Cryptographie

Notes du 06/05/2014

L’examen aura lieu le 30 Juin Elles seront d’une durée de 2h.

2 grandes parties : -histoire de la cryptographie de l’antiquité à nos jours.

* Arithmétique modulaire (entre autre)

**I Terminologie :**

Double jeu, il faut savoir coder /décoder avec une clé. Mais aussi savoir décrypter, c’est-à-dire trouver le message quand on n’a pas la clé.

Quand on déchiffre on a la clé.

Quand on décrypte, on n’a **pas** la clé.

**Sténographie :** Cacher un message dans un tableau, une partition de musique,…

**CRYPTOLOGIE** : la science des documents secrets. Elle recouvre tous les aspects scientifiques, et plus particulièrement mathématiques, relatifs à la cryptologie et à la cryptanalyse

**CRYPTANALYSE** : l’art et la science de décrypter les messages secrets

**CHIFFREMENT** : le processus de transformation d’un message de telle manière à le rendre incompréhensible pour toute personne non autorisée

**CRYPTOGRAMME** : le résultat du processus de chiffrement

**DÉCHIFFREMENT** : le processus de reconstruction du texte clair à partir du texte chiffré, par des personnes autorisées

**DÉCRYPTEMENT** : le processus de reconstruction du texte clair à partir du texte chiffré, par des personnes non autorisées (sans connaître la clef)

**CLEF DE CHIFFREMENT** : un mot, un nombre ou une phrase qui est utilisé par un algorithme de cryptologie pour chiffrer ou déchiffrer un message

**II Chronologie :**

**Polybe :** Carré de Polybe

**César :** « père » de la cryptographie.

**Al Kindy :** Mathématicien arabe, reconnu comme le plus grand mathématicien de l’an 1000.

**Vigenère :** système quasi incassable jusqu’en 1800.

**III Différentes Stratégies :**

**Cacher :** cacher de manière anonyme, Stéganographie

**Coder :** Fabriquer un code, on ne cherche pas à rendre illisible mais seul le destinataire peut comprendre le message.

**Crypter :** Faire en sorte que le message soit lisible uniquement au destinataire. Le message sera incompréhensible pour toute autre personne.

1°) Cacher : noyer le message dans un autre

**Exemple :** technologie MicroDotDNA, il s’agit de la stéganopraphie dans L’AN. Dans le mais MONSANTO, il est écris Monsanto à l’aide d’un code.

En codants sur 4 caractères, on a 44 = 64 caractères.

🡺 On fabrique des lettres par combinaison d’autres lettres.

**Autre exemple :** Rabelais dénonce toute la cryptographie de l’époque dans le chapitre 24 de Pantagruel, à l’aide d’une encre sympathique.

**La grille de cardan :** Permet de cacher un message dans une lettre. Un cache permet d’afficher uniquement le vrai message.

**Bacon :** Il va utiliser différents types de typographie (*Italique*, …) mais sur 5 caractères c’est trop long. 🡺 Utilisation du chiffre trilitère (Trifide) sur 3 caractères soit 3\*3\*3 = 27 caractères.

**Les sonagrammes :** On cache dans une partition de musique : écart entre les notes + type de note.

**Théorème de Borel :** Le théorème de Borel dit qu'en prenant un grand nombre de combinaisons de lettres, on trouve des mots connus et même des rapprochements de mots. Sur un texte de 1 000 lettres, vous pouvez ainsi extraire plusieurs millions de mots par cette méthode des "equidistant letter sequence"

**Brendan McKay** : il prend le texte de la Bible (en hébreux), et il enlève tous les espaces et signes de ponctuation. Puis il envisage, grâce à un ordinateur, les combinaisons de lettres qu'on peut extraire en partant d'une lettre, puis en sautant 20 lettres plus loin, puis 20 lettres plus loin, etc.

2°) CODER

Quand on casse un code, la première chose à faire est de continuer à faire croire que l’on ne le connaît pas.

