628320, 16214176, 1527648, 8440409, 540308, 5860373, 1469601
 8565038, 176310, 5259314, 702479, 14790816, 5898926, 5263406, 21135925, 9449632,
 4378803, 21150363, 736564, 638400, 6039156, 5704864, 2610565, 23251557, 6160384}

decodebloc[liste_, m_] := decode[Flatten[Map[IntegerDigits[#, 32, m] &, liste]]]

decodebloc[codetxclair, 5]

le jour de ses onze ans, harry potter, un orphelin eleve par un
  oncle et une tante qui le detestent, voit son existence bouleversee.
```

Implémentation

```
codetxchiffre = Mod[codetxclair + 12345678, 32^5]

{25092765, 1401299, 12973998, 28559854, 13873326, 20786087,
 12885986, 18206051, 27041694, 20910716, 12521988, 17604992, 13048157,
 27136494, 18244604, 17609084, 33481603, 21795310, 16724481, 33496041,
 13082242, 12984078, 18384834, 18050542, 14956243, 2042803, 18506062}

decodebloc[codetxchiffre, 5]

w'xt'ajxnslk''n,gronmglenszj'glig?bqkskcyyg.:s:ds.k:dpdpyhl lnfj'
  y.donqlx?.pylk.?'x.ctydono:lpa?:f?ilogtbllgxnqqa:bqf,onnhmvsa:j'sqtxjn

decodebloc[Mod[codetxchiffre - 12345678, 32^5], 5]

le jour de ses onze ans, harry potter, un orphelin eleve par un
  oncle et une tante qui le detestent, voit son existence bouleversee.
```

Implémentation

`code[mot]`		chaîne de longueur n
	$\mapsto$	liste de n éléments de $\mathbb{Z}_{32}$
`decode[liste]`		liste de n éléments de $\mathbb{Z}_{32}$
	$\mapsto$	chaîne de longueur n
`ajout[liste,m]`		liste quelconque
	$\mapsto$	liste de longueur divisible par m
`codebloc[liste,m]`		liste de $n.m$ éléments de $\mathbb{Z}_{32}$
	$\mapsto$	liste de n éléments de $\mathbb{Z}_{32^m}$
`decodebloc[liste,m]`		liste de n éléments de $\mathbb{Z}_{32^m}$
	$\mapsto$	chaîne de longueur $n.m$.

Quelques cryptosystèmes historiques

Chiffrement par substitution

Si $\mathcal{P} = \mathcal{C} = \mathbb{Z}_{32}$, alors $\mathcal{K}$ est l'ensemble des permutations de $\{0, \ldots, 31\}$, i.e.,

$$\mathcal{K} = \{\nu \in \mathcal{S}_{32} \mid \nu : \mathbb{Z}_{32} \to \mathbb{Z}_{32} \text{ bijection}\}.$$

pour la clé $k = \nu$, on a

$$e_k(x) = \nu(x) \quad \text{et} \quad d_k(y) = \nu^{-1}(y).$$

Par rapport au chiffrement par décalage,
$\#\mathcal{K}$ est grand : $32! \simeq 2,6 \times 10^{35}$.

Quelques cryptosystèmes historiques

Chiffrement par substitution

	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o
e	:	d	k	,	l	p	n		q	x	f	s	z	.	u

p	q	r	s	t	u	v	w	x	y	z	,	.	’	:	?
’	a	c	i	g	?	t	v	o	y	w	r	b	m	j	h

le jour de ses onze ans, harry potter, un orphelin eleve par un oncle et une tante qui le detestent, voit son existence bouleversee.

slexu ?ce,leilieu.wle :.i,e :ccye’ugglc,e ?.euc’ lsq.elsltle’ :c
e ?.eu.kslelge ?.leg :.glea ?qesle,lgligl.g,etuqgeiu.eloqigl.kl
edu ?sltlcillb

Quelques cryptosystèmes historiques

Chiffrement par substitution

Nombre de clés important, mais ce cryptosystème est cassé en effectuant une analyse des fréquences : rechercher les lettres apparaissant le plus souvent, mais aussi les couples ou les triplets.

Ce cryptosystème NE peut être considéré comme sûr.

Seul intérêt : cryptogrammes dans les livres de jeux.

Quelques cryptosystèmes historiques

Ici, on travaille sur $\mathbb{Z}_n$ et pas nécessairement $\mathbb{F}_q$.

Chiffrement affin

$\mathcal{P} = \mathcal{C} = \mathbb{Z}_n$. Soient $a, b \in \mathbb{Z}_n$ avec $pgcd(a, n) = 1$.

$$\mathcal{K} = \{(a, b) \mid a \in \mathbb{Z}_n^*, b \in \mathbb{Z}_n\}$$

et pour une clé $k = (a, b)$ choisie dans $\mathcal{K}$, on a

$$e_k(x) = ax + b \mod n \quad \text{et} \quad d_k(y) = a^{-1}(y - b) \mod n.$$

a inversible pour que e_k soit injective.

Le nombre de clés est $n\,\varphi(n)$.

Quelques cryptosystèmes historiques

