Cryptographie

F. Simonneau

IUT Nantes

le plan du cours

1. Arithmétique
2. Cryptosystèmes

Définition 1.1 (Divisibilité)

Soit $a, b \in \mathbb{Z}$. On dit que b **divise** *a et on note $b|a$ s'il existe $q \in \mathbb{Z}$ tel que :*

$$a = bq$$

On dit également que a est un multiple de b.

Exemples

- $7|21, -6|24$
- Pour tout $a \in \mathbb{Z}$ on a $a|0$ et $1|a$
- Pour tout $a \in \mathbb{Z}$ on a $a|a$ (Réflexivité)
- Si $a|b$ et $b|a$ alors $b = \pm a$ (pas antisymétrique dans $\mathbb{Z}$ mais antisymétrique dans $\mathbb{N}^*$)
- Si $a|b$ et $b|c$ alors $a|c$ (transitivité)

Théorème de la division euclidienne dans $\mathbb{Z}$

Soit $a \in \mathbb{Z}, b \in \mathbb{Z}^*$. Il existe un unique couple $(q, r) \in \mathbb{Z} \times \mathbb{N}$ tel que :

$$a = bq + r \text{ et } 0 \leq r < |b|$$

Les entiers q et r sont appelés, respectivement, le quotient et le reste de la division euclidienne de a par b.

Cas particulier de la division euclidienne dans $\mathbb{N}$

Soit $a \in \mathbb{N}$, $b \in \mathbb{N}^*$. Il existe un unique couple $(q, r) \in \mathbb{N}^2$ tel que :

$$a = bq + r,\ 0 \leq r < b$$

On va apporter la preuve de cette deuxième version. La preuve de la première s'obtenant ensuite en considérant des disjonctions de cas notamment suivant le signe de b.

PREUVE DE L'EXISTENCE : Soit $E = \{n \in \mathbb{N} | bn \leq a\}$. C'est un ensemble non vide car $n = 0 \in E$. De plus pour $n \in E$ comme on a $b \geq 1$, on en déduit que $n \leq nb \leq a$. Il y a donc un nombre fini d'éléments dans E. Notons $q = max(E)$ le plus grand élément.
Alors $qb \leq a$ car $q \in E$, et $(q+1)b > a$ car $q + 1 \notin E$, donc :

$$qb \leq a < (q+1)b = qb + b$$

On définit alors $r = a - bq$ qui vérifie bien : $0 \leq r = a - bq < b$. PREUVE DE L'UNICITÉ :
Supposons que (q, r) et (q', r') soient deux couples d'entiers qui vérifient les conditions du théorème et montrons que ces couples sont alors nécessairement égaux.
Tout d'abord $a = bq + r = bq' + r'$ et donc $b(q - q') = r' - r$. D'autre part $0 \leq r' < b$ et $0 \leq r < b$ (ou encore $-b < -r \leq 0$) et on en déduit que $-b < r' - r < b$ soit $-b < b(q - q') < b$. On peut diviser par b (car $b > 0$) et on obtient $-1 < q - q' < 1$. Comme $q - q'$ est entier, la seule possibilité est que $q - q' = 0$ soit $q = q'$. En exploitant encore la relation $b(q - q') = r' - r$, on obtient finalement $r = r'$.

Définition 1.2 (PGCD, PPCM)

