Advanced Encryption Standard aka AES

↳ Is a symetric block cipher

↳ The US goverment allows the use of AES-128 for sensitive data and low level clasified data

Steps of AES Algorithm Encryption

→ blanqueamiento → (writing) Operar (a have cuantas veces ser

↳ Campos de galois

Resumen primer parcial

↳ Temas:

- → Definicion ✓
- → Terminologia
- → Algorithm OTP ✓
- → Perfect Secrecy ✓
- → Unconditionally secure Vs Computationally Secure ✓
- → Kerchoff's Principle ✓
- → Classic cryptography
  - ↳ Block ciphers ✓
  - ↳ Substitution ciphers
    - ↳ monoalphabetic ciphers
  - ↳ Transposition ciphers
    - ↳ Product ciphers
- → Data encryption Standard (DES)
- → Advanced encryption Standard (AES)

Cryptography: "to write secretly"

↳ It's a field in Computer science used to encrypt and decrypt message to guarantee the secure of the data

↳ what does the criptography look?

- → Authentication
- → Integrability of the data
- → Confidentaly
- → Availability of the messages

Cryptoanalysis

→ The art of deciphering the cipher message

Criptology

→ The art of encoding messages

One Time Pad (Algorithm)

↳ It's an algorithm teorically unhackeable because we need a message (M) and a key with the same length of the message to cipher using the XOR operation

Example:

message: 0 1 0 1 0 1

Key: 1 0 1 1 1 1

Algorithm:

→

```
  0 1 0 1 0 1   } XOR operation
  1 0 1 1 1 1
-------------
  1 1 1 0 1 1  → message encrypted
```

One time Pad with 26 modulo

↳ In case we need to cypher a message which use the alphabetic we use mod(26) because the XOR operation is equal to addition modulo.

Reminders:

0 12

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.

$a \bmod b = d$
$\Rightarrow a = bc + d$

Example:

MATEO → mesa

12, 0, 19, 4, 14

Key: ATEMM

0, 19, 4, 12, 12

12 mod 26 / 0 mod 26 / 19 mod 26 / 4 mod 26 / 14 mod 26

12 mod 26

→ 12 | 26 → 12 mod 26 = 12
12 | 0 → 12 = 26(0) + 1

→ 12 / 0 / 19 / 4 / 14
0 / 19 / 4 / 12 / 12

12 / 19 / 23 / 16 / 26

→ M T X Q Z

Perfect Secrecy:

→ An algorithm shouldn't give information about how to decypher when is cypher or decrypted.

Kerchoff's Algorithm

↳ "A cryptosystem should be secure even if everything about the system, except the key, is a public message"

Assymetric encryption or Public and Private key are examples

Symetric Encryption

↳ The algorithms which use an unique key are catalogue as "Symetric Encrption Algorithm"

The symetric encryption algorithms use a block cipher

↳ Divide the messages in different blocks to cipher

→ Substitution cypher
→ transposition cypher
→ Product cipher

Replace a block with an other cipher

block. The receptor do the inverse substitution

Changes or permutes the symbols on a block

It's a substitution and Transposition cypher combination

Playfair Cipher (Polygraphic)

↳ Its an substitution cipher which use an 5x5 matrix omitting repeated letters and combine IJ.

Rules: → If is the same column, use the letter below

→ If is the same row: use the right letter

→ neither use the exchange letter

Example:

encrypt the message: "this secret message is encrypted"

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

MATRIX KEY

1) DIVIDE IN PAIRS

→ TH IS SE CR ET ME SX SA GE IS EN CR YP TE DX

2) ENCRIPTED MESSAGE

→ WE DL LK HW LY CF XP QP HF DL HY HW OY YL KP

3) DECRYPTED THE MESSAGE

ZO MB LC WY ZK MN SO NQ DL MT GQ CY KI EC LK SO YI EQ PQ RX EY KR WM NS
DL GY LD GF AB YA QN YE AP GN IX PG HY YS NB HT EC TL KF VN RP YT PU PF
CY EB YA WM KI MP LF UZ LH TC YH NP CK KL LY YT KI GB DH CY EC RD GN CL
GO IH YE TY KI XO UY VN SC LX KF MX PW

OUR FRIEND FROM PARIS EXAMIN....