**Code ma mary stuart** : Le chiffre utilisé n'était pas simplement une substitution, mais plutôt un nomenclateur, comme le montre la figure ci-dessous. Il était constitué de 23 symboles qui remplaçaient les lettres de l'alphabet (sauf j, v et w), ainsi que de 36 symboles représentant des mots ou des phrases. Il y avait en outre quatre nulles et un symbole qui signifiait que la lettre suivante était une lettre doublée.

**Code de popham** : code maritime, Dix fanions de couleurs différentes y correspondent chacun à un chiffre de 0 à 9. Trois séries de dix, soit trente fanions, représentant les unités, les dizaines et les centaines, permettent ainsi de représenter les nombres de 0 à 999.

**Le code morse** : est un code télégraphique utilisant un alphabet conventionnel fait de traits et de points, et, quant au son, de longues et de brèves. Abandonné ensuite au profit d’un système satellitaire

**Code ASCCI**: La mémoire de l'ordinateur conserve toutes les données sous forme numérique. On ne peut pas stocker directement les caractères. Chaque caractère possède donc son équivalent en code numérique. Il ne contient donc pas de caractères accentués, ni de caractères spécifiques à une langue.

**Code des NAVAJO** : langage amérindien, utilisé pendant la seconde guerre mondiale. Voir le film « Les messagers du vent ». Le dialecte navajo est incompréhensible pour toutes les autres tribus et autres peuples. Il équivaut donc à un code secret en face de l'ennemi. Un défaut majeur : cette langue n'offre pas d'équivalent au langage militaire moderne

3°) Crypter :

APPROCHE 1

**Chiffre de transition :** est très sûr mais il faut expliquer comment on a fait à l’expéditeur et l’envoyeur

**La scytale spartiate** (Voir DA VINCI CODE)

Dans un chiffre de transposition, il y a toujours le même nombre de lettre.

**Le chiffre rail fence** : palissade et on peut le chiffre à 3 niveaux

**Grille tournante :** grille 6\*6 avec un cache de 9 tous. Il faut toujours 36 lettre, le sens est très important en crypto.

Avec 36 lettres, il y a !36 solutions possibles. Pour autant la sécurité est très faible car il suffit d’avoir le cache.

**Transposition rectangulaire :** on utilise un mot clé, pour on met les lettres dans l’ordre alphabétique. La sécurité est basée sur le mot clé, mais se casse très facilement.

**Double transposition :** on brasse sur des lignes et des colonnes de 7. 49 caractère soit : !7\* !7 = 5000 \* 5000 = 25 000 000 possibilités.

APPROCHE 2 : Substitution :

Un chiffre de substitution consiste à remplacer les lettres ou les mots par d'autres symboles. Cela présuppose de choisir un ensemble de symboles qui joueront le rôle de substituts.

**Mono alphabétique :** on remplace une lettre une autre du même alphabet. On utilise un mot de passe qui change tous les jours.

Pour casser un chiffre de substitution, on utilise la technique des fréquences d’apparition, puis on compare et enfin on casse.

**Le carre de Polybe** : Polybe est à l'origine du premier procédé de chiffrement par substitution. C'est un système de transmission basé sur un carré de 25 cases (on peut agrandir ce carré à 36 cases, afin de pouvoir ajouter les chiffres). Chaque lettre peut être ainsi représentée par un groupe de deux chiffres: celui de sa ligne et celui de sa colonne. Ainsi "e"=15, "q"=42... cout contre un mur, tuyauterie…

On peut compliquer ce système de chiffrement avec un mot de passe. Par exemple, si le mot de passe est DIFFICILE, on commencera à remplir le carré avec les lettres de ce mot, après avoir supprimé les lettres identiques, puis on complètera le tableau avec les lettres inutilisées.

**ALPHABETS DESORDONNES** : classique de chiffrer des messages consiste à remplacer une lettre par une autre, en utilisant un alphabet désordonné.

Un inconvénient est qu'il est difficile, à moins d'avoir une mémoire remarquable, de se souvenir de la grille de chiffrement. Pour pouvoir la reconstituer rapidement, on peut utiliser comme moyen mnémotechnique un mot-clef.

