CHIFFREMENT AFFINE

SUBSTITUTION MONO-ALPHABÉTIQUE

Chiffrement affine

la **clé est un couple d'entier (a,b)** : chaque lettre de rang $\boldsymbol{i}$ est remplacée par la lettre de rang $\boldsymbol{j = ai + b[26]}$

Chiffrement affine

la **clé est un couple d'entier (a,b)** : chaque lettre de rang i est remplacée par la lettre de rang $\boldsymbol{j = ai + b[26]}$

Mais est-on sûr que l'opération soit **réversible** ?

Chiffrement affine

la **clé est un couple d'entier (a,b)** : chaque lettre de rang i est remplacée par la lettre de rang $\boldsymbol{j = ai + b[26]}$

Mais est-on sûr que l'opération soit **réversible** ?

$$\boldsymbol{j = ai + b[26] \Longrightarrow ai = j - b[26] \Longrightarrow i = a^{-1}(j - b)[26]}$$

Chiffrement affine

la **clé est un couple d'entier (a,b)** : chaque lettre de rang i est remplacée par la lettre de rang $\boldsymbol{j = ai + b[26]}$

Mais est-on sûr que l'opération soit **réversible** ?

$$\boldsymbol{j = ai + b[26] \Longrightarrow ai = j - b[26] \Longrightarrow i = a^{-1}(j - b)[26]}$$

a est-il toujours inversible modulo $\mathbf{26}$, c'est-à-dire dans $\mathbb{Z}/\mathbf{26}\mathbb{Z}$?
Comment calcule-t-on a^{-1}?

PARENTHÈSE D'ARITHMÉTIQUE

PGCD

Le PGCD de deux entiers relatifs a et b est le « plus grand commun diviseur de a et b », c'est-à-dire le plus grand entier d divisant à la fois a et b.

Principe de l'algorithme d'Euclide

Si q et r sont respectivement le quotient et le reste de la division euclidienne de n par m (n≥m) alors : $\boldsymbol{PGCD(n,m) = PGCD(m,r)}$

Théorème de Bezout (identité de Bezout)

Soient $\boldsymbol{n}$ et $\boldsymbol{m}$ deux entiers naturels.

Il existe deux entiers relatifs, u et v de Z, tels que : $\boldsymbol{PGCD(n,m) = u \times n + v \times m}$

Les entiers $\boldsymbol{u}$ et $\boldsymbol{v}$ sont appelés coefficients de Bezout.

PARENTHÈSE D'ARITHMÉTIQUE

Nombres premiers entre eux

Deux entiers n et m sont premiers entre eux s'ils ont pour seuls diviseurs communs 1 et -1.

Inversibilité dans Z/nZ

Soient $\boldsymbol{p}$ et $\boldsymbol{n}$ deux entiers $(\boldsymbol{p} \leq \boldsymbol{n})$

Les propositions suivantes sont équivalentes :

- $\boldsymbol{p}$ est inversible dans $\mathbb{Z}/n\mathbb{Z}$
- $\boldsymbol{n}$ et $\boldsymbol{p}$ sont premiers entre eux
- $\boldsymbol{PGCD(n, p) = 1}$
- Identité de Bezout : $\exists u, v \in Z$ tels que $\boldsymbol{nu + pv = 1}$

Algorithme d'Euclide étendu

Déterminer $\boldsymbol{pgcd(165,72)}$ et les coefficients de Bezout $\boldsymbol{u}$ et $\boldsymbol{v}$ vérifiant :

$$\boldsymbol{pgcd(165,72) = 165 \times u + 72 \times v}$$

Calcul des coefficients de Bezout

$$\boldsymbol{pgcd(165, 72) = 165 \times u + 72 \times v}$$

Principe : reprendre l'algorithme d'Euclide, en exprimant, à chaque étape le reste comme combinaison linéaire de 165 et 72.
Le dernier reste non nul correspond au pgcd et nous donnera donc l'identité de Bezout et ses coefficients

