Shafee Shadman Tonoy

Former President, MIST Cyber Security Club

Founder, MIST_Shaheed_Yamin_Forever

facebook.com/shafee.shadman.tonoy

What is Cryptography?

Cryptography derived its name from a Greek word called "Kryptos" which means "Hidden Secrets".

1. Cryptography is the practice and study of hiding information.
2. It provides Confidentiality, Integrity, Accuracy

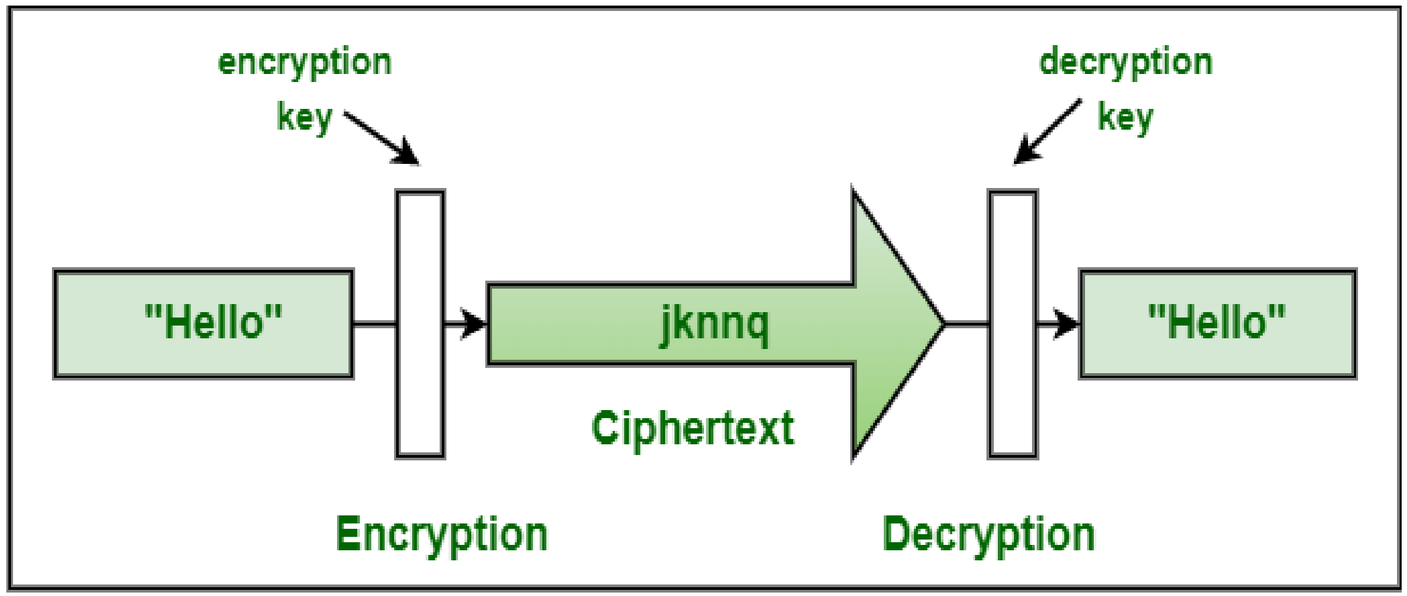
Cryptography

Cryptography is process to secure your information from unauthorise access.