**Le Chiffre de Cesar :** on parle aussi d'alphabet décalé, est un cas particulier d'alphabet désordonné. Il consiste simplement à décaler les lettres de l'alphabet de quelques crans vers la droite ou la gauche. Par exemple, décalons les lettres de 3 rangs vers la gauche, comme le faisait Jules César (d'où le nom de ce chiffre.

Inconvenient : faiblesse du chiffre de César réside dans le fait qu'il y a trop peu de clefs possibles : comme il y a 26 lettres dans l'alphabet, il n'y a que 25 décalages intéressants (un décalage de 26 redonne le message initial). Il suffit donc d'essayer tous les décalages pour trouver le bon.

**Les chiffres Hebreux :** Les hébreux utilisaient trois chiffres. Un chiffre consiste à inverser l’ordre des lettres de l’alphabet, un autre decale les lettre de l’alphabet de 13 positions et le 3eme chiffre dit que ces chiffres sont réversible (= qu'un message chiffré deux fois avec le même chiffre redonnera le message en clair.

**PiG Pen & Templiers** : la croix des templiers pour rédiger un message.

Nous pouvions décrypter un chiffre monoalphabétique par une analyse des fréquences. Une autre technique consiste à deviner un mot qui doit, ou peut, apparaître dans le texte clair. C'est l’attaque par mot probable

**Substitution Homophonique :** Pour échapper à l'analyse de fréquences, une solution consiste à remplacer une lettre non pas par un symbole unique, mais par un symbole choisi au hasard parmi plusieurs. Dans sa version la plus sophistiquée, on choisira un nombre des symboles proportionnel à la fréquence d'apparition de la lettre ; on parle alors de renversement des fréquences.

**Duc de montmorency** : utilisation de symboles en lieu et place des lettres. Pour complexifier le code, les lettres qui apparaissent le plus sont représentées par plusieurs symboles. Le code est « lissé ». Cette technique permet de casser l’analyse des fréquences.

Disque : le disque extérieur tourne, et les lettres s’alignent. Chaque lettre a entre 3 et 4 combinaisons. Mais il est possible d’obtenir facilement la combinaison un fois que l’on a obtenu le disque.

Une autre solution, on passe sur des structures polyalphabétiques 🡺 à chaque fois que l’on code une nouvelle lettre, on change d’alphabet. C’est la base du code de Porta et de Vigenère.

**Polyalphabétique**

Bigramme : fréquence d’apparition de la succession de 2 lettres.

**Chiffre de Porta :** Il faut donc construire des alphabets différents pour que cela fonctionne.

Porta a fabriqué des jeux d’alphabet (13) différents et réversibles.

On travaille avec un mot clé que l’on répète le nombre de fois nécessaire.

**Chiffre de VIGENERE : il a tenu 350 ans,** Dans une table, l'alphabet est répété sur 26 lignes, avec un décalage à gauche d’une lettre pour chaque nouvelle rangée. Faiblesse : les répétitions

3 variante a vigenere :

* Le chiffre de BEAUFORT : Au lieu d'additionner la clef au message clair, Beaufort soustrait le message clair de la clef.
* Le chiffre GRONSFELD : Il améliore le chiffre de César en utilisant un décalage variable donné sous forme d'une clef numérique.
* Le masque jetable : connu comme étant indécryptable. C'est en fait un chiffre de Vigenère avec comme caractéristique que la clef de chiffrement a la même longueur que le message clair.

**Méthode de Bazerie** : permet de casser le code de Vigenère. Le principe est de repérer les successions de lettres qui apparaissent.

**Methode de Babbage** : Babbage comprit que des répétitions de cette sorte lui offraient la prise dont il avait besoin pour attaquer Vigenère. Il va d'abord chercher des séquences de lettres qui apparaissent plus d'une fois dans le texte

**Friedmann** : fabrication d’un indice de coïncidence (= la probabilité que deux lettres choisies aléatoirement dans un texte soient identiques) L’indice de coïncidence dépend de la langue.

