Sunil
DATE
PAGE
"Rough 'n' Fair"

IBC- 603

Network Security & Cyber Laws.

Sunil
DATE
PAGE
"Rough 'n' Fair"

Syllabus

UNIT-1 Introduction to Network Security

Security: Attacks, Services & mechanisms. Conventional Encryption: Conventional Encryption Model & steganography.

Modern Techniques: Thought of Fiestel Design, Block cipher & stream Cipher, Modern Block cipher, simplified DES, Block Cipher Principles, DES standards, DES strength, Differential & Linear Cryptoanalysis, Block Cipher design Principles, Block cipher modes of operation

UNIT-2 [illegible] Function Public Key Encryption

Public Key Cryptography: Principles of public key Cryptosystems, RSA Algorithm, key managment Random Number Generation

UNIT-3 Hash Function

Message Authentication & Hash Function: Authentication Requirement

Sunil
DATE
PAGE
"Rough 'n' Fair"

Authentication Function, Digital signature standards, Digital signature Algorithm.

Network security: Authentication Application - Kerberos, X-509, Electronic mail security, Secure socket layer & Transport layer security.

UNIT-4. Cyber laws.
Introduction to cyber laws, Scope of cyber laws, Privacy & freedom issue in the cyber world, Cyber-Crimes.

Object & Scope of the IT Act: Genesis, Object, Scope of the Act, E-Governance and IT Act 2000 legal recognition of electronic record, legal recogniti-on of digital signature, uses of electronic records & digital signature in Government & its agencies.
IT act in detail.

Sunil
DATE
PAGE
"Rough 'n' Fair"

1

UNIT-5 Information Gathering, Scanning

TraceRoute, Ping sweeping, Port scanning, ICMP scanning

DOC Attacks: Ping of Death, Teardrop, SYN flooding, Land Attacks, Smurf Attacks, UDP flooding, Hybrid DOS attack, Application specific, Distributed DOS Attacks

— x — x —

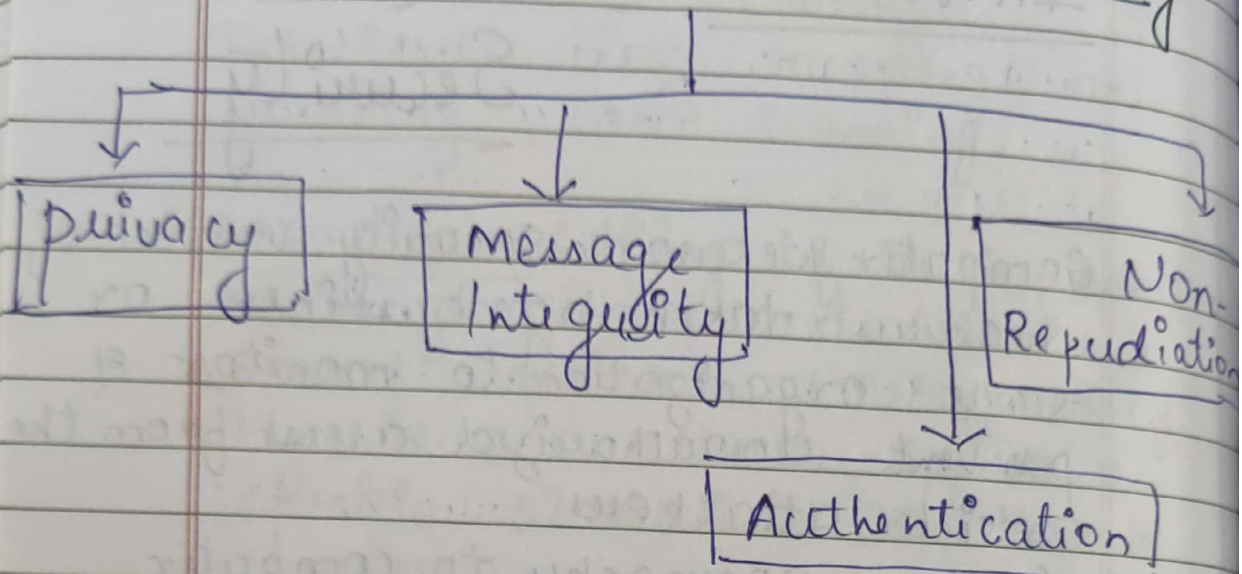
Sunil
DATE 13/1/22
PAGE
"Rough 'n' Fair"

UNIT-1.

Introduction to Network Security

Computer Network security consist of measures taken by business or some organization to monitor & prevent unauthorized access from the outside attackers
Different approaches to computer network security management have different requirement depending on the size of the computer network. For example, a home office requires basic Network security while large bussiness requires high maintainence to prevent the network from malicious attacks.
Network administrator controls access to the data & software on the network. A network administrator assigns the user ID & password to the authorized person.

Aspects of Network Security



- **Privacy**

Privacy means both the sender & Reciver expects confidentiality. The transmitted message should be sent only to the intended reciver while the message should be opaque for other users. Only the sender & reciver should be able to understand the transmitted message as eavesdroppers can intercept the message. Therefore, there is a requirement of encrypt the message so that the message cannot be interrupted. This aspect of confidentiality is commonly used to achive secure communicati

- **Message Intiquity**

Data Intiquity means that the data must arrive at the reciver exactly as it was sent. There must be no changes in the data content during transmission, either maliciously or accident, in a transmit. As their are now a more monetary exchanges over the internet, data intiquity is more crucial. The data intigility must be preserved for secure communication.

- **End-point Authentication**

Authentication means that the reciver is sure of the sender's identity, i.e no imposter has sent the message

- **Non-Repudiation**

Non-Repudiation means that the Reciver must be able to prove that the recived message has come from a specific sender The sendir must not deny sending

a message that he or she send. The burden of providing the identity come on the reciver. For example - if a customer sends a request to transfer the money from one account to another account, than the bank must have proof that the customer has requested for the transaction

Types Of Attacks.

1. Active Attacks
2. Passive Attacks.

1. Active Attack

An Active attack attempts to alter system resources or effect their operations. Active Attack involve some modification of the data stream or the creation of false statement.

Types of active attacks are as follows:

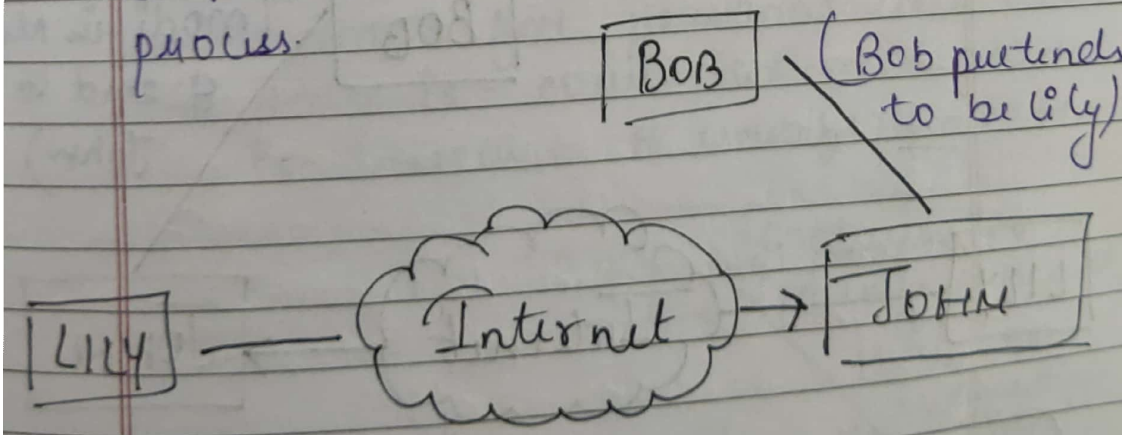
(1) Masquerade
(2) modification of mussage
(3) Repudiation
(4) Riplay
(5) Denial of Services

Entropy

Sunil
DATE
PAGE
"Rough 'n' Fair"

① Masquerade

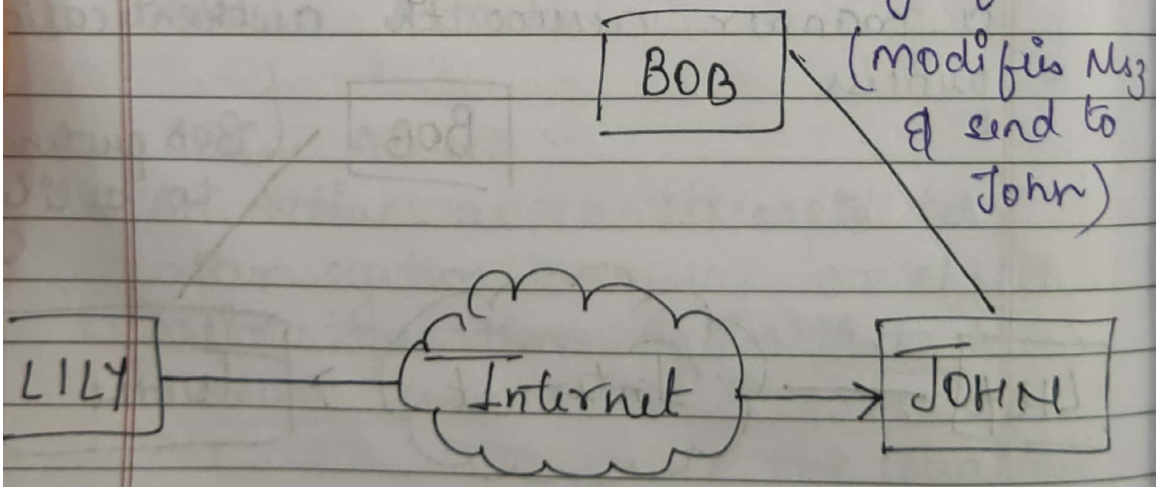
A Masquerade attack takes place when one ~~attacker~~ identity pretends to be a different entity. Masquerade attack involves one of the other forms of active attacks. If an authorization procedure isn't always absolutely protected, it is able to grow to be extraordinarily liable to a masquerad assult. Masquerade assult may be performed using the stolen passwords & logins, with the aid of using finding gaps in proguams, or with the aid of using locating a manner across the authentication process.



② Modification of message

It means that some portion of the message is altered or that message is delayed or reordid to produce an unauthorized effect. Modification is a attack

On integrity of the original message it basically means that unauthorized parties not only gain access to data but also spoof the data by triggering denial-of-service attacks, such as altering transmitted data packets or flooding the network with fake data. Modification is an attack on authentication. For example, a message meaning "Allow JOHN to read confidential file x" is modified as "Allow Smith to read confidential message file x"



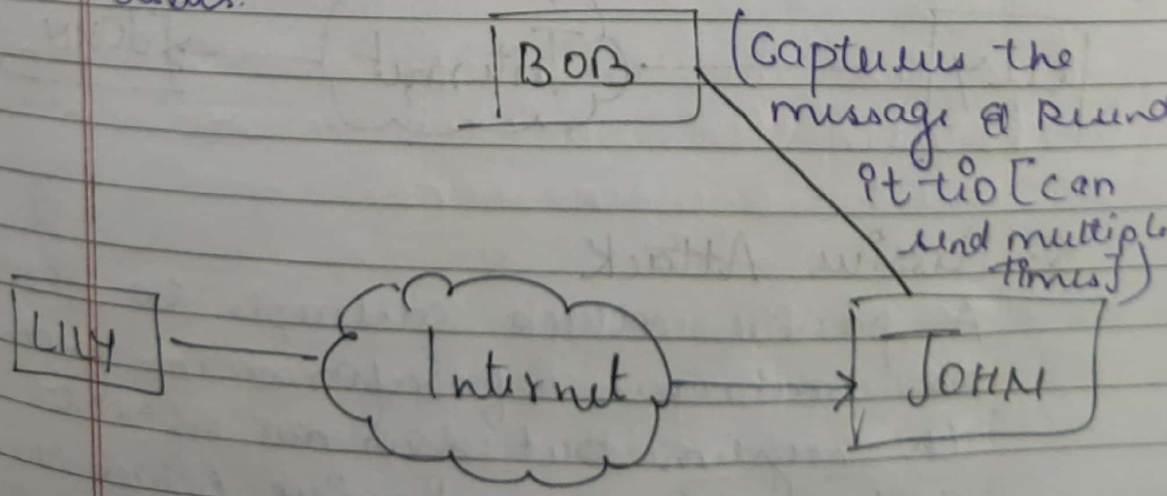
(3) Repudiation

This attack occurs when the network is not completely secured or the login control has been tampered with. With this attack, the author's information can be changed

by action of a malicious user in order to save false data in log file, up to the general manipulation of data on behalf of others, similar to the spoofing of e-mail messages.

(4) **Replay**

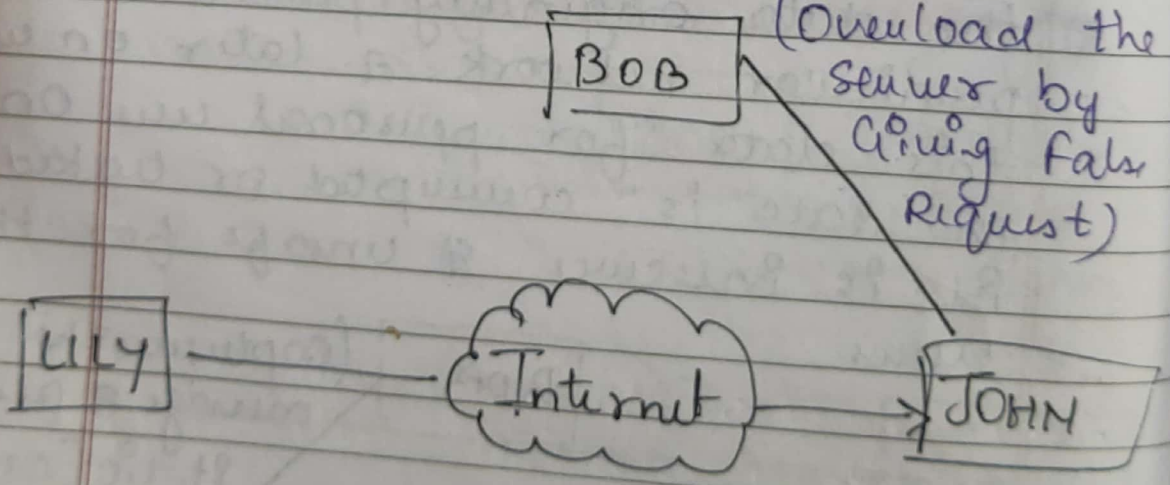
It involves the passive capture of a message & its subsequent transmission to produce an authorized effect. In this attack the basic aim of the attacker is to save a copy of the data originally present on that particular network & later on use this data for personal use. Once the data is corrupted or leaked it is insecure & unsafe for the users.