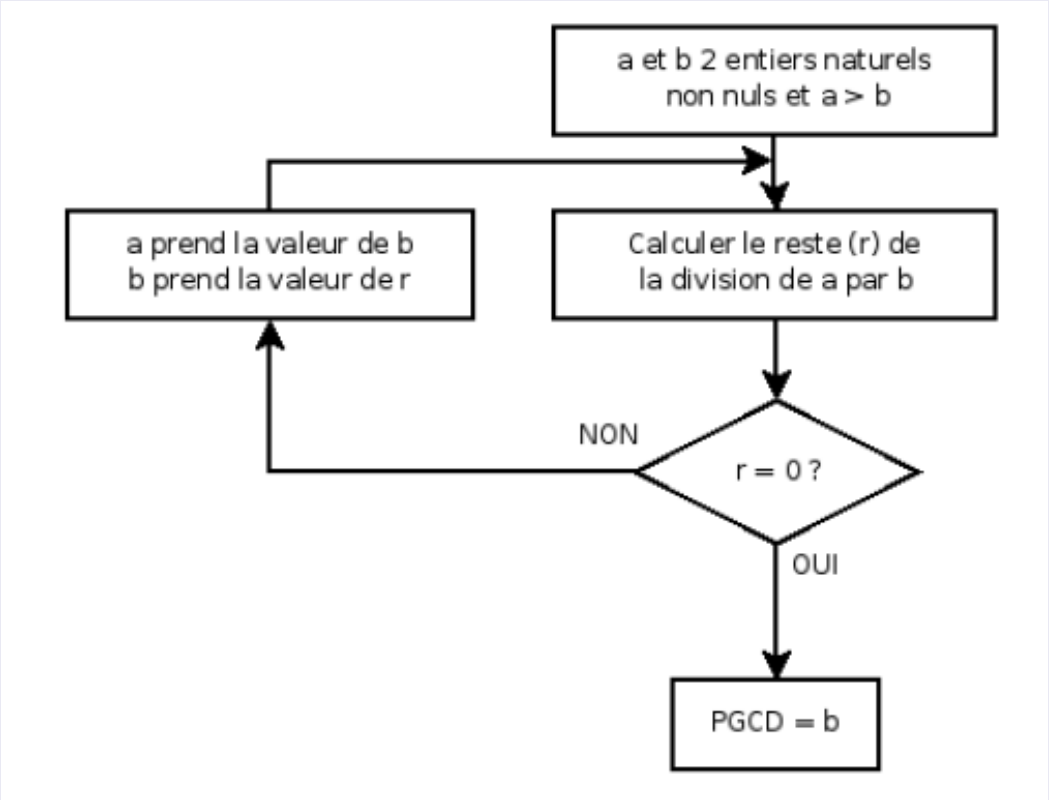
Le plus grand commun diviseur de deux entiers a et b non nuls est le plus grand entier qui les divise simultanément. On le note $PGCD(a, b)$ ou $a \wedge b$.
Le plus petit commun multiple de deux entiers a et b est le plus petit entier naturel qui soit multiple de ces deux nombres. On le note $PPCM(a, b)$ ou $a \vee b$.

Exemples

- $PGCD(90, 12) = 6$ et $PPCM(90, 12) = 180$
- Si $b|a$, alors $PGCD(a, b) = |b|$

Algorithme d'Euclide dans $\mathbb{N}$

Pour deux entiers naturels a et b non nuls avec $a > b$, en écrivant la division euclidienne de a par b : $a = bq + r$, on obtient aisément que $a \wedge b = b \wedge r$. En exploitant ceci on obtient par l'algorithme, décrit schématiquement ci-dessous, le PGCD de a et b :



Identité de Bézout dans $\mathbb{N}$

Soient a, b deux entiers naturels non nuls. Soit d le PGCD de a et b. Alors il existe au moins un couple d'entiers relatifs (u, v) tel que $au + bv = d$. (on dit que u et v sont des coefficients de Bézout)

On obtient u et v avec l'algo d'Euclide étendu (ex pour $a = 210,\ b = 55$) :