Un indice toujours faible indique l’utilisation de la polyalphabetique 🡺 pas d’analyse de la fréquence possible.

**Machine ENIGMA**

Allan Turing était le responsable du centre d’analyse et de cryptanalyse Anglais. La machine enigma sert à chiffrer et déchiffrer. Elle automatise le chiffrement par substitution.

Faille de la machine enigma 🡺 il fallait répéter 2 fois le code pour s’assurer qu’il n’y avait pas d’erreur ce qui est un faille. Cela a permis aux cryptanalystes anglais d’anticiper la position des rotors.

Mécanisme : Quand on presse sur une touche, deux choses se passent. Premièrement, une lettre s'allume sur un panneau lumineux : c'est la lettre chiffrée.

Deuxièmement, un mécanisme fait tourner le rotor de droite d'un cran, toutes les 26 frappes, le deuxième rotor tourne d'un cran, toutes les 676 frappes, puis c'est le troisième rotor qui tourne d'un cran. Certaines Enigmas avaient 3 rotors, celles de la Kriegsmarine en avaient 4 ou 5. Ces rotors tournants modifient les connexions électriques dans la machine, ce qui fait que la touche "A" allumera peut-être le "G" la première fois, mais le "C" la deuxième, etc.

Un tableau de connexions et un réflecteur complique encore le système. Le côté exceptionnel de cette machine est que même si elle tombe entre les mains ennemies, sa sécurité n'est pas compromise. En effet, c'est le nombre faramineux de réglages de la machine qui fait sa force et les réglages changeaient évidemment chaque jour (ordre de rotors, orientation initiale et branchement du tableau de connexions)

**Les substitutions TOMOGRAMMIQUES**

**Chiffre de collon**

1°) trouver la longueur des séries, test de chaine de 1 bigramme, puis 2, puis 3, jusqu’à trouver la bonne longueur, c’est-à-dire inférieur à la longueur de l’alphabet

2°) décrypter les bigrammes. Il n’y a pas plus de 25 bigrammes (5\*5).

3°) si substitution simple alors on peut utiliser la méthode de l’analyse de fréqeunce afin de décrypter les bigrammes

**Chiffrement delastelle**

Il repère les coordonnées de plusieurs lettres claires, mélange ces coordonnées, puis lit dans la grille les lettres chiffrées correspondant aux nouvelles coordonnées obtenues.

Comment casser :

1/ On choisit d'abord la longueur de séries n.

2/ On regroupe les lettres du message clair n par n (au besoin, on rajoute des nulles pour que la longueur du message soit multiple de n).

3/ Sous chaque lettre, on note les coordonnées des lettres verticalement (p. ex. J=21, E=45)

4/ On lit ensuite horizontalement les coordonnées des lettres chiffrées (24=U, 44=V, 21=J), série par série.

**Chiffrement digraphide**

C'est un chiffre qui utilise un tableau contenant deux alphabets désordonnés. Les lettres du message clair sont chiffrées par bigrammes.

Dans une première étape, ces bigrammes sont transformés en nombres de trois chiffres. Après un mélange simple, ces nombres sont retransformés en lettres et donnent les bigrammes chiffrés.

**LE CHIFFRE ADFGVX**

Un chiffre inspiré du carré de Polybe. Les lettres ADFGVX ont été choisies de façon que leurs correspondances en morse soient très différentes les unes des autres, de façon à éviter les erreurs de transmission par radio (TSF). L'originalité de ce système venait que le texte obtenu après une première substitution était ensuite soumis à une permutation des colonnes du carré.

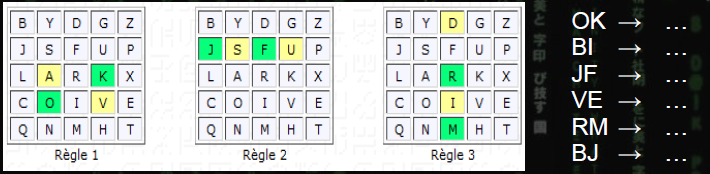
Le chiffre utilisant le carré de 36 symboles (alphabet+chiffre) est connu sous le nom de chiffre ADFGVX.

