Lecture 3 🪴

> **Class**: Implementing Confidentiality
>
> **Date**: 16.22 AM , 10 Nov
>
> **Author**: Lasal Hettiarachchi

Key learnings:

- Cryptography
- Symmetric key , Asymmetric key encryption
- DES , Tripple DES, AES
- RSA , PDP

Encryption

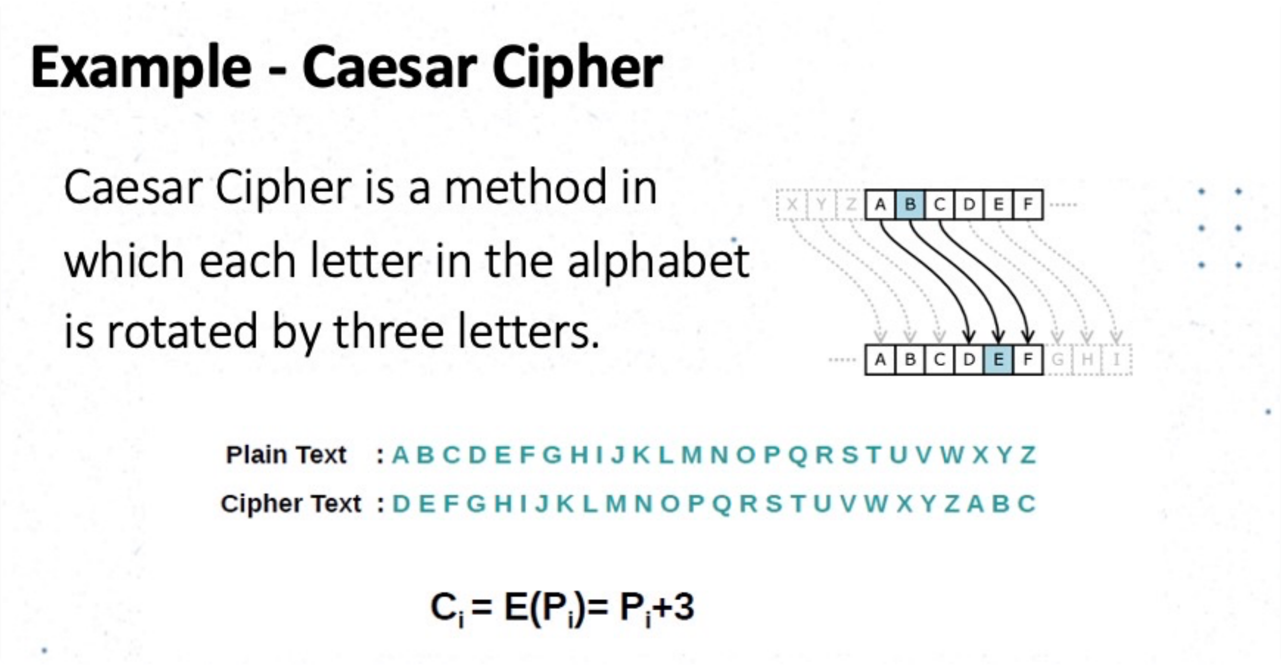
- Cryptography → Encryption
- Only the intended recipients can get the data
- Security through obscurity: Keeping the security by not knowing the principles of how the system is secured
- Kirchoff principle: The cryptography system should be secure eventhough everything about the system other than the key is known

Key phrases

- Plain text: Original message intended for the recipient
- Encryption : The process of converting plain text to cipher text
- Cipher text: The converted message which is uncreadabble
- Decryption : The process of converting cipher text to plain text

In kirchhoff: both encryption algorithm and decryption algorithm is widely known

Ceasar Cipher



Example - Caesar Cipher

Caesar Cipher is a method in which each letter in the alphabet is rotated by three letters.