$$210 = 55 \times 3 + 45 \rightarrow 210 + 55 \times (-3) = 45$$

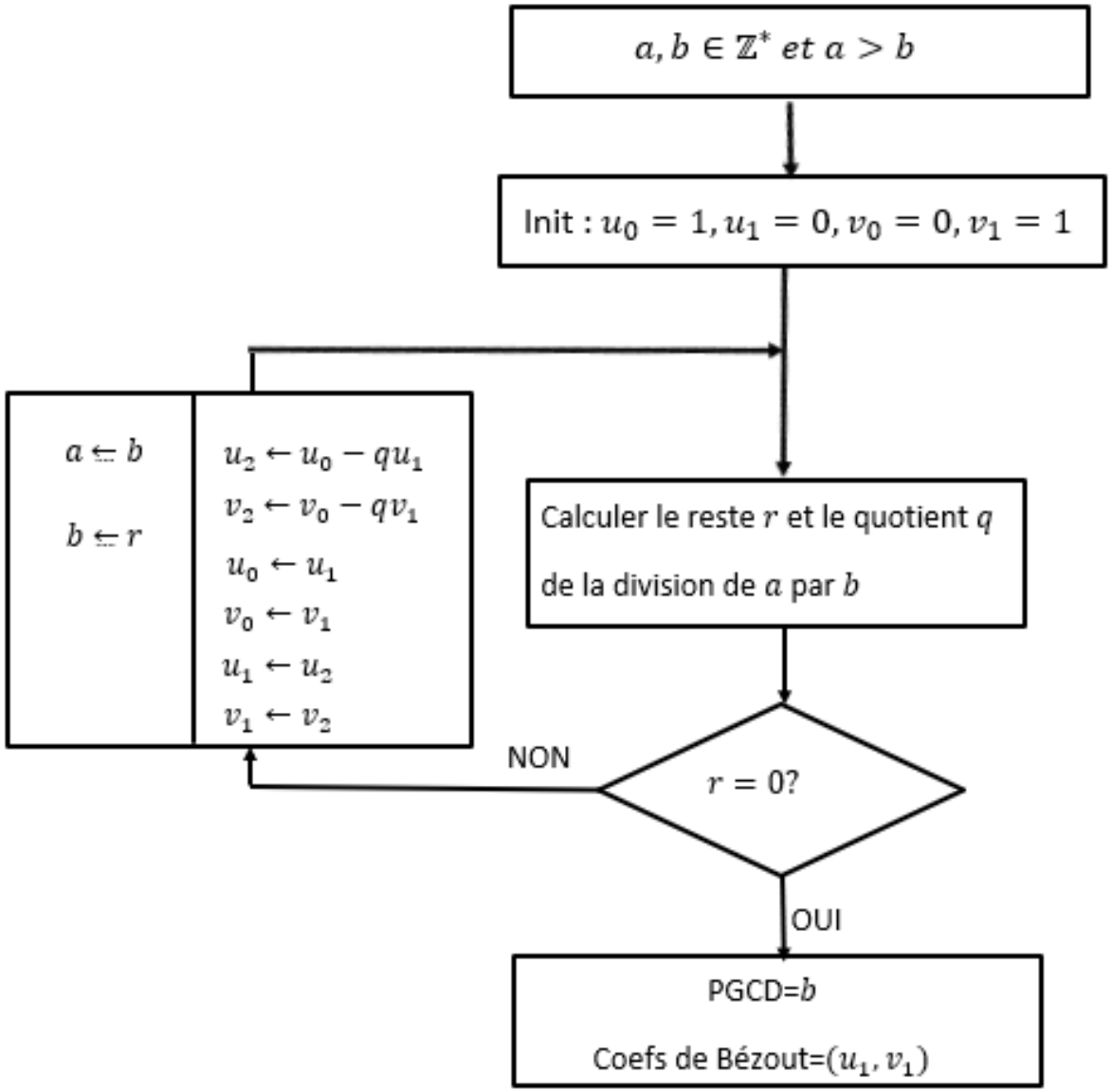
$$55 = 45 \times 1 + 10 \rightarrow \begin{cases} 55 + 45 \times (-1) = 10 \\ 55 + (210 + 55 \times (-3)) \times (-1) = 10 \\ 210 \times (-1) + 55 \times 4 = 10 \end{cases}$$

$$45 = 10 \times 4 + 5 \rightarrow \begin{cases} 45 + 10 \times (-4) = 5 \\ 210 + 55 \times (-3) + (210 \times (-1) + 55 \times 4) \times (-4) = 5 \\ 210 \times 5 + 55 \times (-19) = 5 \end{cases}$$

$$10 = 5 \times 2 + 0$$

On obtient donc 5 comme PGCD de 210 et 55(grâce à l'algo d'Euclide sur la partie gauche) et on obtient les coefficients de Bézout $u = 5$ et $v = -19$ sur la partie droite.

On remarque que pour exprimer un reste comme combinaisons linéaires de a et b il nous faut faire appel aux expressions des deux précédents restes.



Théorème de Bézout

Soient $a, b \in \mathbb{N}$. Les assertions suivantes sont équivalentes :

- a et b sont premiers entre eux.
- Il existe $u, v \in \mathbb{Z}$ tels que : $au + bv = 1$

Un corollaire : Théorème de Gauss

Soient $a, b, c \in \mathbb{Z}$
Si $a|bc$ et $a \wedge b = 1$ alors $a|c$.

