Sécurité Informatique
TD2 : Cryptographie classique

Exercice 1 :

1. Chiffrez le texte en clair « **INTERNET OF THINGS** » en utilisant le chiffre **Rail Fence** avec la **clé 4**.
2. Déchiffrez avec la **clé 5** les textes chiffrés « **MIMATCIINTAATZOHMLPAIEOT**» et « **AAIRILLGTCILEIINENEFTC**».
3. Déchiffrez le texte chiffré « **SESRERTASODCPW**» sans connaitre la clé.

Solution d'exercice 1 :

1.

I	**.**	**.**	**.**	**.**	**.**	**E**	**.**	**.**	**.**	**.**	**.**	**I**	**.**	**.**	**.**
.	**N**	**.**	**.**	**.**	**N**	**.**	**T**	**.**	**.**	**.**	**H**	**.**	**N**	**.**	**.**
.	**.**	**T**	**.**	**R**	**.**	**.**	**.**	**O**	**.**	**T**	**.**	**.**	**.**	**G**	**.**
.	**.**	**.**	**E**	**.**	**.**	**.**	**.**	**.**	**F**	**.**	**.**	**.**	**.**	**.**	**S**

Le texte chiffré : « **IEINNTHNTROTGEFS** »

2. Pour déchiffrer le message il faut calculer **K** : un nombre entier qui représente la taille du premier et dernier bloc.

a.

N = 5 le nombre de rails (lignes).
L = 24 la longueur de la chaine.
K = L/(2(N-1)) = 24 / (2(5 - 1)) = 3.

La longueur du premier et du dernier bloc est **K** et la longueur de chaque bloc intermédiaire est de **2K**, donc on divise le texte chiffré comme suit : « **MIM ATCIIN TAATZO HMLPAI EOT**»

M	**.**	**.**	**.**	**.**	**.**	**.**	**.**	**I**	**.**	**.**	**.**		**.**	**.**	**.**	**M**	**.**	**.**	**.**	**.**	**.**	**.**	**.**
.	**A**	**.**	**.**	**.**	**.**	**.**	**T**	**.**	**C**	**.**	**.**	**.**	**.**	**.**	**I**	**.**	**I**	**.**	**.**	**.**	**.**	**.**	**N**
.	**.**	**T**	**.**	**.**	**.**	**A**	**.**	**.**	**.**	**A**	**.**	**.**	**.**	**T**	**.**	**.**	**.**	**Z**	**.**	**.**	**.**	**O**	**.**
.	**.**	**.**	**H**	**.**	**M**	**.**	**.**	**.**	**.**	**.**	**L**	**.**	**P**	**.**	**.**	**.**	**.**	**.**	**A**	**.**	**I**	**.**	**.**
.	**.**	**.**	**.**	**E**	**.**	**.**	**.**	**.**	**.**	**.**	**.**	**O**	**.**	**.**	**.**	**.**	**.**	**.**	**.**	**T**	**.**	**.**	**.**

Le texte en clair est donc : « **MATHEMATICAL OPTIMIZATION** »

b.

N = 5 le nombre de rails (lignes).
L = 22 la longueur de la chaine.
K = L/(2(N-1)) = 22 / (2(5 - 1)) = 2.

Les taille des blocs sont $B_1 = 2$, $B_2 = 4$, $B_3 = 4$, $B_4 = 4$, et $B_5 = 2$ et $\sum_{i=1}^{5} B_i = 16$, alors que L = 22, donc on ajoute 1 à chaque bloc commençant par B_1 (en zigzag), on aura : $B_1 = 3$, $B_2 = 5$, $B_3 = 5$, $B_4 = 6$, $B_5 = 3$.
On divise le texte chiffré comme suit : « **AAI RILLG TCILE IINENE FTC**»

