

rythmétique

cryptologie

arith-crypte

C1: Cryptographie synthétique

- protéger msgs, infos, usant / ^{secrets} clés sans cacher le msg.
- f cryptographique ou chiffrement $f: M \rightarrow C$ bijective.
où M: ens msgs clairs / C: ens msg cryptés
- Ens f (f_k)_k où k: paramètre clé
- Cryptanalyse : science : décoder msg sy envoi la clé.
- Cryptog. synthétique : ce dé chiffre + le point de retrouver msg clair & clé de chiffrement.

I/ Chiffre monoalphabétique "général"

© BAC → EZI

Principe : remplacer arbitrairement 1 lettre par 1 autre de msg.

Clé: donnée de la $f: \{A, \dots, Z\} \rightarrow \{A, \dots, Z\}$ bijective

26! clés possibles pour un alphabet de 26 lettres.

MS système sensible aux attaques statistiques (fréq. chq lettre)
S'il est assez long : + fréq. (E, A, S, I, N, T) R, L, U, O, D)

II/ Chiffre de César

: décalage lettres du alpbt.

A	B	C	D	E	F	...
w	x	y	z	a	b	...

① f déchiffrent = décalage des sens inverse.

• Espace des clés: m lettres $\rightarrow m$ clés de chiffrement (décalage)

• Cryptanalyse: faible nbr clés, tester toutes les clés.

@ "BONJOUR" \rightarrow "CP0KPLS" CDC 1.

Congruences:

D) $b|a$ si $\exists q \in \mathbb{Z}, a = bq$.
(a est un multiple de b).

@ $7|_{21}, 5 \nmid_{21}$

Prop) $\forall a \in \mathbb{Z}, a \equiv_0$ et si $a \equiv_1$ alors $a = \pm 1$

si $a|b$ & $b|c$ alors $a|c$

si $a|b$ & $b|a$ alors $b = \pm a$

si $a|b$ et $a|c$ alors $a|(b+c)$

TH) Division euclidienne

$b \neq 0, \exists ! (q, r) \mid a = bq + r$ et $0 \leq r < b$.

DÉMO. 1

D) $a \equiv b \pmod{m}$ si m divise $a - b$.

$a, b \in \mathbb{Z}, m \in \mathbb{N}^*$

Prop) ✓ Réflexivité $a \equiv a \pmod{m}$

✓ Symétrie $a \equiv b \pmod{m}$

✓ Transitivité $a \equiv b \pmod{m}$ et $b \equiv c \pmod{m} \Rightarrow a \equiv c \pmod{m}$

Relat° d'équivalence ②

D) $\overline{k} \quad \{k \in \mathbb{Z}, k \equiv l \pmod{m}\}$

\overline{k} : classe d'équivalence modulo m de k .

$$n=26, \overline{2} \{ -24, 2, 26, 54, -24, \dots \} = \overline{28}$$

Prop) $a_1 \equiv b_1 \pmod{m}$ et $a_2 \equiv b_2 \pmod{m} \Rightarrow a_1 + a_2 \equiv b_1 + b_2 \pmod{m}$

D'où $\overline{a} + \overline{b} = \overline{a+b}$ et $\overline{ab} = \overline{ab}$

@ $n=26, \overline{2} + \overline{3} = \overline{5}$ mais $\overline{2} = \overline{28}$ et $\overline{3} = \overline{29}$

Donc $\overline{28} + \overline{29} = \overline{57} = \overline{5} \quad (57-5) = 52 = 2 \times 26$.

Rq: Un représentant de la classe de \overline{k} dans $\{0, \dots, n-1\}$
Prendre le reste de la division de k par m .

Gm note $\mathbb{Z}/m\mathbb{Z} = \{\overline{k}, k \in \mathbb{Z}\} = \{0, \overline{1}, \dots, \overline{m-1}\}$

Rq: Classe de $k \pmod{m}$ s'obtient en python $k \% m$.