Encrypted **501393c26075af84b9e612b5d90b4cff790ce10c**

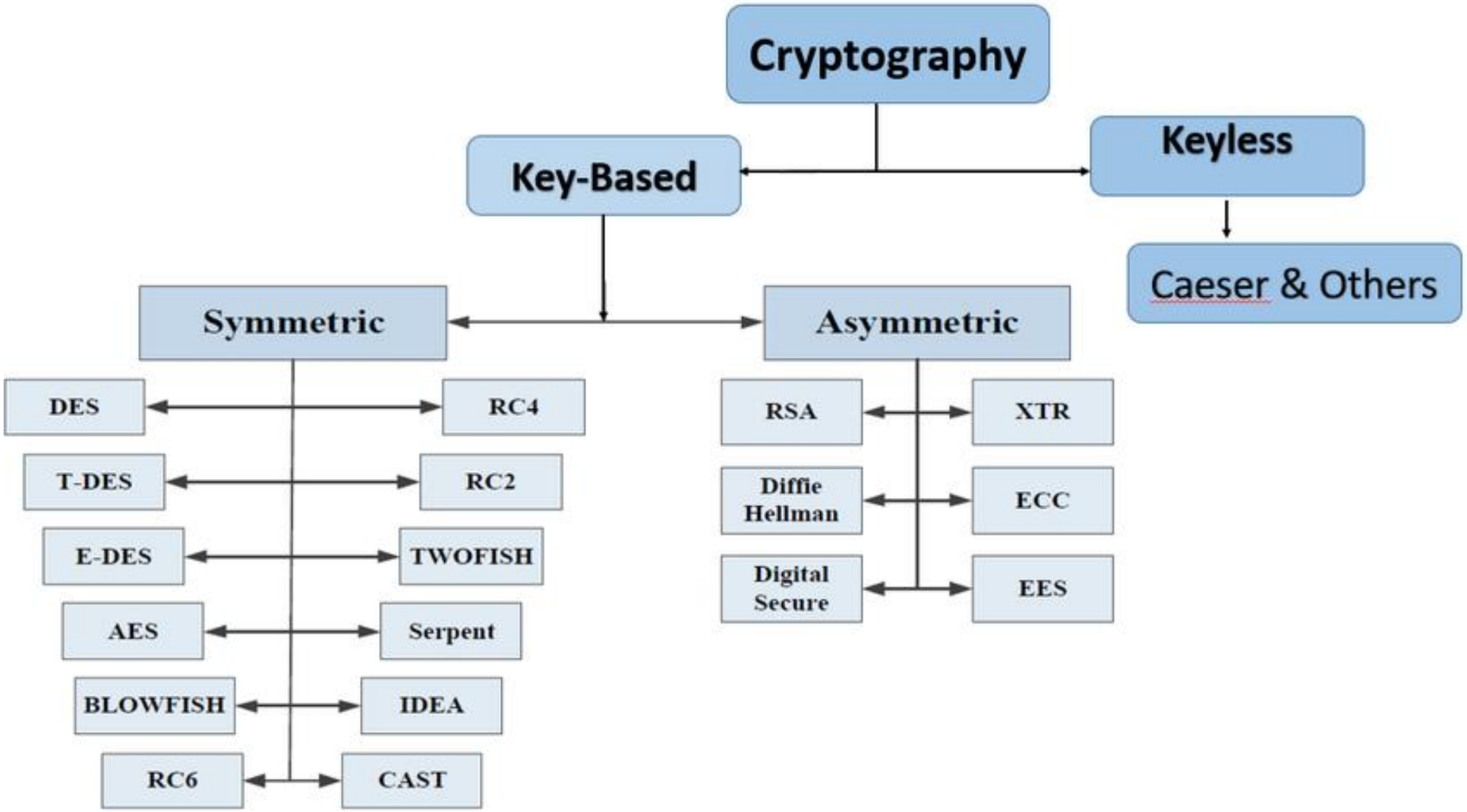
Decrypted **Hello_NSU_Hackers**

Encryption & Decryption



Cryptography

What are the Types of Cryptography



Some Common Cryptography

Example

- Caesar Cipher
- Rot 13
- Vigenere Cipher
- Morse code
- Bacon Cipher
- Alphabetical substitution

Tools

- Cyberchef
- dcode.fr
- boxentriq.com
- cryptii.com

Symmetric Cryptography

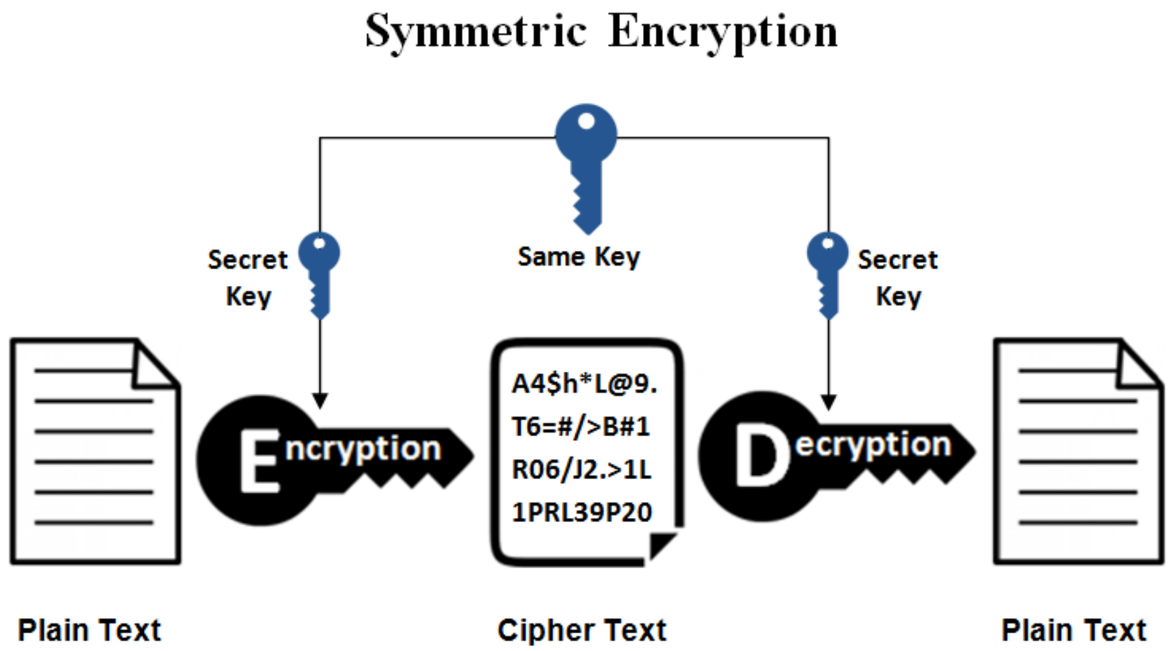
Symmetric cryptography is type of cryptography where both sender and receiver use same private key.