A	**.**	**.**	**.**	**.**	**.**	**.**	**.**	**A**	**.**	**.**	**.**		**.**	**.**	**.**	**I**	**.**	**.**	**.**	**.**	**.**	**.**	**.**
.	**R**	**.**	**.**	**.**	**.**	**.**	**I**	**.**	**L**	**.**	**.**	**.**	**.**	**.**	**L**	**.**	**G**	**.**	**.**	**.**	**.**	**.**	**.**
.	**.**	**T**	**.**	**.**	**.**	**C**	**.**	**.**	**.**	**I**	**.**	**.**	**.**	**L**	**.**	**.**	**.**	**E**	**.**	**.**	**.**	**.**	**.**
.	**.**	**.**	**I**	**.**	**I**	**.**	**.**	**.**	**.**	**.**	**N**	**.**	**E**	**.**	**.**	**.**	**.**	**.**	**N**	**.**	**E**	**.**	**.**
.	**.**	**.**	**.**	**F**	**.**	**.**	**.**	**.**	**.**	**.**	**.**	**T**	**.**	**.**	**.**	**.**	**.**	**.**	**.**	**C**	**.**	**.**	**.**

Le texte en clair est donc : « **ARTIFICIAL INTELLIGENCE** ».

3.

a. On commence par clé = 2.
N = 2
L = 14
K = 14 / (2(2-1)) = 7
Donc on divise le texte chiffré comme suit : « **SESRERT ASODCPW** ».

S	**.**	**E**	**.**	**S**	**.**	**R**	**.**	**E**	**.**	**R**	**.**	**T**	**.**
.	**A**	**.**	**S**	**.**	**O**	**.**	**D**	**.**	**C**	**.**	**P**	**.**	**W**

Texte déchiffré = « **SAESSORDECRPTW** ».

Puisque le texte déchiffré n'est pas compréhensible, ce n'est pas alors la bonne clé.

b. On essaye clé = 3.
N = 3
L = 14
K = 14 / (2(3-1)) = 3

Les taille des blocs sont $B_1 = 3$, $B_2 = 6$, $B_3 = 3$ et $\sum_{i=1}^{3} B_i = 12$, alors que L = 14, donc on ajoute 1 à chaque bloc commençant par B_1 (en zigzag), on aura : $B_1 = 4$, $B_2 = 7$, $B_3 = 3$.
On divise le texte chiffré comme suit : « **SESR ERTASOD CPW** »

S	**.**	**.**	**.**	**E**	**.**	**.**	**.**	**S**	**.**	**.**	**.**	**R**	**.**
.	**E**	**.**	**R**	**.**	**T**	**.**	**A**	**.**	**S**	**.**	**O**	**.**	**D**
.	**.**	**C**	**.**	**.**	**.**	**P**	**.**	**.**	**.**	**W**	**.**	**.**	**.**

Texte déchiffré = « **SECRET PASSWORD** ».

Puisque le texte déchiffré est pas compréhensible, c'est donc la bonne clé.

Exercice 2 :

1. Chiffrez le message « **BYZANTINE** » à l'aide du chiffre de César.
2. Est-il possible de déchiffrer le texte « **QHUBHYF** » chiffré par un chiffrement par décalage sans connaitre la clé ? Déchiffrez ce message sachant qu'il a été créé avec la **clé 7**.
3. Déterminez la clé puis déchiffrez le texte suivant :
« **YMJHFJXFWHNUMJWNXFGFXNHYJHMSNVZJYTJSHWDUYYJCYX**».

Solution d'exercice 2 :

1.

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

Texte en clair : « **BYZANTINE**»

Texte chiffré : « **EBCDQWLQH**»

2. **Non**, car le message est trop court pour qu'une analyse fréquentielle donne suffisamment d'information.

Texte chiffré : « **QHUBHYF** »

Texte en clair : « **JANUARY** »

3. L'analyse des fréquences d'apparition de chaque lettre dans le message chiffré est :

J : 7, Y : 6, H : 5, F : 4, N : 4, X : 4.