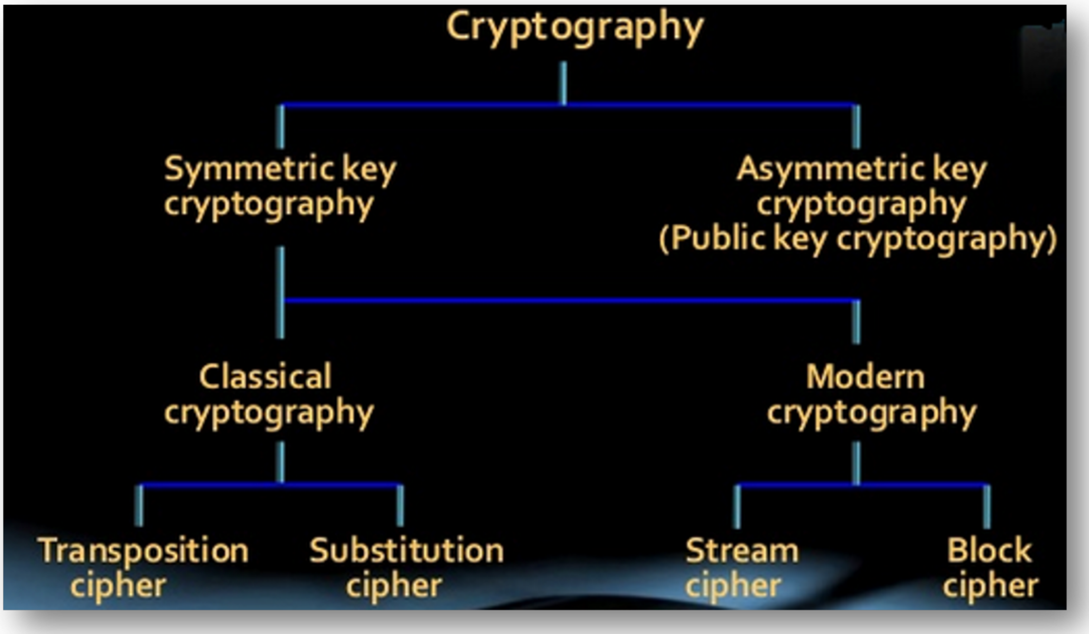
X Y Z A B C D E F
A B C D E F G H I

Plain Text : 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

Cipher Text : 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

$$C_i = E(P_i)= P_i+3$$

Classification



Cryptography

Symmetric key cryptography

Asymmetric key cryptography (Public key cryptography)

Classical cryptography

Modern cryptography

Transposition cipher

Substitution cipher

Stream cipher

Block cipher

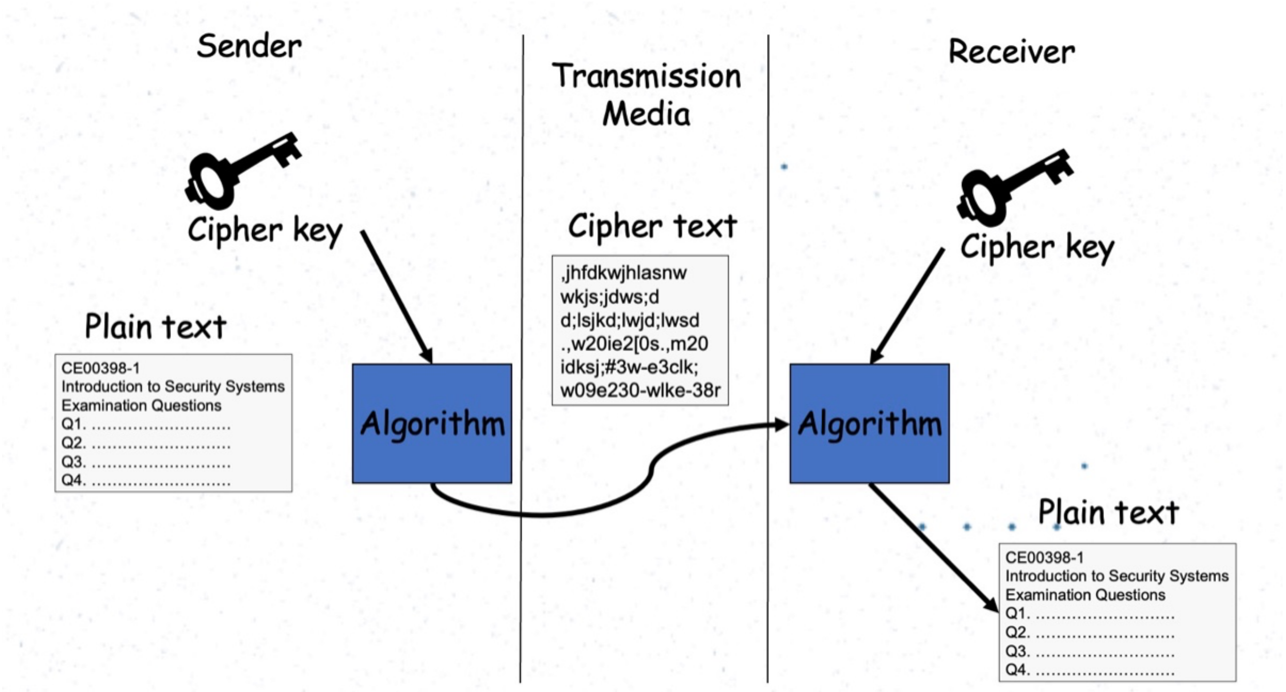
Symmetric key : For both encryption and decryption the same key is used.