Advantage:

Simpler and Faster

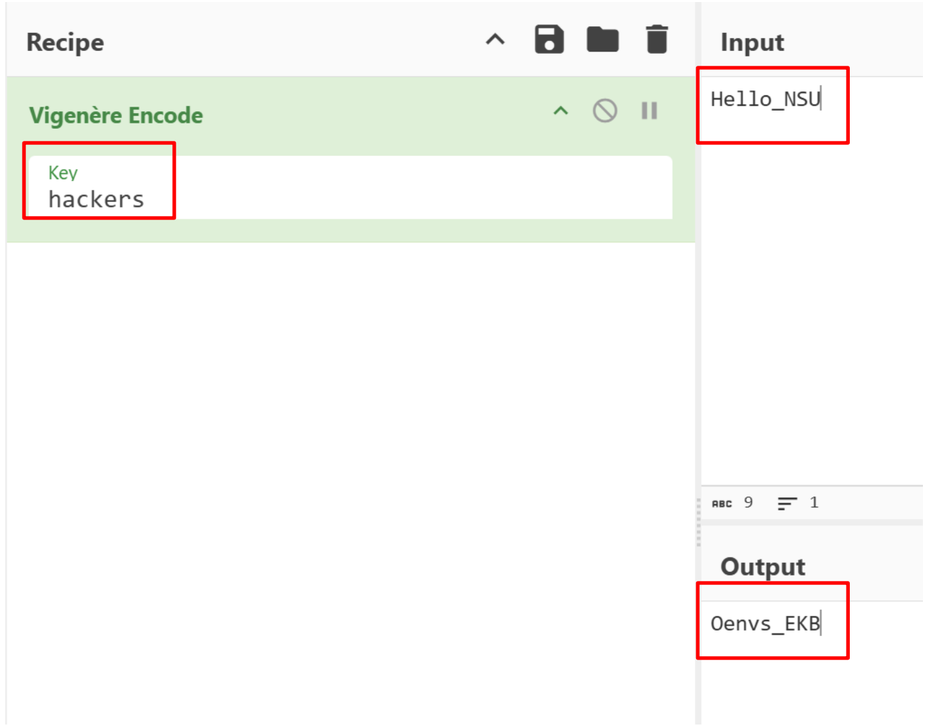
Disadvantage:

Less Secured

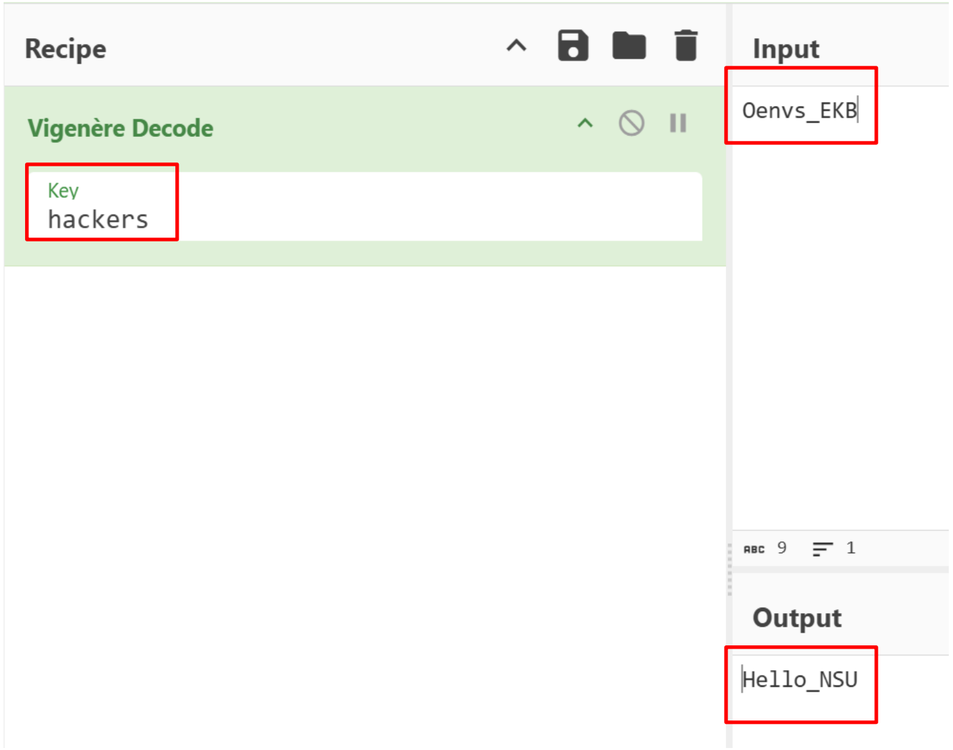


Symmetric Cryptography

Example



Encrypt

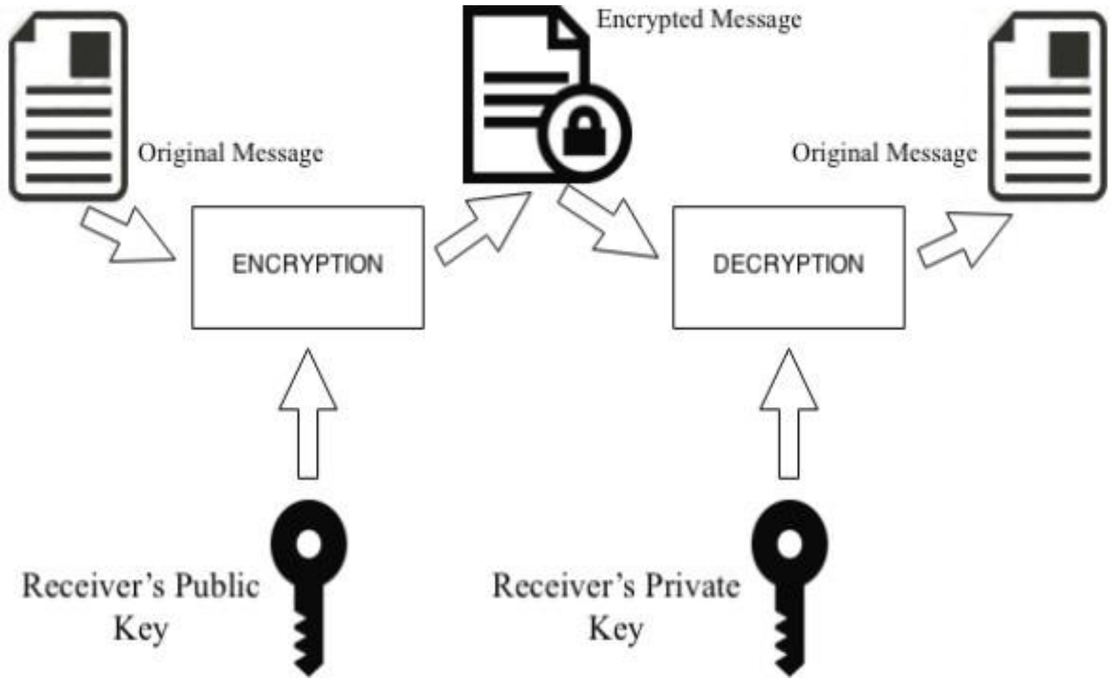


Decrypt

Asymmetric Cryptography

Use public and private key:

- Public key use for encryption
- Private key use for decryption



Advantage:

1. More Secured
2. Authentication

Disadvantage:

1. Relatively Complex

Asymmetric Cryptography

Example

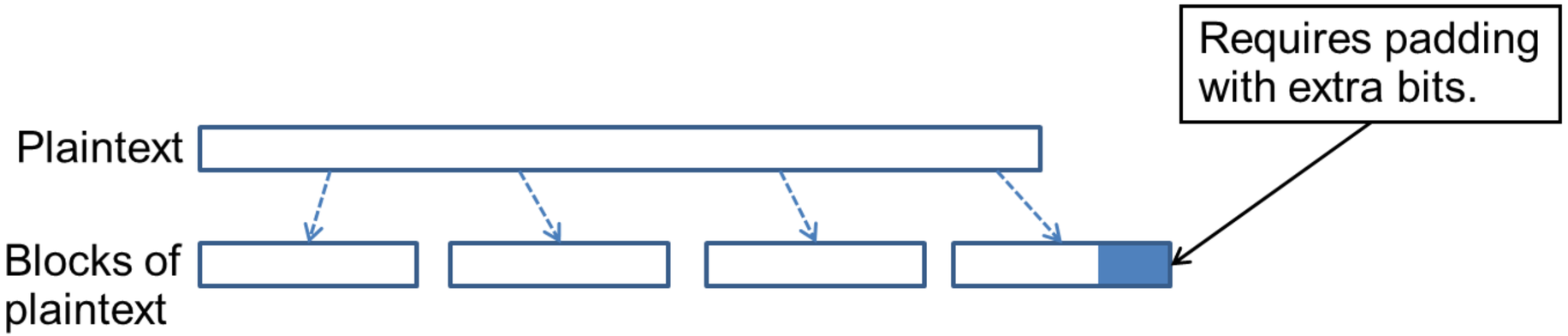
- RSA Algorithm
- Diffie-Hellman
- Elliptic Curve (ECC)