Cette fréquence montre que la lettre **J** est la plus fréquente avec **7** apparitions, il correspond probablement à la lettre **E** (qui a la plus grande fréquence en langue anglaise) et on obtient donc un décalage de **5**.

Le texte clair donne : « **THE CAESAR CIPHER IS A BASIC TECHNIQUE TO ENCRYPT TEXTS** »

Exercice 3 :

On représente les lettres avec des entiers selon le schéma, A → 0, B → 1, ..., Z → 25.

On définit la relation de multiplication « * » sur les entiers de la manière suivante : pour calculer le produit de deux lettres, on transforme les lettres en entiers, on multiplie ces deux entiers et on réduit le résultat modulo 26, puis on le retransforme en une lettre.

Exemple : pour le produit de D et L, on a D = 3 et L = 11, 3 * 11 mod 26 = 7, donc D * L = H.

Le cryptogramme de César **multiplicatif** consiste à multiplier toutes les lettres du message par une lettre fixé qui sert de **clé**.

1. En utilisant ce cryptogramme, chiffrez le message « **MAIL** » avec la **clé N**, qu'est-ce que vous remarquez?
2. En déduire que certaines clés donnent des messages chiffrés non déchiffrables. Déterminer toutes ces mauvaises clés.
3. Chiffrez le message ci-dessus avec la clé **F**.

Solution d'exercice 3 :

1. On N = 13, M = 12, A = 0, I = 8, L = 11.
   N * M = 13 * 12 mod 26 = 156 mod 26 = 0.
   N * A= 13 * 0 mod 26 = 0 mod 26 = 0.
   N * I = 13 * 8 mod 26 = 104 mod 26 = 0.
   N * L = 13 * 11 mod 26 = 143 mod 26 = 13.
   Le texte chiffré est " **AAAN** ".
   On remarque que en utilisant la clé **N** on ne peut pas déchiffrer le message, donc la clé **N** n'est pas convenable.
2. Pour qu'une une **clé** permet un déchiffrement, il faut que le nombre correspondant à cette clé soit **inversible modulo 26,** cela veut dire qu'il doit être **premier avec 26** (PGCD (Clé, 26) =1).
   Les mauvaises clés donc sont ceux qui sont **divisibles par 2 ou par 13**.
   Ainsi les mauvaises lettres sont : **A, B, C, E, G, I, K, M, N, O, Q, S, U, W, Y**.
3. La clé F correspondant à 5.
   On M = 12, A = 0, I = 8, L = 11.
   F * M = 5 * 12 mod 26 = 60 mod 26 = 8.
   F * A = 5 * 0 mod 26 = 0 mod 26 = 0.
   F * I = 5 * 8 mod 26 = 40 mod 26 = 14.
   F * L = 5 * 11 mod 26 = 55 mod 26 = 3.
   On trouve le message crypté suivant : « **IAOD** ».

Exercice 4 :

1. Chiffrez le message « **DETECTIVE** » à l'aide de la méthode de Vigenère et le mot **clé** « **EUREKA** ».
2. Déchiffrez le message « **MFJWXTLIM**» chiffré par le chiffre de Vigenère et la clé « **TRUE** ».

Solution d'exercice 4 :

1. Texte en clair : « **DETECTIVE** »
   Clé : « **EUREKAEUR** »
   Texte chiffré : « **HYKIMTMPV**»
2. Texte chiffré : « **MFJWXTLIM**»
   Clé : « **TRUETRUET** »
   Texte en clair : « **TOPSECRET** »

Exercice 5 :

Dans cet exercice, on s'intéresse à une variante du chiffre de Vigenère.

On utilise pour le chiffrement et le déchiffrement une clé de taille **m** pour chiffrer un texte composé de plusieurs blocs de taille **m** chacun.

Pour chiffrer le premier bloc $\mathbf{B_0}$ du texte on utilise le chiffre de Vigenère avec la clé **K**.