Asymmetric key: Public key cryptography

Modern → Stream : if 0,1 s are fed into the algorithm as a stream

Modern → Block : if the input is split in to blocks of 0,1 s and fed into the algorithm.

Symmetric key: Classical Cryptography


Sender
Transmission Media
Receiver
Cipher key
Plain text
CE00398-1
Introduction to Security Systems
Examination Questions
Q1. ....
Q2. ....
Q3. ....
Q4. ....
Algorithm
Cipher text
,jhfdkwjhlasnw
wkjs;jdws;d
d;lsjkd;lwjd;lwsd
.,w20ie2[0s.,m20
idksj;#3w-e3clk;
w09e230-wlke-38r
Cipher key
Algorithm
Plain text
CE00398-1
Introduction to Security Systems
Examination Questions
Q1. ....
Q2. ....
Q3. ....
Q4. ....

- Cipher text and key are sent to the reciever.
- The key shouldnt be compramised.
- Sender has encryption Algorithm
- Reciever has decryption Algorithm

Classical Cryptography : Substitution Ciphers

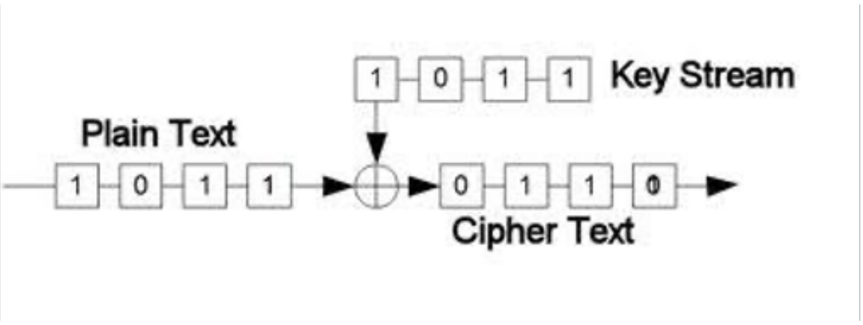
- Obtain a key for the algorithm, then shift the alphabet.
- Ceaser cipher , Kamasutra
- Since a letter is changed to a single letter, they are easy to decrypt
- ex: A → Z awlways

Classical Cryptography : Transposition Ciphers

- The order of the Characters is shifted. Letters dont change
- ex: scytale cipher