Sunil
DATE
PAGE
"Rough 'n' Fair"

(5) Denial of service

It prevents the normal use of communication facilities. This attack may have a specific target. For example:- an entity may suppress all messages directed to a particular destination. Another form of service denial is the disruption of an entire network either by disabling the network or by overloading it with message so as to degrade performance.



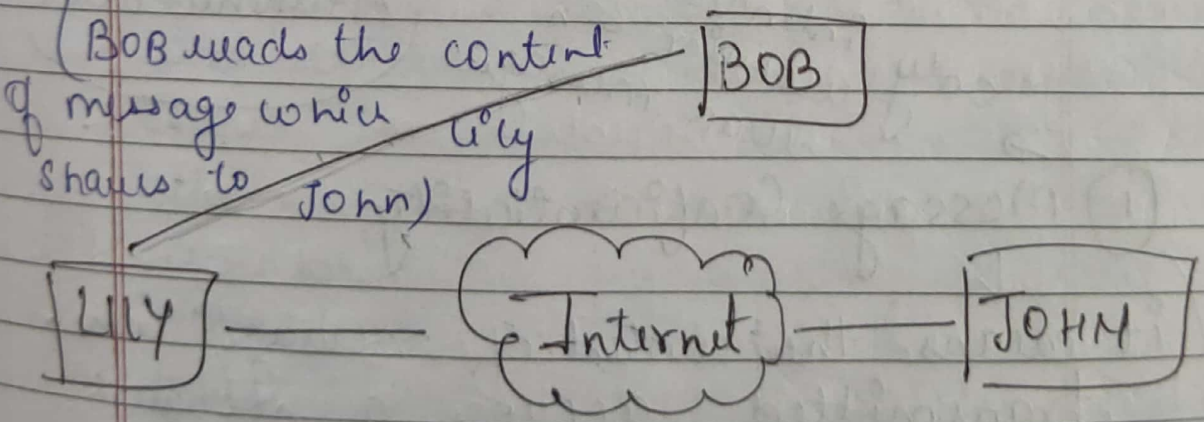
2. Passive Attack

A passive attack attempts to learn or make use of information from the system but does not affect system resources. Passive Attack are in the nature of eavesdropping on or monitoring transmission.

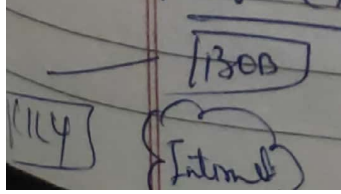
The goal of the opponent is to obtain information that is being transmitted. Types of Passive attack are as follows.

1. The release of message content
2. Traffic Analysis.

1. **The Release of Message Content:**
Telephonic conversation, an electronic Mail message, or a transfered file may contain sensitive or confidential information. We would like to ~~prevent~~ prevent an opponent from learning the contents of these transmission.



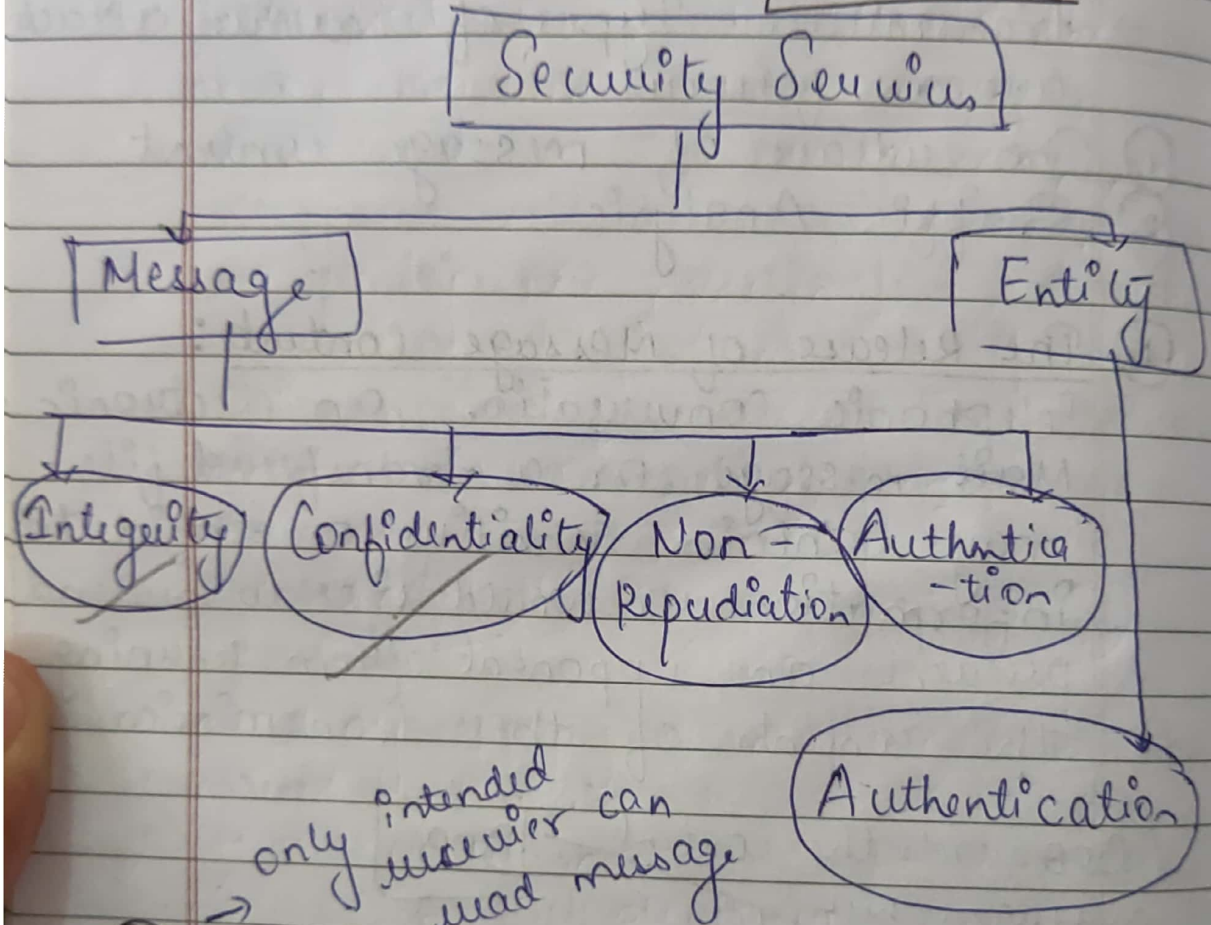
2. **Traffic Analysis**
In this type of attack attacker tries to predict the nature of the message.
For ex.



(BOB observes the pattern of message exchanges b/w Lily & John

Sunil
DATE
PAGE
"Rough 'n' Fair"

Security Services & Mechanisms



→ only intended receiver can read message

① Message Confidentiality

↓

it means the content of message when transmitted accross a network must remain confidential.

Therefore users want to encrypt the message they want to send so that no other can read it.

must not be any changes during transmission

② Message Intiguity → means message reach the dutination with-out adultration

↓

ensured by attaching a checksum to msz.

③ Message Authentication

↓

Different method to check geneuiness of sender :

↓

means reciver need to be sure about sender identity.

1. Two parties shares a common secret code word. A party is required to show the secret code word to the other for authentication
2. can be done by sending digital signature.
3. trusted thiud party varifies authenticity.

④ Message Non-Repudiation → can achive by authentication & intiguity

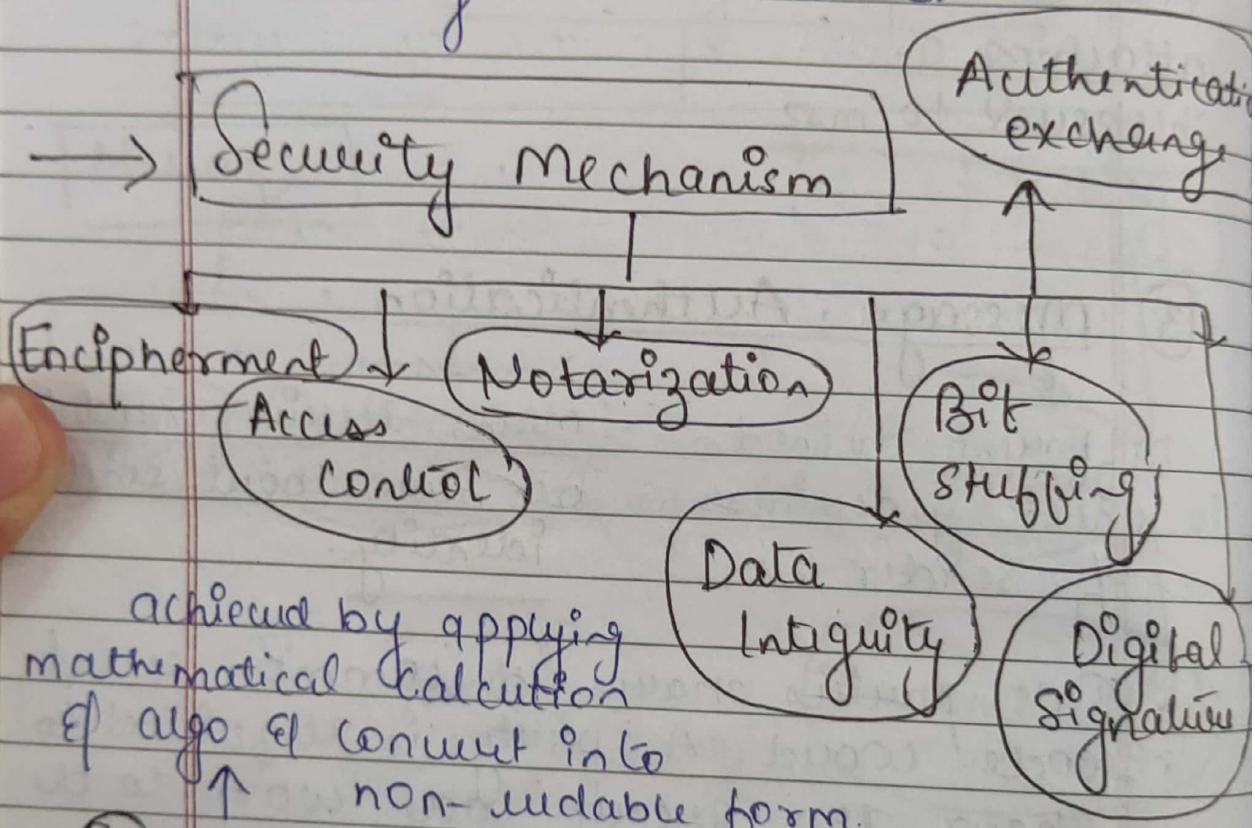
↓ means sender must not able to deny sending a message that is sent.

↓ burden of proof falls on reciver

↓ not only respect to ownership of message but also check content of message is same

Sunil
DATE
PAGE
"Rough 'n' Fair"

⑤ Entity Authentication (User Authenti-cation)
↓
verified prior to access to the system resource.



achieved by applying mathematical calculation & algo & convert into non-readable form.

① Encipherment → deals with hiding & coding data which help data to become confidential.
↓
can be done by two techniques
① Cryptography ② Encipherment

level of data encryption is depend upon the algorithm used for encipherment.

Sunil
DATE
PAGE
"Rough 'n' Fair"

(2) Access Control → used to stop unattended access to data which you are sending
↓
achieved by techniques such as applying password, using firewall of adding pin to data.

(3) Notarization → This uses trusted third party in comm.
↗ Keeps record of request made by sender.
↓
It acts as mediator b/w receiver & sender so chance of conflict are less.

(4) Data Integrity → Just like sending packet of info. to both sender & receiver so before & after data is received
↓
used by appending value to data to which is created by data itself

When this packet or data which is appended is checked & is same which sending & receiving data integrity is maintained.

Achieved at TCP/IP layer

Sunil
DATE
PAGE
"Rough 'n' Fair"

(5) Authentication Exchange
- deals with identity to be known in communication
- two-way handshaking mechanism is used

(6) Bit Stuffing → used to add some extra bit into data which is transmitted

achieved by adding

(7) Digital Signature → used to pursue data which is not more confidential by senders identity is notified
- digital data that is not visible by eyes
- form of electronic signature send by sender & checked by receiver electronically
- fast process

Conventional Model Encryption
- System uses same key for encryption as well as decryption

↓ used prior also known as public key encryption

Key is a method or algo which is used to encrypt & decrypt

Sunil
DATE
PAGE
"Rough 'n' Fair"

plain text → Encryption → cipher text
key →

cipher text → Decryption → plain text
key →

∴ 5 ingredients of conventional encryption model

- plain text → original data
- Encryption Algorithm → various algo performed on plain text
- Secret key → Input to algo
- cipher text → contains encrypted info
- Decryption Algorithm.
  ↓
  used to run encryption algo in reverse to get original plain text back.

