Tutorial N°1 : Intro. To Classical Cryptography

Exercise 1 : crypto classique

1. Describe the Caeser Cipher.
2. What is the size of the key space? → all possible keys
3. Describe at least two ways of breaking a Caeser cipher on an English-language message.

We consider the following recursive Caeser cipher. We denote $m_1, m_2, \ldots, m_n, \ldots$ the plain letters and $c_1, c_2, \ldots, c_n, \ldots$ their matching cipher letters, respectively. The following table matches the letters of the alphabet by numbers :

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
0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25

Letter K stands for the key. The recursive Caeser cipher is described by the following two equations :

$$c_1 = m_1 + K \pmod{26}, \text{ et pour } i \geq 2,\ c_i = m_i + c_{i-1} \pmod{26}$$

4. Encrypt the message "MESSAGE" with the key "C".
5. Decrypt the message "PNAAMUKEI" encrypted with the key "M".
6. Discuss the security of this cipher.

Exercise 2 :

We recall the correspondence between letters of the alphabet and the numbers {0,1, ...,25}:

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
0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25

We consider the message M = LESMAISONSBLANCHES

1. Let's K = ULOIDTGKXYCRHBPMZJQVWNFSAE be the encryption key. The following table defines the employed substitution cryptographic primitive :

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

key space 26!

Encrypt the message M. Which properties related to plaintext/ciphertext still be unchanged after applying the substitution mechanism ?

2. Encrypt the message M by applying transposition cryptographic primitive under the key K = [3,5,2,6,1,4]. We note that transposition mechanism encrypt the message bloc by bloc depending on the length of the key, it consists of rearranging the order of the plain letters based on the key. Which properties related to plaintext/ciphertext still be unchanged after applying the transposition mechanism ?
3. Encrypt the message M by applying Vigénère cipher under the key $K = SECURITE$. what happens to the frequencies of letters after encryption ?

3 pagine. M

Exercise 3 :

We suppose that we have a message expressed by letters from A to Z in uppercase, and we want to encrypt it using Hill cipher. The idea around Hill cipher is to arrange the letters of the message by groups of fixed number of letters according to the key.

1. Encrypt the message MATHEMATIQUE with the key $\begin{pmatrix} 9 & 4 \\ 5 & 7 \end{pmatrix}$.
2. Explain why these two matrices $\begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}$ and $\begin{pmatrix} 1 & 2 \\ 2 & 4 \end{pmatrix}$ can't be employed for Hill encryption.
3. $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ is a matrix in $Z|Z_{26}$, we set $B = \begin{pmatrix} d & -b \\ -c & a \end{pmatrix}$ compute AB.

4. Deduce the inverse of the matrix A and the condition of inverse-existence.
5. Decrypt the message « UWGMWZRREIUB » using the matrix $\begin{pmatrix} 9 & 4 \\ 5 & 7 \end{pmatrix}$ as an encryption key.
6. You have intercepted the following message from your enemy : YKTZZUDCLWQOAGKIHXRVANYSPWBYDCLS. You have been informed that this message is encrypted using Hill cipher. Moreover, by having a knowledge of the protocol side of the military messages, you come to have a assumpltion that this message begins with MONGENERAL. We denote A the encryption message.
   a. Justify $\begin{pmatrix} 24 & 19 \\ 10 & 25 \end{pmatrix} = A\begin{pmatrix} 12 & 13 \\ 14 & 6 \end{pmatrix}$ (1)
   b. What is the sufficient condition to find A. Why in this case is impossible ?
   c. Find A by exploiting other similar eauation as (1).
   d. Decrypt the whole message !

Exercise 4 :

The transposition cryptographic primitives, and the Hill cipher have the common property that their decryption key is disimilar to their encryption key, notably there is a simple mathematical problem that relies these two different keys (i.e., the decryption key is the inverse of the decryption key).