Message crypté par des coordonnées dans un carré de polybe.

**Les substitutions POLYGRAMMIQUES**

**Le chiffre de Playfair**

On dispose les 25 lettres de l'alphabet (W exclu car inutile, on utilise V à la place) dans une grille 5x5, ce qui donne la clef. Ensuite on chiffre le texte par groupes de deux lettres (des bigrammes) en appliquant des règles



DECHIFFRER A L'AIDE DE LA GRILLE PRECEDENTE : DCOTSCPVOCZIVQMRRIITOTQZ

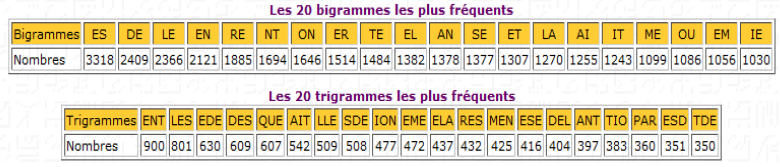
BIEN JOUE CE DECHIFFREMENT B

Déchiffrement :

Si le cryptogramme est assez long, on peut l'attaquer en regardant quels bigrammes apparaissent le plus souvent et en supposant qu'ils représentent les bigrammes les plus courants, il faut ensuite essayer de reconstituer la grille de chiffrement

Bigramme 🡺 analyse de fréquence.

Trigramme 🡺 on peut varier, avec la possibilité d’avoir des trigrammes différents pour une même lettre.

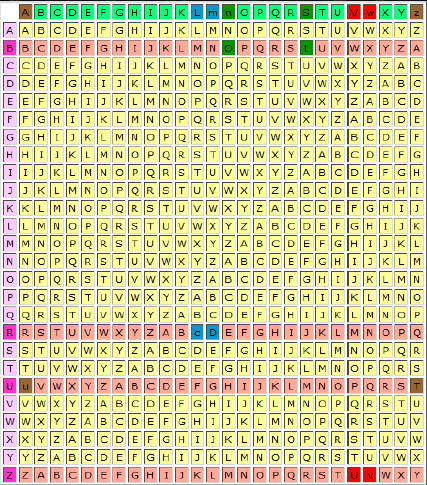


**Le chiffre de Slidefair**

Le chiffre Slidefair utilise le tableau de Vigenère, mais la façon de chiffrer ressemble beaucoup au chiffre Playfair. Il melange le chiffre de Playfair et le chiffre de Vigénère. C'est un chiffre polygrammique, car les lettres sont chiffrées par bigramme.

Avantage de BRUZ : aucune lettre se répète (sinon affaibli le carré de vigenère; petit mot clé donc analyse de fréquence possible ; mot clé qui ne veut rien dire

Vigenère + playfair = slidefair



Exemple : prenons comme mot-clef BRUZ et comme message clair

"SOLDAT VU".

Le bigramme SO devient nt (rectangle vert foncé), LD devient mc

(rectangle bleu), AT devient zu (rectangle brun) et VU devient wv (cas

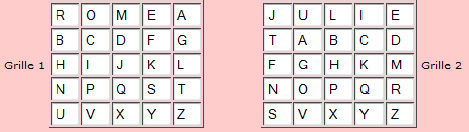
particulier, rectangle rouge).

Le message chiffré sera donc " n t m c z u w v ".

**Différence Playfair et Slidefair**

**POLYGRAMMIQUES A DEUX CARRES**

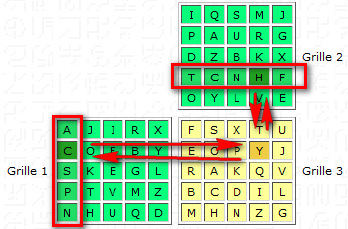
On utilise deux grilles pour chiffrer les bigrammes. Ici, on a fabriqué les deux grilles à l'aide des 2 mots clés : ROMEO / JULIETTE



MESSAGE EN CLAIR : CE CODAGE RESSEMBLE A UN PLAYFAIR

MESSAGE CHIFFRE : DOAPA DDAER NYEKB RUFSN POIZA FMP

**POLYGRAMMIQUES A TROIS CARRES**



Une caractéristique intéressante de ce système de chiffrement est qu'un même message peut être chiffré de très plusieurs façons avec les mêmes mots de passe

On chiffre les lettres du message clair par bigramme. Un bigramme deviendra un trigramme. À titre d'exemple, chiffrons le bigramme C H .