Calcul des coefficients de Bezout

$$\boldsymbol{pgcd(165,72) = 165 \times u + 72 \times v}$$

Division euclidienne (algorithme d'Euclide)	**Reste =** $\boldsymbol{165 \times u + 72 \times v}$
$165 = 2 \times 72 + 21$	$\boldsymbol{21 = 165 - 2 \times 72}$
$72 = 3 \times 21 + 9$	$9 = 72 - 3 \times \boldsymbol{21}$ $9 = 72 - 3 \times (\boldsymbol{165 - 2 \times 72})$ $\boldsymbol{9 = -3 \times 165 + 7 \times 72}$
$21 = 2 \times 9 + 3$	$3 = \boldsymbol{21} - 2 \times \boldsymbol{9}$ $3 = \boldsymbol{165 - 2 \times 72} - 2 \times (\boldsymbol{-3 \times 165 + 7 \times 72})$ $\boldsymbol{3 = 7 \times 165 - 16 \times 72}$
$9 = 3 \times 3 + \boldsymbol{0}$	$\boldsymbol{pgcd(165,72) = 3}$ (dernier reste non nul) **Identité de Bezout :** $\boldsymbol{pgcd(165,72) = 7 \times 165 - 16 \times 72}$

Calcul des coefficients de Bezout

$$\boldsymbol{pgcd(165,72) = 165 \times u + 72 \times v}$$

Division euclidienne (algorithme d'Euclide)	**Reste =** $\boldsymbol{165 \times u + 72 \times v}$
$165 = 2 \times 72 + 21$	$\boldsymbol{21 = 165 - 2 \times 72}$ **égalité1**
$72 = 3 \times 21 + 9$	$9 = 72 - 3 \times \boldsymbol{21}$ $9 = 72 - 3 \times (\boldsymbol{165 - 2 \times 72})$ $\boldsymbol{9 = -3 \times 165 + 7 \times 72}$ **égalité2**
$21 = 2 \times 9 + 3$	$3 = \boldsymbol{21} - 2 \times \boldsymbol{9}$ $3 = \boldsymbol{165 - 2 \times 72} - 2 \times (\boldsymbol{-3 \times 165 + 7 \times 72})$ $\boldsymbol{3 = 7 \times 165 - 16 \times 72}$ **égalité3 = égalité1 – 2x égalité2**
$9 = 3 \times 3 + \boldsymbol{0}$	$\boldsymbol{pgcd(165,72) = 3}$ (dernier reste non nul) **Identité de Bezout :** $\boldsymbol{pgcd(165,72) = 7 \times 165 - 16 \times 72}$

Etape n : $r_n = 165 \times u_n + 72 \times v_n$

Calcul des coefficients de Bezout

$$pgcd(165, 72) = 165 \times u + 72 \times v$$

Division euclidienne (algorithme d'Euclide)	**Reste =** $165 \times u + 72 \times v$
$165 = 2 \times 72 + 21$	$21 = 165 - 2 \times 72$ **égalité1**
$72 = 3 \times 21 + 9$	$9 = 72 - 3 \times 21$ $9 = 72 - 3 \times (165 - 2 \times 72)$ $9 = -3 \times 165 + 7 \times 72$ **égalité2**
$21 = 2 \times 9 + 3$	$3 = 21 - 2 \times 9$ $3 = 165 - 2 \times 72 - 2 \times (-3 \times 165 + 7 \times 72)$ $3 = 7 \times 165 - 16 \times 72$ **égalité3 = égalité1 – 2x égalité2**
$9 = 3 \times 3 + 0$	$pgcd(165, 72) = 3$ (dernier reste non nul) **Identité de Bezout :** $pgcd(165, 72) = 7 \times 165 - 16 \times 72$

Calcul des coef

$$\boldsymbol{pgcd(165,72) = 16}$$

Etape n : $r_n = 165 \times u_n + 72 \times v_n$

Etape n : division euclidienne entre les restes des étapes précédentes

$$r_n = r_{n-2} - q_n \times r_{n-1}$$

Division euclidienne (algorithme d'Euclide)	**Reste =$165 \times u + 72 \times v$**
$165 = 2 \times 72 + 21$	$\mathbf{21 = 165 - 2 \times 72}$ **égalité1**
$72 = 3 \times 21 + 9$	$9 = 72 - 3 \times \mathbf{21}$ $9 = 72 - 3 \times (\mathbf{165 - 2 \times 72})$ $\mathbf{9 = -3 \times 165 + 7 \times 72}$ **égalité2**
$21 = 2 \times 9 + 3$	$3 = \mathbf{21} - 2 \times \mathbf{9}$ $3 = \mathbf{165 - 2 \times 72} - 2 \times (\mathbf{-3 \times 165 + 7 \times 72})$ $\mathbf{3 = 7 \times 165 - 16 \times 72}$ **égalité3 = égalité1 – 2x égalité2**
$9 = 3 \times 3 + \mathbf{0}$	$\boldsymbol{pgcd(165,72) = 3}$ (dernier reste non nul) **Identité de Bezout :** $\boldsymbol{pgcd(165,72) = 7 \times 165 - 16 \times 72}$