Tools

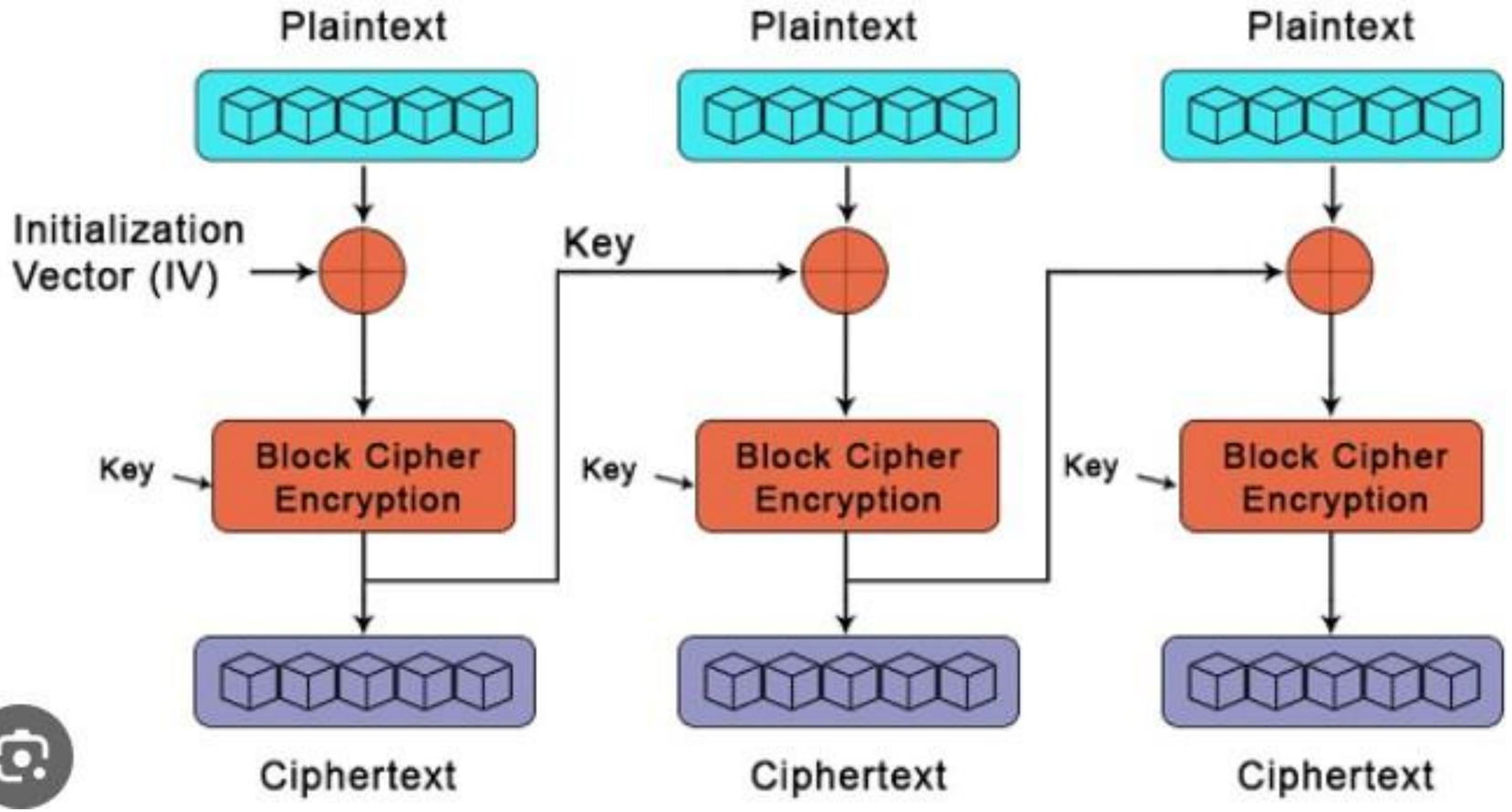
- Python code
- openssl (Default on Kali Linux OS)
- Online Tools

Block Ciphers

- In a **block cipher:**
  - Plaintext and ciphertext have fixed length b (e.g., 128 bits)
  - A plaintext of length n is partitioned into a sequence of m **blocks**, P[0], …, P[m–1], where $n \leq bm < n + b$
- Each message is divided into a sequence of blocks and encrypted or decrypted in terms of its blocks.



Block Cipher



Paddings

- Block ciphers require the length n of the plaintext to be a multiple of the block size b
- Padding the last block needs to be unambiguous (cannot just add zeroes)

Where are block ciphers used

Data Encryption Standard (DES) → 64-bit blocks & 56-bit keys

Triple DES (3DES)

- **Nested application of DES with three different keys KA, KB, and KC**
- **Effective key length is 168 bits, making exhaustive search attacks unfeasible**

Advanced Encryption Standard (AES) → 128-bit blocks
key lengths: 128, 192 & 256 bits