Caesar Cipher's Algorithm

The caesar cipher algorithm is used to encrypt message in a substitution cesay. Works using block ciphers (c) to divide the message and change the letter with the next letter in the alphabet.

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.

Example:

→ Message: RETURN TO ROME

→ 'C= C strings of length) =5

→ K= Permutation =3.

2) RETUR NTORO ME ⇒ Divide in block ciphers

3) UHWU QWRUR PH ⇒ Remake each letter

MESSAGE ENCRYPTED

ROT 13

Is an algorithm which moves each letter 13 positions ahead

Polyalphabetic substitution ciphers

Is Are algorithms develop to change a simple key or letter into differents ways.

Vigènere Cipher

It's an algorithm used to cypher message using a keyword (It's the main idea of the enigma machine) and a permution using the message to encrypt.

1) Select a keyword and put n times to complete the message.

2) Using the table change the intersection with the letter.

Example:

Cypher the message

"MATEO GUTIERREZ"

with the keyword SA

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

Note: There is an equation to encrypt the message using the vigenere cipher

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

- C_i: Cipher letter in position i
- P_i: letter in Alphabet i
- K_i: letter in the i-esima key position
- $\bmod 26$: Guarantee all encrypted letters exist in the alphabet space

Example:

TO BE OR NOT TO BE THAT IS THE QUESTION

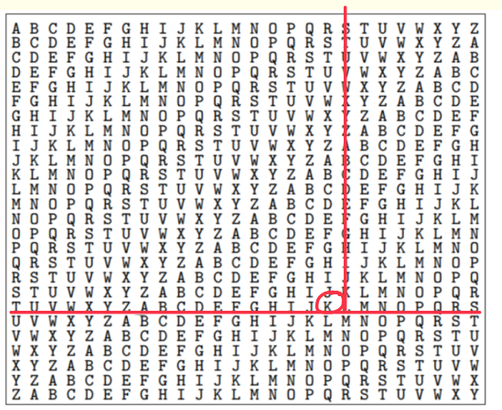
MESSAGE TO ENCRYPT

0 12
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.
19 26

0 8
RELATIONS

KEY WORD

→ (19 + 17) mod 26 ⇒ 36 mod 26 = 10 in the alphabet is the letter K



Hill Cipher (Polyalphabetic)

There is different ways to have a different encryption for each letter

Note: The next part talks about linear combination and their use in the Hill Cipher.

Linear Combination

↳ The linear combination is an operation between two vectors. Adding the multiplication of scalars and vectors

$$w = a_1 c_1 + a_2 c_2 + a_3 c_3 + \dots$$

That can be represent how:

$$v_1 = \begin{pmatrix} v_1 \\ v_2 \end{pmatrix}, \quad v_2 = \begin{pmatrix} v_3 \\ v_4 \end{pmatrix}$$

$$\rightarrow \quad w = a_1 v_1 + a_2 v_2$$

$$= a_1 \begin{pmatrix} v_1 \\ v_2 \end{pmatrix} + a_2 \begin{pmatrix} v_3 \\ v_4 \end{pmatrix}$$

$$= \begin{pmatrix} a_1 v_1 \\ a_1 v_2 \end{pmatrix} + \begin{pmatrix} a_2 v_3 \\ a_2 v_4 \end{pmatrix}$$

$$\underbrace{w} = \begin{pmatrix} a_1 v_1 + a_2 v_3 \\ a_1 v_2 + a_2 v_4 \end{pmatrix}$$

Result vector

Example:

Given two vectors in $\mathbb{R}^2$ we have

$a_1 = (1,2)$ and $a_2 = (3,1)$, and $c_1 = 2$ y $c_2 = 3$

$$v = 2v_1 + 3a_2$$

$$= 2\begin{pmatrix} 1 \\ 2 \end{pmatrix} + 3\begin{pmatrix} 3 \\ 1 \end{pmatrix}$$

$$= \begin{pmatrix} 2+9 \\ 4+3 \end{pmatrix} = \begin{pmatrix} 11 \\ 7 \end{pmatrix}$$

That means $v = (11,7)$.