Calcul des coef

$$\boldsymbol{pgcd(165,72) = 16}$$

Division euclidienne (algorithme d'Euclide)	Res
$165 = 2 \times 72 + 21$	$\color{red}{\mathbf{21}}$
$72 = 3 \times 21 + 9$	$9 =$ $9 =$ $\color{green}{\mathbf{9} =}$
$21 = 2 \times 9 + 3$	$3 =$ $3 =$ $\mathbf{3} = 7 \times 165 - 16 \times 72$ égalité3 = égalité1 − 2x égalité2
$9 = 3 \times 3 + \mathbf{0}$	$\boldsymbol{pgcd(165,72) = 3}$ (dernier reste non nul) **Identité de Bezout :** $\boldsymbol{pgcd(165,72) = 7 \times 165 - 16 \times 72}$

Etape $\boldsymbol{n}$: $\boldsymbol{r_n = 165 \times u_n + 72 \times v_n}$

Etape $\boldsymbol{n}$: division euclidienne entre les restes des étapes précédentes

$$\boldsymbol{r_n = r_{n-2} - q_n \times r_{n-1}}$$

Comme, à chaque étape, on procède par division euclidienne des restes, on peut considérer que la première étape (division de 165 par 72) correspond à la division de $\boldsymbol{r_0}$ par $\boldsymbol{r_1}$.

D'où l'initialisation suivante :

$$\boldsymbol{r_0 = 165}$$

$$\boldsymbol{r_1 = 72}$$

Opérations sur les lignes		r : reste	u (coefficient de 165)	v (coefficient de 72)	Division euclidienne	q : quotient
Initialisation	L_0	165	1	0	$165 = 165 \times 1 + 72 \times 0$	
	L_1	72	0	1	$72 = 165 \times 0 + 72 \times 1$	

Opérations sur les lignes		r : reste	u (coefficient de 165)	v (coefficient de 72)	Division euclidienne	q : quotient
Initialisation	L_0	165	1	0		
	L_1	72	0	1	$165 = 2 \times 72 + 21$ $21 = 1 \times 165 - 2 \times 72$	2
$L_2 = L_0 - 2L_1$		21	1	-2	$72 = 3 \times 21 + 9$ $9 = 72 - 3 \times 21$	3

$$L_0 : 165 = 165 \times 1 + 72 \times 0$$

$$L_1 : 72 = 165 \times 0 + 72 \times 1$$

$$L_2 = L_0 - 2L_1 : 165 - 2 \times 72 = 165 \times 1 + 72 \times 0 - 2 \times (165 \times 0 + 72 \times 1)$$

$$L_2 :\ 21 = (1 - 2 \times 0)165 + (0 - 2 \times 1)72$$

$$L_2 :\ 21 = 165 \times 1 + 72 \times (-2)$$

Opérations sur les lignes		r : reste	u (coefficient de 165)	v (coefficient de 72)	Division euclidienne	q : quotient
Initialisation	L_0	165	1	0		
	L_1	72	0	1	$165 = 2 \times 72 + 21$ $21 = 1 \times 165 - 2 \times 72$	2
$L_2 = L_0 - 2L_1$		21	1	-2	$72 = 3 \times 21 + 9$ $9 = 72 - 3 \times 21$	3
$L_3 = ?$						

Opérations sur les lignes		r : reste	u (coefficient de 165)	v (coefficient de 72)	Division euclidienne	q : quotient
Initialisation	L_0	165	1	0		
	L_1	72	0	1	$165 = 2 \times 72 + 21$ $21 = 1 \times 165 - 2 \times 72$	2
$L_2 = L_0 - 2L_1$		21	1	-2	$72 = 3 \times 21 + 9$ $9 = 72 - 3 \times 21$	3
$L_3 =?$		9				