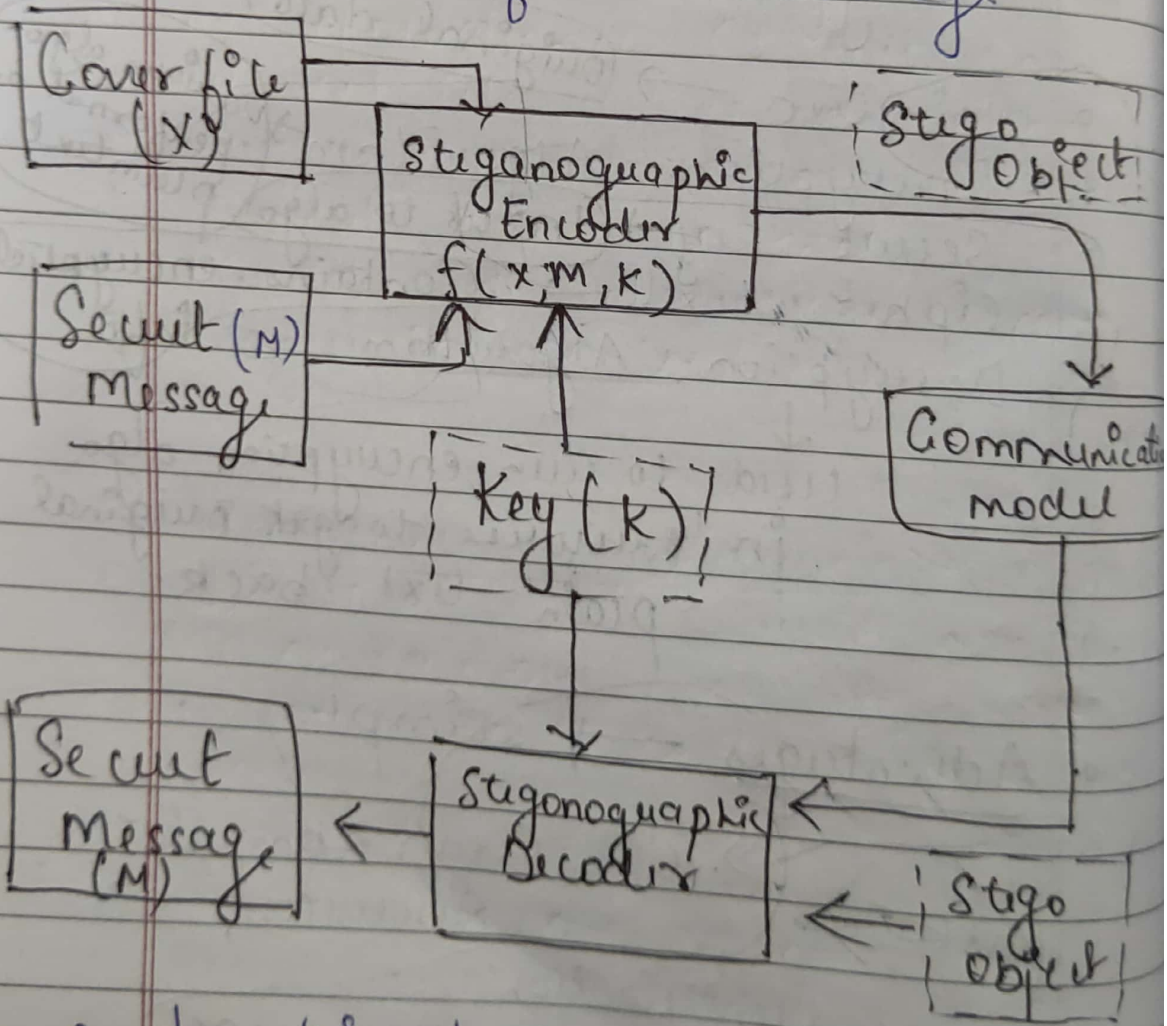
- Advantages → simple
  ↓
  fast
  → uses fewer computer Resources
  → Identification of origin of msg
- DisAdvantages → Not much secure
  ↓
  not suitable for large no. of users
  → Lost of secret key

two greek words
stegano- covered
graphia- writing

Sunil
DATE
PAGE
"Rough 'n' Fair"

Steganography

Steganography is the art & science of embedding secret message in a cover message in such a way that no one apart from the sender & intended recipient suspect the existence of the message.



- In this both cover file (X) & Secret message (M) are fed into Steganographic ~~Encoder~~ Encoder as input.

Sunil
DATE
PAGE
"Rough 'n' Fair"

- Steganographic Encoder function $f(X, M, K)$ embeds the secret message into a cover file.
- Resulting stego object looks like cover file, with no visible changes. This computes Encoding
- To retrieve the secret message, stego object is fed into Steganographic decoder.

	Steganography	Cryptography
Defination	technique to hide the existence of communication	technique to convert data into unreadable form
Purpose	Keep communication secure	Provide data protection
Data Visibility	Never	Always
Data Structure	Doesn't alter the overall structure of data	Alters the overall structure of data
Key	Optional, but offers more security if used	Necessary requirement

∴ Stiganography is more discreet than cryptography when we want to send confidential information.

→ Stiganographic Techniques

① Text Stiganography → it involves changing format of text, changing words within text hiding information inside text file
→ Various method to hide data
- format based method
- Random & statistical Generation
- Linguistic method.

② Image Stiganographic → In digital Stiganography, image are widely used hiding data by taking cover object as image.

→ Various method to hide data
- least significant bit incertion
- masking & filtering
- Encrypt & Scatter
- Redundant pattern Encoding.

difficult process
↑ as compared to other

Sunil
DATE
PAGE
"Rough 'n' Fair"

(3) Audio Steganography → store in MP3, AU, WAV.
↓
message embedded in audio signal which alter the binary sequence

→ various method of audio steganography
- last significant bit Encoding
- Parity Encoding
- Phase encoding

combination of Audio & image.

(4) Video Steganography → hides in digital video format
↓
large amount of data can be hidden inside & the fact that it is a moving stream of image & sound

→ two main classes of Video are:-
1. Embedding data in uncompressed raw video & compressing later
2. Embedding data directly into the compressed data stream

(5) Network/Protocol Steganography
↓
technique of embedding info. within network control protocol. such as TCP/IP, UDP, ICMP etc.

Sunil
DATE
PAGE
"Rough 'n' Fair"

→ Best tools to perform Steganography

① Stegosuite → you can easily hide confidential info in image file
↓ ↓
free written in java

② Stghide → used to hide a secret file in image & audio
↓
Open source

③ Xiao Steganography → free software
↓
hide data in BMP image or WAV file

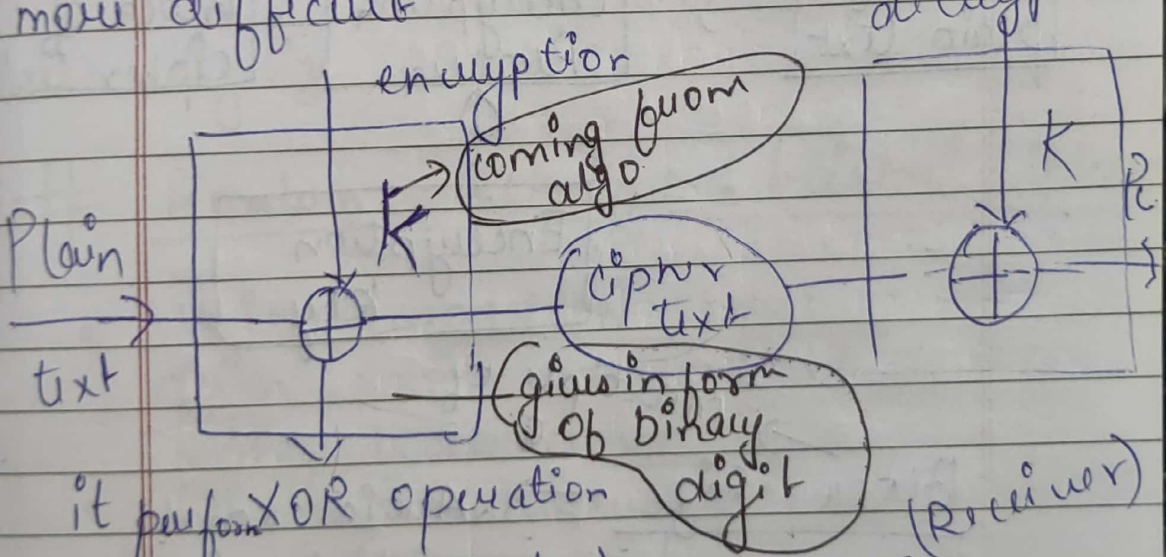
④ SSuite Picsel → hide text inside image but it takes different approach compared to other tools
↓ portable
free ~~protected~~
application

⑤ Open Puff → files stored in image, audio, video or flash file
↓
professional steganographic

Sunil
DATE
PAGE
"Rough 'n' Fair"

Modern Techniques - Stream Cipher

- Stream cipher used to convert plain text to cipher text.
- 1 byte is encrypted at a single time
- It is also symmetric key cipher means single key is used.
- Stream cipher use the sequence of pseudorandom numbers
- Advantage of stream cipher is that it makes script analysis more difficult



(Sender)

Ex. For encryption

plain txt	10011001
Key	11000010
	01011011 (cipher)

XOR: 01, 10 → 1
11, 00 → 0

(Receiver)

For decryption

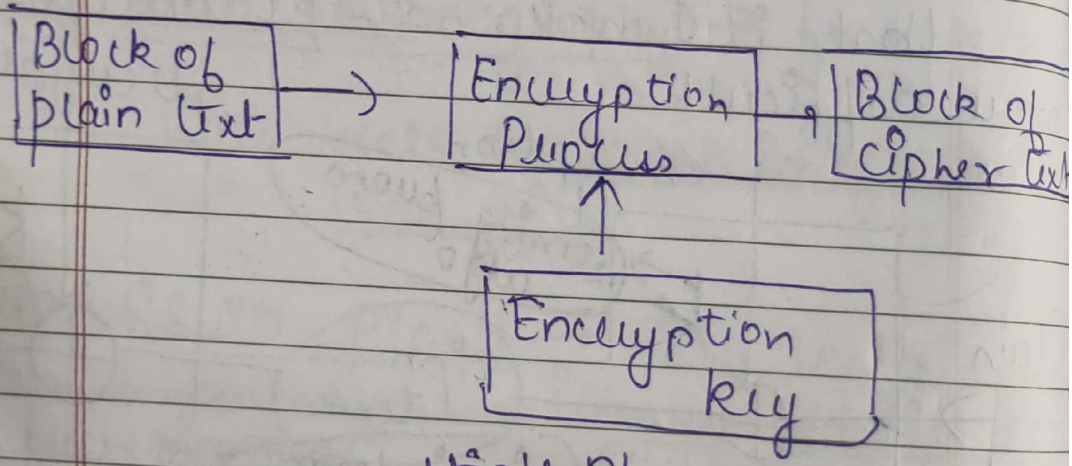
Cipher Text	01011011
Key	11000010
	10011001 (plain txt)

Sunil
DATE
PAGE
"Rough 'n' Fair"

Modern Technique: Block Cipher

- Encrypts data in the form of blocks
- takes block of plain txt & produce block of cipher txt
- symmetric key encryption
- size of block = 64 bit & 128 bit

→ Block diagram



→ multiple of 8

Block size → Avoid small block size

Do not have very large block size

→ Adding Bit to the last block of plain txt to make it similar as other & multiple of 8 is known as Padding in Block cipher

→ Block cipher streams

- DES (Digital Encryption Standards)
  - popular in 1990s
  - small key size
- Triple DES → useful now-a-days
- AES (Advanced Encryption Standard)
- IDEA → strongest
  - Block size of 64 bit
  - Key size 128 bit

Mordern Technique : Feistal Cipher

- It is a model or structure or design which is used to develop many block cipher
- Feistal structure works on several rounds

Algorithm →
- convert a list of all the plain text characters
- Convert the plain text into ASCII
- Convert into 8 bit binary
- Divide the plain binary

text string into two halves
- left half (L1) & right (R1)
- Generate Random binary key (K1 & K2) of equal length to the length of plain text.

