Introduction To Cryptography

Hello!

I am Mokrane Abdelmalek

2nd Year Computer Science Student .

CTF player @ShellSec & @CyberErudites

1. First Step into Cryptography

What is Cryptography?

“ Cryptography is the set of methods and tools that ensure a secure transmission and communication between two entities

Terminology

- **Cipher PlainText$\longrightarrow$ CipherText**
- **Cryptosystem**
- **Cryptanalysis**

Cryptography Objectives

Authentication

Integrity

Non Repudiation

Confidentiality

Why So Important ?

Most Vulnerabilities are Cryptography based

Cryptography are used everywhere

Once learned you can be secure

Learning How to exploit Systems

Art To Exploit

The Most Important Thing is
To Learn How to Exploit A
cryptography System

2.Types of cryptography

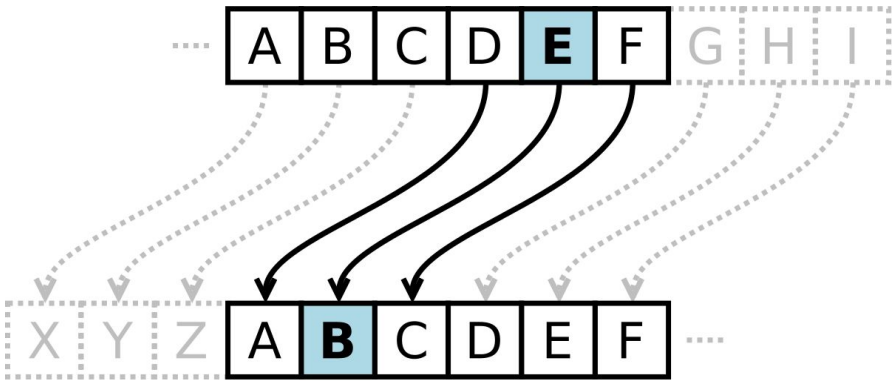
I.Classical cryptography

II.Modern cryptography

I . Classical cryptography

Caesar Cipher

Shift each letter of plaintext with a given **Key**



Specifications:

- Very simple
- Easy to break

Break Me This

Z yrmv cvrievu yfn kf sivrb Trvjri Tzgyvi !!!

Substitution Cipher

Replace each letter with its corresponding new value

Specifications:

- Very simple
- Needs some time to break

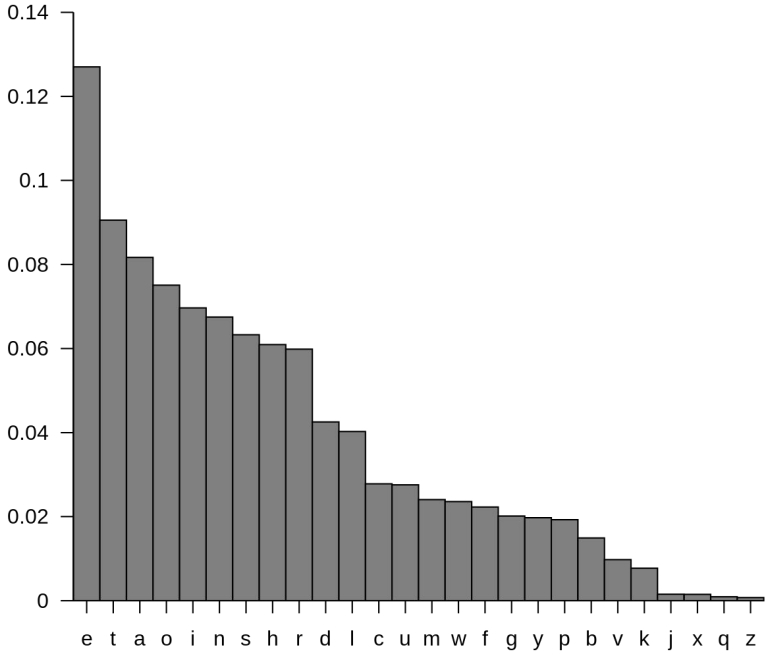
CIPHER ALPHABET

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

Figure 1

How to break IT?