Opérations sur les lignes		r : reste	u (coefficient de 165)	v (coefficient de 72)	Division euclidienne	q : quotient
Initialisation	$\boldsymbol{L_0}$	165	1	0		
	$\boldsymbol{L_1}$	72	0	1	$165 = 2 \times 72 + 21$ $21 = 1 \times 165 - 2 \times 72$	2
$\boldsymbol{L_2 = L_0 - 2L_1}$		21	1	-2	$72 = 3 \times 21 + 9$ $9 = 72 - 3 \times 21$	3
$\boldsymbol{L_3 = L_1 - 3L_2}$		9	-3	7	$21 = 2 \times 9 + 3$ $3 = 21 - 2 \times 9$	2

Opérations sur les lignes		r : reste	u (coefficient de 165)	v (coefficient de 72)	Division euclidienne	q : quotient
Initialisation	L_0	165	1	0		
	L_1	72	0	1	$165 = 2 \times 72 + 21$ $21 = 1 \times 165 - 2 \times 72$	2
$L_2 = L_0 - 2L_1$		21	1	-2	$72 = 3 \times 21 + 9$ $9 = 72 - 3 \times 21$	3
$L_3 = L_1 - 3L_2$		9	-3	7	$21 = 2 \times 9 + 3$ $3 = 21 - 2 \times 9$	2
$L_4 = L_2 - 2L_3$		3	7	-16	$9 = 3 \times 3 + 0$ Reste nul, c'est fini. Le pgcd est le dernier reste non nul : $3 = 7 \times 165 - 16 \times 72$	

Opérations sur les lignes		r : reste	u (coefficient de 165)	v (coefficient de 72)	Division euclidienne	q : quotient
Initialisation	L_0	165	1	0		
	L_1	72	0	1	$165 = 2 \times 72 + 21$ $21 = 1 \times 165 - 2 \times 72$	2
$L_2 = L_0 - 2L_1$		21	1	-2	$72 = 3 \times 21 + 9$ $9 = 72 - 3 \times 21$	3
$L_3 = L_1 - 3L_2$		9	-3	7	$21 = 2 \times 9 + 3$ $3 = 21 - 2 \times 9$	2
$L_4 = L_2 - 2L_3$		3	7	-16	$9 = 3 \times 3 + 0$ Reste nul, c'est fini. Le pgcd est le dernier reste non nul : $3 = 7 \times 165 - 16 \times 72$	

Notations ?

Opérations sur les lignes		r : reste	u (coefficient de 165)	v (coefficient de 72)	Division euclidienne	q : quotient
Initialisation	L_0	r_0 165	u_0 1	v_0 0		
	L_1	r_1 72	u_1 0	v_1 1	$165 = 2 \times 72 + 21$ $21 = 1 \times 165 - 2 \times 72$	2
$L_2 = L_0 - 2L_1$		21	1	-2	$72 = 3 \times 21 + 9$ $9 = 72 - 3 \times 21$	3
$L_3 = L_1 - 3L_2$		9	-3	7	$21 = 2 \times 9 + 3$ $3 = 21 - 2 \times 9$	2
$L_4 = L_2 - 2L_3$		3	7	-16	$9 = 3 \times 3 + 0$ Reste nul, c'est fini	

Notations ?

Opérations sur les lignes		r : reste	u (coefficient de 165)	v (coefficient de 72)	Division euclidienne	q : quotient
Initialisation	L_0	$\boldsymbol{r_0}$ 165	$\boldsymbol{u_0}$ 1	$\boldsymbol{v_0}$ 0		
	L_1	$\boldsymbol{r_1}$ 72	$\boldsymbol{u_1}$ 0	$\boldsymbol{v_1}$ 1	$165 = 2 \times 72 + 21$ $21 = 1 \times 165 - 2 \times 72$	2
$L_2 = L_0 - 2L_1$		21	1	-2	$72 = 3 \times 21 + 9$ $9 = 72 - 3 \times 21$	3
$L_3 = L_1 - 3L_2$		9	-3	7	$21 = 2 \times 9 + 3$ $3 = 21 - 2 \times 9$	2
$L_4 = L_2 - 2L_3$		3	7	-16	$9 = 3 \times 3 + 0$ Reste nul, c'est fini	