Pour le bloc $\mathbf{B_i}$ (i > 0) on utilise le chiffre de Vigenère en prenant comme clé le texte chiffré du bloc $\mathbf{B_{i-1}}$.

1. Représentez le processus de chiffrement et de déchiffrement d'un texte de **n** blocs de taille **m** chacun à l'aide des schémas.
2. Chiffrez le texte « **MICROSOFT** » à l'aide de cet algorithme et la clé **K** = « **CPU** ».
3. Déchiffrez le texte « **JDAGWGNK** » avec la clé **K** = « **CD** ».
4. Quelle information permettra à un attaquant de déchiffrer une bonne partie du texte chiffré sans connaitre la clé **K** ?

Solution d'exercice 5 :

1. Schéma de chiffrement.

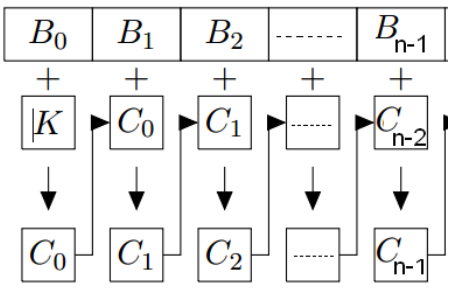
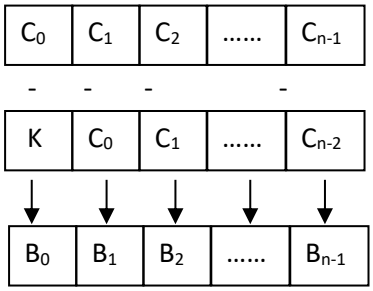


Schéma de déchiffrement.



2. Texte clair : « **MICROSOFT** ». Bloc : B_0 : « MIC », B_1 : « ROS », B_2 : « OFT ».
   Le chiffrement de B_0 avec la clé K donne C_0 « OXW ».
   Le chiffrement de B_1 avec la clé C_0 donne C_1 « FLO ».
   Le chiffrement de B_2 avec la clé C_1 donne C_2 « TQH ».
   Le texte chiffré : « **OXWFLOTQH** »
3. Texte clair : « **JDAGWGNK** ». Bloc : C_0 : « JD », C_1 : « AG », C_2 : « WG », C_3 : « NK ».
   Le déchiffrement de C_0 avec la clé K donne B_0 « HA ».
   Le déchiffrement de C_1 avec la clé C_0 donne B_1 « RD ».
   Le déchiffrement de C_2 avec la clé C_1 donne B_2 « WA ».
   Le déchiffrement de C_3 avec la clé C_2 donne B_3 « RE ».
   Le texte en clair : « HARDWARE ».
4. La connaissance de la taille de la clé suffit pour déchiffrer le tout le texte sauf le premier bloc.

Exercice 6 :

1. Chiffrez le texte en clair « **MEMORY** » en utilisant le chiffre **affine** avec la **clé (9, 4)**.
2. Déchiffrez le texte chiffré « **EXXYRO** » avec la même **clé de chiffrement (9, 4)**.
3. En utilisant la méthode d'**analyse de fréquence**, déchiffrez le texte chiffré suivant sachant qu'il est écrit en anglais : « **USNIVCIUQVKJSKCJDIHVGUJKUIAPBIPITBKTWUAMHQJIVCSCJIM**».

Correction exercice 6 :

1. Pour chiffrer le message **M** en utilisant le chiffre affine, on utilise la fonction de chiffrement suivante : **$E(M) = (k_1 * M + k_2) \bmod 26$**. **M** est l'équivalent numérique de la lettre en clair donnée.
   Avec **$k_1 = 9$ et $k_2 = 4$** : **$E(M) = (9 * M + 4) \bmod 26$**.