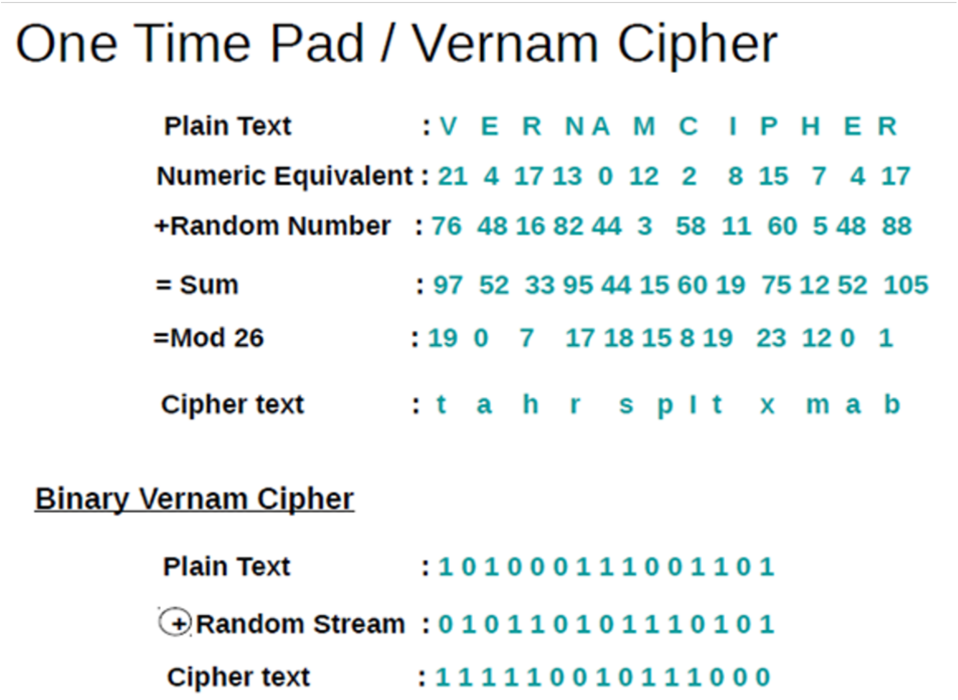
Modern Cryptography : Stream Ciphers

- Encrypt a single bit at a time
- Stream of 0,1 → different stream of 0,1
- Key stream should be of infinite in length(atleast the size of the input)



- Extremely Secure
- But the overhead is high cause the key stream must be generated
- The overhead is not in the engryption or decryption but in the random number generation of the key stream

ex:



One Time Pad / Vernam Cipher

Plain Text	: V E R NA M C I P H E R
Numeric Equivalent	: 21 4 17 13 0 12 2 8 15 7 4 17
+Random Number	: 76 48 16 82 44 3 58 11 60 5 48 88
= Sum	: 97 52 33 95 44 15 60 19 75 12 52 105
=Mod 26	: 19 0 7 17 18 15 8 19 23 12 0 1
Cipher text	: t a h r s p l t x m a b

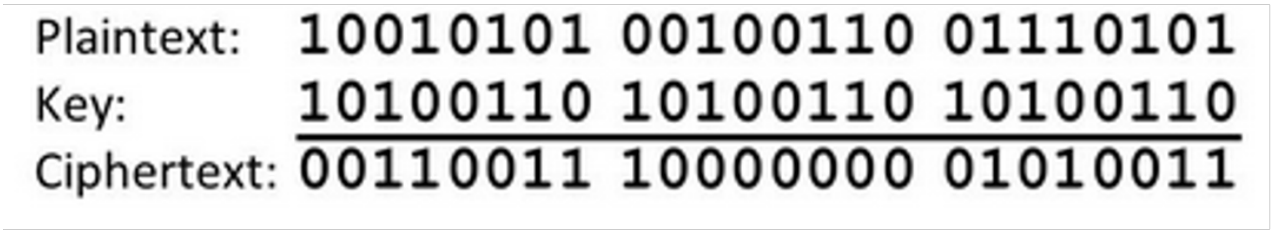
Binary Vernam Cipher

Plain Text	: 1 0 1 0 0 0 1 1 1 0 0 1 1 0 1
$\oplus$**Random Stream**	: 0 1 0 1 1 0 1 0 1 1 1 0 1 0 1
Cipher text	: 1 1 1 1 1 0 0 1 0 1 1 1 0 0 0

- Pros – Fast, Low error propagation
- Cons – Less Diffusion, Susceptible to malicious inserts and modifications

Modern Cryptography : Block Ciphers.