$$\boldsymbol{q_2 = r_0 // r_1}$$

$$\boldsymbol{r_2} = r_0 \% \, r_1 = \boldsymbol{r_0 - q_2 \times r_1}$$

Opérations sur les lignes		r : reste	u (coefficient de 165)	v (coefficient de 72)	Division euclidienne	q : quotient
Initialisation	L_0	r_0 165	u_0 1	v_0 0		
	L_1	r_1 72	u_1 0	v_1 1	$165 = 2 \times 72 + 21$ $21 = 1 \times 165 - 2 \times 72$	2
$L_2 = L_0 - 2L_1$		21	1	-2	$72 = 3 \times 21 + 9$ $9 = 72 - 3 \times 21$	3
$L_3 = L_1 - 3L_2$		9	-3	7	$21 = 2 \times 9 + 3$ $3 = 21 - 2 \times 9$	2
$L_4 = L_2 - 2L_3$		3	7	-16	$9 = 3 \times 3 + 0$ Reste nul, c'est fini	

$q_2 = r_1 // r_0$

$r_2 = r_0 \% r_1 = r_0 - q_2 \times r_1$

$u_2 = u_0 - q_2 u_1$

$v_2 = v_0 - q_2 v_1$

Opérations sur les lignes		r : reste	u (coefficient de 165)	v (coefficient de 72)	Division euclidienne	q : quotient
Initialisation	L_0	r_0 165	u_0 1	v_0 0		
	L_1	r_1 72	u_1 0	v_1 1	$165 = 2 \times 72 + 21$ $21 = 1 \times 165 - 2 \times 72$	2
$L_2 = L_0 - 2L_1$		21	1	-2		
$L_3 = L_1 - 3L_2$		9	-3	7		
$L_4 = L_2 - 2L_3$		3	7	-16		

$q_2 = r_1 // r_0$

$r_2 = r_1 \% r_0$

$u_2 = u_0 - q_2 u_1$

$v_2 = v_0 -$

$r_0 = 165$
$r_1 = 72$
$u_0 = 1$ et $v_0 = 0$
$u_1 = 0$ et $v_1 = 1$

A chaque étape :

$q_n =$ **quotient de la division de** r_{n-2} **par** r_{n-1}

$r_n =$ **reste de la division de** r_{n-2} **par** r_{n-1}

$u_n = u_{n-2} - q_2 u_{n-1}$

$v_n = v_{n-2} - q_2 v_{n-1}$

Pseudo Code :

$r_0 = 165$
$r_1 = 72$
$u_0 = 1$ et $v_0 = 0$
$u_1 = 0$ et $v_1 = 1$

Tant que r_1 non nul faire :

début :

q ← quotient de la division de r_0 par r_1

$r_2 \leftarrow r_0 - qr_1$
$u_2 \leftarrow u_0 - qu1$
$v_2 \leftarrow v_0 - qv1$
$r_0 \leftarrow r_1 \,;\, r_1 \leftarrow r_2$
$u_0 \leftarrow u_1 \,;\, u_1 \leftarrow u_2$
$v_0 \leftarrow v_1 ; v_1 \leftarrow v_2$

fin

Renvoyer (u_0, v_0, r_0)

ent)	Division euclidienne	q : quotient
	$165 = 2 \times 72 + 21$ $21 = 1 \times 165 - 2 \times 72$	2

$$q_2 = r_1 // r_0$$

$$r_0 = 165$$
$$r_1 = 72$$
$$u_0 = 1 \text{ et } v_0 = 0$$
$$u_1 = 0 \text{ et } v_1 = 1$$

A chaque étape :

$$q_n = \text{quotient de la division de } r_{n-2} \text{ par } r_{n-1}$$
$$r_n = \text{reste de la division de } r_{n-2} \text{ par } r_{n-1}$$
$$u_n = u_{n-2} - q_2 u_{n-1}$$
$$v_n = v_{n-2} - q_2 v_{n-1}$$

Pseudo Code :