```
texteclair = "ving minutes plus tard, harry sortit du
magasin de hiboux avec une grande cage a l'interieur de
laquelle une magnifique chouette aux plumes blanches comme
la neige dormait paisiblement.";
```

$k = (13, 8)$

decode[Mod[13 code[texteclair]+8, 32]]

```
"f':chq':yli?hxdy?hlur.gpurrmh?krl'lh.yhqucu?'
:h.ihp'bky hufiohy:ihcru:.ihoucihuhda':lir'iyr
h.ihdueyiddihy:ihquc:'v'eyihopkyillihuy hxdyqi
?hbdu:opi?hokqqihduh:i'cih.krqu'lhxu'?'bdiqi:lt"
```

Remarque

Cas particulier de chiffrement par substitution.
cryptanalyse : analyse statistique des fréquences d'apparition des lettres.

Monoalphabétique vs. polyalphabétique

Chiffrement monoalphabétique

- e_k s'applique à un seul élément de $\mathcal{P}$ à la fois (une lettre, un élément de $\mathbb{Z}_{32}$) ;
- à chaque élément de $\mathcal{P}$ est appliquée la même fonction de chiffrement.
- Les chiffrements par décalage, par substitution et affin sont monoalphabétiques.
- Pour un bloc de m symboles, aussi un système monoalphabétique : $\mathcal{P} = \mathbb{Z}_{32^m}$

Le chiffrement de Vigenère (Blaise de Vigenère, XVIè siècle) est polyalphabétique car il traite m symboles simultanément.

Quelques cryptosystèmes historiques

Chiffrement de Vigenère

Il s'agit en quelque sorte de m chiffrements par décalage, $\mathcal{P} = \mathcal{C} = \mathcal{K} = (\mathbb{Z}_{32})^m$, si $k = (k_1, \ldots, k_m) \in (\mathbb{Z}_{32})^m$, alors

$$e_k(x_1, \ldots, x_m) = (x_1 + k_1, \ldots, x_m + k_m) \mod 32$$

$$d_k(y_1, \ldots, y_m) = (y_1 - k_1, \ldots, y_m - k_m) \mod 32.$$

Pour chiffrer une suite de longueur $rm + s$ de $\mathbb{Z}_{32}$, $0 \leq s < m$,

$$\mathbf{x} = x_1 \cdots x_m \,|\, \cdots \,|\, x_{(r-1)m+1} \cdots x_{rm} \,|\, x_{rm+1} \cdots x_{rm+s},$$

on calculera

$$\begin{aligned} \mathbf{y} \;=\; & (x_1 + k_1) \cdots (x_m + k_m) \,|\, \cdots \,|\, (x_{(r-1)m+1} + k_1) \cdots (x_{rm} + k_m) \,| \\ & (x_{rm+1} + k_1) \cdots (x_{rm+s} + k_s) \mod 32. \end{aligned}$$

Quelques cryptosystèmes historiques

L'implémentation est très simple

```
In[2]:= PadRight[{1, 2}, 10, {5, 3, 7}]

Out[2]= {1, 2, 7, 5, 3, 7, 5, 3, 7, 5}
```

Quelques cryptosystèmes historiques

```
texteclair = "ving minutes plus tard,harry sortit du magasin de
    hiboux avec une grande cage a l'interieur de laquelle une magnifique
    chouette aux plumes blanches comme la neige dormait paisiblement.";

codetxclair = code[texteclair];