- Encrypt one block of text at a time
- Key is typically of 62,128,256 bits

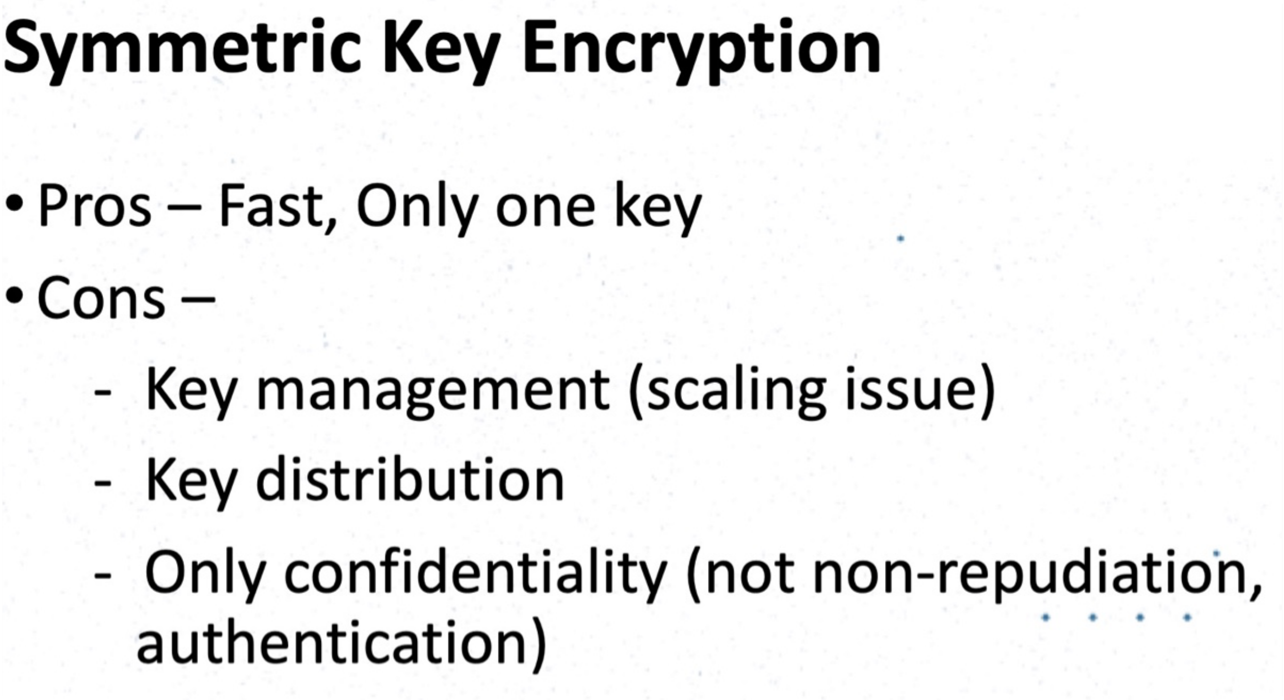


Plaintext:	10010101 00100110 01110101
Key:	10100110 10100110 10100110
Ciphertext:	00110011 10000000 01010011

- Key doesnt change

both modern and asymetric are used with binary data

- Pros – Diffusion, Immunity to insertion
- Cons – Error propagation, slow



Symmetric Key Encryption

- Pros – Fast, Only one key
- Cons –
  - Key management (scaling issue)
  - Key distribution
  - Only confidentiality (not non-repudiation, authentication)