1. Find the inverse key K^{-1} associated to the key $K = [3,5,2,6,1,4]$, using transposition.
2. Let's A denotes the l'alphabet $\{A, B, \dots, Z\}$ identified in $Z/26Z$ and let's E_A be the Hill cipher, and the following A be the encryption key matrix :

$$A\begin{pmatrix} 2 & 1 \\ 1 & 1 \end{pmatrix}$$

Demonstrate that A has an inverse A^{-1} in $/26Z$, and compute it.

Exercise 5 :

Assume that the Affine cryptosystem is implemented in Z_{126}.

1. Determine the number of possible keys.
2. For the encryption function $e(x) = (23x + 7) mod\ 126$ find the corresponding decryption function.
3. Perform the encryption and decryption routines for a message of your choice.

Exercice 01 : | Notes | TD 1

Caesar Cipher

1). Encryption Algorithm (ENC)

$$\begin{cases} C = (P + K) \bmod 26 \\ P = (C - K) \bmod 26 \end{cases}$$

C ciphertext
P plaintext
K Key | Ke , Kd

2)- Key space size = $[0, 25]$, 26 possible keys.

⇒ Recursive Caesar:

(Enc) : $\begin{cases} C_1 = (m_1 + K) \bmod 26 \; ; \; i = 1 \\ C_i = (m_i + C_{i-1}) \bmod 26 \quad i \geq 2 \end{cases}$

4)- Encryption of "MESSAGE" ;

* Key = "C" → 2

• C_1 = "O" = 14

• C_2 = "S" = 18 ; • C_3 = "K" = 10 ; • C_4 = "C" = 2 ; • C_5 = "C" = 2 ; • C_6 = "I" = 8 ; • C_7 = "M" = 12

$\boxed{\text{ciphertext = "OSKCCIM"}}$

5)- Decryption of "PNAAMUKEI" :

Ke = "M" = 12

$$\begin{cases} m_1 = (c_1 - K) \bmod 26 \; ; \; i = 1 \\ m_i = (c_i - c_{i-1}) \bmod 26 \; ; \; i \geq 2 \end{cases}$$

* $m_1 = (c_1 - 12) \bmod 26 = 3$ = "D"

• $m_2 = (c_2 - c_1) \bmod 26 = \underbrace{(13 - 15)}_{4 + 26} \bmod 26 = 24$ "Y"

• $m_3 = 13$ = "N"
• $m_4 = 0$ = "A"
• $m_5 = 12$ = "M"
• $m_6 = 8$ = "I"
* m_7 = "Q"
* m_8 = "U"
* m_9 = "E"

⇒ $\boxed{\text{Message = "DYNAMYQU}}$

* La bijection assure que 1 seule clé peut donner un message "meaningful" après "decryption".

$\left(\;\right) \underset{K_d}{\overset{K_e}{\rightleftarrows}} \left(\;\right)$ bijection

3)- Breaking a Caesar cipher:
1. brute force attack
2. known plain text attack
3. frequency attack

* The security doesn't belong in cryptography
* Crypto Analysis vs cryptography
* Cryptographer is not necessary by a crypto analyser

4) - in Recursive Caesar, we can decrypt the Cipher text without a key ; Key space = 0.

Exercice 2:

1)- M = "LES/MAIS/ONS/BLAN/CHES"

C = "RDQHUXQPBQLRUBOKDQ"

Scope ?

Diffusion / confusion

=> Properties that still be unchanged:
- length
- letters statistic

} => frequency of each letter has changed

2)- Bloc by Bloc encryption: (transposition)

P = "LES MAI/SON/S BLA NCHES" ; K = [3, 5, 2, 6, 1, 4]

C = "SAEILMNBOLSSCENSAH" => transformation linéaire

Scoop => Diffusion

=> Freq of letters remain the same.

3)- Vigirère Cipher:

Enc : $C_i = (P_i + K_i) \bmod 26$

Dec : $D_i = (C_i - K_i) \bmod 26$

} key space $|26^L|$ L: length of the key

with: K = "SECURITE" we will get:

C = "DIUGRQLSFUDFRU LW

EXO 7 : . . . .