Encryption Model for Feistal Cipher

Round 1:

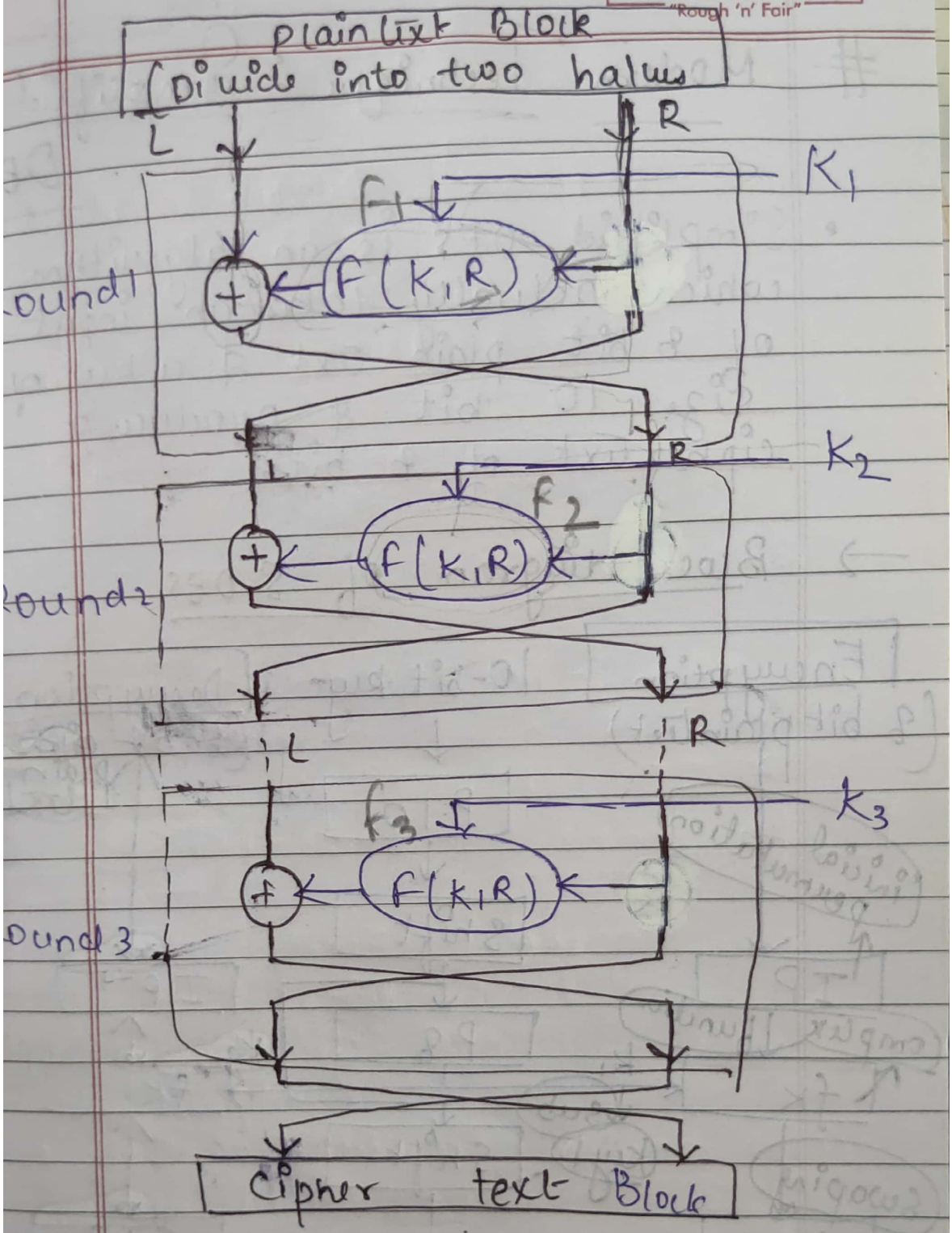
(1) Generate function (F1)
$F_1 = XOR(R_1, K1)$

values of R_2 & L_2 after round 1:
$R_2 = XOR(F_1, L_1)$
$L_2 = R_1$

Round 2:

(1) Generati function (F_2)
$F_2 = XOR(R_2, K_2)$

values of R_3 & L_3 after Round 2
$R_3 = XOR(F_2, L_2)$
$L_3 = R_2$



Genuate Function for Round 1

$F_1 = XOR(R_1, K_1)$

values of R_2 & L_2.

$R_2 = XOR(F_1, L_1)$

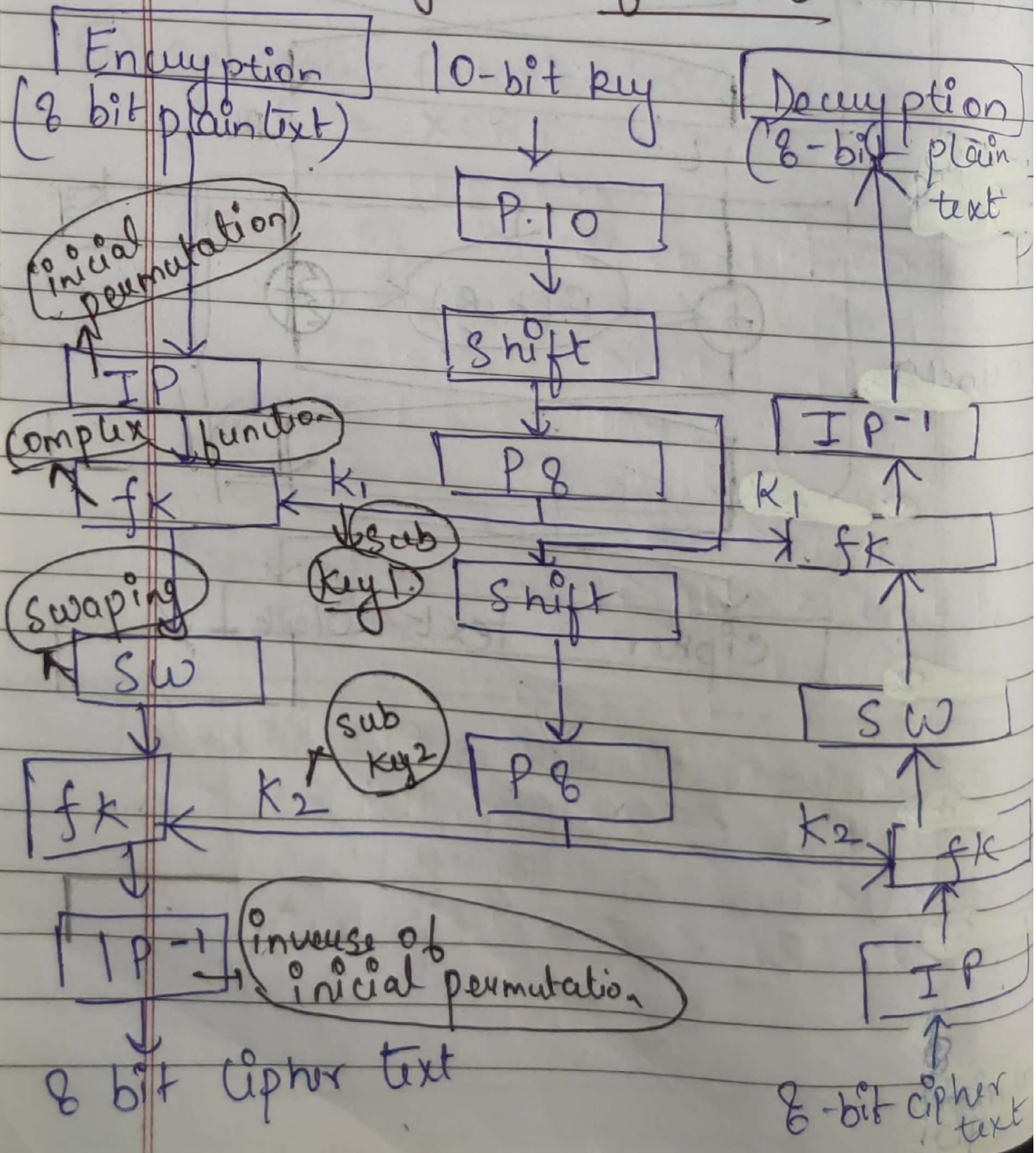
$L_2 = R_1$

Sunil
DATE
PAGE
"Rough 'n' Fair"

Modern Technique : Simplified DES

- Simplified DES is an algorithm which actually takes an input of 8 bit plain text & a key of size 10 bit & produce a ciphertext of 8 bits

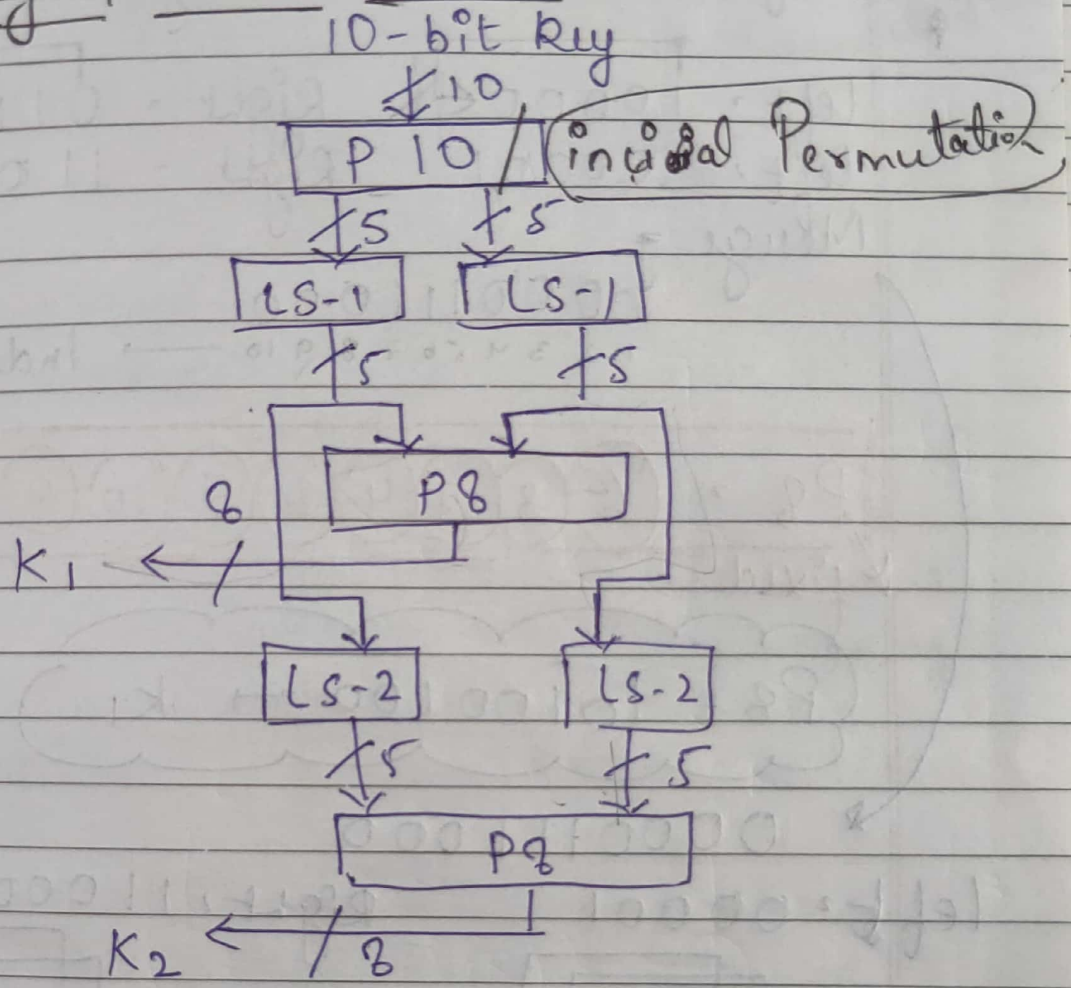
→ Block diagram of SDES



3527410986

Sunil
DATE
PAGE
"Rough 'n' Fair"

Key Generation Block



→ Example of Sub Key Generation

Encryption

Key = 1010000010

Position fixed.

Sol^n P10 = (3)(5)(2)(7)(4)(1)(0)(9)(8)(6)

Key = 1 0 1 0 0 0 0 0 1 0
1 2 3 4 5 6 7 8 9 10 ← Indexing

P = 10 1000001100

next break into two equal parts

3527410986

Left = 10000 Right = 01100

Left = 10000 Right = 01100

Left = 00001 Right = 11000

Merge → 0000111000

1 2 3 4 5 6 7 8 9 10 → Indexing

P8 = 6 3 7 4 8 5 10 9 ← Key

fixed

P8 = 10100100 → K1

0000111000

Left = 00001 Right = 11000

Left = 00001 Right = 11000

(two values are shifted)

Left = 00100 Right = 00011

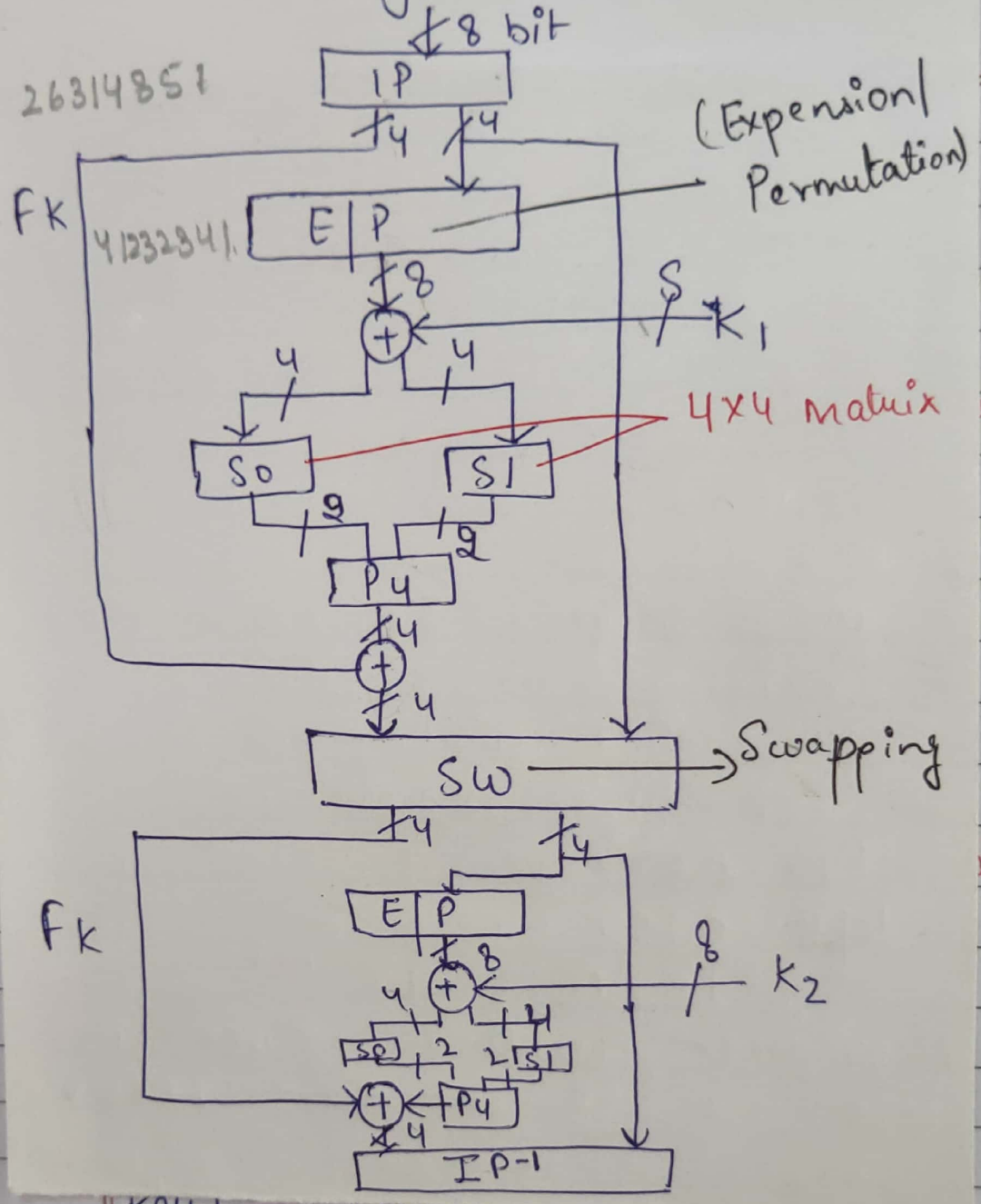
Merge = 00100000 11

1 2 3 4 5 6 7 8 9 10

P8 = 6 3 7 4 8 5 10 9 → 01000011

K2

Encryption Process



key1 = 10100100

01001111

left = 0100 Right = 1111

Put dijit

S0	00	01	10	11
00	1	0	3	2
01	3	2	1	0
10	0	2	1	3
11	3	1	3	2

S1	00	01	10	11
00	0	1	2	3
01	2	0	1	3
10	3	0	1	0
11	2	1	0	3

Encryption

Qw Key = 1010000010 K_1 = 10100100
K_2 = 01000011
plain txt = 10010111

Position fixed

Soln IP = (2)(6)(3)(1)(4)(8)(5)(7)

