

*CESAR:

Position de la lettre

↑
l'index

→ dans \mathbb{Z}_{26}

-chiffrement: $C = (P + K) \text{ mod } 26$

-déchiffrement: $D = (C - K) \text{ mod } 26$

*AFFINE:

premier
multiplié

-chiffrement: $C = (a * p + b) \text{ mod } 26$ } cle'

-déchiffrement: $D = \bar{a}^{-1} (C - b) \text{ mod } 26$ } cle' inversée

Avant de la calculer on doit s'assurer que:
 $(a, b) \in \mathbb{Z}_{26} \times \mathbb{Z}_{26}$ et $\text{PGCD}(a, 26) = 1$

*VIGENÉAUX:

-chiffrement: (lettre du Mess + lettre du Mot cle') mod 26

exemple: $J \quad 10 \quad 10$
+ $M \quad 12 \quad 12$: message

$$\begin{array}{r} + \\ \hline 22 \end{array}$$

On peut donc

écrire le

Résultat

à partir de

①

~~Déchiffrement : (lettre Mess chiffré - lettre du Mot) mod clé~~

exemple : U R X G : Message chiffré

commencer
par la
clé

- 4 19 23 6
I N F O : clé
8 13 5 14
M E S S
12 4 18 18

Remarque :

$x \text{ mod } y$

Si $x > 0$:

$x \text{ mod } y = \text{reste div de } x \text{ par } y$

Si $x < 0$:

② $x \text{ mod } y = x + y + y \dots \text{ jusqu'à } x > 0 \text{ et } x < y$

* PLAYFAIR: former les grilles de chiffrement avec mot-clé secret et les autres lettres de l'alphabet sont ajoutées dans l'ordre pour compléter la grille. (5x5)

exemple: Mot= Salut

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

→ dans la Version anglaise I et J sont regroupés dans la même case.

Remarque (Anglais):

- si 2 lettres en clair sur les coins d'un rectangle, alors les lettres différées sont sur les 2 autres coins. A E → T C

- 2 lettres sur la même ligne, on prend les 2 lettres qui les suivent immédiatement. S L → A U ③

Si 2 lettres sont sur la même colonne, on prend les 2 lettres qui les suivent immédiatement en dessous.

TR → ~~TR~~

- Si un groupe de lettre à chiffrer est composé de la même lettre, on la sépare par un X entre les 2.

SS → SXS

* HILL:

étape 1:
- Chiffrement: condition ~~nécessaire~~ pour vérifier la validité : la Matrice doit être inversible (A^{-1}) dans \mathbb{Z}_{26} preuve ça on a par exemple : $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$
- Calculer $\det(A) = ad - cb$ puis calculer $\text{PGCD}(\det(A), 26) = 1$

étape 2: diviser le message en bloc en fonction de la dimension de la Matrice de facteur $n = ?$ ④

exemple : si $k = \begin{pmatrix} 3 & 4 \\ 5 & 7 \end{pmatrix}$ dimension 2 alors $n=2$

- ensuite une fois on a diviser le message

en calcul : $\begin{pmatrix} C_1 \\ C_2 \end{pmatrix} = \left[k \times \begin{pmatrix} P_1 \\ P_2 \end{pmatrix} \right] \text{ mod } 26 \quad \left. \begin{array}{l} \text{cas} \\ n=2 \end{array} \right\}$

- déchiffrement : pour commencer c'est $\begin{pmatrix} P_1 \\ P_2 \end{pmatrix} = k^{-1} \times \begin{pmatrix} C_1 \\ C_2 \end{pmatrix} \text{ mod } 26$
Pour calculer $k^{-1} = \text{Det}(k)^{-1} \times \text{CoMat}(k) \text{ mod } 26$

$$k = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \quad \text{CoMat}(k) = \begin{pmatrix} d & -b \\ -c & a \end{pmatrix}$$

prendre 1^{re} diagonale et inverser leur position

prendre 2^{emp} diagonale et inverser leur signe

ensuite pour calculer $\text{det}(k)^{-1}$ on doit

$$\text{Resoudre : } \text{det}(k) u + 26v = 1$$

⑤

$$U = (\det(k))^{-1} \text{ si } \det(k) \neq 0$$

- Aprés Appliquer la Méthode de l'équation diophantiniennes pour Trouver U et V , ensuite Calculer le k^{-1} afin de calculer les Positions avec $(P_i) = [k^{-1} \times (C_1)] \bmod 26$