Inverse and Identity matrix

↳ A identity matrix is a matrix which

has 1's in their leading

$$I = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}$$

↳ An inverse matrix of the A^{-1} is a matrix which has the property

$$\Rightarrow AB = BA = I$$

$$\Rightarrow AA^{-1} = A^{-1}A = I$$

Not all matrix has inverse

Example:

$$\begin{pmatrix} 11 & 8 \\ 3 & 7 \end{pmatrix} = A \quad \text{and} \quad A^{-1} = \begin{pmatrix} 7 & 18 \\ 23 & 11 \end{pmatrix}$$

$$\rightarrow \quad AA^{-1} = A^{-1}A = I$$

$$\Rightarrow \begin{pmatrix} 11 & 8 \\ 3 & 7 \end{pmatrix} \begin{pmatrix} 7 & 18 \\ 23 & 11 \end{pmatrix} = \begin{pmatrix} 7 & 18 \\ 23 & 11 \end{pmatrix} \begin{pmatrix} 11 & 8 \\ 3 & 7 \end{pmatrix}$$

$$\Rightarrow \begin{pmatrix} (11)(7) + (8)(23) & (11)(18) + (8)(11) \\ (7)(3) + (7)(23) & (3)(18) + (7)(11) \end{pmatrix}$$

$$\Rightarrow \begin{pmatrix} 77 + 184 & 198 + 88 \\ 21 + 161 & 54 + 77 \end{pmatrix}$$

$$\Rightarrow \begin{pmatrix} 261 & 286 \\ 182 & 131 \end{pmatrix} = \begin{pmatrix} 131 & 182 \\ 286 & 261 \end{pmatrix}$$

$$\Rightarrow \begin{pmatrix} 261 \bmod 26 & 286 \bmod 26 \\ \cdots & \cdots \end{pmatrix} = \begin{pmatrix} 131 \bmod 26 & 182 \bmod 26 \\ \cdots & \cdots \end{pmatrix}$$

$\begin{pmatrix} 162 \bmod 26 & 134 \bmod 26 \\ 286 \bmod 26 & 251 \bmod 26 \end{pmatrix}$

$= \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$

Hill Cipher

↳ Each letter is represented by a number according with the alphabet. And the idea is take a linear combination with each letter.

$M = C = (\mathbb{Z}^{26})^{\epsilon}$ → Is the size of the key matrix ($\epsilon \times \epsilon$)

$$(c_1, c_2) = (m_1, m_2)\begin{pmatrix} 11 & 8 \\ 3 & 7 \end{pmatrix}$$

Encrypted — Value transformed in the Alphabet — Key Values

↳ To decrypt we use the inverse matrix

$$m = cK^{-1}$$

m: decrypted value; c: Encrypted transformed in Alphabet; K^{-1}: matrix Key's inverse

Example:

Encrypt the message "JULY" using $K = \begin{pmatrix} 11 & 8 \\ 3 & 7 \end{pmatrix}$

0 6 12
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.
19 25

1) Transform July into matrix

Divided in Block Cipher (2)

JULY = (JU) = (9 20)

(LY) = (11 24)

Representation in the Alphabet

2) Encrypt using the linear combination

$$(c_1, c_2) = (m_1, m_2)\begin{pmatrix} 11 & 8 \\ 3 & 7 \end{pmatrix}$$

$$C_1 = \underset{1\times2}{(9\ 20)}\underset{2\times2}{\begin{pmatrix} 11 & 8 \\ 3 & 7 \end{pmatrix}}$$

$$= (99+60,\ 72+140)$$

$$= (159, 212) \bmod 26$$

$$= (3, 4) \Leftrightarrow D\ E$$

$$C_2 = (11\ 24)\begin{pmatrix} 11 & 8 \\ 3 & 7 \end{pmatrix}$$

$$= (121+72,\ 88+168)$$

$$= (193, 256) \bmod 26$$

$$= (11, 22) \Rightarrow L\ W$$

July using the Hill cipher is DELW

Example 2:

Decrypt VZFZRUWTIAZSMISGKA

Using Key = $\begin{pmatrix} 11 & 8 \\ 3 & 7 \end{pmatrix}$

→ to decrypt a message using Hill cipher we use the formula

$$m = c\,k^{-1}$$

$k^{-1} \Rightarrow$ Exists if $\det(A) \neq 0$.