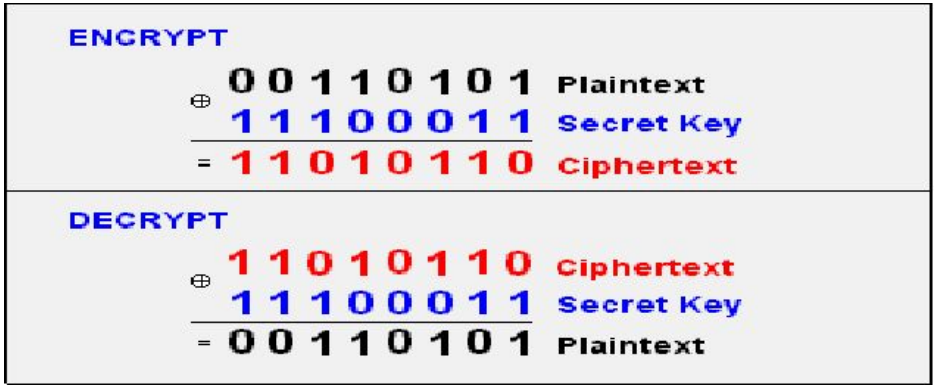
Frequency Analysis



Xor Operator

Xor is reversible that is why it is widely used

Input		Output
A	B	A xor B
0	0	0
0	1	1
1	0	1
1	1	0



Encodings

What are encodings ?

Encoding Examples

BASE 64

Index	Binary	Char	Index	Binary	Char	Index	Binary	Char	Index	Binary	Char
0	000000	A	16	010000	Q	32	100000	g	48	110000	w
1	000001	B	17	010001	R	33	100001	h	49	110001	x
2	000010	C	18	010010	S	34	100010	i	50	110010	y
3	000011	D	19	010011	T	35	100011	j	51	110011	z
4	000100	E	20	010100	U	36	100100	k	52	110100	0
5	000101	F	21	010101	V	37	100101	l	53	110101	1
6	000110	G	22	010110	W	38	100110	m	54	110110	2
7	000111	H	23	010111	X	39	100111	n	55	110111	3
8	001000	I	24	011000	Y	40	101000	o	56	111000	4
9	001001	J	25	011001	Z	41	101001	p	57	111001	5
10	001010	K	26	011010	a	42	101010	q	58	111010	6
11	001011	L	27	011011	b	43	101011	r	59	111011	7
12	001100	M	28	011100	c	44	101100	s	60	111100	8
13	001101	N	29	011101	d	45	101101	t	61	111101	9
14	001110	O	30	011110	e	46	101110	u	62	111110	+
15	001111	P	31	011111	f	47	101111	v	63	111111	/

SGVsbG8gV29ybGQ=

Hexadecimal

68656c6c6f20776f726c64

Morse Code

A a	•▬	J j	•▬▬▬	S s	•••
B b	▬•••	K k	▬•▬	T t	▬
C c	▬•▬•	L l	•▬••	U u	••▬
D d	▬••	M m	▬▬	V v	•••▬
E e	•	N n	▬•	W w	•▬▬
F f	••▬•	O o	▬▬▬	X x	▬••▬
G g	▬▬•	P p	•▬▬•	Y y	▬•▬▬
H h	••••	Q q	▬▬•▬	Z z	▬▬••
I i	••	R r	•▬•		