plain txt = 10010111
1 2 3 4 5 6 7 8 → Indexing

IP = 01011101
Left = 0101 Right = 1101

EP = (4)(1)(2)(3)(2)(3)(4)(1) → fixed

Right = 1101
1 2 3 4 → Indexing

EP = 11101011
Key1 = 10100100
01001111

left = 0100 Right = 1111

Pre defined

S_0	00	01	10	11	
00	1	0	3	2	0
01	3	2	1	0	1
10	0	2	1	3	2
11	3	1	3	2	3

S_1	00	01	10	11
00	0	1	2	3
01	2	0	1	3
10	3	0	1	0
11	2	1	0	3

refers to Row no.

(00 row, 10 column)

So

left = 0100 → 3 → 11 (Decimal to binary)

refers to column.

S1.

Right = 1111 = 3 = 11

merge S0 & S1 = 1111

12 3 4 → Indexing

P4 = ②④③① → fixed

P4 = 1111

left = 0101

1010 (old)

New left = 1010 Right = 1101

End of R1

Swapping

left = 1101 Right = 1010

Right = 1010

E/P = 41232341

E/P = 01010101

K2 = 01000011

00010110

left = 0001 Right = 0110

Sunil
DATE
PAGE
"Rough 'n' Fair"

So
left = 0001 = 3 = 11 Right = 0110
= 6 = 11

Merge = 1111

P4 = (2)(4)(3)(1) → 1111

left = 1101

(After swaping) 0010

New left = 0010 Right = 1010

End of Round 2

IP^{-1} = (4)(1)(3)(5)(7)(2)(8)(6)

fixed

Merge left & Right = 00101010
12345678

IP^{-1} = 00111000 → cipher text

- Decryption

cipher text = 00111000
12345678

IP = (2)(6)(3)(1)(4)(8)(5)(7)

IP = 00101010

left = 0010 Right = 1010
1234

EP = (4)(1)(2)(3)(2)(3)(4)(1)

EP = 01010101

01000011 — Key 2.

00010110

So

Left = 0001 = 3 = 11 Right = 0110 = 3 = 11

Merge = 1111 (1 2 3 4)

P4 = 2 4 3 1 = 1111

left = 0010

1101

New left = 1101 Right = 1010

End of Round 1.

Swapping

left = 1010 Right = 1101 (1 2 7 4)

E/P = 4 1 2 3 2 3 4 1

= 11101011

K1 = 10100100

01001111

left = 0100 = 3 = 11 Right = 1111 = 3 = 11

Merge = 1111

P4 = 2 4 3 1 = 1111

left 1010

0101

New left 0101 Right = 1101

End of Round 2.

IP-1 = 4 1 3 5 7 2 8 6

Merge = 01011101 (1 2 3 4 5 6 7 8)

IP-1 = 10010111 → plain text

Name - Rishita Agarwal Course: BCA 6B

DATE
PAGE
"Rough 'n' Fair"

ASSIGNMENT-1

Ques: Perform encryption & decryption process on the plain text as 10010111 with key as 10100000 using stream cipher

Soln **Encryption**

plain text = 10010111
key = 10100000
(XOR) 00110111 = cipher

Decryption

cipher text = 00110111
key = 10100000
10010111 = plain text

Ques: Using the Sdes, decrypt the string (10100010) using the key (0111111101) show the intermediate results after each function.

Soln Key Generation

P_{10} = 3 5 2 7 4 10 1 9 8 6
key = 0 1 1 1 1 1 1 1 0 1
1 2 3 4 5 6 7 8 9 10 → Indexing

P_{10} = 1 1 1 1 1 1 0 0 1 1
left = 1 1 1 1 1 ↺ Right = 1 0 0 1 1 ↺

left = 1 1 1 1 1 Right = 0 0 1 1 1
P_8 = 0 1 0 1 1 1 1 1 = Key 1

Sunil
DATE
PAGE
"Rough 'n' Fair"

left = 11111 ← Right = 00111
left = 11111 Right = 11100
merge = P8 = 11111100 = key2

Decryption cipher txt = 10100010
K1 = 01011111 K2 = 11111100
Ip of cipher txt = 00110001
left = 0011 Right = 0001
E/p = 41232341 (1234)
= 10000010
K2 = 11111100
01111110
left = 0111 = 0,00 Right = 1110 = 0,
P4 = 0000
left = 0011
0011
New left = 0011
Right = 0001
End of Round 1
swapping - left = 0001 Right = 001
E/p = 10010110
Key1 = 01011111
11001001
left = 1100 Right = 1001
New left = 1011
Right = 0011
Round 2
IP^{-1} = 11101010
↓
plain txt
2 1 = 01 & 2 = 10
Merge S0 & S1
= 0110
1234 - Index
P4 = 1010
left = 0001
1011

Sunil
DATE
PAGE
"Rough 'n' Fair"

Block cipher Principles

Block cipher Principles are built in Feistal structure ~~principle~~. Block cipher has a specific no. of rounds & keys for generating cipher text. For defining the complexity level of an algorithm few design principle are following below.

1. No. of Rounds
2. Design of function f
3. key schedule Algorithm

(1) Number of Rounds.

The no. of Rounds is regularly considered in design criteria, it just reflects the no. of Rounds to be suitable for an algorithm to make it more complex. In DES = 16, AES = 10

(2) Design of ~~Roun~~ function f → increasing no., increase complexity

↓ core part of the Feistal structure is Round function

↓ complexity of cryptoanalysis can be defined

Avalanche effect
make it more complex
in ↑ deriving sub key

Sunil
DATE
PAGE
"Rough 'n' Fair"

(3) Key schedule Algorithm

↓ ↓

In fiestal each round will generate a subkey to make algo complex.

decryption should be done very carefully

Block cipher modes of operations

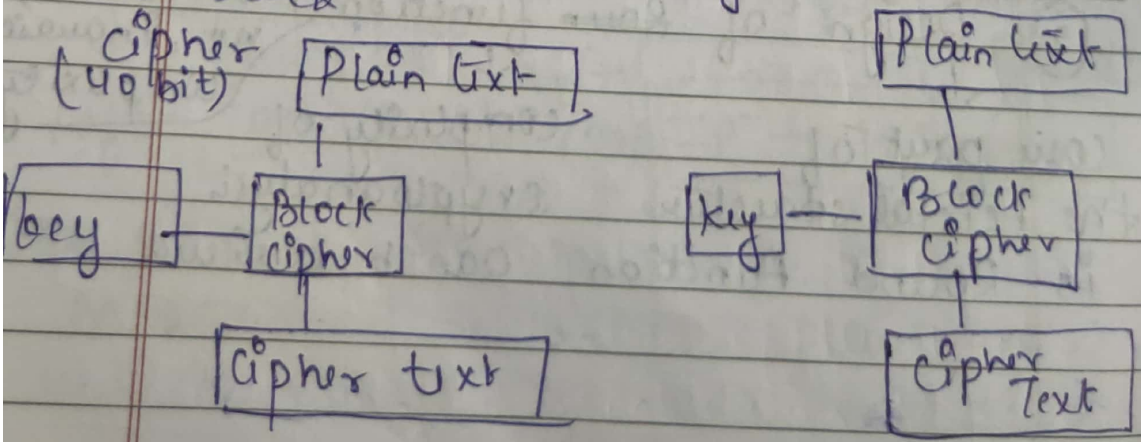
ECB CBC CF OF Counter

(Electronic Code Block)

fast ↑

(1) ECB → simple
↓ → In this plain text is divided into block ($P_1, P_2 - P_n$) each block is encrypted separately with same key

not good for small block cipher (40 bit)



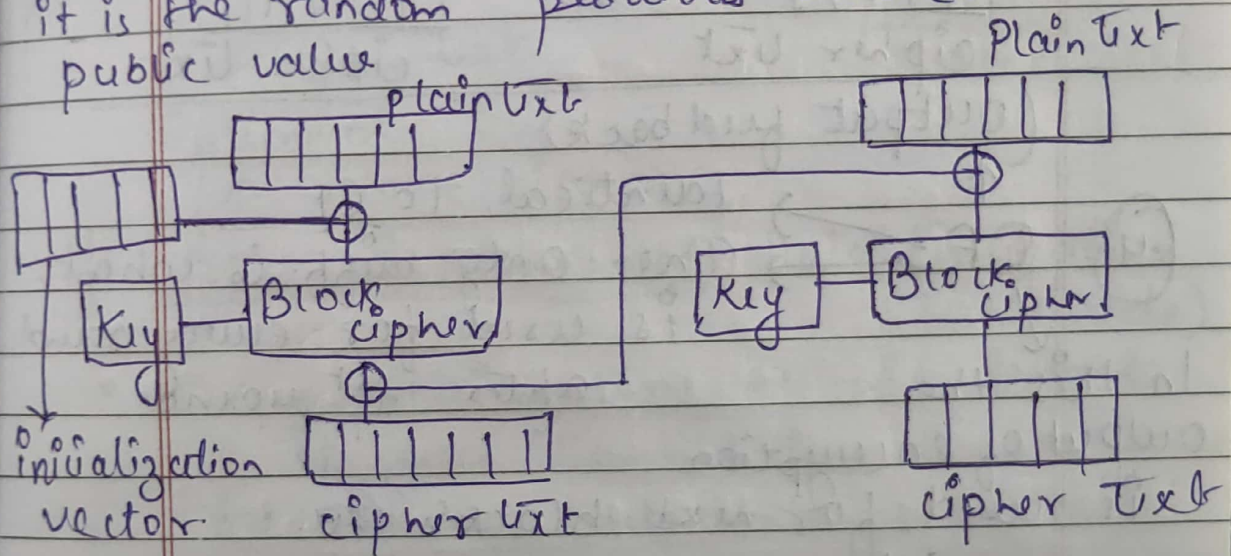
(Cipher Block chaining)

an Initialization Vector (IV)

② CBC → is exclusive-ored with plain text prior to encryption.

for the first round of encryption it is the random public value

for subsequent round it is the cipher text of previous round.



* INIGIALIZATION VECTOR (IV)

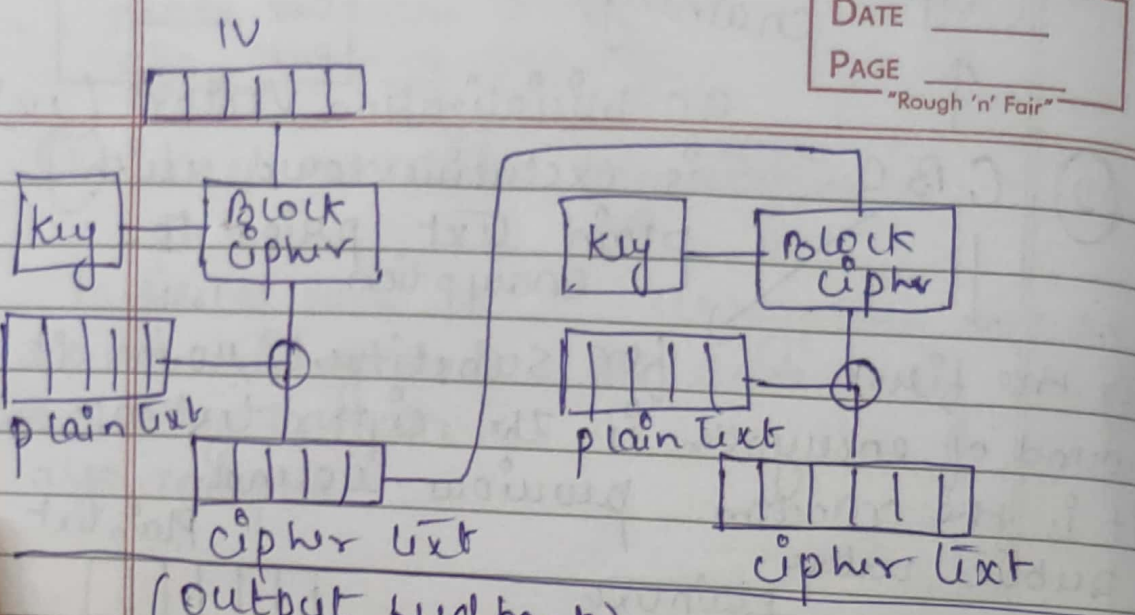
↓ avoid repetation during the data encryption process

↓ It is an arbitary no. that used with secret key for encrypt

(cipher feedback mode)

③ CFB → feedback never passes through encryption instead IV is encrypted & result is exclusive-ored with plain text to create cipher