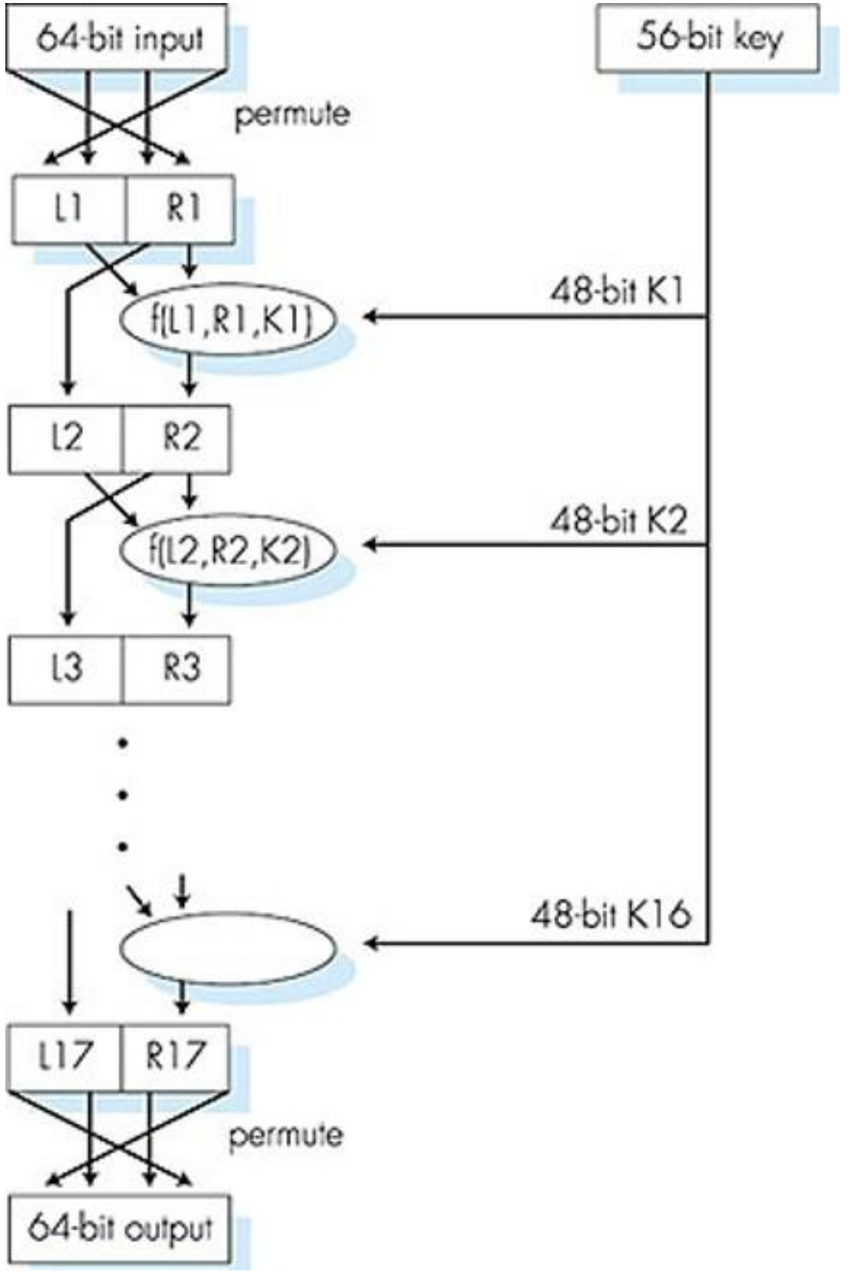
Symmetric key crypto: DES

DES operation

initial permutation

16 identical "rounds" of function application, each using different 48 bits of key

final permutation

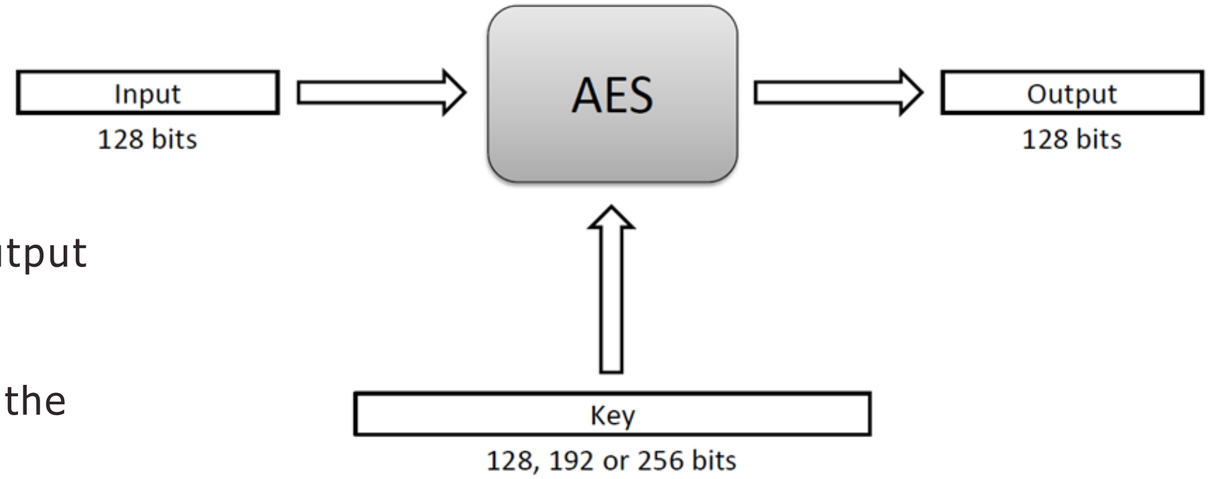


Advanced Encryption Standard (AES)