Using gauss-Jordan

Example = $A = \begin{bmatrix} 2 & 0 \\ 4 & -1 \end{bmatrix}$

1) Create aumented matrix $[A|I]$

↳ $\left[\begin{array}{cc|cc} 2 & 0 & 1 & 0 \\ 4 & -1 & 0 & 1 \end{array}\right]$

2) Operations allowed:

1) multiply a row by number $\neq 0$
2) adding or substraction the multiple of another
3) Change the order of the rows

↳

2) Make operations to transform to I

↳ $\left[\begin{array}{cc|cc} 2 & 0 & 1 & 0 \\ 4 & -1 & 0 & 1 \end{array}\right] \xrightarrow{i_1 := 2} \left[\begin{array}{cc|cc} 1 & 0 & 1/2 & 0 \\ 4 & -1 & 0 & 1 \end{array}\right] i_2 = i_2 - 4i_1$

↳ $\left[\begin{array}{cc|cc} 1 & 0 & 1/2 & 0 \\ 0 & -1 & -2 & 1 \end{array}\right] \xrightarrow{i_2 = -i_2} \left[\begin{array}{cc|cc} 1 & 0 & 1/2 & 0 \\ 0 & 1 & 2 & -1 \end{array}\right]$

$$A^{-1} = \begin{bmatrix} 1/2 & 0 \\ 2 & -1 \end{bmatrix}$$

Example 2:

Exercise: Decrypt VKFZRVWTIAZSMISGKA using the same key as above.

using Key= $\begin{pmatrix} 11 & 8 \\ 3 & 7 \end{pmatrix}$

→ to decrypt a message using Hill cipher we use the formula

$$m = c\,k^{-1}$$

k^{-1} ⇒ Exists if $\det(A) \neq 0$.

$k^{-1} \Rightarrow \begin{pmatrix} 7 & 18 \\ 23 & 11 \end{pmatrix}$

0 6 12
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.
19 25

$VK = \langle 21, 10 \rangle \begin{pmatrix} 7 & 18 \\ 23 & 11 \end{pmatrix} \Rightarrow (377, 1889)$

$\Rightarrow \langle 13, 20 \rangle \Rightarrow NU$

using an algorithm

Modular inverse of a Matrix

The inverse of a matrix mod n is

$$AA^{-1} \equiv I \mod n$$

To calculate A^{-1} we need

- $\det(A) = ad - bc$
- $\gcd(\det(A), n) = 1$
- $(\det(A))^{-1} \mod n$
- $Adj = \begin{pmatrix} d & -b \\ -c & a \end{pmatrix}$

With that information

$$A^{-1} = \det(A)^{-1} \, Adj \mod n$$

Steps:

→ $\gcd(\det A, n) = 1$

→ $\det A = (ad) - (bc)$

→ Use euclides algorithm

→ $A^{-1} = \frac{1}{\det(A)} \, Adj(A) \mod m$

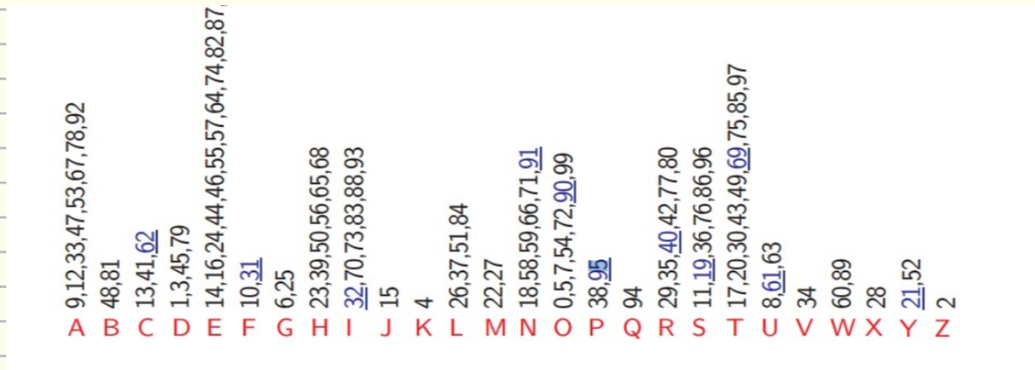
Example:

Homophonic Substitution Ciphers

A homophonic substitution ciphers are algorithms where each letter has many ways to be

translate. That is a powerful key to reduce the frecuency analysis of the words.