* Transposition simple par colonnes:

- chiffrement: Disposer horizontalement le Message en colonne \Leftrightarrow nbr colonnes = n . et collecter les lettres Verticalement.

exemple: BONSOEUR \Rightarrow BJRDOOND

6 Hauteur des
mots à col partagée
est: $m \div n$
 $= 7 \div 3 = 2$

BON

JOU

R

7 mod 3 = 1 > 0

6 Hauteur de la 1^{ere} col
 $= m \div n + 1 = 3$

⑥

- Déchiffrement: Déposer Véritablesment le Message chiffré ~~top~~ nbr col = n, et collecter les lettres Horizontalement.

Exemple: TRIMROOPAGNEADSEST^{TJ}
m=15 (nbr de lettres)
n=5
TRANS } $m \bmod n = 15 \bmod 5 = 0$
POSIT } $n \bmod m = 5 \bmod 15 = 5$
IONSE } $m \bmod n = 15 \bmod 5 = 0$
MPLE }

Remarque: Avant de commencer à positionner:

- * chiffrement: pour un Message longueur m alors
 - $m \bmod n = 0$: dans ce cas, Toutes les colonnes ont la Même hauteur $m \bmod n$
 - $m \bmod n = l$, tel que $l > 0$ dans ce cas:
 - la hauteur des i premières colonnes est $(m \bmod n) + 1$
 - la hauteur des $n-i$ dernières colonnes restantes est $m \bmod n$ (pareil pour déchiffrement)

* Transposition complete per calendar.

- chiffrement à clé: si le message donne le nbr de colonnes et l'ordre de la recette des lettres, on dispose le message horizontalement, on collecte verticalement les lettres suivant l'ordre croissant des lettres de la clé.

Exemple: CHIFFREMENT D'AFFINE avec clef AVAILE

CHIFFRE
AEMEN
TDAFF
INE

* Rechiffrement: ~~re~~ disposer Verte et collecte flotjan
exemplaire

exemples: CRTS FE & FNE iMER HEDA des AVAIL

Collecte 11/11 : CHIFFREMENT DE CESAR 15423
 CHIFFREMENT DE CESAR { 1 5 4 2 3 7 12 mod 5 + 3 15423
 DECESAR { C H F A F E C D B G S P X
 A E B W C T S U V Y Z
 T B D F G H J K L M N O P Q R
 S C E G I K M P Q R V X Y Z
 D E C E S A R

Cryptographie Moderne :

* Protocole de DIFFIE-HELLMAN (DH) :

- Role : vérifier si les clés sont valides ou pas.
- ① Choix des paramètres : p nombre premier et g (un entier plus petit que p) $1 \leq g \leq p-1$
- ② Génération des clés privées : chaque participant génère confidentiellement sa propre clé privée.
- A génère x_A tel que $x_A < p$
- B // x_B // $x_B < p$
- ③ Calcul des clés publiques :
- A calcule : $y_A = g^{x_A} \text{ mod } p$
- B calcule : $y_B = g^{x_B} \text{ mod } p$
- ④ Echange des clés publiques : les 2 participants s'échangent leurs clés publiques y_A et y_B
- ⑤

⑤ Calcul de la clé secrète: chaque participant calcule sa clé secrète en utilisant la clé pub de l'autre participant et sa propre clé privée;

- A calcule : $K = (Y_B)^{X_A} \text{ mod } P$ } clé K partagée
- B calcule : $K = (X_A)^{X_B} \text{ mod } P$ } de secret partagé entre les 2 participants.