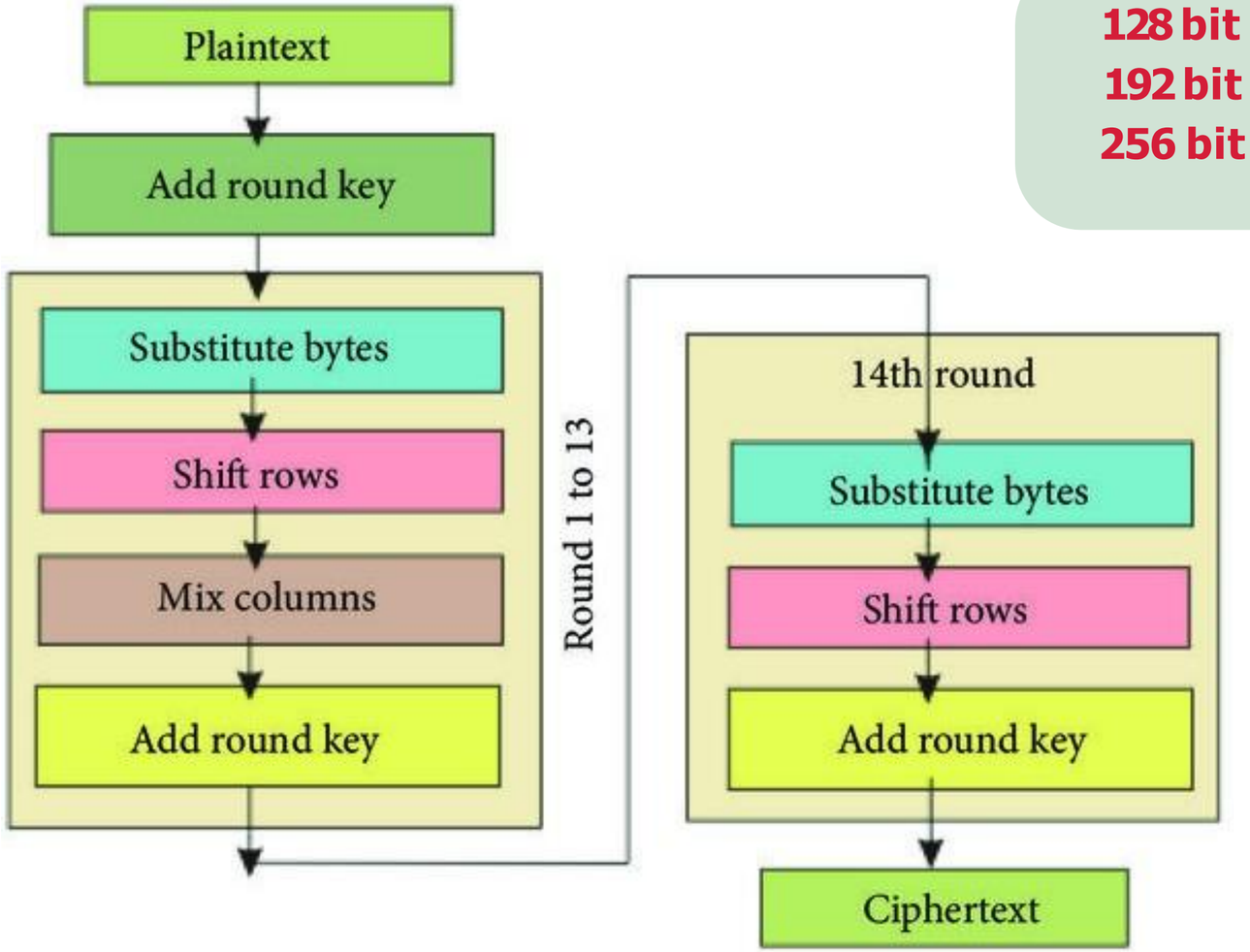
- Block-based symmetric encryption
- input is chunked into blocks of 16, 24, or 32 bytes (128, 192, 256 bits)

Multiple modes

- ECB
  - Flaw: same input block results in the same output block
- CBC
  - Flaw: malleable. XOR on the ciphertext XORs the plaintext when decrypted
- CTR
- GCM
- …many more