Définition 1.3

Soit $n \in \mathbb{N}^*, (a,b) \in \mathbb{Z}^2$; on dit que a est **congru** *à b* **modulo** *n, et on note $a \equiv b[n]$ si et seulement si n divise $b-a$.*

Propriété

Pour tout $n \in \mathbb{N}^*$, la relation $\equiv [n]$ est une relation d'équivalence dans $\mathbb{Z}$.

Notation

Pour tout $n \in \mathbb{N}^*$, on note $\mathbb{Z}_{/n\mathbb{Z}}$ l'ensemble des classes d'équivalence au lieu de $\mathbb{Z}_{\equiv[n]}$

Pour tout $x \in \mathbb{Z}$, on note $\overline{x}$ la classe de x dans $\mathbb{Z}_{/n\mathbb{Z}}$:
$\overline{x} = \{y \in \mathbb{Z} | x \equiv y[n]\} = \{x + \lambda n | \lambda \in \mathbb{Z}\}$

Propriété

Soit $n \in \mathbb{N}^*$. On a, pour tout $(a, b, c, d) \in \mathbb{Z}^4$:

$$\left.\begin{array}{l} a \equiv b[n] \\ c \equiv d[n] \end{array}\right\} \Rightarrow a + c \equiv b + d[n]$$

et :

$$\left.\begin{array}{l} a \equiv b[n] \\ c \equiv d[n] \end{array}\right\} \Rightarrow a \times c \equiv b \times d[n]$$

En particulier si $a \equiv b[n]$, alors $a^k \equiv b^k[n]$ pour tout $k \in \mathbb{N}$.

Exemples d'exploitation

- La preuve par neuf
  Principe : chaque nombre en écriture décimale étant congru modulo 9 à la somme des chiffres le composant, on peut montrer que le résultat d'un calcul est faux si les règles de compatitibilité modulo 9 ne sont pas respectées. L'assertion suivante $137 \times 55 + 58^3 = 202647$ est peut-être vraie car :
  - $137 \times 55 + 58^3 \equiv 11 \times 10 + 13^3[9] \equiv 2 \times 1 + 1[9] \equiv 3[9]$
  - $202647 \equiv 21[9] \equiv 3[9]$
- L'arithmétique de l'horloge
  Principe : Une horloge avec aiguilles s'est arrêtée 50 heures plus tôt. Pour évaluer le déplacement à effectuer sur la petite aiguille on évalue 50 modulo 12.
- Montrer que $2^{345} + 5^{432}$ est divisible par 3.
  Démonstration : $2^{345} + 5^{432} \equiv (-1)^{345} + (-1)^{432} \equiv -1 + 1 \equiv 0[3]$.

Définition 1.4 (Elément générateur)

Un élément $\overline{x}$ est dit générateur de $\mathbb{Z}_{/n\mathbb{Z}}$ (ou engendre $\mathbb{Z}_{/n\mathbb{Z}}$) si pour toute classe c de $\mathbb{Z}_{/n\mathbb{Z}}$, il existe $k \in \mathbb{N}$ tel que $c = k\overline{x}$.

Propriété

Soit $x \in \mathbb{N}$ tel que $0 \leq x \leq n-1$. Les affirmations suivantes sont équivalentes :

- $\overline{x}$ engendre $\mathbb{Z}_{/n\mathbb{Z}}$
- x et n sont premiers entre eux $(x \wedge n = 1)$.
- Il existe k tel que $k\overline{x} = \overline{1}$ ($\overline{x}$ est inversible)

Petit théorème de Fermat

Soit p un nombre premier et $a \in \mathbb{Z}$. Alors $a^p \equiv a[p]$
Et si a est premier avec p (i.e. tel que $a \wedge p = 1$), alors $a^{p-1} \equiv 1[p]$

Dém : Si a est multiple de p alors a^p aussi (nullité modulo p), donc $a^p \equiv a[p]$. Supposons à présent a non multiple de p. On considère :

$$f : \left| \begin{array}{ccc} [\![1; p-1]\!] & \to & [\![1; p-1]\!] \\ n & \mapsto & na[p] \end{array} \right.$$