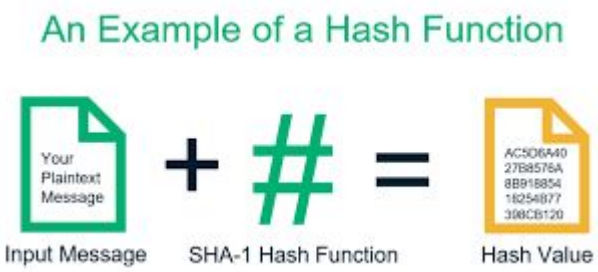
Hash Functions

One way to go

Encoding Examples

One Way function

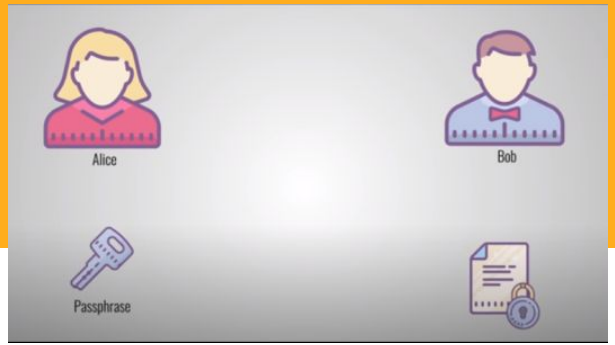
A function that takes message as input and give a supposedly unique output
f(x) = Y



Known Hash Algorithms

m="admin"
md5(m) = 21232f297a57a5a743894a0e4a801fc3 - 32 hex
sha1(m) = d033e22ae348aeb5660fc2140aec35850c4da997 - 40 hex
sha256(m) = 8c6976e5b5410415bde908bd4dee15dfb167a9c873fc4bb8a81f6f2ab448a918 - 64 hex

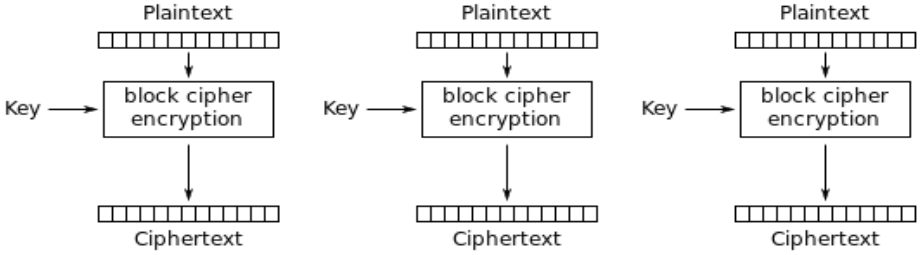
II. Symmetrical cryptography



Advanced Encryption Standard “AES”

- The most widely used symmetric cipher today
- A block cipher which operates on block size of 128 bits (16 bytes) for both encrypting and decrypting

  There are multiple modes : ECB,CBC,CTR ..

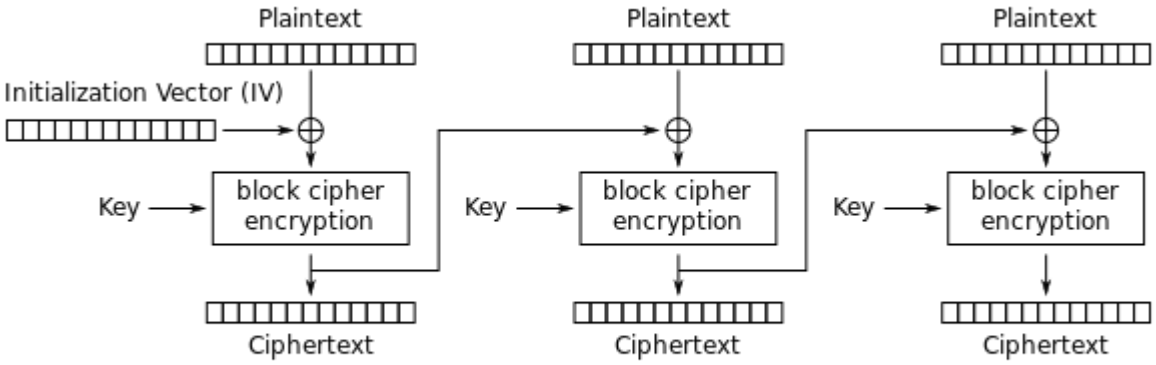


Electronic Codebook (ECB) mode encryption

Advanced Encryption Standard “AES”