Example:



Using the layout encrypt the message

crypto is fun

→ A posible message can be.

13 29 21 38 70 32 29 10 8 18

Example #2

13 5 26 0 22 81 88 47

COLOMBIA

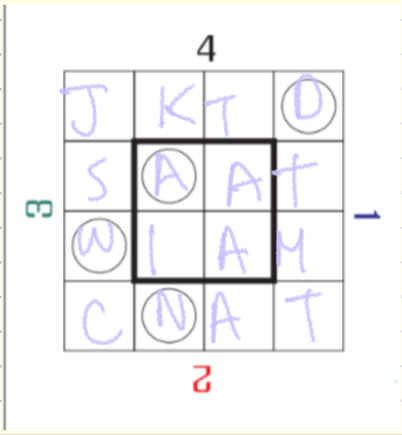
Transposition Cipher

Instead of change letters with others, the transposition algorithms change the positon of the letters, to write message.

Turning Grille

Using this grill we can get the message

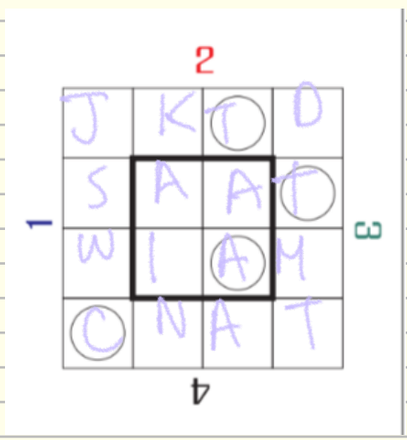
"JIM ATTACKS ÁT DAWN"



Then the message is

J K TO S A A T W I A M C N A T

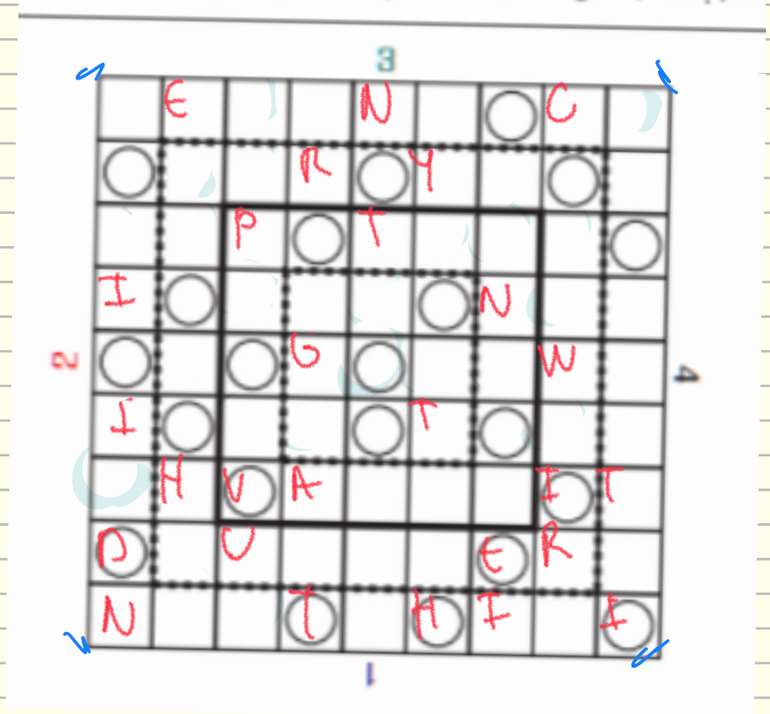
TO decrypt we can use the same grill in reverse way



JIM ATTACK AT DAWN

Example #2

~~TESHN INCIG LSRGY LRIUS PITSA TLILM REENS ATTOG~~
~~SIAWG IPVER TOTEH HVAEA XITDT UAIME~~ RANPM TLHIE I



The message is

THIS IS A MESSAGE
THAT I AM SILLUS TRATIVEEXAMPLE
NO GRILLE TO

Permutation and Substitution Ciphers

Notation

↳ E_K: Encryption function E using key k

→ E_K^{-1}: Decryption function E^{-1} using key k

→ m: message

→ IV : Initialization Vector

→ >> : shift to right

↳ ⊕→ : Encryption

↳ ←⊕ : Decryption

Electronic Code Block (ECB)

Let E_π be a permutation cipher, and $\mathcal{A} = \{0, 1\}$.