Shallow[codetxclair]

{22, 9, 14, 7, 0, 13, 9, 14, 21, 20, <<174>>}

vigenere[liste_, cle_] := Mod[liste + PadRight[cle, Length[liste], cle], 32]

codetxchiffre = vigenere[codetxclair, {10, 8, 20}]

{0, 17, 2, 17, 8, 1, 19, 22, 9, 30, 13, 7, 10, 24, 0, 31, 27, 20, 30, 9, 6, 14, 3, 28,
 26, 6, 3, 8, 7, 25, 26, 8, 19, 28, 20, 14, 29, 20, 23, 9, 27, 11, 27, 29, 24, 8, 24,
 15, 8, 28, 19, 10, 3, 31, 0, 20, 11, 30, 25, 13, 8, 9, 24, 13, 20, 17, 26, 21, 24, 12,
 25, 10, 11, 21, 17, 13, 20, 11, 8, 0, 7, 17, 2, 30, 13, 6, 19, 13, 9, 28, 8, 24, 15,
 8, 0, 11, 25, 9, 15, 20, 0, 15, 8, 9, 24, 13, 20, 23, 9, 27, 24, 17, 26, 19, 25, 9,
 15, 8, 23, 18, 23, 9, 15, 28, 8, 15, 8, 21, 31, 0, 20, 26, 20, 9, 23, 13, 7, 10, 10,
 0, 11, 22, 23, 18, 13, 7, 10, 11, 3, 23, 21, 25, 10, 20, 21, 10, 22, 25, 19, 15, 25,
 10, 12, 3, 28, 21, 21, 19, 28, 20, 26, 9, 29, 29, 17, 22, 22, 13, 1, 15, 22, 8, 6}

decode[codetxchiffre]

 qbqhasvi:mgjx ?,t:ifnc.kzfchgyzhs.tn'twi,k,'xhxoh.sjc? tk:
  ymhixmtqzuxlyjkuqmtkh gqb:mfsmi.hxoh kyiot ohixmtwi,xqzsyiohwrwio.
  hohu? tztiwmgjj kvwrmgjkcwuyjtujvysoyjlc.uus.tzi''qvvmaovhf
```

Quelques cryptosystèmes historiques

Pour le déchiffrement...