M = M : 12	Chiffrement : (9 * 12 + 4) mod 26 = 112 mod 26 = 08	C = I.
M = E : 04	Chiffrement : (9 * 04 + 4) mod 26 = 40 mod 26 = 14	C = O.
M = M : 12	Chiffrement : (9 * 12 + 4) mod 26 = 112 mod 26 = 08	C = I.
M = O : 14	Chiffrement : (9 * 14 + 4) mod 26 = 130 mod 26 = 00	C = A.
M = R : 17	Chiffrement : (9 * 17 + 4) mod 26 = 157 mod 26 = 01	C = B.
M = Y : 24	Chiffrement : (9 * 24 + 4) mod 26 = 220 mod 26 = 12	C = M.

   Le message chiffré est donc **C = « IOIABM ».**
2. Pour déchiffrer le message **C** en utilisant le chiffre affine, on utilise la fonction de déchiffrement suivante : **$D(C) = (k_1^{-1} * (C - k_2)) \bmod 26$**. **C** est l'équivalent numérique de la lettre chiffrée donnée.
   Il faut donc trouver **k_1^{-1}** et **$- k_2$** l'inverse modulaire multiplicatif et additif de **k_1 et k_2** respectivement.
   $- k_2 = -4$ (car (**$k_2 - k_2$) mod 26 =** 0), et **$k_1^{-1} = 3$** (car (**$k_1^{-1} * k_1$) mod 26 =** 1).
   La fonction de déchiffrement est donc : **$D(C) = (3 * (C - 4)) \bmod 26$.**

C = E : 04	Déchiffrement : (3 * (04 – 4)) mod 26 = 0 mod 26 = 0	M = A.
C = X : 23	Déchiffrement : (3 * (23 – 4)) mod 26 = 57 mod 26 = 5	M = F.
C = X : 23	Déchiffrement : (3 * (23 – 4)) mod 26 = 57 mod 26 = 5	M = F.
C = Y : 24	Déchiffrement : (3 * (24 – 4)) mod 26 = 60 mod 26 = 8	M = I.
C = R : 17	Déchiffrement : (3 * (17 – 4)) mod 26 = 39 mod 26 = 13	M = N.
C = O : 14	Déchiffrement : (3 * (14 – 4)) mod 26 = 30 mod 26 = 4	M = E.

   Le message en clair est donc **M = « AFFINE ».**
3. Le nombre d'occurrence de chaque lettre dans le texte chiffré est :
   I : 8 fois, U : 5 fois, J : 5 fois, V : 4 fois, C : 4 fois, K : 4 fois.
   a) Comme première supposition, on peut supposer que **I** est le chiffrement de **E**, et **U** est le chiffrement de **T** (comme **E** et **T** sont les deux caractères les plus courants).
      I → 8, E → 4, U → 20, T → 19.
      La fonction de chiffrement **f** donne : **$f(4) = 8$** & **$f(19) = 20$**. Et nous savons que la fonction de chiffrement s'écrit : **$f(x) = a*x + b$**. Donc, $\begin{cases} \mathbf{4} * \boldsymbol{a} + \boldsymbol{b} = \mathbf{8} \\ \mathbf{19} * \boldsymbol{a} + \boldsymbol{b} = \mathbf{20} \end{cases}$
      On soustrait la première équation de la deuxième, on trouve :
      $(15 * a) \bmod 26 = 12$
      $a = 6$.
      $b = 10$.
      Mais c'est une clé invalide car il faut que **$pgcd(a, 26) = 1$**, mais **$pgcd(6, 26) = 2$**.

b) Comme deuxième supposition, on peut supposer que **I** est le chiffrement de **E**, et **J** est le chiffrement de **T** (comme **E** et **T** sont les deux caractères les plus courants).
I → 8, E → 4, J → 9, T → 19.
La fonction de chiffrement **f** donne : **f (4) = 8** & **f (19) = 9**. Et nous savons que la fonction de chiffrement s'écrit : **f (x) = a*x + b**. Donc, $\begin{cases} \mathbf{4} * \boldsymbol{a} + \boldsymbol{b} = \mathbf{8} \\ \mathbf{19} * \boldsymbol{a} + \boldsymbol{b} = \mathbf{9} \end{cases}$
On soustrait la première équation de la deuxième, on trouve :

(15 * a) mod 26 = 1
a = 7.
b = 6.