* Pour vérifier la validité de la clé partagée:

$$g^{X_A X_B} \text{ mod } p$$

* Chiffrement de RSA:

- 2 grands nombres premiers p & q (distincts) sont choisis
- calculer $n = p \times q$
- calculer $\phi(n) = (p-1) \times (q-1)$
- un entier e est choisi tel que : $1 < e < \phi(n)$ et $\text{PGCD}(e, \phi(n)) = 1$
- calculer d tel que $e \times d \text{ mod } \phi(n) = 1$ avec équation diophantiniennes ($e x + \phi(n) y = 1$) (lo)

- la clé publique (e, p). la clé privée (d, n)
- * chiffrement: $C = M^e \text{ mod } n$ tel que: $M \leq n$
(M : message en clair, C : message chiffré)
- * Déchiffrement: $M = C^d \text{ mod } n$
- * chiffrement de Elgamal:

- choisir un grand nombre premier p et 2 nombres a et g tel que: $a < p$ et $g < p$
- calculer $A = g^a \text{ mod } p$ pour avoir la clé publique: (A, g, p) et la clé privée (a)
- * chiffrement: $M \leq p$
- choisir un nombre aléatoire b ($b < p$ et $\text{pgcd}(b, p-1) = 1$)
- calculer $B = g^b \text{ mod } p$
- calculer $C = (M \times A^b)^{\text{mod}} p$
- le chiffre du message: (B, C)

11

* Déchiffrement:

$$M = (C \times B^{(p-a-1)}) \bmod p$$

* Signature Numérique:

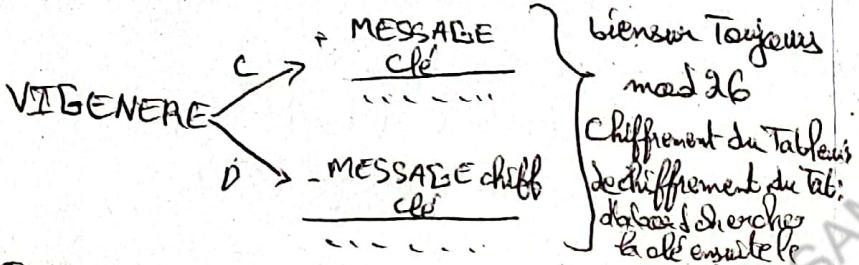
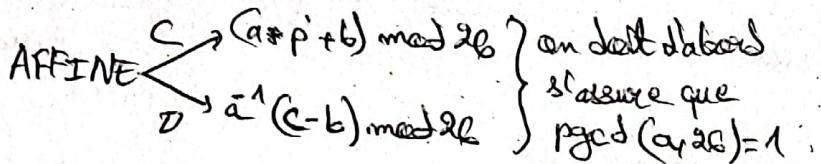
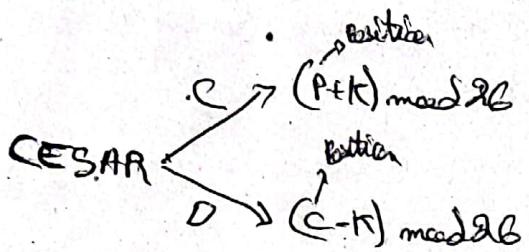
RSA: clés de l'expéditeur $\Rightarrow \{ (e, m), (d, n) \}$

Generation de la S de M	Vérification de la S
- calculer $h = H(M)$	- calculer $h^d = H(M)$
- calculer $S = h^d \bmod n$	- calculer $h^d = S \bmod n$
- La Signature Numéro (M, S)	- Si $h^d = S \Rightarrow S$ valide

ELGAMAL: clés expéditeur $\Rightarrow \{ (A, g, p), b \}$

Generation de la S de M	Vérification de la S
- calculer $h = H(M)$	- calculer $h^d = H(M)$
- choisir un nbr aléatoire b	- Si $(A^B \times B^e) \bmod p \approx h \bmod p$
- $b < p$ et $\text{pgcd}(b, p-1) = 1$	\Rightarrow La signature est valide
- calculer $B = g^b \bmod p$	
- calculer C tel que $C \equiv (A^B \times B^e) \bmod (p-1) \Rightarrow C \equiv (B, e) \bmod (p-1)$	
- signature num $\Rightarrow (M, S)$	