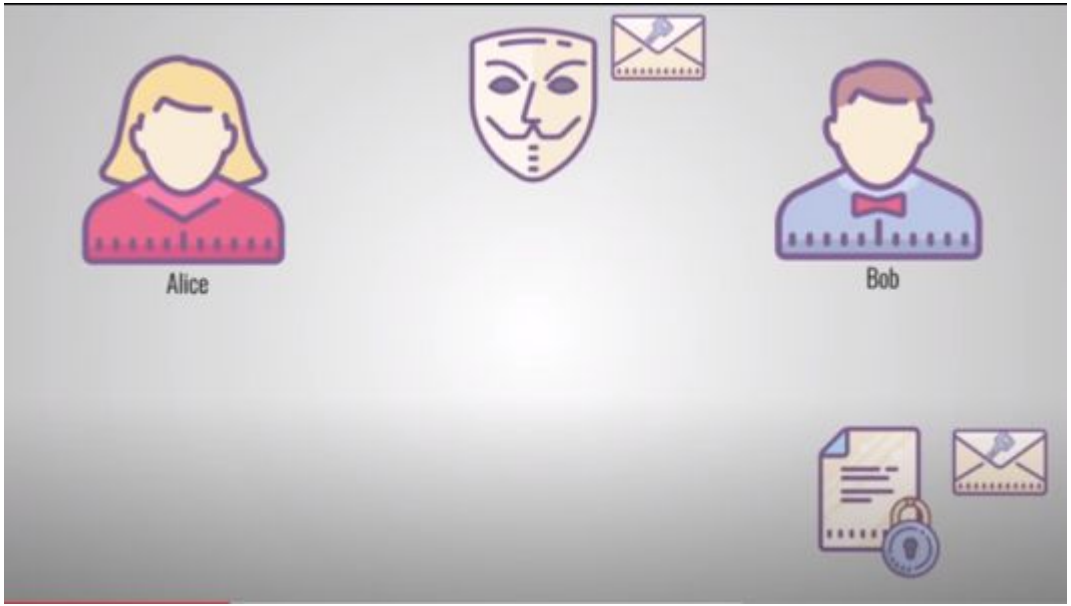
CBC mode is like ECB mode but with an additional key:

IV , which will initiate the xor of the blocks



Cipher Block Chaining (CBC) mode encryption

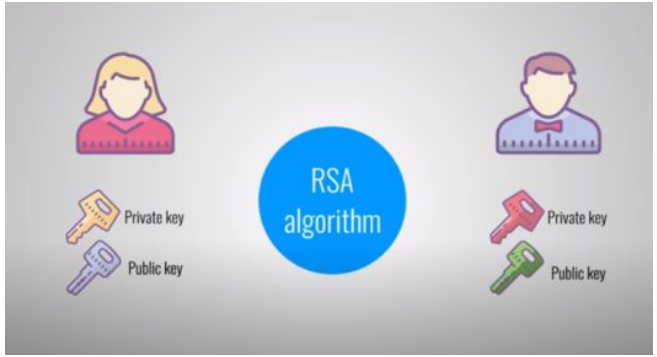
But there is an issue



II. Asymmetrical cryptography

RSA

- The most famous algorithm in Public key cryptography
- It's Math based operations (power,modular Inverse, GCD,Euler toTient)
- It has 2 keys (private and public)
- We use the public key to encrypt
- and the private one to decrypt
- It lies on the factorization problem



RSA

To generate RSA keys :

- **p** and **q** are prime numbers.
- **N** :the modulus is the product of p and q.
- **phi**(N) = (p-1)*(q-1) Euler totient
- **e**:public exponent (it has to be prime with phi)
- **d**: private exponent ((e**d)% phi == 1)

public_key = (N,e)

private_key = (N,d)

ciphertext = (**plaintext** ** e)%N

plaintext = (**ciphertext** ** d)%N

What is next ?

What should we do next !

Learning Resources

- **CryptoHack** best website to learn cryptography
- **Rootme** Best website to learn cybersecurity and specially to get started
- **Cryptopals** A website filled with good cryptography resources and it contains a numerous number of ciphers
- **CTFTime** To checkout the writeups of old crypto challenges
- **Coursera** course of Cryptography 1 and Cryptography 2

Thanks!

Any questions?

You can find me at:

- fb.com/m0kr4n3
- twitter.com/m0kr4n3
- jm_abdelmalek@esi.dz