Cette fois-ci la clé valide car **pgcd (7, 26) = 1**.
Donc **(7, 6)** est la clé de chiffrement, on cherche maintenant la clé de déchiffrement ($\mathbf{k_1^{-1}}$, $\mathbf{-k_2}$).
L'inverse additif de 6 est 20 (car 26-6=20, ou bien on peut utiliser **-6)**, et l'inverse multiplicatif de 7 est **15** ((7 × 15) mod 26 = 1).
On déchiffre donc à l'aide de la clé **(15, -6) ou (15, 20).**

C : U → 20	Déchiffrement : ((20 - 6) × 15) mod 26 = 02	M : 02 → C
C : S → 18	Déchiffrement : ((18 - 6) × 15) mod 26 = 24	M : 24 → Y
C : N → 13	Déchiffrement : ((13 - 6) × 15) mod 26 = 01	M : 01 → B
C : I → 08	Déchiffrement : ((08 + 20) × 15) mod 26 = 04	M : 04 → E
C : V → 21	Déchiffrement : ((21 + 20) × 15) mod 26 = 17	M : 17 → R
C : C → 02	Déchiffrement : ((02 + 20) × 15) mod 26 = 18	M : 18 → S

…

On continue ainsi avec toutes les lettres, on trouve le texte clair comme suit :

« **CYBERSECURITY IS THE PRACTICE OF DEFENDING COMPUTER SYSTEM** ».

Exercice 7 :

1. Chiffrez le texte en clair « **LAMB** » en utilisant le chiffre de **Hill** avec la **clé « KDFC »**.
2. Déchiffrez le texte chiffré « **PNMQ** » avec la même **clé** de chiffrement.
3. Trouvez la clé de chiffrement utilisée pour chiffrer le texte « **HDBC** » et obtenir le texte chiffré « **JNFF** », sachant la taille de la clé est **m = 2**.

Correction exercice 7 :

1. On écrit le texte en clair et la clé de chiffrement dans des matrice de taille (2x2).

$$M = \begin{bmatrix} L & A \\ M & B \end{bmatrix} = \begin{bmatrix} 11 & 00 \\ 12 & 01 \end{bmatrix}, \qquad K = \begin{bmatrix} K & D \\ F & C \end{bmatrix} = \begin{bmatrix} 10 & 3 \\ 5 & 2 \end{bmatrix}$$

Pour chiffrer, on utilise la fonction : C = (M * K) mod 26.

$$\mathbf{C} = \begin{bmatrix} \mathbf{11} & \mathbf{00} \\ \mathbf{12} & \mathbf{01} \end{bmatrix} * \begin{bmatrix} \mathbf{10} & \mathbf{3} \\ \mathbf{5} & \mathbf{2} \end{bmatrix} = \begin{bmatrix} \mathbf{110} & \mathbf{33} \\ \mathbf{125} & \mathbf{38} \end{bmatrix} \boldsymbol{mod}\ \mathbf{26} = \begin{bmatrix} \mathbf{6} & \mathbf{7} \\ \mathbf{21} & \mathbf{12} \end{bmatrix} = \begin{bmatrix} \boldsymbol{G} & \boldsymbol{H} \\ \boldsymbol{V} & \boldsymbol{M} \end{bmatrix} = \mathbf{GHVM}$$

2. Pour déchiffrer le texte « **PNRS** », on utilise la fonction de déchiffrement : M = (C * K^{-1}) mod 26.

Donc on commence par trouver l'inverse de la clé K : K^{-1}. Pour cela, on calcule **det (K)**

det (K) = (10*2 – 5*3) mod 26 = 5.