Asymmetric key

- In symmetric key 2 way communication is allowed since the key can be used for both encryption and decryption
- Buy asymmetric key can be allowed only one way communication
- Two keys generated, one used with decryption algorithm (private key) and one with encryption algorithm (public key).
- Generation of private key, given public key is computationally hard.
- Does not need secure key transmission mechanism for key distribution.
- mechanism: Assume that I want to build a comminication with the class. I generate 2 keys, private and public and share the public key with the class. The students can use the public key to encrypt a message and send the encrypted message to me. Then when I want to decrypt it, it can only be done by the private key. In a similar way if I need to communicate with the class.
- The key used are related to each other mathematically
- The key used are related to each other mathematically

Practical Cryptography

- Symmetric overhead is much less but a mechanism needed to share the key
- Asymmetric overhead is much more.

- Solution :
  - Use symetric for actual message
  - Use asymetric for key share

- Confusion – Interceptor should not be able to predict how changing one character in plaintext will change the ciphertext(shouldnt be able to use know encrpyted messages to get the key. Although both cipher text and plain text are known shouldnt be able to deduce the key)
- Diffusion – The characteristic of distributing the plaintext over the entire ciphertext(How plain text letters are spead over the cipher text)

Unconditiional vs Computational Security

- Unconditional: Cipher cannot be broken irrespective of computer power and time
- Computational: Cipher can be broken using a brute force attack. However, it would take a very (very) long time to do so. Figure out the threats and try to find solutions to threats.
- Computational security are different organization wise. Computational security for me vs Computational security for FBI head are different

Digital Signatures

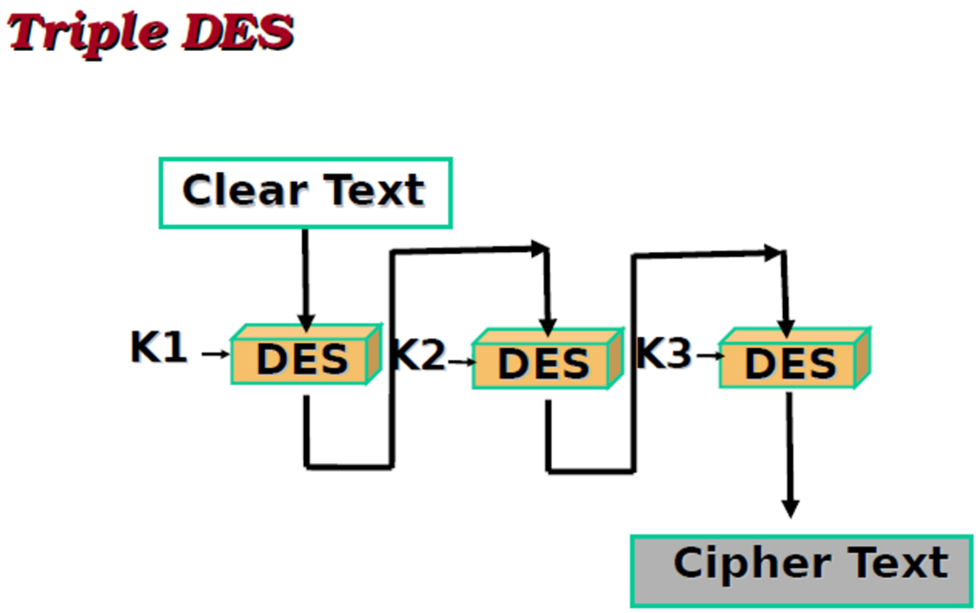
Authenicity and non-rupediation depends on this

Digital Encryption Standards(DES)

- Encrypts a 64 but key using a 56 bit key
- Can be subjected to brute force (can guess 56 bits fairly eaisily)