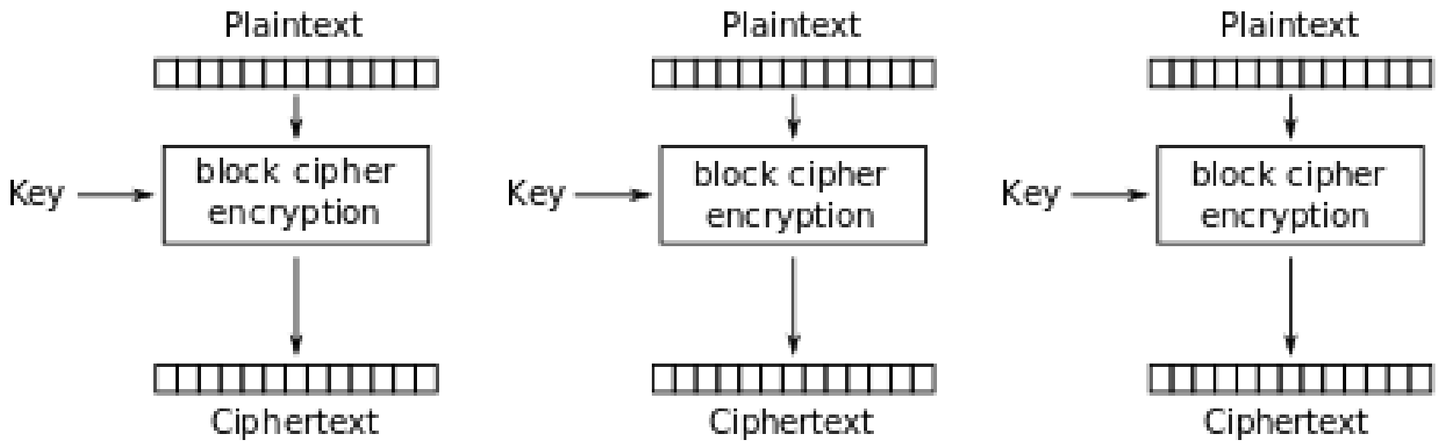
AES Round Structure



128 bit key – 10 rounds
192 bit key – 12 rounds
256 bit key – 14 rounds

ECB Mode

- Electronic Code Book (ECB) Mode (is the simplest):
  - Block P[i] encrypted into ciphertext block $C[i] = E_K(P[i])$
  - Block C[i] decrypted into plaintext block $M[i] = D_K(C[i])$



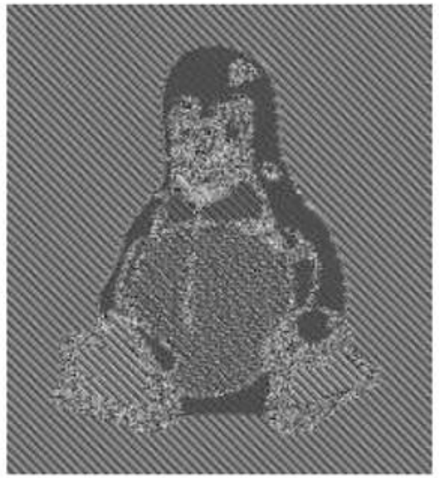
Electronic Codebook (ECB) mode encryption

Strengths & Weaknesses of ECB

- Strengths:
  - Is very simple
  - Allows for parallel encryptions of the blocks of a plaintext
  - Can tolerate the loss or damage of a block

- Weakness:
  - Documents and images are not suitable for ECB encryption since patters in the plaintext are repeated in the ciphertext:

(a)



(b)

RSA

RSA (Rivest-Shamir-Adleman) is a public-key cryptosystem that is widely used for secure data transmission.

RSA: Choosing keys

1. Choose two large prime numbers p, q. (e.g., 1024 bits each)
2. Compute $n = pq$, $z = (p-1)(q-1)$
3. Choose e (with $e<n$) that has no common factors with z. (e, z are "relatively prime").
4. Choose d such that $ed-1$ is exactly divisible by z. (in other words: $ed \bmod z = 1$).
5. *Public* key is (n,e). *Private* key is (n,d).

K_B^+ K_B^-

RSA: Encryption & Decryption

0. Given (n,e) and (n,d) as computed above

1. To encrypt bit pattern, m, compute

   $c = m^e \bmod n$ (i.e., remainder when m^e is divided by n)

2. To decrypt received bit pattern, c, compute

   $m = c^d \bmod n$ (i.e., remainder when c^d is divided by n)

Magic happens!

$$m = (\underbrace{m^e \bmod n}_{c})^d \bmod n$$

RSA Cryptography
Example

Bob chooses *p=5*, *q=7*. Then *n=35*, *z=24*.

e=5 (so *e*, *z* relatively prime).

d=29 (so *ed-1* exactly divisible by z).

encrypt:

letter	m	m^e	$c = m^e \bmod n$
l	12	1524832	17

decrypt:

c	c^d	$m = c^d \bmod n$	letter
17	48196857210675091509141182522307169 7	12	l

RSA Algorithm

RSA Basic Term:

1.Choose **two prime numbers p, q**

2. Multiply**, n= p * q**

3. **phi(n) = (p-1) (q-1)**

4. Generate Public key, Choose an **integer number e** --- **where 1 < e <phi(n) and e is co-prime of phi(n**)

- 5. Generate Private key, Compute **d** to satisfy, (d * e) MOD phi(n) = 1

d = inverse(e, phi) ----------python code

Note :

For Publice key:

- **1. Must be prime number**
- **2. Must be less than phi(n)**
- **3. NOT be a factor of phi(n)**

RSA Cryptography

Encrypt Message :

Public key is (n = 3233 , e = 17)

suppose, m = 123

So, Cipher **$c = m^e \bmod n$**

$= 123^{17} \bmod 3233$

$= 855$

Decrypt Message :

Private Key is (n=3233 ,d = 2753)

$m = C^d \bmod n$

$= 855^{2753} \bmod 3233$

$= 123$

Encrypt:

$C = m^e \bmod n$

Here, C → Cipher text

m → Message

Decrypt:

$M = C^d \bmod n$

THANK YOU