Deux nombres différents modulo p ont nécessairement leurs images par f différentes (raisonnement par l'absurde en s'appuyant sur l'existence d'un inverse pour a). L'ensemble des $p-1$ images $a[p]; 2a[p]; \ldots; (p-1)a[p]$ coïncide donc avec les $p-1$ valeurs de l'ensemble d'arrivée $1; 2; \ldots; p-1$ (pas dans le même ordre). On a donc en faisant les produits modulo p :

$$1 \times 2 \times \cdots \times (p-1) \equiv a \times 2a \times \cdots \times (p-1)a[p]$$

Chaque élément de $[\![1; p-1]\!]$, étant premier avec p, possède un inverse modulo p et en multipliant successivement par ces inverses on obtient :

$$1 \equiv a^{p-1}[p]$$

Définition 1.5 (Fonction d'Euler)

La fonction indicatrice d'Euler associe à tout entier naturel n non nul le cardinal, noté $\varphi(n)$, de l'ensemble des nombres naturels inférieurs à n et premiers avec n.

Théorème d'Euler (Généralisation du petit théorème de Fermat)

Soient $a \in \mathbb{Z}$ et $n \in \mathbb{N}^*$ Si $pgcd(a, n) = 1$ alors $a^{\varphi(n)} \equiv 1[n]$

Système de cryptographie de César

Jules utilisait le système suivant pour communiquer secrètement : chaque lettre de l'alphabet était décalée de 3 unités via la permutation :

$$\begin{array}{r} \text{caractère initial :} \\ \text{caractère chiffré :} \end{array} \quad \begin{pmatrix} a & b & \dots & y & z \\ d & e & \dots & b & c \end{pmatrix}$$

Ajoutons à l'alphabet quelques caractères de ponctuation : espace, virgule, point, ' ?' et ' :' pour disposer d'un alphabet de 31 caractères (la primalité de 31 soit premier va permettre l'existence d'inverse). Ainsi on a la nouvelle permutation :

$$\begin{array}{r} \text{caractère initial :} \\ \text{caractère chiffré :} \end{array} \quad \begin{pmatrix} a & b & \dots & y & z & \text{Espace} & , & . & ? & : \\ d & e & \dots & , & . & ? & : & a & b & c \end{pmatrix}$$

Chaque caractère est donc chiffré avec la relation :

$$position(\text{caractère chiffré}) = position(\text{caractère initial}) + 3[31]$$

On peut inversement déchiffrer un caractère avec la relation :

$$position(\text{caractère initial}) = position(\text{caractère chiffré}) - 3[31]$$

Chiffrement affine

On peut modifier le chiffrement en utilisant une bijection (Pourquoi ?) de $\mathbb{Z}_{/31\mathbb{Z}}$ aisément inversible (Pourquoi ?) comme une fonction affine, par exemple :

$$position(\text{caractère chiffré}) = 15 \times position(\text{caractère initial}) + 13[31]$$

En utilisant cette fonction on obtient par exemple les chiffrements suivants :

$$\begin{array}{lcccl} a & : 1 & \rightarrow & 15 \times 1 + 13 = 28[31] & \rightarrow & ',' \\ b & : 2 & \rightarrow & 15 \times 2 + 13 = 13[31] & \rightarrow & m \end{array}$$

Pour déchiffrer un message on utilisera la fonction inverse de la précédente (en ayant identifié que l'inverse de 15 dans $\mathbb{Z}_{/31\mathbb{Z}}$ est 29) :

$$position(\text{caractère initial}) = 29 \times (position(\text{caractère chiffré}) - 13)[31]$$

Chiffrement de Hill

Le principe est ici de chiffrer un message avec des blocs de n caractères représentés sous forme de matrices colonne A dans $\mathbb{Z}_{/p\mathbb{Z}}$. Pour ce chiffrement on utilise une matrice A de taille $n \times n$ inversible dans $\mathbb{Z}_{/p\mathbb{Z}}$. Si on souhaite envoyer le message "LOVE" on envoie deux vecteurs et on désigne le premier codant "LO" par le vecteur A et le message chiffré reçu est alors le vecteur $C = M.A$:

$$C = \begin{bmatrix} C_1 \\ C_2 \end{bmatrix} = \begin{pmatrix} 3 & 2 \\ 1 & 3 \end{pmatrix} \times \begin{bmatrix} 12 \\ 15 \end{bmatrix} = \begin{bmatrix} 4 \\ 26 \end{bmatrix} (mod\ 31)$$