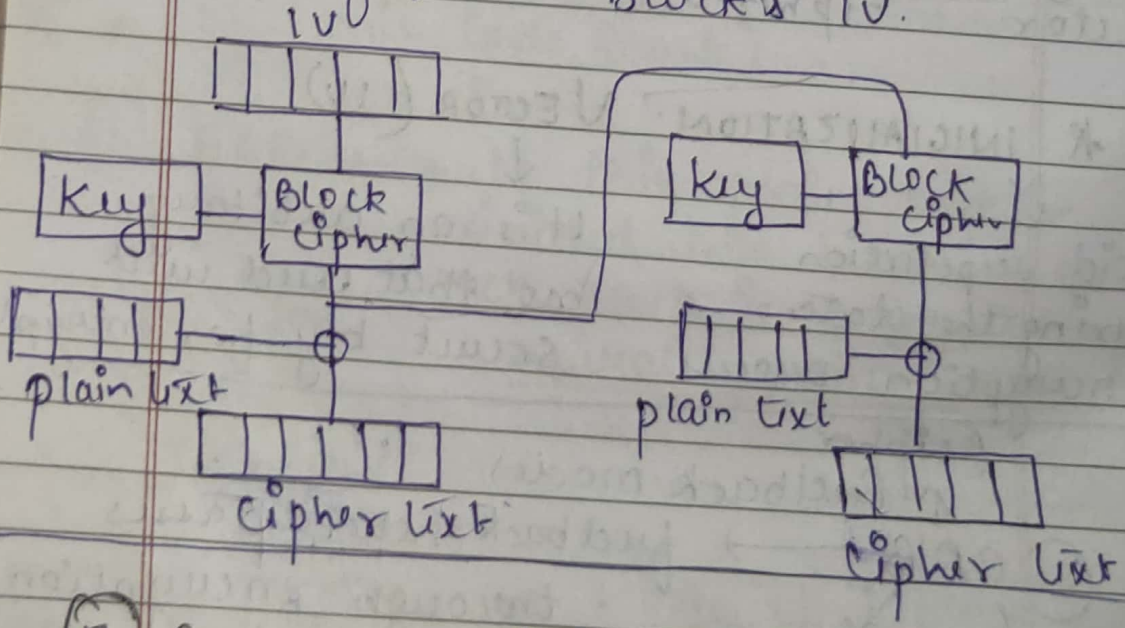
↓ similar to CBC IV is some random value



(output feedback)

(4) OF → Identical to CF
→ The only diff is what is used for every round after 1st round

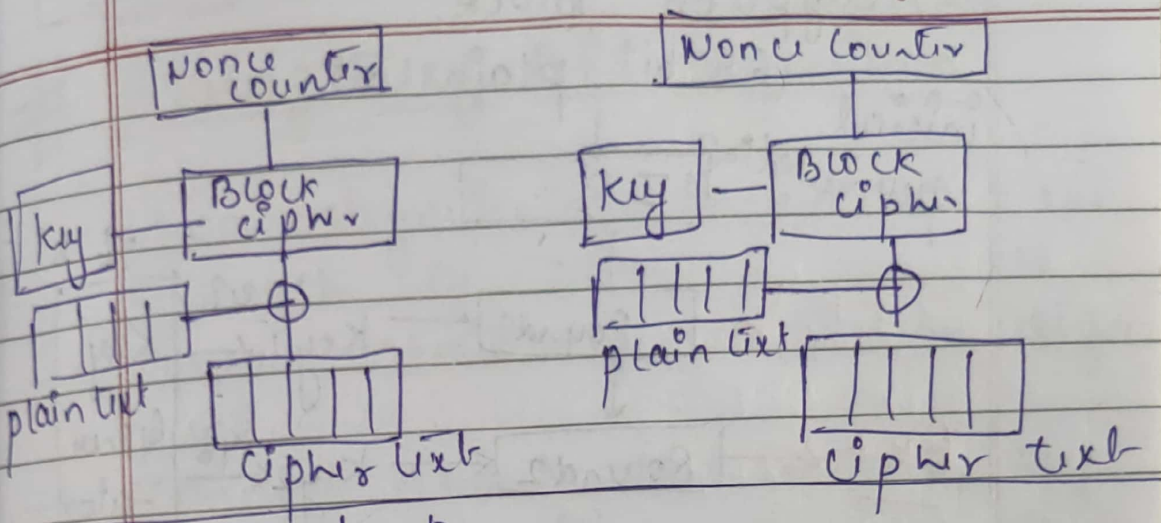
In this the output of encryption is used for next block's IV.



(5) Counter → similar to ECB
→ Instead of IV it uses combination None & counter.

Every encryption is different which gives parallization

ENCRYPTION

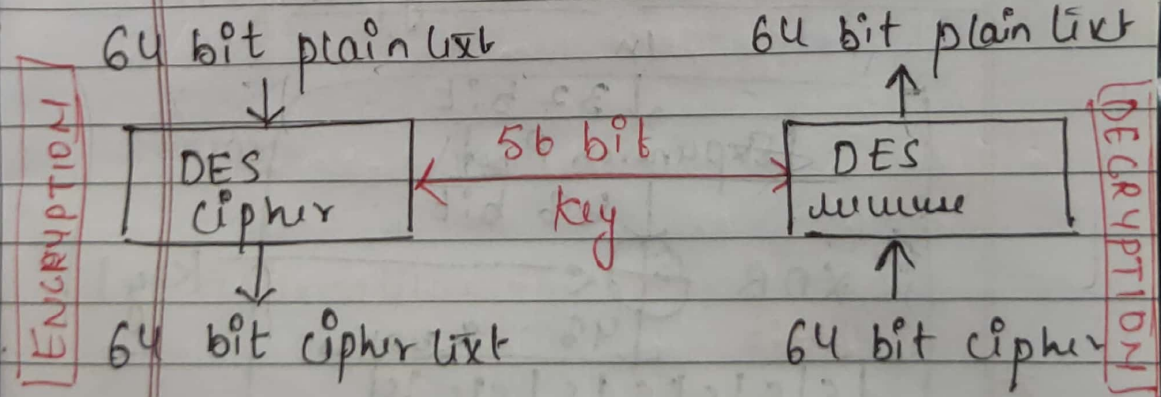


Systemmatic Key
↑ block cipher

DES ALGORITHM (Data Encryption Standards)

- Takes an input of 64 bit ~~input~~ & it uses 56 bit key & produces 64 bit key output

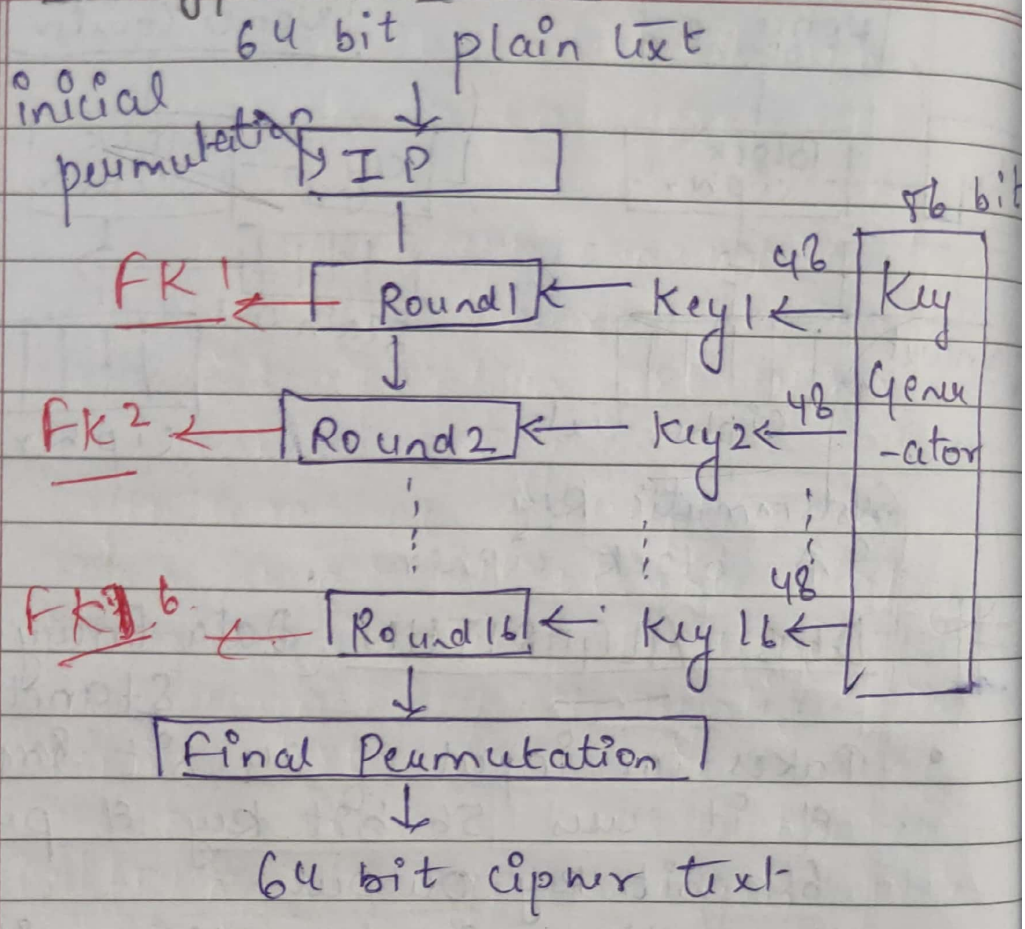
Encryption & decryption with DES



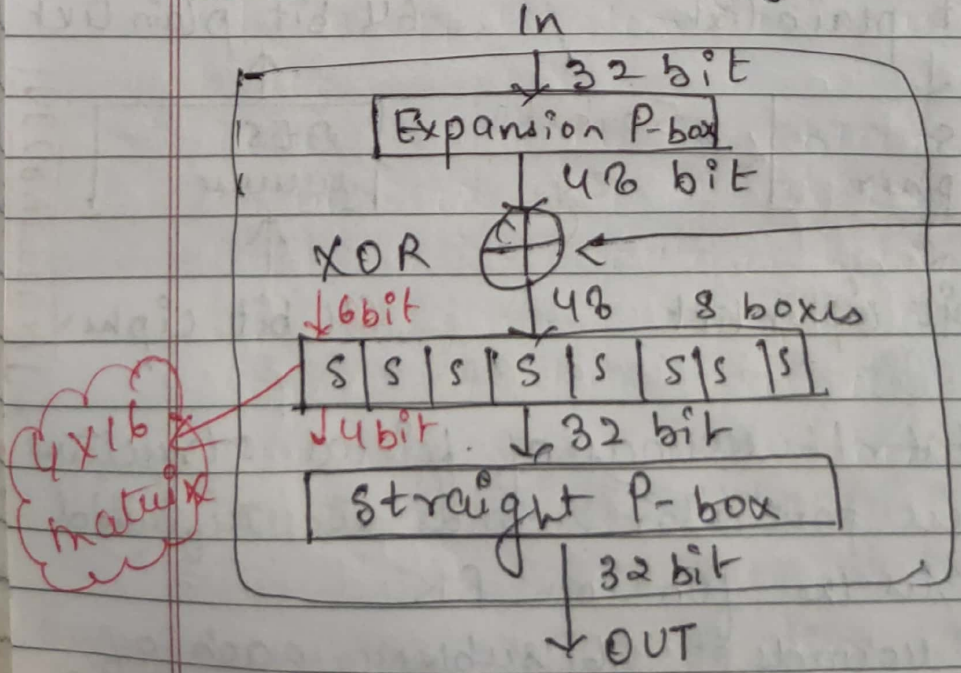
- Total 16 rounds of feistal structure these particular rounds are referred to as the funtion FK
16 rounds = 16 subkey each of 48 bits

56 bit key → K_1 (48 bit)
⋮
K_{16} (48 bit)

Encryption Block



Function Fk in Encryption



Strength of DES algorithm

- two categories of concern about the strength of DES.

→ concern about the particular algo used.

→ concerns about the usage of key of size 56 bit.

① concern about the particular algo used. ↙

addressing the possibility of cryptoanalysis.

↑ refered as code breaking / cracking

Cryptanalysis → process of analysing systems information

- linear
- differential.

∴ Alternatives of DES → AES, 3DES.

Linear Cryptoanalysis

- first defined by Matsui and Yamagishi in 1992.
- linear cryptoanalysis is a known-plain text attack in which analyst

access larger plain text & cipher text along with an encrypted unknown key.

- role of the cryptoanalyst is to identify the linear relation b/w some bit of plain text, cipher text & unknown key.
- cryptoanalyst decrypts each cipher using all possible subkey.
- focus on statical analysis against one round of decrypted cipher text.

Differential cryptoanalysis

- method of breaking certain classes of cryptosystem is invented in 1990s.
- It is available to obtain clues about some bit of the key
- Differential analysis focus on the statical analysis of two input & two output of a cryptographic algorithm.

Sunil
DATE 19/2/22
PAGE

Date.
Page No.

Principle of public key Cryptosystem

2 basic principle

Confidentiality

Authenticity

- In symmetric key cryptosystem we have problem with confidentiality, is that we all know in symmetric key cryptosystem a secret key is used to encrypt as well as decrypt message. So this key must be shared by both the communication parties by any means they must rely on the third party for the distribution of the key. But this relying on a third party again risk the secrecy of the secret key.

- Symmetric key also had an

Sunil
DATE
PAGE

issue with authentication. To became widespread there was a need of Digital signature that assure all parties that a particular message has been sent from a particular person.

Sunil
DATE 19/2/22.
PAGE
"Rough 'n' Fair"

UNIT-2.

Public Key Encryption

Encryption is a process of taking data & encoding it into a form that cannot be read by any unauthorized person.

Symmetric Key	Public Key
(Single Key used for encryption & decryption)	(Assymmetric Key) (uses two Key one for encryption & other for decryption
Problems in Symmetric Key must be stored securely	• Every sender & reciver has its own 2 two keys (Private & pubic).
sharing of the key securely.	