Classical Crypto

EXO3 : HILL CIPHER (1929)

$\boxed{\mathbb{Z}/\mathbb{Z}_{26}}$

P = ME|SS|AG|E|Z → padding

ENC:

$$* \begin{pmatrix} C_n \\ C_{n+1} \end{pmatrix} = \begin{pmatrix} a & b \\ c & d \end{pmatrix} * \begin{pmatrix} P_n \\ P_{n+1} \end{pmatrix} \bmod 26$$

$$\begin{cases} C_n = (aP_n + bP_{n+1}) \bmod 26 \\ C_{n+1} = (cP_n + dP_{n+1}) \bmod 26 \end{cases} \quad \Bigg| \quad K = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$$

DEC

$\det(K) = (ad - bc)$; $PGCD(\det(K), 26) = 1$

$$K^{-1} = \det(K)^{-1} * \begin{pmatrix} d & -b \\ -c & a \end{pmatrix} \bmod 26$$

$$\begin{pmatrix} P_n \\ P_{n+1} \end{pmatrix} = K^{-1} \cdot \begin{pmatrix} C_n \\ C_{n+1} \end{pmatrix}$$

1)- Encryption:

⇒ we write the Enc Algorithm

⇒ P = "MA|TH|EM|AT|IQ|UE"

$$\begin{pmatrix} C_1 \\ C_2 \end{pmatrix} = \begin{pmatrix} 9 & 4 \\ 5 & 7 \end{pmatrix} \cdot \begin{pmatrix} 12 \\ 0 \end{pmatrix} \bmod 26 = \begin{pmatrix} 4 \\ 8 \end{pmatrix} = \begin{pmatrix} E \\ I \end{pmatrix}$$

⇒ we continue . . .

we will have ⇒ C = "EIROGAYDGWOY"

2)- $K_1 = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}$; $K_2 = \begin{pmatrix} 1 & 2 \\ 2 & 4 \end{pmatrix}$

- $\det(K_1) = ab - bc = 0$

$GCD(\det(K_1), 26) \neq 1$

the Matrix K_1 is not Invertible in $\mathbb{Z}/\mathbb{Z}_{26}$

$$\begin{pmatrix} c_1 \\ c_2 \end{pmatrix} = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix} \begin{pmatrix} P_1 \\ P_2 \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \end{pmatrix}$$

$\Rightarrow \forall P_1 P_2 \in \mathbb{Z}/\mathbb{Z}_{26}$

$$\begin{pmatrix} c_n \\ c_{n+1} \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \end{pmatrix}$$

ambiguity.

$\det(K_2) \Rightarrow K_2$ Not inversible.

$$\begin{pmatrix} c_1 \\ c_2 \end{pmatrix} = \begin{pmatrix} 1 & 2 \\ 2 & 4 \end{pmatrix} * \begin{pmatrix} 0 \\ 0 \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \end{pmatrix}$$

$$\begin{pmatrix} c_3 \\ c_4 \end{pmatrix} = \begin{pmatrix} 1 & 2 \\ 2 & 4 \end{pmatrix} * \begin{pmatrix} 0 \\ 13 \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \end{pmatrix}$$

$\Rightarrow$ Directly, when $\det(K_2) \neq 0$, K_2 is not Inversible, then we will find ourselves in ambiguity.

3)- $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$; $B = \begin{pmatrix} d & -b \\ -c & a \end{pmatrix}$

- compute AB:

$$A \cdot B = \begin{pmatrix} ad - bc & 0 \\ 0 & -cb + da \end{pmatrix} \Rightarrow AB = \underbrace{ad - bc}_{\det(A)} \underbrace{\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}}_{I_2}$$

$$AB = \det(A) * I_2 \Rightarrow A \det(A)^{-1} B = I_2 \qquad \boxed{AA^{-1} = I_2}$$

$$A \cdot A^{-1} = I_2$$

$$\Rightarrow \boxed{A^{-1} = \det(A)^{-1} \cdot B} \longrightarrow \boxed{A^{-1} = \det(A)^{-1} \begin{pmatrix} d & -b \\ -c & a \end{pmatrix} \bmod}$$