CRYPTOGRAPHIE classique



REMARQUE:

$x \bmod y$
 si $x > 0$:

$x \bmod y = \text{reste div de } x \text{ par } y$

si $x < 0$:

$x \bmod y = x + y + \dots$ jusqu'à $x \geq 0$ et $x \leq y$

PLAYFAIR

former des grilles de chiffrement avec le mot-clé secret et les autres lettres de l'alphabet sont ajoutées dans l'autre pour compléter la grille (5x5)

MOTS = Salut

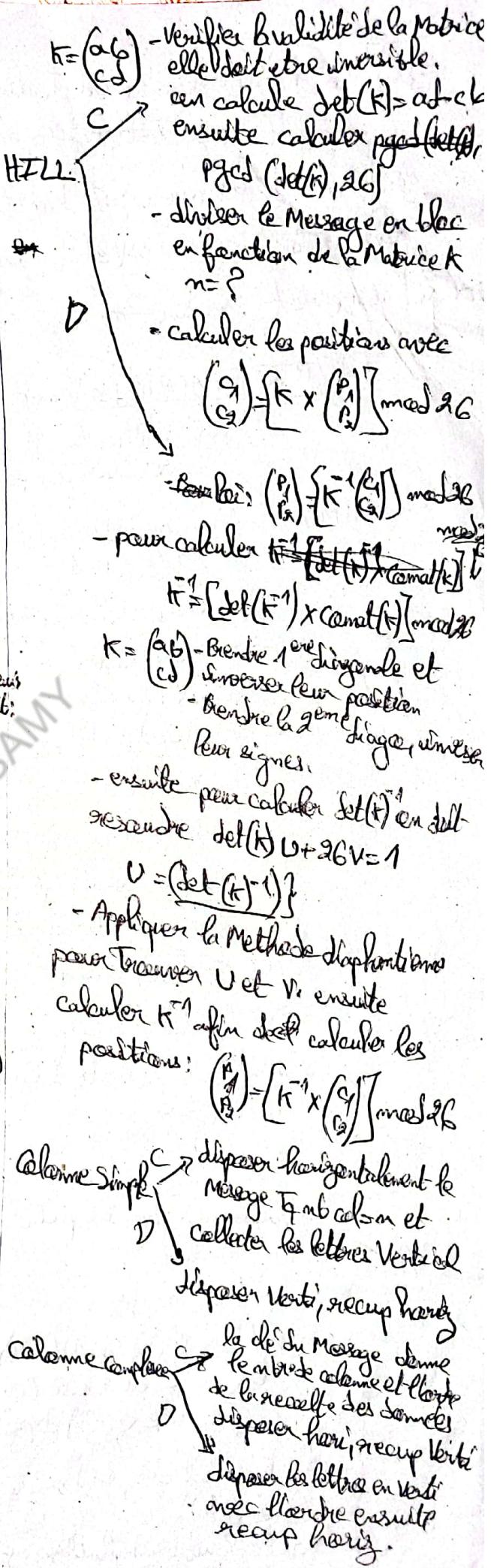
S	A	L	N	T
B	C	D	E	F
G	H	I	J	K
M				
N	O	P	Q	R
V	W	X	Y	Z

AT → TC (les autres cas)

SL → (AU) (même ligne)

TA → TZ (même colonne)

- un groupe de lettres à chiffrer est composé de 2 lettres (on le sépare par le caractère les 2) : CS → SX



Remarque:

- * chiffre m mod n = 0 : dans ce cas, toutes les colonnes ont la même hauteur mod n
- * mod n = u tel que u > 0 dans ce cas:
 - la hauteur des u premières col est: $(m \text{ div } n) + 1$
 - le reste est: $m \text{ div } n$.

CRYPTOGRAPHIE Moderne

But: vérifier les clés si elles sont valide ou pas.