Public Key scenrios

Case 1:

Communication using public & private Key

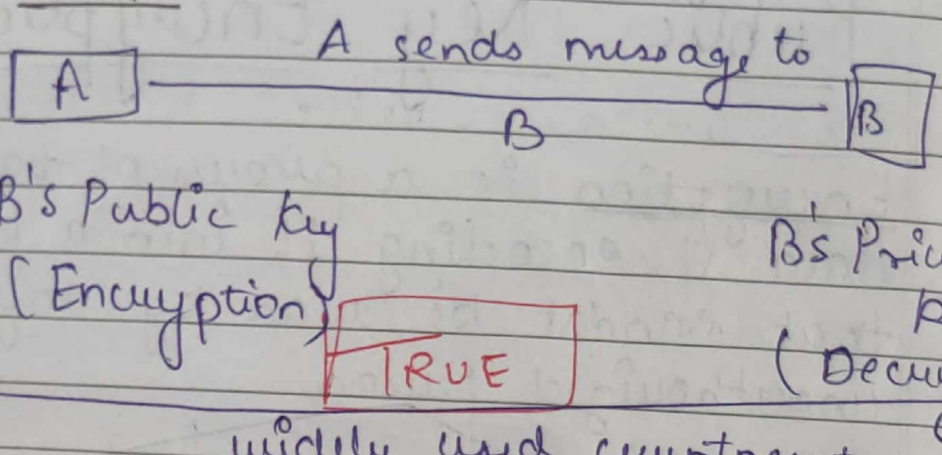
A ——— A sends message to B ——— B

A's Public Key (to encrypt)

∴ B will be able to decrypt message using A's private key.

False.

Case 9



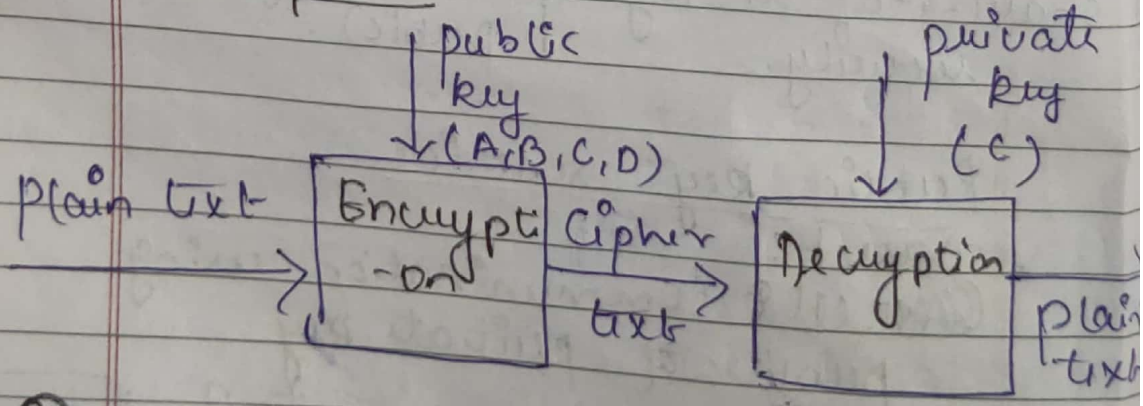
widely used cryptosystem
↑ RSA algorithm.

Characteristics of Public key Encryption

↓ two keys are used to encrypt & decrypt.

↓ because of public key encrypt public key can be shared freely

Components



(1) plain txt → readable, understandable
→ given as input in encryption algorithm.

(2) Cipher txt → hard to understand
↓
Output of Encryption Algo

convert plain text to cipher text

Sunil
DATE
PAGE
"Rough 'n' Fair"

(3) Encryption Algorithm

(4) Decryption Algorithm → convert cipher to plain text

(5) Public & private → (secret key)
(Known to everyone) → One is used for encrypt other to decrypt

Applications

- Encryption / Decryption
→ confidentiality can be achieved
→ plain text is encrypted using receiver's public key & decrypted using receiver's private key.

- Digital signature
→ for sender's authentication purpose.

- Key Exchange
→ algo can be used for both key management & securely transmission of data.

Sunil
DATE
PAGE
"Rough 'n' Fair"

RSA (Rivest Shamir Adleman)

- invented by Rivest Shamir Adleman in 1978.
- Asymmetric Algorithm means it work on two different keys

Ques. In RSA algorithm cryptosystem, a particular 'A' uses two prime numbers, p = 13 & q = 17. To generate his public & private key. If the public key of 'A' is 35. The private key of 'A' will be?

Steps of RSA Algorithm

1. Choose two different large random prime number
2. Calculate $n = p * q$
3. Calculate $\phi(n) = (p-1) * (q-1)$
4. Choose 'e' such that $1 < e < \phi(n)$, 'e' is co-prime to $\phi(n)$, $GCD(e, \phi(n)) = 1$
5. Calculate 'd', such that $de \equiv 1 \bmod \phi(n)$
6. public key = 'e' Private key = "d"

Sunil
DATE
PAGE
"Rough 'n' Fair"

two prime no.

step-1 $p = 13$ & $q = 17$

step2: $n = p * q = 13 * 17$

$\boxed{n = 221}$

step3: $\phi(n) = (p-1) * (q-1)$

$= (13-1) * (17-1)$

$= 12 * 16$ $\Rightarrow \boxed{\phi(n) = 192}$

step4. $e = 35$ (given)

$GCD(35, 192) = 1$

step5 $\boxed{de \bmod \phi(n) = 1}$

$\boxed{d * 35 \bmod 192 = 1}$

or $de \equiv 1 \bmod \phi(n)$

$de = 1 + K\,\phi(n)$

$d = \frac{1 + K\,\phi(n)}{e}$ $\quad (K = 0, 1, 2, 3 \ldots)$

when $K = 0$ $\quad d = 1/35$ X.

when $K = 2$ $\quad d = \frac{1 + 2 \times 192}{35} = 11$

$\boxed{d = 11}$

step6. (c) public key = (e, n) $= 35$

(d) private key = 11.

Rishita Agarwal
BCA 6B
44

22/02/2022

Assignment-2.

Ques. In RSA algorithm, if p = 7 & q = 11 & e = 13 then what will be the value of d?

p = 7 q = 11

$n = p \times q = 7 \times 11$

$\boxed{n = 77}$

$\phi(n) = (p-1) * (q-1)$

$= (7-1) * (11-1)$

$= 6 \times 10 = \boxed{60 = \phi(n)}$

e = 13

$de = 1 + K\phi(n)$

$d = \frac{1 + K\phi(n)}{e}$

when K = 0

$d = \frac{1 + 0 \cdot 4/13}{13}$

$= 0.07$

when K = 1

$d = \frac{1+1(60)}{13}$

$= \frac{61}{13} = 4.69$

60
x 2
120

when K = 2

$d = \frac{1+120}{13} = \frac{121}{13}$

$= 9.30$

when K = 3

$d = \frac{1+3(60)}{13}$

$= \frac{181}{13} = 13.9$

when K = 4

$$d = \frac{1 + 4(60)}{13}$$

$$= \frac{1 + 240}{13} = \frac{241}{13}$$

$$= 18.5$$

when K = 5

$$d = \frac{1 + 300}{13} = \frac{301}{13}$$

$$= 23.15$$

when k = 6

$$d = \frac{1 + 360}{13} = \frac{361}{13}$$

$$= 27.76$$

when K = 7

$$d = \frac{421}{13} = 32.3$$

when K = 8

$$d = \frac{481}{13} = 37 \cdot d$$

public key (e) = 13

private key (d) = 37

Ques 2 In a system an RSA, if p = 5 & q = 11. Is implemented for data security. what is the value of decryption key if the value of encryption key is 27.

Sol^n

given:

p = 5 ; q = 11 ; e = 27

$n = p \times q = 5 \times 11$

$n = 55$

$\phi(n) = (p-1) * (q-1) = (5-1) * (11-1)$

$= 4 \times 10 = 40$

e = 27

$de = 1 + k(\phi(n))$

$d = \frac{1 + k(\phi(n))}{e}$

when $k = 0 = \frac{1+0}{27} = \frac{1}{27}$

$k = 1$

$= \frac{1+1(40)}{27} = \frac{41}{27} = 1.$

when $k = 2 = \frac{1+80}{27} = \frac{81}{27} = 3$

$\boxed{d = 3}$

public key (e) = 27

private key (d) = 3

Ques3 In RSA cryptosystem, Tom uses two prime no 3 & 11, to generate private key of 7. What is the value of Tom's public key?

Soln $p = 3$ & $q = 11$ $d = 7$

$n = p \times q = 3 \times 11$

$\boxed{n = 33}$

$\phi(n) = (p-1) * (q-1)$

$= (3-1) * (11-1)$

$= 2 * 10 = \boxed{20}$

$d = 7$

$de = 1 + k(\phi(n))$

$$e = \frac{1 + k(\phi(n))}{d}$$

when $k = 0$

$e = \frac{1+0}{7} \cdot 1/7$

$k = 1$

$e = \frac{1+1/20)}{7} - \frac{21}{7}$

$e = 3$

public key $(e) = 3$
private key $(d) = 7$.

Qm In RSA cryptosystem a particular user X uses two prime no $P = 13$ & $q = 17$. If the public key is 35 then what is private key

Key Management

Aspects of key management
- Distribution of public key
- Use of public key encryption to distribute secrets.

① Distribution of public key

→ public Announcement :

→ Public available directory

→ Public key authority

→ Public key certificates

Random Number Generator (RNG)
↓
actually a device which generate a sequence of no. & these no. are not predicted.

Entropy = physical movement

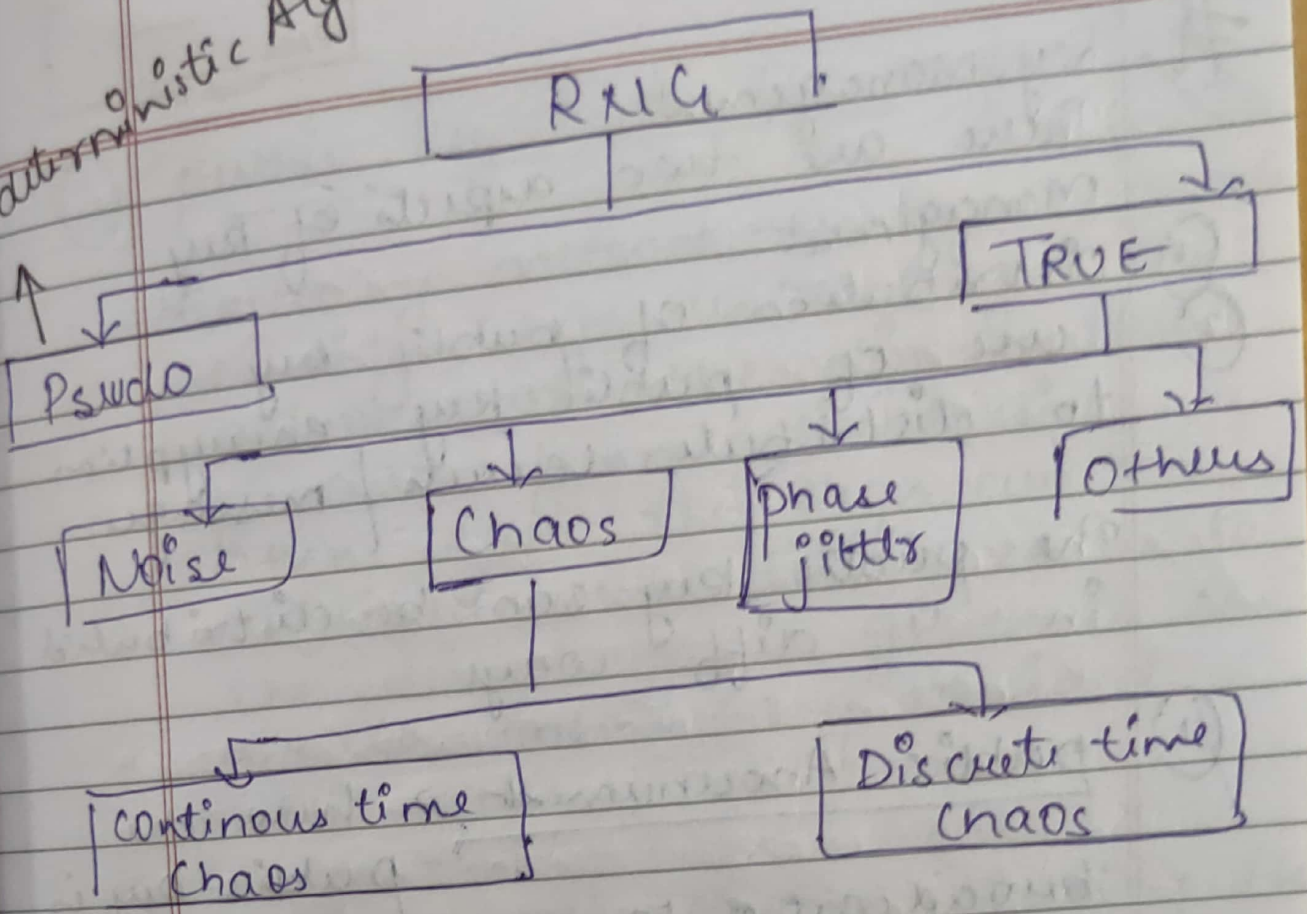
Sunil

DATE

PAGE

"Rough 'n' Fair"

deterministic Algo.