On obtient "DZ" pour le chiffrement de ces deux premières lettres et en chiffrant "VE" on obtient "NF" Un résultat d'algèbre linéaire est le suivant : $M.{}^t com(M) = ({}^t com(M)).M = (detM)I_n$ Le déchiffrement reposant sur l'existence d'une matrice inverse pour M, ceci est assuré dès lors que $det(M)$ est inversible dans $\mathbb{Z}_{/p\mathbb{Z}}$. Ici $p = 31$ étant premier cela revient à ce que $det(M) \neq 0$ or on a $det(M) = 7$ dont l'inverse dans $\mathbb{Z}_{/31\mathbb{Z}}$ est 9. On peut alors exprimer l'inverse de M

$$M^{-1} = 9 \begin{pmatrix} 3 & -2 \\ -1 & 3 \end{pmatrix} \equiv \begin{pmatrix} 27 & -18 \\ -9 & 27 \end{pmatrix} \equiv \begin{pmatrix} 27 & 13 \\ 22 & 27 \end{pmatrix} (mod\ 31)$$

Pour déchiffrer les deux premiers caractères « DZ », on utilise :

$$M^{-1}C = \begin{pmatrix} 27 & 13 \\ 22 & 27 \end{pmatrix} \cdot \begin{bmatrix} 4 \\ 26 \end{bmatrix} \equiv \begin{bmatrix} 446 \\ 790 \end{bmatrix} \equiv \begin{bmatrix} 12 \\ 15 \end{bmatrix} (mod\ 31)$$

On retrouve donc bien les deux premiers caractères « LO ».

Système cryptographique de Vigenère

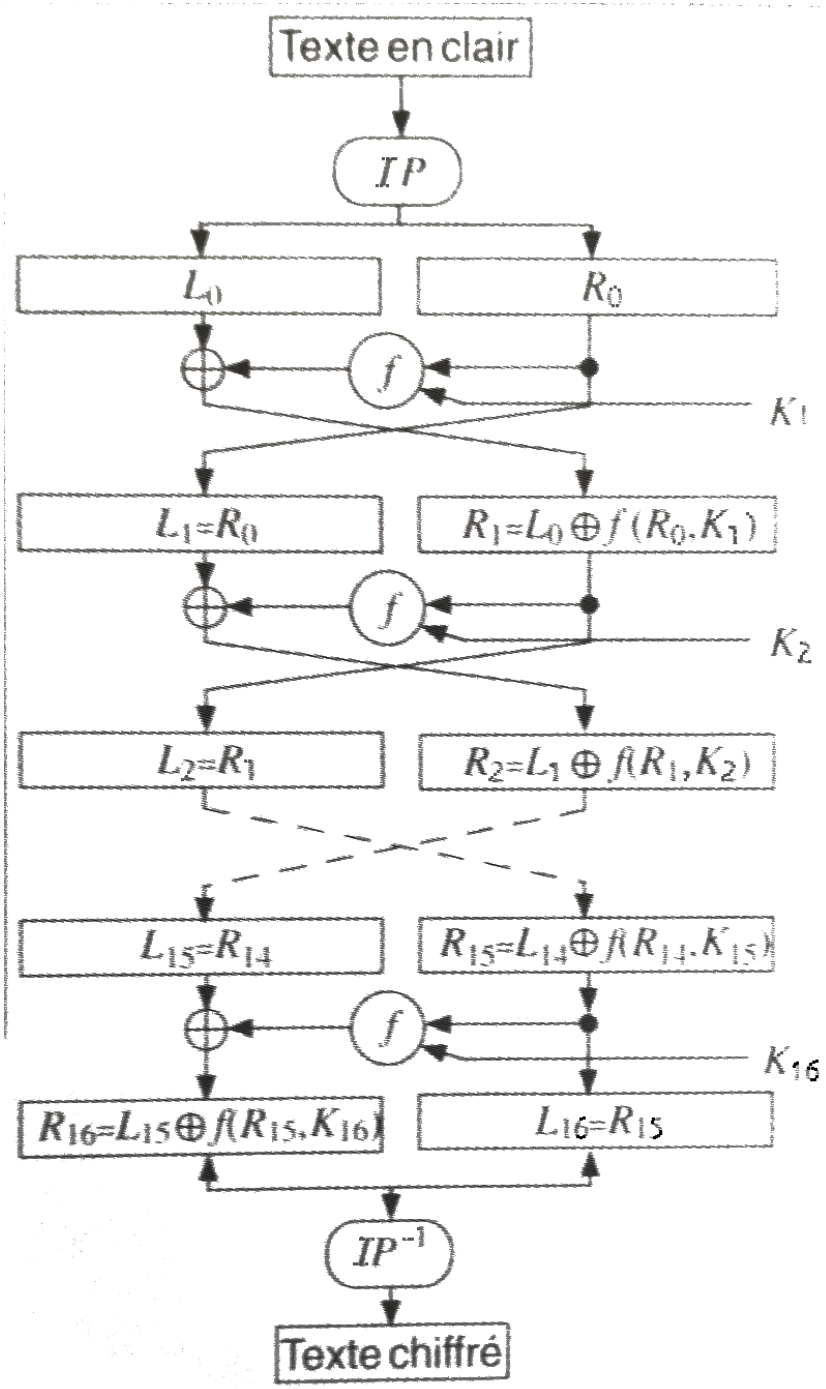
La clé utilisée consiste en une série de d lettres écrites de manière cyclique sous le texte. On additionne caractère par caractère les positions associées (modulo 31 toujours ici) :