5)- Decryption : "UWGMWZRREJUB"

$K = \begin{pmatrix} 9 & 4 \\ 5 & 7 \end{pmatrix}$; $\det(K) = ad - bc = 43 \bmod 26 = \underline{17}$

$\det(K) . \det^{-1}(K) \equiv 1 [26]$

$17 . \det^{-1}(K) \equiv 1 [26]$

$17 . 23 = 1 [26]$ Donc : $\boxed{\det^{-1}(K) = 23}$

$K^{-1} = \det^{-1}(K) \begin{pmatrix} d & -b \\ -c & a \end{pmatrix} \bmod 26 \Rightarrow \boxed{K^{-1} = \begin{pmatrix} 5 & 12 \\ 15 & 25 \end{pmatrix}}$

$\Rightarrow$ Decrypty :

$$\begin{pmatrix} P_n \\ P_{n+1} \end{pmatrix} = K^{-1} \begin{pmatrix} C_n \\ C_{n+1} \end{pmatrix} \bmod 26$$

maura :

P = "ASS AUTDE MAIN"

6)- Crypt Analysis :

* Known plaintext Attack : we know the ciphertext, plaintext

$\begin{cases} C = YKTZ \; ZUD \; CLW \; ... \\ P = MONG \; ENERAL \; ... \end{cases}$

$$\underbrace{\begin{pmatrix} \overset{Y}{24} & \overset{T}{19} \\ \overset{K}{10} & \overset{Z}{25} \end{pmatrix}}_{C} = \underset{A}{A} . \underbrace{\begin{pmatrix} \overset{M}{12} & \overset{N}{13} \\ \overset{O}{14} & \overset{G}{6} \end{pmatrix}}_{P}$$

$\Rightarrow \det(B) = ad - bc = 410 \bmod 26 = 20$

$GCD(\det(B), 26) \neq 1$

$$\begin{array}{c} \begin{array}{cc} T & Z \\ \end{array} \\ \begin{pmatrix} 19 & 25 \\ Z & U \\ 25 & 20 \end{pmatrix} \end{array} = A + \underbrace{\begin{pmatrix} 13 & 4 \\ 6 & 13 \end{pmatrix}}_{B}$$

$\det(B) = ab - bc = 145 \bmod 26 = 15$

$GCD(\det(B), 26) = 1$

$\det(B) \cdot \det^{-1}(B) = 1\ [26]$

$15 \times 7 = 1\ [26]$

Donc :

$$\begin{pmatrix} 19 & 25 \\ 25 & 20 \end{pmatrix} \begin{pmatrix} 13 & 4 \\ 6 & 13 \end{pmatrix}^{-1} = A \times \begin{pmatrix} 13 & 4 \\ 6 & 13 \end{pmatrix} \cdot \begin{pmatrix} 13 & 4 \\ 6 & 13 \end{pmatrix}^{-1}$$

$$A = \begin{pmatrix} 19 & 25 \\ 25 & 20 \end{pmatrix} \times \begin{pmatrix} 13 & 4 \\ 6 & 13 \end{pmatrix}^{-1}$$

$$\boxed{A = \begin{pmatrix} 3 & 1 \\ 5 & 2 \end{pmatrix}}$$

Dec Algo :

$$\begin{pmatrix} P_n \\ P_{n+1} \end{pmatrix} = \begin{pmatrix} 3 & 1 \\ 5 & 2 \end{pmatrix} \begin{pmatrix} C_n \\ C_{n+1} \end{pmatrix} \bmod 26$$

DEC :

$$\begin{pmatrix} P_n \\ P_{n+1} \end{pmatrix} = \begin{pmatrix} 3 & 1 \\ 5 & 2 \end{pmatrix} \begin{pmatrix} C_n \\ C_{n+1} \end{pmatrix} \bmod 26$$