Pour chiffrer msg $\alpha \beta = ABC\dots Z$, on \Leftrightarrow chq élmt de $\mathbb{Z}/m\mathbb{Z}$
 $A \leftrightarrow \overline{0}, B \leftrightarrow \overline{1}, \dots, Z \leftrightarrow \overline{25}$.

f chiffrent CDC avec k : $C_k: \mathbb{Z}/26\mathbb{Z} \rightarrow \mathbb{Z}/26\mathbb{Z}$

$$\overline{m} \rightarrow \overline{m+k}$$

f déchiffrent CDC avec k : $D_k: \mathbb{Z}/26\mathbb{Z} \rightarrow \mathbb{Z}/26\mathbb{Z}$

$$\overline{m} \rightarrow \overline{m-k}$$

@

$$\text{"BAC"} \rightarrow \overline{1}, \overline{0}, \overline{2} \xrightarrow{C_4} \overline{5}, \overline{4}, \overline{6} \rightarrow \text{"FEG"}$$

III / Chiffrement affine

$$A(a, b) : \frac{\mathbb{Z}}{26\mathbb{Z}} \rightarrow \frac{\mathbb{Z}}{26\mathbb{Z}}$$

$$\bar{m} \mapsto \frac{am + b}{26}$$

→ mbr ch' 26×26 (26 chx $m \in \mathbb{Z}$, 26 chx $\mu \in b$)

→ MS ts chx de ce n'est pas possible.

$$@ A(13, 0)(\bar{0}) = \overline{13 \times 0 + 0} = \bar{0} \quad & A(13, 2)(\bar{2}) = \overline{13 \times 2 + 0} = \bar{0}$$

$\Rightarrow A(13, 0)$ n'est pas f bijection. Dc $k = (13, 0)$ impossible.

PGCD 2 entiers :

cf

① $\text{pgcd}(a, b)$ ou $a \wedge b$. ($a, b \in \mathbb{Z} ; (a, b) \neq (0, 0)$)

② $\text{pgcd}(21, 14) = 7$; $\text{pgcd}(-21, 14) = 7$

③ $\text{pgcd}(a, b) = \text{pgcd}(|a|, |b|) = \text{pgcd}(\pm a, \pm b)$ cf

④ $\text{pgcd}(a, ka) = |a|$ $\forall a \in \mathbb{Z}^*, \forall k \in \mathbb{Z}$

⑤ $\text{pgcd}(a, 1) = 1$ et $\text{pgcd}(a, 0) = |a|$

Calcul pgcd 2 entiers:

Théorème $\text{pgcd}(a, b) = \text{pgcd}(a, b - ka)$

(4)

> AE

$a, b > 0$ car $\text{pgcd}(a, b) = \text{pgcd}(|a|, |b|)$
 On suppose $b < a$; DE de a par b : $a = bq_1 + r_1$, $0 < r_1 < b$
 si $r_1 = 0$, $b \mid a$ et $\text{pgcd}(a, b) = b$
 si $r_1 \neq 0$, $\text{pgcd}(a, b) = \text{pgcd}(a - bq_1, b) = \text{pgcd}(r_1, b)$
 \hookrightarrow Le pgcd est le dernier reste non nul

Alg. Euclide

$$\begin{aligned} @ \text{pgcd}(625, 95) &= \text{pgcd}(55, 95) \quad \text{car } 625 = 6 \times 95 + 55 \\ \text{pgcd}(625, 95) &= \text{pgcd}(40, 55) \quad \text{car } 95 = 1 \times 55 + 40 \\ \text{pgcd}(40, 55) &= \text{pgcd}(15, 40) \quad \text{car } 55 = 1 \times 40 + 15 \\ \text{pgcd}(15, 40) &= \text{pgcd}(15, 15) \quad \text{car } 40 = 2 \times 15 + 15 \\ \text{pgcd}(15, 15) &= \text{pgcd}(15, 0) = 15 \end{aligned}$$

D Les mbrs st l'ns \Leftrightarrow si l' pgcd vaut 1.