$r_0 = 165$

$r_1 = 72$

$u_0 = 1$ et $v_0 = 0$

$u_1 = 0$ et $v_1 = 1$

Tant que r_1 non nul

début :

q ← quoti

$r_2 \leftarrow r_0$

$u_2 \leftarrow u_0$

$v_2 \leftarrow v_0$

$r_0 \leftarrow r_1$

$u_0 \leftarrow u_1$

$v_0 \leftarrow v_1;$

fin

Renvoyer (u_0, v_0, r

```python
def euclide_etendu(m,n):
    if m < n:
        cop=m
        m = n
        n = cop
    # Initialisation
    r0, r1 = m, n
    u0, v0 = 1, 0
    u1, v1 = 0, 1
    # Boucle, tant que le reste est non nul
    while r1 != 0:
        q = r0 // r1
        r2, u2, v2 = r0 - q*r1, u0 - q*u1, v0 - q*v1
        r0, u0, v0 = r1, u1, v1
        r1, u1, v1 = r2, u2, v2
    return (r0, u0, v0)

euclide_etendu(165,72)   #  --> (3, 7, -16)
```

ent	Division euclidienne	q : quotient
	+ 21	2
	2 × 72	
	+ 0	2

$q_2 = r_1 // r_0$

5

2

$v_0 = 0$

$v_1 = 1$

ape :

on de r_{n-2} par r_{n-1}

de r_{n-2} par r_{n-1}

$u_n = u_{n-2} - q_2 u_{n-1}$

$v_n = v_{n-2} - q_2 v_{n-1}$

Exercice1

1. Euclide étendu

Écrire une fonction `pgcd_euclide_etendu(n,m)` prenant en paramètres deux entiers **n** et **m**, et renvoyant le tuple **(pgcd, u, v)** dans lequel :

- pgcd=pgcd(n,m)
- u et v sont les coefficients de Bezout dans l'égalité : $\boldsymbol{pgcd = u \times n + v \times m}$

2. Inverse modulaire

En utilisant la fonction **pgcd_euclide_etendu(n,m)**, écrire en Python une fonction `inversemod(nb,mod)` prenant en entrée deux entiers **nb** et **mod** et renvoyant l'inverse modulaire de nb quand celui-ci existe.

Exercice2

1. Si on utilise un chiffrement affine sur un alphabet de 26 lettres, combien de a-t-on de clés possibles ?
2. Programmer les fonctions suivantes :

- `chiffreaffine(message,a,b)` prenant en entrée le message et la clé (a,b) et renvoyant le cryptogramme
- `dechiffreaffine(cryptogramme,a,b)` prenant en entrée le cryptogramme et la clé (a,b) et renvoyant le message.

Exercice 2 : cryptanalyse chiffrement affine

'lqdmadtfkahuhqutadnkxxutesdstqutrqmadtfkalsrpqumqdtmq
psstnawulsfswrpulsxkatmlshsfmstladsqtwkmrnsfsmaudtqdtsd
kdrpamyaadtfkamsedamqxpkddsavmqdmfusdrkafmqmmskufd
umafyakuwqdgsfestqutadtfkalsnkxxutesyauuwrpuyaspsekdzkf
tbfftkpiusdxupxkpsnkxxut'

Cryptanalyse

On cherche la clé $(\boldsymbol{a}, \boldsymbol{b})$ *qui a permis de transformer chaque lettre de rang* $\boldsymbol{i}$ *en une lettre de rang j par la formule :* $\boldsymbol{j} = (\boldsymbol{a}\boldsymbol{i} + \boldsymbol{b})[\mathbf{26}]$

Nous avons surtout besoin de décoder le message c'est-à-dire d'exprimer $\boldsymbol{i}$ en fonction de $\boldsymbol{j}$:

$$\boldsymbol{j} = (\boldsymbol{a}\boldsymbol{i} + \boldsymbol{b})[\mathbf{26}] \Longrightarrow \boldsymbol{i} = \boldsymbol{a}^{-\mathbf{1}}(\boldsymbol{j} - \boldsymbol{b})[\mathbf{26}] = (\boldsymbol{a}^{-\mathbf{1}}\boldsymbol{j} - \boldsymbol{a}^{-\mathbf{1}}\boldsymbol{b})[\mathbf{26}]$$

$$\boldsymbol{i} = (\boldsymbol{\alpha}\boldsymbol{j} + \boldsymbol{\beta})[\mathbf{26}] \quad \text{avec} \quad (\boldsymbol{\alpha}, \boldsymbol{\beta}) = (\mathbf{a}^{-\mathbf{1}}, -\mathbf{a}^{-\mathbf{1}}\mathbf{b})$$