DIFFIE-HELLMAN

- choisir paramètres p (nombres premiers)
- $1 \leq g \leq p-1$
- génération des clés publiques:
 - * A génère x_A tel que: $x_A < p$ (pareil pour B)
 - calculer les clés publiques:

$$A: X_A = g^{x_A} \text{ mod } p$$

$$B: X_B = g^{x_B} \text{ mod } p$$

- échange des clés publiques.

- calculer la clé secrète:

$$A: K = (X_B)^{x_A} \text{ mod } p$$

$$B: K = (X_A)^{x_B} \text{ mod } p$$

- vérifier la validité de la clé partagée:

$$g^{x_A x_B} \text{ mod } p$$

2 grands nbr premiers p et q (distincts) sont choisis.

RSA

- calculer $n = pq$
- calculer $\phi(n) = (p-1)(q-1)$
- un entier e est choisi tel que:

$$1 \leq e < \phi(n) \text{ et } \text{pgcd}(e, \phi(n)) = 1$$

- calculer d tel que $e \cdot d \text{ mod } \phi(n) = 1$
- $(1 \leq d < \phi(n))$

ancres équations diophantiennes: $e \cdot d \cdot \phi(n) = 1$

de public: (e, n) . de privée (d, n)

* Chiffrement:

$$C = M^e \text{ mod } n \text{ tel que } M < n$$

* Déchiffrement:

$$M = C^d \text{ mod } n$$

ELGAMAL \rightarrow choisir nbr premier p et 2 nombres a et g tel que: $a < p$ et $g < p$

- calculer $A = g^a \text{ mod } p$: pour avoir la clé publique (A, g, p) .

* Chiffrement:

- choisir nbr b ($b < p$ et $\text{pgcd}(b, p-1) = 1$)

$$\text{calculer } B = g^b \text{ mod } p$$

$$\text{calculer } C = (M \times A^b) \text{ mod } p$$

message chiffré (B, C)

* Déchiffrement:

$$B^{-1} M = (C \times B^{(p-a-1)}) \text{ mod } p$$

* Signature Numérique (Certificat):

RSA

ELGAMAL

Génération de la S: $(S=?)$

$$\text{calculer } h_1 = H(m)$$

$$\text{calculer } S = h_1^d \text{ mod } n$$

\Rightarrow Signature $\Rightarrow (M, S)$

* Vérification de la S:

$$\text{calculer } h_1 = H(m)$$

$$\text{calculer } h_2 = S^e \text{ mod } n$$

$\text{si } h_1 = h_2 \Rightarrow \text{signature}$

valide

ELGAMAL

Génération de la S:

$$\text{calculer } h = H(m)$$

$$\text{choisir nbr } b \text{ ($b < p$ et $\text{pgcd}(b, p-1) = 1$)}$$

$$\text{calculer } B = g^b \text{ mod } p$$

$$\text{calculer } C$$

$$h = (a \cdot B + b \cdot C) \text{ mod } (p-1)$$

\Rightarrow Signature $\Rightarrow (B, C)$

valide

* Vérification de la S:

$$\text{calculer } h = H(m)$$

$$\text{si } (A^e \times B^c) \text{ mod } p$$

$$= g^h \text{ mod } p$$

\Rightarrow Signature Valide

Diffiérence (ELGAMAL):

$$B=? \quad C=?$$

calculer $h = f(m)$

- calculer $B = g^b \text{ mod } p$

- calculer $C : (axB + bxC) \text{ mod } (p-1) = R$

exemple: $a=13 \quad B=119 \quad b=3 \quad p=131 \quad h=15$

$$13 \times 119 + 3C \text{ mod } 130 = 15$$

$$\Rightarrow 1539 + 3C \text{ mod } 130 = 15$$

$$\Rightarrow 1539 - 3C \text{ mod } 130$$

$$\Rightarrow 130Y - 3C = 1539$$

pour $130Y - 3C = 1$ on aura $(Y, C) = (1, 43)$

$$C = 43 \times 1539 \text{ mod } 130 = 96$$

$$B = 119 \quad C = 96$$

Dans le cas où on a B et C :

- calculer $h = f(m)$

- calculer $A^B \times B^C \text{ mod } p = g^h \text{ mod } p$