On calcule ensuite la comatrice de K :

La comatrice de la matrice (2x2) est : $Adj\begin{bmatrix} a & b \\ c & d \end{bmatrix} = \begin{bmatrix} d & -b \\ -c & a \end{bmatrix}$.

$Adj\ (K) = \ Adj\begin{bmatrix} 10 & 3 \\ 5 & 2 \end{bmatrix} = \begin{bmatrix} \mathbf{2} & \mathbf{-3} \\ \mathbf{-5} & \mathbf{10} \end{bmatrix}$.

La matrice inverse de K est : (1/det(K)) * $Adj\ (K)$ = ($\det(K)^{-1}$ * $Adj\ (K)$) mod 26.

L'inverse modulaire de 5 est 21. (5*21 mod 26 = 1).

$K^{-1} = 5^{-1} * \begin{bmatrix} 2 & -3 \\ -5 & 10 \end{bmatrix}$ mod 26 = $\begin{bmatrix} 42 & -63 \\ -105 & 210 \end{bmatrix}$ mod 26 = $\begin{bmatrix} 16 & 15 \\ 25 & 2 \end{bmatrix}$

Maintenant on peut déchiffrer avec la fonction : M = (C * K^{-1}) mod 26.

$\mathbf{M = \begin{bmatrix} 15 & 13 \\ 12 & 16 \end{bmatrix} * \begin{bmatrix} 16 & 15 \\ 25 & 2 \end{bmatrix} = \begin{bmatrix} 565 & 251 \\ 722 & 291 \end{bmatrix} mod\ 26 = \begin{bmatrix} 19 & 17 \\ 20 & 04 \end{bmatrix} = \begin{bmatrix} T & R \\ U & E \end{bmatrix}}$ **= TRUE.**

3. Comme la fonction de chiffrement est **C = M * K**, on peut utiliser la relation $\mathbf{K = M^{-1} \times C}$ pour trouver la clé si **M** est inversible.

$$M = \begin{bmatrix} H & D \\ B & C \end{bmatrix} = \begin{bmatrix} 7 & 3 \\ 1 & 2 \end{bmatrix}, \qquad C = \begin{bmatrix} J & N \\ F & F \end{bmatrix} = \begin{bmatrix} 9 & 13 \\ 5 & 5 \end{bmatrix}$$

On calcule donc M^{-1} :

det (M) = (7 * 2 – 1 * 3) mod 26 = **11.** Puisque det (M) ≠ 0, M est inversible.

Adj (M) = Adj $\begin{bmatrix} 7 & 3 \\ 1 & 2 \end{bmatrix} = \begin{bmatrix} 2 & -3 \\ -1 & 7 \end{bmatrix}$.

$M^{-1} = 11^{-1} * \begin{bmatrix} 2 & -3 \\ -1 & 7 \end{bmatrix}$ mod 26 = 19 * $\begin{bmatrix} 2 & -3 \\ -1 & 7 \end{bmatrix}$ mod 26 = $\begin{bmatrix} 38 & -57 \\ -19 & 133 \end{bmatrix}$ mod 26 = $\begin{bmatrix} 12 & 21 \\ 7 & 3 \end{bmatrix}$

On applique maintenant la relation $\mathbf{K = M^{-1} \times C}$ pour trouver la clé :

$\mathbf{K = \begin{bmatrix} 12 & 21 \\ 7 & 3 \end{bmatrix} * \begin{bmatrix} 9 & 13 \\ 5 & 5 \end{bmatrix} = \begin{bmatrix} 213 & 261 \\ 78 & 106 \end{bmatrix} mod\ 26 = \begin{bmatrix} 5 & 1 \\ 0 & 2 \end{bmatrix} = \begin{bmatrix} F & B \\ A & C \end{bmatrix}}$ **= FBAC.**