On repère le c dans la grille 1 ; la première lettre du trigramme sera une lettre quelconque choisie dans la même colonne que le c dans la grille 1.

On repère le h dans la grille 2 ; la dernière lettre du trigramme sera une lettre quelconque choisie dans la même ligne de le h dans la grille 2.

La lettre du milieu du trigramme sera la lettre de la grille 3 qui se trouve sur la même ligne que le c et la même colonne que le h.

Ainsi, le bigramme clair ch deviendra par exemple le trigramme chiffré P Y F. Il y a 16 possibilités si l'on exclut la lettre claire, 25 si on permet de la prendre.

**DIFFERENCES SUBSTITUTIONS TOMOGRAMMIQUES et POLYGRAMMIQUES :**

Les substitutions tomogrammiques aussi appelées par fractions de lettres : chaque lettre est tout d'abord représentée par des groupes de deux ou plusieurs symboles, qui sont ensuite chiffrés séparément par substitution ou transposition.

( COLLON, DELASTELLES, DIGRAPHIDE, ADFGVX )

Les substitutions polygrammiques : les lettres ne sont pas chiffrées séparément, mais par groupes de plusieurs lettres (deux ou trois généralement). C'est Giovanni Porta qui présenta le premier chiffre bigrammatique.

( PLAYFAIR, CHIFFREMENTS À DEUX CARRÉS, À TROIS CARRÉS, À QUATRE CARRÉS, HILL, RSA )

**Le chiffre de Affine**

Le chiffre affine est un chiffre de substitution simple. Il est cependant placé ici car on peut le voir comme la version unidimensionnelle du chiffre de Hill.

L'idée est d'utiliser comme fonction de chiffrage une fonction affine du type y = a x + b, où a et b sont des constantes, et où x et y sont des nombres correspondant aux lettres de l'alphabet selon le tableau ci-dessous :



Pour que la lettre chiffrée (y) soit encore un nombre entre 0 et 25, on travaillera modulo 26.

La vraie formule sera donc y = ( a x + b ) mod 26. 🡨 Arithmétique modulaire

On peut remarquer que si a=1, alors on retrouve le chiffre de César et b est le décalage.

On remarquera aussi que si b=0, alors "a" est toujours chiffré "A".

APPRENDRE :

Affine, Hill big

Reste chinois

**Arithmétique Modulaire**



143 est congrus à 15 modulo 16

Supposons par exemple que l'on veuille calculer 11 x 13 dans Z16. Comme entiers ordinaires, on a 11 x 13 = 143. Pour réduire 143 modulo 16, on fait une division euclidienne : 143 = 8 x 16 + 15, donc 143 mod 16 = 15, et, donc, 11 x 13 = 15 dans Z16.

Propriété importante :

L'inverse modulo n de b est le nombre entier b^1 tel que b·b^-1 mod n = 1

On peut le calculer avec l'algorithme d'Euclide étendu. (voir cours d'Arithmétique)

Exemple : l'inverse de 5 modulo 16 est 13 car 5 x 13 = 65 mod 16 = 1 → 5^1 = 13

**Le chiffre de hill**

Chiffre publié en 1929 par Lester S. Hill, c’est un chiffre polygrammique 🡺 c'est-à-dire qu'on ne (dé)chiffre pas les lettres les unes après les autres, mais par paquets

Fonctionnement par paquets.

Matrice 2\*2 🡺 on code par paquets de 2.

Matrice 3\*3 🡺 on code par paquets de 3.