IV / TH de Bézout

TH $\exists u, v \in \mathbb{Z}, au + bv = \text{pgcd}(a, b)$ $a, b \in \mathbb{Z}, \neq (0, 0)$ DM-3

@ $a = 600$ et $b = 124$

> AE

$$\begin{aligned} 600 &= 124 \times 4 + 104 \\ 124 &= 104 \times 1 + 20 \\ 104 &= 20 \times 5 + 4 \\ 20 &= 4 \times 5 + 0 \end{aligned}$$

$$\text{Dc } (u, v) = (6, -29).$$

> B $\therefore \text{pgcd}(600, 124) = 4$

$$\begin{aligned} 600 &= 124 - 20 \times 5 = 124 - 5(124 - 104 \times 1) \\ &= 6 \times 124 - 5 \times 124 \\ &= 6 \times (600 - 4 \times 124) - 5 \times 124 \\ &= 6 \times 600 - 29 \times 124 \end{aligned}$$

⑥ Tout diviseur de a & b divise $\text{pgcd}(a, b)$.

$a, b \in \mathbb{Z}; (a, b) \neq (0, 0)$ (5)

DM-4

$\text{P} \quad \text{pgcd}(a, b) = 1 \Leftrightarrow au + bv = 1 \quad [\text{DM. 6}]$

- cas de gauze $a \mid bc$ & $\text{pgcd}(a, b) = 1 \Rightarrow a \mid c$

II / Équations diophantiennes

TH (ED) $au + bv = c$, $a, b, c \in \mathbb{Z}$ $\Leftarrow_{u, v \in \mathbb{Z}}$

Alors i (ED) a solu^s (u_0, v_0) ssi $\text{pgcd}(a, b) \mid c$.

ii Si $(u_0, v_0) \in \mathbb{Z}^2$ est solu^s (ED) alors

$$(x, y) = \left(u_0 + k \cdot \frac{b}{\text{pgcd}(a, b)}, v_0 - k \cdot \frac{a}{\text{pgcd}(a, b)} \right)_{k \in \mathbb{Z}}$$

M i Remonter à AE ii $au + bv = \text{valeur}$

iii Sol^s part (i), multiplié par coeff iv en divisant par $\text{pgcd}(a, b)$

Q (E) $161x + 368y = 115$

i $\text{pgcd}(368, 161) = 23$

Puis $115 = 5 \times 23$ dc (E) a solu^s.

ii $368u + 161v = 23 \quad \left| \begin{array}{l} 23 = 161 - 46 \times 3 \\ 23 = 161 - 3(368 - 2 \times 161) \\ 23 = 7 \times 161 - 3 \times 368 \end{array} \right.$

iii (□) $(x_0, y_0) = (35, -15)$ multiplié par coeff.

iv $161(x_0 - x) = 368(y - y_0)$ en divisant par $(161, 368)$

$7 \mid 16(y - y_0)$ MS $\text{pgcd}(7, 16) = 1 \rightarrow ?$ de $y - y_0 = 7k$
d'après lemme de gauze $y = y_0 + 7k$

$7(x_0 - x) = 16 \times 7k \rightarrow x = x_0 - 16k$
 $\Rightarrow (x, y) = (x_0 - k \frac{368}{\text{pgcd}(161, 368)}, y_0 + k \frac{161}{\text{pgcd}(161, 368)})$

VII / Inverse module m

D b est inverse à $[m]$ si $ab \equiv 1 \pmod{m}$. ($ab \equiv 1 \pmod{m}$)

P i a admet inverse $[m]$ ssi $\text{pgcd}(a, m) = 1$.

ii si $au + bv = 1$ alors u est inverse à $[m]$.

VIII / MÉO Chiffre Affine

$$A(a, b) : \mathbb{Z}/26\mathbb{Z} \rightarrow \mathbb{Z}/26\mathbb{Z} \rightarrow \bar{x} \mapsto \bar{ax} + \bar{b}$$

$$(\bar{x} = \bar{u}(\bar{ax} + \bar{b}) - \bar{ub}) \quad \text{et} \quad \bar{uu} = \bar{1}.$$

Si \bar{u} est inverse de $a [26]$ alors $A(a, b)$ est inversible
& son inverse est $A(u, -ub)$.

Si $A(a, b)$ est bijective, $\exists \bar{x} \in \mathbb{Z}/26\mathbb{Z}, \bar{ax} + \bar{b} = \bar{1} + \bar{b}$

Dc $\bar{ax} = \bar{1}$ dc x est inverse de $a [26]$ & $\text{pgcd}(a, 26) = 1$

\Rightarrow Ens clés possibles : ens couples (a, b) tq $\text{pgcd}(a, 26) = 1$

$\rightarrow f$ déchiffre \Leftrightarrow $\bar{u} = \text{dé}(a, b)$ est $A(u, -ub)$.