$E_\pi = \{0, 1\}^4 \to \{0, 1\}^4$, $\pi = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 4 & 1 \end{pmatrix}$

Encrypt the plaintext m = 101100010100101.

→ It's a permutation

move the bits of characters in diferent positions

substitution

substitute the bits of character by others

It's the length to divide the message in cipher blocks

m_1 : 1011 → $c_1 = E_\pi(m_1)$ → 0111

m_2 : 0001 → $c_2 = E_\pi(m_2)$ → 0010

m_3 : 0100 → $c_3 = E_\pi(m_3)$ → 1000

m_4 : 1010 → $c_4 = E_\pi(m_4)$ → 0101

Group all c_i

C = 0111 0010 1000 0101

1101

E_π (011)

→ 110

110

↳ 011

INPUT: $m,\ k \quad \{m = m_1, m_2, \ldots, m_t,\ |m_i| = n\}$

1 (⊕→) $c_j \leftarrow E_k(m_j) \quad \forall j \in \{1 \ldots t\}$

2 (←⊕) $m_j \leftarrow E_k^{-1}(c_j) \quad \forall j \in \{1 \ldots t\}$

Cipher-Block Chaining

INPUT: $m,\ k,\ IV \quad \{m = m_1, m_2, \ldots, m_t,\ |m_i| = |IV| = n\}$

1 $(\mapsto)$ $c_0 \leftarrow IV;\ c_j \leftarrow E_k(c_{j-1} \oplus m_j) \quad \forall j \in \{1 \ldots t\}$

2 $(\leftarrow)$ $c_0 \leftarrow IV;\ m_j \leftarrow c_{j-1} \oplus E_k^{-1}(c_j) \quad \forall j \in \{1 \ldots t\}$

The cipher-block chaining is similar to ECB but with the XOR operation. That means, there isn't a pattern in case of similar message because depends on the context (vector inizial)

$E_\pi = \{0,1\}^4 \rightarrow \{0,1\}^4,\ \pi = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 4 & 1 \end{pmatrix}$

Encryption:

$m_1 = 1011,\ m_2 = 0001,\ m_3 = 0100,\ m_4 = 1010$

Let IV = 1010

C_0 = IV = 1010

The operation is XOR = $\oplus$

Permutation

$c_0 = E_\pi(C_0 \oplus m_0)$

$m_0 : 1011 \rightarrow c_0 = E_\pi(1010 \oplus 1011) \Rightarrow E_\pi(0001) \Rightarrow 0010$

$m_1 : 0001 \rightarrow c_1 = E_\pi(0010 \oplus 0001) \Rightarrow E_\pi(0011) \Rightarrow 0110$

$m_2 : 0100 \rightarrow c_2 = E_\pi(0110 \oplus 0100) \Rightarrow E_\pi(0010) \Rightarrow 0100$

$m_3 : 1010 \rightarrow c_3 = E_\pi(0100 \oplus 1010) \Rightarrow E_\pi(1110) \Rightarrow 1101$

$C = 0010\ 0110\ 0100\ 1101$

Decryption: $m_j = c_{j-1} \oplus E_\pi^{-1}(c_j)$

$C_0 = 1010,\ c_1 = 0010,\ c_2 = 0110,\ c_3 = 0100,\ c_4 = 1101$

$m_1 : 0010 \rightarrow c_1 = 1010 \oplus E^{-1}(0010) \Rightarrow 1010 \oplus 0001 \Rightarrow 1011$

$m_2 : 0110 \rightarrow c_2 = 1011 \oplus E^{-1}(0110) \hookrightarrow 1011 \oplus 0011$

$m_3 : 0100 \rightarrow$