```
vigenere[codetxchiffre, -{10, 8, 20}]
```

```
{22, 9, 14, 7, 0, 13, 9, 14, 21, 20, 5, 19, 0, 16, 12, 21, 19, 0, 20, 1, 18, 4, 27, 8,
 25, 0, 19, 15, 18, 20, 9, 20, 0, 4, 21, 0, 13, 1, 7, 1, 19, 9, 14, 0, 4, 5, 0, 8, 9, 2,
 21, 24, 0, 1, 22, 5, 3, 0, 21, 14, 5, 0, 7, 18, 1, 14, 4, 5, 0, 3, 1, 7, 5, 0, 1, 0, 12
 29, 9, 14, 20, 5, 18, 9, 5, 21, 18, 0, 4, 5, 0, 12, 1, 17, 21, 5, 12, 12, 5, 0, 21, 14
 5, 0, 13, 1, 7, 14, 9, 6, 9, 17, 21, 5, 0, 3, 8, 15, 21, 5, 20, 20, 5, 0, 1, 21, 24, 0,
 16, 12, 21, 13, 5, 19, 0, 2, 12, 1, 14, 3, 8, 5, 19, 0, 3, 15, 13, 13, 5, 0, 12, 1, 0,
 5, 9, 7, 5, 0, 4, 15, 18, 13, 1, 9, 20, 0, 16, 1, 9, 19, 9, 2, 12, 5, 13, 5, 14, 20, 28
```

Remarques

Dans le chiffrement de Vigenère, un même symbole peut être transformé en m symboles distincts suivant la position qu'occupe ce symbole dans un m-uple donné.

Cryptanalyse : test de Kasiski (1863) / indice de coïncidence

Chiffrement de Hill, Lester S. Hill (1929)

Cryptosystème polyalphabétique. $\mathcal{P} = \mathcal{C} = (\mathbb{Z}_{32})^m$ et

$$\mathcal{K} = GL_m(\mathbb{Z}_{32}),$$

l'ensemble des matrices inversibles à coefficients dans $\mathbb{Z}_{32}$.

Proposition

Une matrice carrée A à coefficients dans $\mathbb{Z}_n$ est inversible, i.e., il existe B tel $AB = BA = I$, SSI $\det(A)$ est inversible dans $\mathbb{Z}_n$.

règle des mineurs :

$$A\,\widetilde{\mathrm{cof}(A)} = \det A\ I = \widetilde{\mathrm{cof}(A)}\,A$$

$\mathrm{cof}(A)$: matrice des cofacteurs (ou mineurs algébriques) de A.

$\Leftarrow$. Si $\det A$ est inversible, l'inverse de A est $(\det A)^{-1}\widetilde{\mathrm{cof}(A)}$.

$\Rightarrow$. Si A est inversible et d'inverse A^{-1}, alors

$$1 = \det(AA^{-1}) = \det A \det A^{-1}$$

ce qui montre que $\det A$ est inversible.

Chiffrement de Hill

Si $k = (a_{ij}) \in GL_m(\mathbb{Z}_{32})$,
$e_k : \mathbb{Z}_{32}^m \to \mathbb{Z}_{32}^m : (x_1, \ldots, x_m) \mapsto (y_1, \ldots, y_m)$ est donné par

$$\begin{pmatrix} y_1 \\ \vdots \\ y_m \end{pmatrix} = \begin{pmatrix} a_{11} & \cdots & a_{1m} \\ \vdots & & \vdots \\ a_{m1} & \cdots & a_{mm} \end{pmatrix} \begin{pmatrix} x_1 \\ \vdots \\ x_m \end{pmatrix}.$$

Chiffrement/Déchiffrement

La matrice A détermine une bijection $x \mapsto Ax$ de $(\mathbb{Z}_n)^m$ dans lui-même SSI A inversible.

$\Leftarrow$ Si $Ax = Ay$, en multipliant par A^{-1} : $x = y$ (injectif).
(surjectif) $\forall y \in (\mathbb{Z}_n)^m$, $x = A^{-1}y$ est tel que $Ax = y$.

$\Rightarrow$ $x \mapsto Ax$ est surjectif, pour tout e_i, $i = A, \ldots, m$, il existe un vecteur colonne C_i tel que $AC_i = e_i$. De là, la matrice dont les colonnes sont $C_1, \ldots, C_m$ est inverse de A.

Quelques cryptosystèmes historiques

```
texteclair = "le phenix sur lequel a ete preleve la plume qui se trouve dans
    votre baguette a egalement fourni une autre plume a une autre baguette.";

codetxclair = ajout[code[texteclair], 2];

Shallow[codetxclair]

{12, 5, 0, 16, 8, 5, 14, 9, 24, 0, <<124>>}

a = {{5, 17}, {4, 21}};

MatrixForm[a]
```

$$\begin{pmatrix} 5 & 17 \\ 4 & 21 \end{pmatrix}$$

```
hill[a_, liste_] := Flatten[Map[Mod[a.# , 32] &, Partition[liste, Length[a]]]]

codetxchiffre = hill[a, codetxclair]

{17, 25, 16, 16, 29, 9, 31, 21, 24, 0, 4, 5, 26, 8, 17, 25, 26, 29, 5, 16, 17, 21,
 21, 9, 25, 25, 16, 16, 15, 17, 17, 25, 3, 1, 12, 28, 5, 4, 28, 28, 6, 5, 25, 20,
 26, 29, 13, 4, 20, 21, 20, 4, 25, 3, 31, 2, 25, 20, 5, 5, 9, 7, 22, 14, 31, 0, 15,
 17, 2, 10, 28, 23, 30, 29, 24, 20, 25, 20, 5, 4, 16, 7, 17, 0, 22, 5, 7, 26, 4, 16,
 29, 19, 27, 14, 31, 21, 5, 25, 27, 1, 17, 21, 29, 24, 15, 17, 16, 16, 1, 9, 22, 29,
 17, 21, 5, 25, 27, 1, 17, 21, 29, 24, 15, 17, 2, 10, 28, 23, 30, 29, 24, 20, 21, 0}
```

Quelques cryptosystèmes historiques