(où u est l'inverse de $a [26]$).

(312 clés possibles par 26 lettres).

IX / Espace des clés

I (a, b) est clé valide par C si $a \perp m$ si $a \perp m = 1$.

II matr de clé $\alpha \times m$

définie par $\sum_{j=1}^m \alpha_j \cdot \text{clé}_j$

$(\alpha \leq m-1)$

8/ Cryptanalyse

✓ tester \forall clés possibles & chercher msg "cours" avec peu de clés.

✓ Analyse statique pour réduire notre clé

✓ 60^{es} 2 caractères pour trouver clé codage & clé décoding.

@ msg IKH5K1T codé à \oplus A $\oplus B = AB \dots 20123456789 = 37$ carac

I $\xrightarrow{\text{code}}$ 3 soit $8 \rightarrow 1$ & $5 \rightarrow 5$ soit $32 \rightarrow 9$.

$$\begin{array}{l} \text{Clé de codage} \\ \left\{ \begin{array}{l} E(a, b) \circ (\bar{1}) = \bar{8} \\ E(a, b) \circ (\bar{5}) = \bar{32} \end{array} \right. \Rightarrow \begin{cases} a \cdot 1 + b \equiv 8 \pmod{37} \\ a \cdot 5 + b \equiv 32 \pmod{37} \end{cases} \quad (*) \end{array}$$

$$\begin{array}{l} \text{Clé de décoding} \\ \left\{ \begin{array}{l} D(a, b) \circ (\bar{8}) = \bar{1} \\ D(a, b) \circ (\bar{32}) = \bar{5} \end{array} \right. \Rightarrow \begin{cases} 8a + b \equiv 1 \pmod{37} \\ 32a + b \equiv 5 \pmod{37} \end{cases} \quad 8a - 37k = 24 \end{array}$$

$$* \Rightarrow 8a \equiv 24 \pmod{37} \Rightarrow \exists k \in \mathbb{Z}, 8a = 24 + 37k. \quad (\text{ED}).$$

$$\begin{aligned} 37 &= 4 \times 8 + 5 & 1 &= 3 - 2 = 3 - (5 - 3) = 3 \times 2 - 5 = (8 - 5) \times 2 - 5 = 8 \times 2 - 3 \times 5 \\ 8 &= 5 \times 1 + 3 & 1 &= 8 \times 2 - 3(37 - 4 \times 8) = 16 \times 8 - 3 \times 37. \\ 5 &= 3 \times 1 + 2 \\ 3 &= 2 \times 1 + 1 \\ 2 &= 2 \times 1 + 0 \end{aligned}$$

comme $8 \wedge 37 = 1$ divise 24, l'équation a solutions.

$$6m \text{ on écrit } (16 \times 24) \times 8 - 37(3 \times 24) = 24 \Rightarrow 336 \times 8 - 37 \times 72 = 24$$

soit $(a_0, b_0) = (336, 72)$ est solut^e particulièr^e.

$$(a_m, b_m) = \left(a_0 - \frac{37}{8 \wedge 37} \times m, b_0 - \frac{8}{8 \wedge 37} \times m \right) = (336 - 37m, 72 - 8m)$$

on cherche $m \in \{0, \dots, 36\}$; on fait $\text{DE } 336 \text{ par } 37$. $336 = 9 \times 37 + 3$.

Ainsi pr $m = 9$, on a $(a, b) = (3, 5)$.

Pour trouver b on remplace a par 3 dans l'égalité (1) ou (2).

$$a \times 1 + b = 8 \pmod{37} \Rightarrow 3 + b = 8 \pmod{37} \Leftrightarrow b = 5 \pmod{37}$$

\Rightarrow Clé de chiffrement est $(3, 5)$.