Tripple DES

- DES rin 3 times



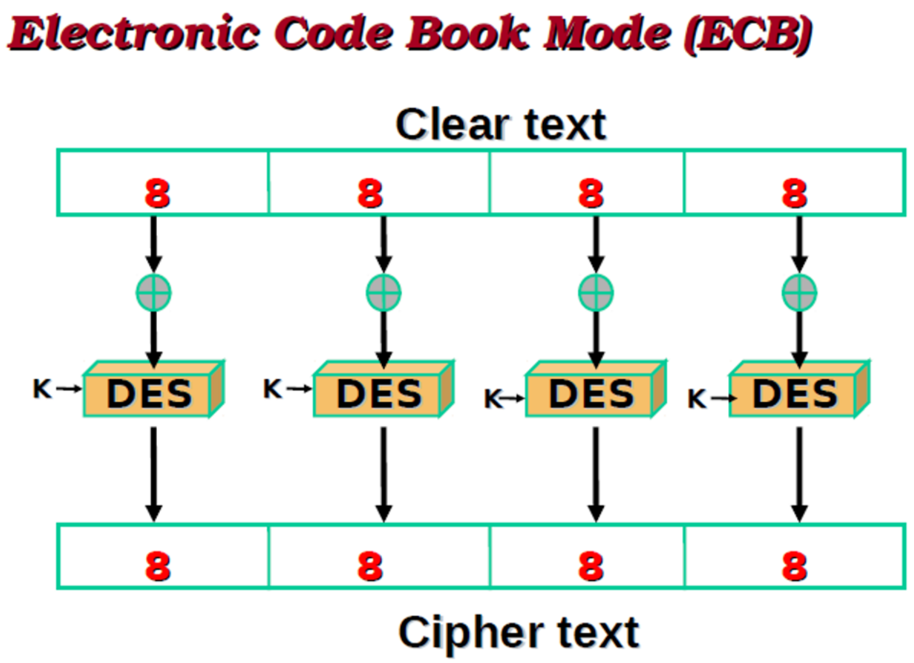
Advance Encryption Standard

- AES block length : 128
- Supoted key lengths: 128,192,256
- AES: 10 rounds of proccessing
- Key is expanded into 10 individual keys

AES and DES are both block ciphers

Modes of Operaion

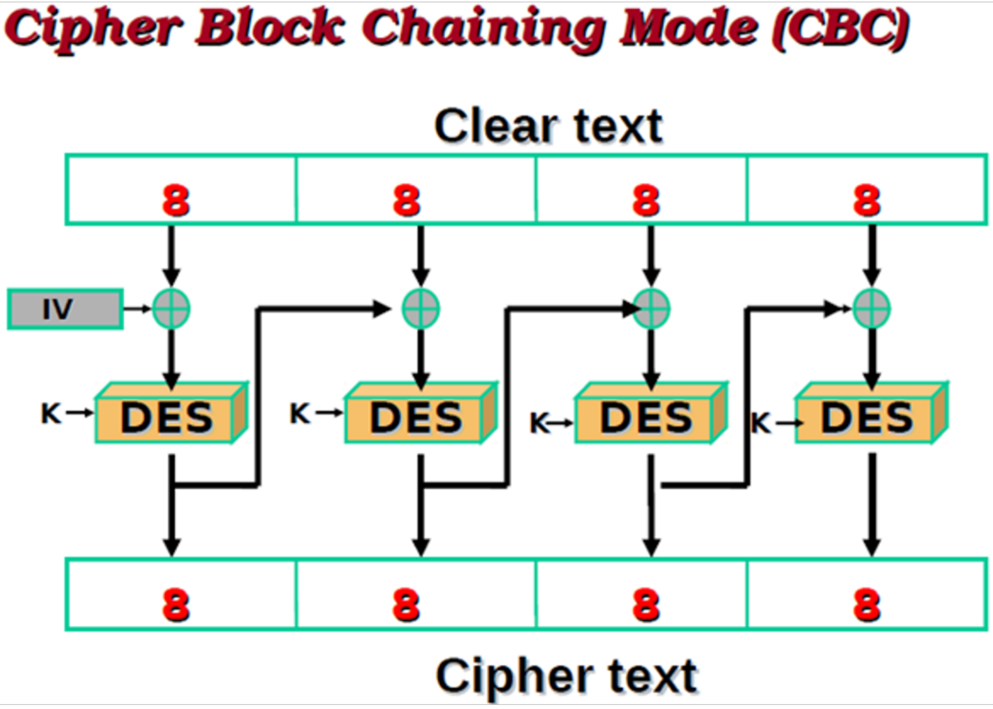
- ECB (Electronic code book)
  - Message, breakes into blocks and are encrypted
  - Each block is a value which is substituted, like a codebook, hence name