Les lettres sont d'abord remplacées par leur rang dans l'alphabet. Les lettres Pk et Pk+1 du texte clair seront chiffrées Ck et Ck+1 avec la formule ci-dessous :

Ce qui signifie que les deux premières lettres du message clair (P1 et P2) seront chiffrées (C1 et C2) selon les deux équations suivantes :

C1 = a P1 + b P2 (mod 26)

C2 = c P1 + d P2 (mod 26)

Et ainsi de suite

Chiffrement :

On prend une clé pour chiffrer le mot Maths. MATH. Après avoir remplacé les lettres par leur rang (a=1, b=2, etc.), elle obtient :

C1 = 9 . 13 + 4 . 1 (mod 26) = 121 mod 26 = 17 = Q

C2 = 5 . 13 + 7 . 1 (mod 26) = 72 mod 26 = 20 = T

C3= 9 . 20 + 4 . 8 (mod 26) = 212 mod 26 = 4 = D

C4= 5 . 20 + 7 . 8 (mod 26) = 156 mod 26 = 0 = Z

Le message chiffré est donc QTDZ

L’ordre des lettres en partant de 1 à 26 (pour éviter des divisions par 0) :

M = 13

A = 1

T = 20

H = 8

MA =

= = = = QT

DECHIFFREMENT :

Pour déchiffrer, le principe est le même que pour le chiffrement : on prend les lettres deux par deux, puis on les multiplie par la matrice inverse (modulo 26) de la matrice de chiffrement.



La matrice inverse se calcule à l'aide de la formule : -1 =

On a donc : -1 =

= 🡺 43-1 est l’inverse de 43, équivalent à

Comme pgdc (43,26) = 1, (43)-1 existe dans Z26 et (43)-1 égale 23 . En effet, 43 . 23 = 989 modulo 26 = 38 . 26 + 1 = 1 modulo 26

🡺 43 \* m où 1<=m<=26

La matrice de chiffrement : 

PHOTO JR NEGATIVE

Bob prend donc la matrice pour déchiffrer le message "QTDZ". Après avoir remplacé les lettres par leur rang dans l'alphabet (A=1, B=2,etc.), il obtiendra :

P1 = 5 . 17 + 12 . 20 (mod 26) = 325 mod 26 = 13 = M

P2 = 15 . 17 + 25 . 20 (mod 26) = 755 mod 26 = 1 = A

P3 = 5 . 4 + 12 . 0 (mod 26) = 20 mod 26 = 20 = T

P4 = 15 . 4 + 25 . 0 (mod 26) = 60 mod 26 =

8 = H

**IV°) La cryptographie moderne**

**CHIFFREMENT PAR BLOCS**

Feistel

Marqué par l’apparition et l’utilisation de l’informatique à partir des années 1970.

La clé des systèmes modernes réside sur des problèmes mathématiques que l’homme ne sait pas résoudre.

Exemple : Le RSA n’est valide car on ne sait pas factoriser les (très) grands nombre premiers.

Factoriser :

12 = 4\*3 = 2\*2\*3 = 22\*3

26 = 2\*13

39 = 3\*13

43 = 11\*13

1°) Chiffrement par bloc : AES

DES en 1977 pour AES.

Process de DES :

1°) On remplace les caractères par des nombres binaires. Utilisation de fonctions binaires.

2°) Le message est décomposé en blocs.

3°) On chiffre les blocs bits par bits.

La fonction que l’on utilise avec la partie droite est la clé de cryptage. DES utilise uniquement une table XOR car c’est la seule qui permet d’avoir un comportement uniquement pour chaque valeur rentrée.

2°) Système de clée

a) Clé publique

Une clé pour chiffrer, une autre pour déchiffrer.

La clé publique est la clé de chiffrement. La clé publique est l’équivalent d’un cadenas. Le déverrouillage est réalisé par une clé privée qui est unique.

**RSA**

Alive envoi, Bob reçoit.

n = p\*q

RAS est basé sur une exponentiation complexe.

180² = 32400 m 41= 10