$$\begin{array}{c} \text{Message initial :} \\ + \text{ Clé K :} \\ =\text{Message chiffré :} \end{array} \left(\begin{array}{cccccccccccc} j & o & h & n & & i & s & & g & o & o & d \\ a & b & c & a & b & c & a & b & c & a & b & c \\ k & q & k & o & . & l & t & . & j & p & q & g \end{array} \right)$$

Le système de chiffrement DES, aujourd'hui désuet, est un algorithme de chiffrement par bloc.
Le message d'origine est découpé en blocs de 64 bits et chaque message M ainsi obtenu est lui-même partagé en deux : $M = (L_0, R_0)$.
La clé K est un nombre binaire sur 64 bits mais seuls 56 interviennent dans le chiffrement (pour chaque octet le dernier bit est réservé au contrôle de la clé en calculant la parité de la somme des bits), par exemple :

$$\begin{array}{ccccccc|c} 0 & 1 & 0 & 1 & 1 & 1 & 1 & \dots \\ 0 & 1 & 0 & 1 & 1 & 0 & 1 & \dots \\ 0 & 1 & 0 & 1 & 0 & 0 & 1 & \dots \\ 0 & 1 & 1 & 1 & 1 & 1 & 1 & \dots \\ 0 & 1 & 0 & 1 & 0 & 0 & 0 & \dots \\ 0 & 0 & 0 & 1 & 1 & 0 & 1 & \dots \\ 1 & 0 & 1 & 1 & 1 & 1 & 0 & \dots \\ 1 & 0 & 0 & 1 & 0 & 0 & 0 & \dots \end{array} \Longrightarrow \begin{array}{ccccccc|c} 0 & 1 & 0 & 1 & 1 & 1 & 1 & 1 \\ 0 & 1 & 0 & 1 & 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 & 0 & 0 & 1 & 1 \\ 0 & 1 & 1 & 1 & 1 & 1 & 1 & 0 \\ 0 & 1 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 1 & 0 & 1 & 1 \\ 1 & 0 & 1 & 1 & 1 & 1 & 0 & 1 \\ 1 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \end{array}$$

Une fonction f permet de "brouiller les cartes" en appliquant des manipulations d'expansion, permutations et substitutions sur les blocs.



Le message subit un certain nombre de rondes :

Après chaque ronde la partie droite est placée à gauche, tandis que la partie gauche est additionnée (mod 2) au résultat de la fonction f appliqué à la partie droite et à la clé utilisée sur cette ronde (ces clés K_d étant obtenues par diverses manipulations de permutations et compressions sur des blocs (G, D) définis à partir de K).

On remarque par ailleurs une permutation initiale IP avant les 16 rondes et son inverse IP^{-1} après les 16 rondes.