Clear text (XOR) DES

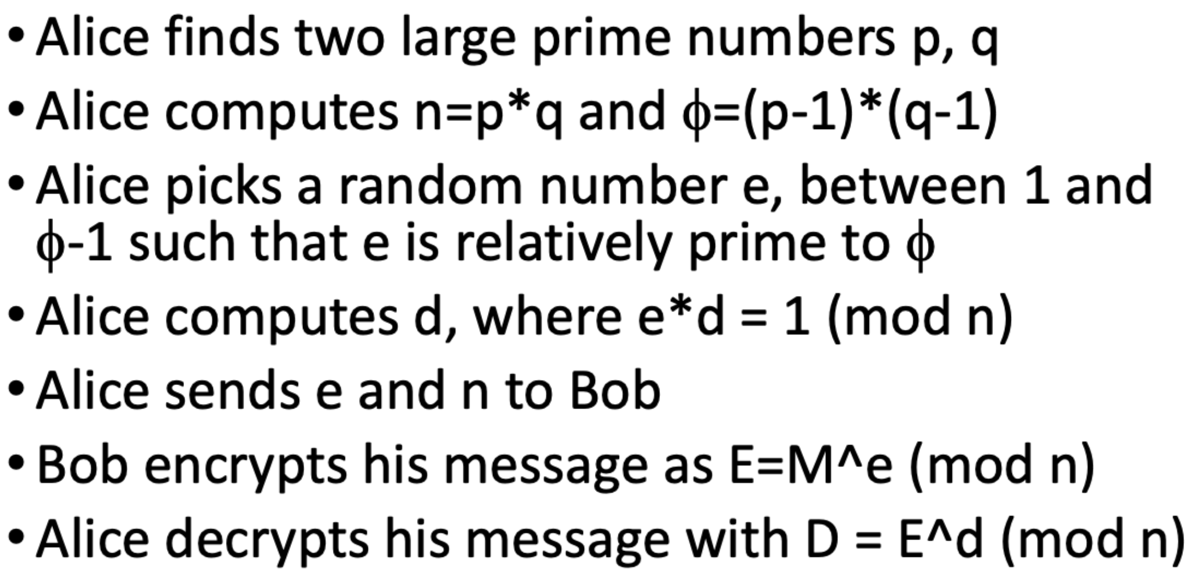
   - Weakness: Majority of the message remains the same

- Cipher block chaining (CBC)
   - Encryption of the previous cipher is used in the next



Initialization vector : Random vector of 0,1

RSA Algorithm(Assymetric key)



- Alice finds two large prime numbers p, q
- Alice computes n=p*q and ϕ=(p-1)*(q-1)
- Alice picks a random number e, between 1 and ϕ-1 such that e is relatively prime to ϕ
- Alice computes d, where e*d = 1 (mod n)
- Alice sends e and n to Bob
- Bob encrypts his message as E=M^e (mod n)
- Alice decrypts his message with D = E^d (mod n)

Weaknesses:

- Theres no algorithm to generate prime numbers
- There are no algorithms to factor large numbers

Quantum computing can do both therefore RSA can be broken bu them

PDP(Assymetric key)

- Used for emails
- Generally available, and can be used for encryption of message digital signatures.
- PGP combines Symmetric and Asymmetric
  - Symmetric has key distribution problem
  - Asymmetric is slower, but no key distribution problem
  - Solution: Use Asymmetric to encrypt and distribute key for Symmetric encryption

Breaking Cryptography

- **Cryptanalysis** is treaking an encrypted code without knowing the key but by studying and analyzing the ciphertext and the techniques used.