```
Inverse[a, Modulus → 32]
```

```
{{17, 3}, {12, 1}}
```

```
hill[Inverse[a, Modulus → 32], codetxchiffre]
```

```
{12, 5, 0, 16, 8, 5, 14, 9, 24, 0, 19, 21, 18, 0, 12, 5, 17, 21, 5, 12, 0, 1, 0, 5, 20, 5, 0,
 18, 5, 12, 5, 22, 5, 0, 12, 1, 0, 16, 12, 21, 13, 5, 0, 17, 21, 9, 0, 19, 5, 0, 20, 18, 15,
 21, 22, 5, 0, 4, 1, 14, 19, 0, 22, 15, 20, 18, 5, 0, 2, 1, 7, 21, 5, 20, 20, 5, 0, 1, 0, 5,
 7, 1, 12, 5, 13, 5, 14, 20, 0, 6, 15, 21, 18, 14, 9, 0, 21, 14, 5, 0, 1, 21, 20, 18, 5, 0,
 16, 12, 21, 13, 5, 0, 1, 0, 21, 14, 5, 0, 1, 21, 20, 18, 5, 0, 2, 1, 7, 21, 5, 20, 20, 5, 28
```

Pour trouver cet inverse manuellement, on calcule $\det A = 5$, son inverse modulo 32 grâce à l'algorithme d'Euclide étendu, $(\det A)^{-1} = 13$ et enfin, la matrice des cofacteurs transposée,

$$\widetilde{\operatorname{cof} A} = \begin{pmatrix} 21 & -17 \\ -4 & 5 \end{pmatrix}.$$

On trouve,

- $13.21 = 273 \equiv 17 \mod 32$,
- $13.(-17) = -221 \equiv 3 \mod 32$,
- $13.(-4) = -52 \equiv 12 \mod 32$,
- $13.5 = 65 \equiv 1 \mod 32$.

Cryptanalyse du chiffrement

cas où un texte clair de longueur m^2 est connu. Si Oscar connaît la valeur $m = 2$, le texte clair $12, 5, 0, 16$ et le texte chiffré correspondant $17, 25, 16, 16$, alors il en déduit que

$$A \underbrace{\begin{pmatrix} 12 & 0 \\ 5 & 16 \end{pmatrix}}_{B} = \begin{pmatrix} 17 & 16 \\ 25 & 16 \end{pmatrix}.$$

Pas de chance B n'est pas inversible, $\det(B) = 0$.

Oscar doit construire une matrice inversible dont les colonnes correspondent à des couples de texte clair lorsque ce dernier est décomposé en m-uples consécutifs.

Cryptanalyse du chiffrement

On peut par exemple prendre pour premier couple $(12, 5)$ correspondant au texte chiffré $(17, 25)$ et comme second couple $(19, 21)$ qui correspond à $(4, 5)$

$$A \begin{pmatrix} 12 & 19 \\ 5 & 21 \end{pmatrix} = \begin{pmatrix} 17 & 4 \\ 25 & 5 \end{pmatrix}.$$

Puisque

$$\det \begin{pmatrix} 12 & 19 \\ 5 & 21 \end{pmatrix} \equiv 29 \mod 32, \quad A = \begin{pmatrix} 17 & 4 \\ 25 & 5 \end{pmatrix} \begin{pmatrix} 12 & 19 \\ 5 & 21 \end{pmatrix}^{-1}$$

et Oscar retrouve A.

Chiffrement par permutation

Cas particulier du chiffrement de Hill, matrice pour le chiffrement : une matrice de permutation P.

Le chiffrement de Hill revient alors à permuter les lettres d'un même m-uple au moyen de la permutation définie par P.

Quelques cryptosystèmes historiques

```
p = {{0, 1, 0}, {0, 0, 1}, {1, 0, 0}}
```

```
{{0, 1, 0}, {0, 0, 1}, {1, 0, 0}}
```

```
decode[hill[p, codetxclair]]
```

```
e lhepixnsu  lrquel e eae trepevl le pauml qei ue srotveuda s
  notve ragbetue t eaalgmeet noufnirun  aetru peuml aeun  aetru beguatte
```