P = "MONGENERALSOUSMATINENNEMIREPEREZ

EXO4 :

1) - Finding K^{-1} of $K = [3,5,2,6,1,4]$

$K^{-1}(K(i)) = i \Rightarrow \begin{cases} K^{-1}(\overset{2}{K(1)}) = 1 \\ K^{-1}(\overset{5}{K(2)}) = 2 \\ \vdots \\ K^{-1}(\overset{4}{K(6)}) = 6 \end{cases} \Rightarrow K^{-1} = [5,3,1,6,2,4]$

2) - sna: $A = \begin{pmatrix} 2 & 1 \\ 1 & 1 \end{pmatrix}$

$\det(A) = 1$; $GCD(\det(A), 26) = 1$

$\det(A) \cdot \det(A)^{-1} \equiv 1 [26]$

$1 \times 1 = 1 [26]$

$A^{-1} = \det(A)^{-1} \cdot \begin{pmatrix} d & -b \\ -c & a \end{pmatrix} \bmod 26 = 1 \begin{pmatrix} 1 & -1 \\ -1 & 2 \end{pmatrix}_{\bmod 26} = \begin{pmatrix} 1 & 25 \\ 25 & 2 \end{pmatrix}$

EXO5 : AFFINE CIPHER

Z/Z_{26} ; $K = (K_1, K_2)$

ENC: $C_i = ((K_1 * P_i) + K_2) \bmod 26$

Dec: $P_i = ((K_1^{-1} * (C_i) - K_2)) \bmod 26$

Keyspace : : $K_2 \in [0, 25] = 26$ possible keys.

$Z_{26} = \{0, 1, \cdots 25\}$

$Z_{26}^{*} = \{1, 3, 5, 7, 9, 11, 15, 17, 19, 21, 23, 25\}$

$K = Z_{26} \cdot Z_{26}^{*} \rightarrow \# K = 26 * 12 = \boxed{312}$ possible keys

1- number of possible keys

$$\begin{cases} C_i = \left((k_1^{-1} \cdot p_i) + k_2\right) \bmod 126 \\ P_i = \left((k_1^{-1} \cdot C_i) - k_2\right) \bmod 126 \end{cases}$$

=> Keyspace:

$\Rightarrow k_1 \in Z_{126}^*$

$126 = 2.9.7$

$$\Rightarrow \begin{cases} Z_{126}^* = Z_2^* \cdot Z_9^* \cdot Z_7^* \\ \bullet |Z_2^*| = 1 \\ \bullet Z_9 = \{0,1,2,3,4,5,6,7,8\} \\ \bullet |Z_9^*| = 6 \ ; \ Z_9^* = \{1,2,4,5,7,8\} \\ \bullet Z_7 = \{0,1,2,3,4,5,6\} \\ \bullet |Z_7^*| = 6 \quad Z_7^* = \{1,2,3,4,5,6\} \end{cases}$$

$\Rightarrow \boxed{|Z_{126}^*| = |Z_9^*| \cdot |Z_7^*| \cdot |Z_2^*|}$

$\Rightarrow |Z_2^*|\,|Z_9^*|\,|Z_7^*| = \boxed{36}$

2)- $e(x) = (23x + 7) \bmod 126$

alice cipher

plain text

$\Rightarrow d(y) = (23^{-1} y - 7) \bmod 126$

$23 \cdot 23^{-1} \equiv 1\ [126] \quad \Rightarrow d(y) = (11y - 7) \bmod 126$

we have:
$P = \text{hello} = (7, 4, 11, 11, 14)$

. $e(h) = (23 \times 7 + 7) \bmod 126 = \boxed{42}$

. $e(e) = (23 \times 4 + 7) \bmod 126 = \boxed{99}$

. $e(l) = (23 \times 11 + 7) \bmod 126 = \boxed{18}$

. $e(o) = (23 \times 14 + 7) \bmod 126 = \boxed{77}$