(8)

$$\begin{array}{l} \text{Résoudre } \begin{cases} 720x + 54y = 56 \\ 720 \wedge 54 = 18 \end{cases} \Rightarrow \text{AEE} \end{array} \Rightarrow (1, -13, 18)$$

$720 \wedge 54 = 18 \neq 56 \Rightarrow$ dc pas de solut^es.

$$407x + 129y = 1 \quad \text{AEE} \Rightarrow (-58, 183, 1)$$

$$407 \wedge 129 = 1 \mid 1 \Rightarrow \text{équat^e a solut^es.}$$

$$\Rightarrow (-58 \times 1) \times 407 + (183 \times 1) \times 129 = 1$$

$$-58 \times 407 + 183 \times 129 = 1$$

soit $(a_0, b_0) = (-58, 183)$ est solut^e particulièr^e.

$$(a_m, b_m) = \left(a_0 - \frac{a_0 \times m}{a \wedge b}, b_0 + \frac{b_0 \times m}{a \wedge b} \right)$$

$$(a_m, b_m) = (-58 + 58m, 183 + 183m)$$

(9)

XI / Chiffre de Vigenère

CDV utilise carré de Vigenère

lettres de la clé	A	B	C	D	E	...	Y	Z	lettres text plain
A	A	B	C	D	E	...	Y	Z	
B	B	C	D	E	F	...	Z	A	
C	C	D	E	F	G	...	Z	A	B
D	D	E	F	G	H	...	Z	A	C
Z	Z	A	B	C	D	...	X	Y	

Pour chiffrer msg "COUCOU", choisir dé : "B A D A" sa forme mat

D: intersection B (ligne) \wedge C (colonne)

O: A \wedge O ; V: D \wedge U ; C: A \wedge C ; P: B \wedge O ; U: A \wedge U

Donc COUCOU est chiffré par DOXCPU.

(RQ) C'est pas codé 2 fois m façon, tt comme U.

(RQ) Ce chiffrage revient à grouper les lettres en bloc de longueur k ou k est la longueur de la clé : k

Si clé ss forme k-uplet (m_1, \dots, m_k) : chiffrer consiste :

x faire chiffrer de césar de clé m_1 sur 1^e lettre

m_2 sur 2^e lettre

⋮

MÉO

Une clé (m_1, \dots, m_k) où $m_1, \dots, m_k \in \mathbb{Z}/26\mathbb{Z}$

• $f_{\text{chiffr}}: C(m_1, \dots, m_k) \in \mathbb{Z}/26\mathbb{Z} \times \dots \times \mathbb{Z}/26\mathbb{Z} \rightarrow \mathbb{Z}/26\mathbb{Z} \times \dots \times \mathbb{Z}/26\mathbb{Z}$

• $f_{\text{dichiffr}}: C(-m_1, \dots, -m_k)$

11

2/ Espace des clés & Atk

En clé de longueur k des alphabets 26 lettres : 26^k clés.

→ une lettre n'est pas chiffrée 2x m façon sauf si elles se retrouvent dans la même place du bloc. ↓ ↓

Exemple de clé de longueur 4 ; les 2 A m façon ALPHABET.

Ainsi si on connaît longue clé : faire atk statique ou moy.

XII / Le chiffrement "parfait"

Alice pour Bob : ATTAQUE LE CHATEAU.

→ le chiffre msg. clé → aussi long que msg (sans espaces)

→ clé : complètement aléatoire.

C : [9, 18, 8, 0, 21, 42, 18, 13, 7, 11, 23, 22, 19, 2, 16, 9]

Elle chiffre la i ème lettre du msg en utilisant César et ième lettre de clé.

ELVALGW YL NEWLGQD (chiffrement de Vigenère + clé de longueur du texte)

(Rq) les lettres T chiffrees en L, V, M.

$$m + c = e$$

{ m : lettre en clair
c : clé
e : lettre chiffrée

Si on ne connaît que e, il est impossible de retrouver m.
(peut y avoir plusieurs de c st possibles).

Si on connaît c alors $m = e - c$ & on peut déchiffrer msg.

Défaut : Clé aussi grande que texte & généralement aléatoire.

Si Eve intercepte msg, force Alice donner la clé, elle peut donner clé factice.

C : [13, 7, 19, ...]

ce q. Eve vend parfait

RECETTE DE CUISINE