3/3/22

Sunil
DATE
PAGE
"Rough 'n' Fair"

Key Management

There are two aspects of key management

1. Distribution of public key
2. use of public key encryption to distribute secrets / messages

The public key can be distributed in 4 diff ways

1. **public Anounument** → how the public key is broadcasted to everyone. The major **drawback** of this method is forgery. Anyone can create a key claiming it to be someone's else & broadcasted

2. **publically available directory**

In this type the public key is stored in public directory electronic directory are trusted here with properties like participants registration no., exces & allow to modify values at any time that contain entries like { name, public key }

Swati
DATE
PAGE
"Rough 'n' Fair"

(3) public key authority → It is similar to directory method but upgrade security by restricting the control over the distribution of data from directories. When ever the keys are required real time access to the directory is given to the user to obtain any desired public key.

(4) public certification → This time the authority provide certificate (which binds an identity to public key) to allow key exchange without real time access to public authority each time. The certificate is accomplished by some other info. such as period of valuability, rights to use etc. All of the above content is signed by the private key of the certificate authority & it can be verified to anyone possessing the authority of public key. First under & receiver both request both

for CA (Certificate Authority) for a certificate which contain a public key & other related info & then they can exchange the certificate & start their communication.

7/3/22

Random Number Generator (RNG)

Random Number Generator is a device that generates a sequence of numbers such that they cannot be predicted. There are two types of random Number Generator.

1. Pseudo RNG
2. TRUE RNG.

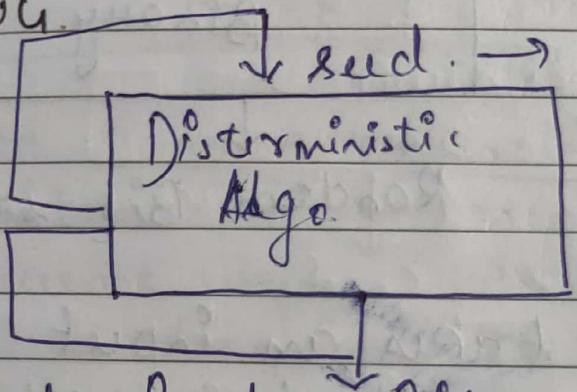
1. Pseudo RNG. (PRNG)

A PRNG is a deterministic Algo that produces seemingly random numbers. It needs a seed value as an initial value to produce the Random number. Games, simulators etc uses such generators.

Sunil
DATE
PAGE
"Rough 'n' Fair"

(2) TRNG (True Random NG)
TRNG is a device that generate truly Random Numbers. Thermal Noise, Quantum phenomenon etc are the ex. of TRNG.

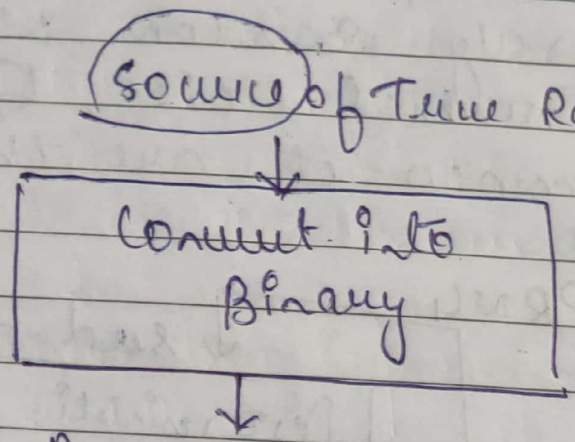
→ PRNG



PRNG takes an input of a fixed value called the seed value & produces a sequence of output using a deterministic Algo. the output bit stream is determined solely by the input value or values, so an attacker who knows the algorithm & the seed value can reproduce the entire output Bit stream. Therefore the seed value that serves as an input to the PRNG must be Random or A pseudo Random Number. Typically ~~Received~~ a

by a seed value is generated for TRNG

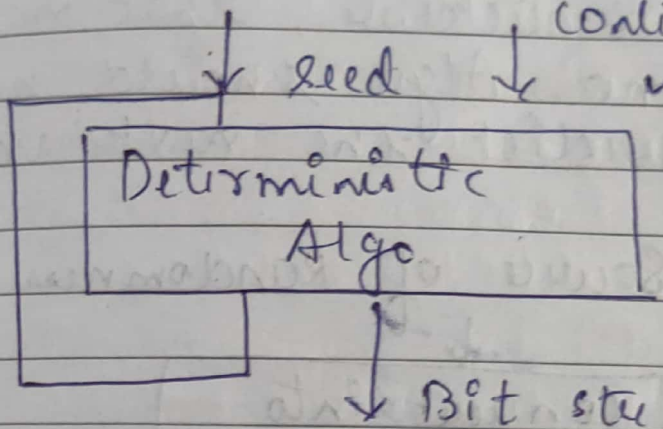
→ TRNG.



TRNG takes an input as a source that is effectively Random. This source is referred to as ENTROPY & is drawn from the physical environment of the comp machine. This Entropy include various things such as key stroke timing pattern, Disc electrical activity, mouse movements etc. The source or combination of sources serves as input to an algo that produces Random Binary output. This TRNG may simply involve the conversion of an Analog source to the Binary output

Sunil
DATE
PAGE
"Rough 'n' Fair"

PRF (Pseudo Random function)

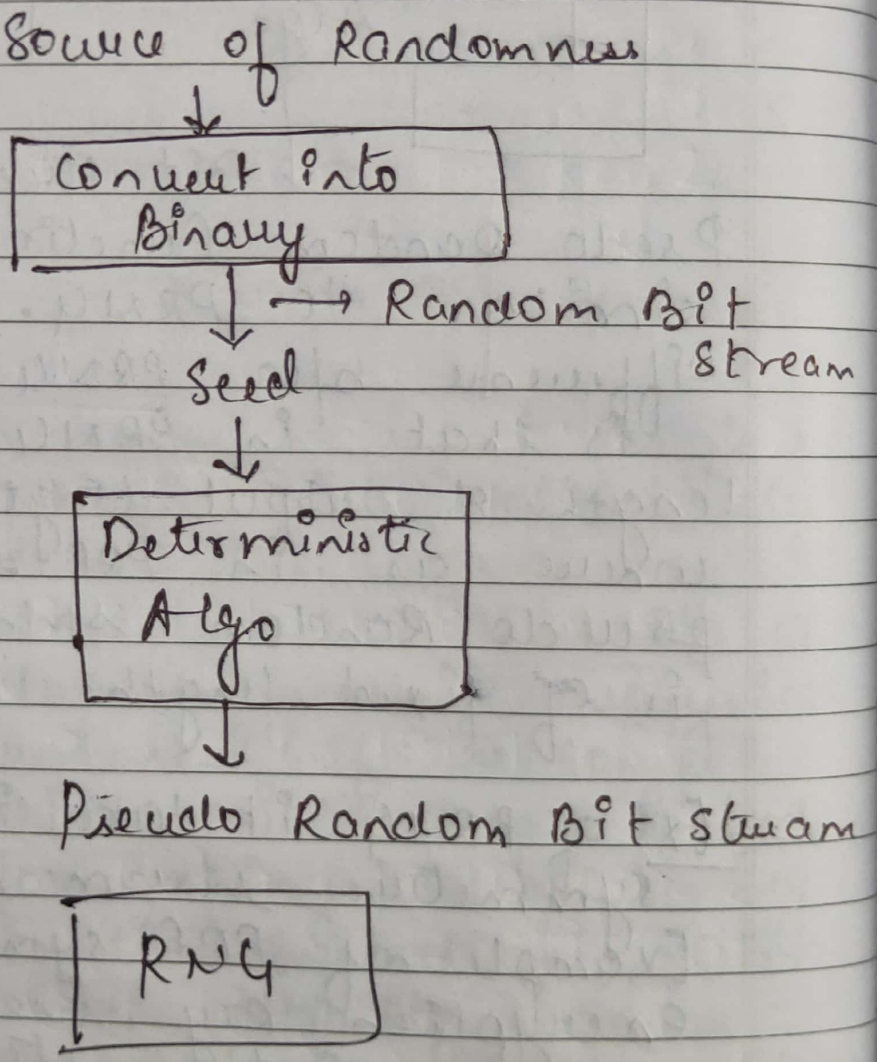


Pseudo Random function are similar to PRNG. The major Difference b/w PRNG & PRF is that in PRNG the input length & output length differs. where as in PRF the produced pseudo Random string of bits is of fixed length.

Ex of PRNG it takes input from symmetric stream cipher.
Example of PRF symmetric encryption key, user Id or are application etc

Note: other than the no. of bits produce there is not such difference b/w PRNG & PRF as both takes an input a seed value that showcases Randomness with should be

out of sequence or series & unpredictable, that no body or no Algo. should be able to predict the next value.



Qun In RSA Algo if $P = 7$ & $q = 11$

12/4/22

Sunil

DATE

PAGE

"Rough 'n' Fair"

Qu If the Input Bit Block is 84, and key is 21 generate the cipher text using S DES algorithm

key = 21 (10 bit).

2	21
2	10
2	5
2	2
	1

input bit = 84 (8)

2	84	0
2	42	0
2	21	1
2	10	0
2	5	1
2	2	0
	1	

84 = 01010100

→ Key = 21 (10 bit)

2 0000010101 ← Key

1 2 3 4 5 6 7 8 9 10

2	21	1
2	10	0
2	5	1
2	2	0
	1	

P_{10} = 3 5 2 7 4 10 1 9 8 6

P_{10} = 0000010011

Left

2 00000 ← 1 2 3 4 5

Right

00111 ← 6 7 8 9 10

Merge = 0000000111

P_8 = 6 3 7 4 6 8 10 9

P_8 = 00001011 ← Key 1

Sunil
DATE
PAGE
"Rough 'n' Fair"

Merge = 0000000111

Left

00000

Right

00111

1 2 3 4 5 6 7 8 9 10

Merge = 0000011100

P8 = 10101000 → key 2

Encryption

Key 1 → 00001011

Key 2 → 10101000

Key → 0000010101

plain txt = 01010100

IP = (2)(6)(3)(1)(4)(8)(5)(7)

plaintext = 01010100

1 2 3 4 5 6 7 8

IP = 11001000

Left = 1100 Right = 1000

Sunil
DATE
PAGE
"Rough 'n' Fair"

E|P : (4)(1)(2)(3)(2)(3)(4)(1)

Right : 1000
1234

E|P = 01000001
Ky1 = 00001011
01001010

left = 0100 Right = 1010
= 3 = 11 = 00

Merge : 1100
1234

Py = (2)(4)(3)(1)

Py = 1001
left = 1100
0101

New left = 0101
Right = 1000

Round (1)

Swapping

left = 1000 Right = 0101
Right = 0101
1234

E|P = (4)(1)(2)(3)(2)(3)(4)(1)

Sunil

DATE

PAGE

"Rough 'n' Fair"

E/P = 10101010

Key2 = 10101000

00000010

Left: 0000 → 12 → 01

Right: 0010 → 34 → 01

P4 = 1100

Left: 1000

0100

New Left = 0100 → 1234

IP⁻¹ = 00000111

8676

0101

Right: ~~0000~~

3 5 2 7 4 10 1 9 8 6 — P10

6 3 7 4 8 5 10 9 — P8

2 6 3 1 4 8 8 7 — IP

4 1 2 3 2 3 4 1 — E/P

Sunil
DATE
PAGE
"Rough 'n' Fair"

Q) Using sdes encrypt the string 10100010 using the key 0111111101 show the intermediate result after each function

Soln plain text = 10100010

Key = 0111111101
1 2 3 4 5 6 7 8 9 10

P_{10} = (3)(5)(2)(7)(4)(10)(1)(9)(8)(6)

P_{10} = 11111 10011

left = 11111 ← Right = 10011 ←

= 11111 00111

Merge = 1111100111
1 2 3 4 5 6 7 8 9 10

P_8 = (6)(3)(7)(4)(8)(5)(10)(9)

P_8 = 01011111 ——— Key 1.

→ 1111100111

left = 11111 ← Right = 00111 ←

= 11111 = 11100

merge = 1111111100
1 2 3 4 5 6 7 8 9 10

P_8 = (6)(3)(7)(4)(8)(5)(10)(9)

= 11111100 ——— Key 2.

Sunil

DATE

PAGE

"Rough 'n' Fair"

Encryption

Key1 = 01011111 Key2 = 11111100

plain text = 10100010

1 2 3 4 5 6 7 8

IP = (2) (6) (3) (1) (4) (8) (5) (7)

IP = 00110001

left = 0011 Right = 0001

Right = 0001

1 2 3 4

E/P = (4) (1) (2) (3) (2) (3) (4) (1)

E/P = 10000010

Key1 = 01011111

11011101

left = 1101 Right = 1101

S_0 =

1	0	3	2
3	2	1	0
0	2	1	3
3	1	3	2

S_1 =

0	1	2	3
2	0	1	3
3	0	1	0
2	1	0	3

18/4/22

RSA Algorithm

RSA Algorithm was invented by Rivest Shamir Aldirman in year 1978 Therefor it is named as RSA.

RSA Algo is Asymmetric Algo that means it works on 2 different keys that is public and private.

As the name describes public key is given to everyone & private key is kept private.

Algo of RSA

Steps:
1. Choose 2 different large random prime no.
2. Calculate $n = p * q$
3. Calculate $\phi(n) = (p-1) * (q-1)$
4. Choose e such that $1 < e < \phi(n)$. e is co-prime to $\phi(n)$. i.e gcd of e & $\phi(n) = 1$
5. Calculate 'd' such that $de = 1 \bmod \phi(n)$

e = public key
d = private key

Sunil
DATE
PAGE
"Rough 'n' Fair"

Qu In RSA cryptosystem a particular user A uses 2 prime no p = 13 & q = 17 to generate its public & private keys. if the public key of A is 35 calculate the private key of A

Soln

$p = 13 \quad q = 17$

$n = p * q$

$= 13 \times 17$

$= 221$

$\phi(n) = (p-1) * (q-1)$

$= (13-1) * (17-1)$

$= 12 \times 16 = 192$

$e = 35$

$d = \frac{1 + K\,\phi(n)}{e}$

$K = 0$	$K = 1$	$K = 2$
$d = \frac{1}{35}$	$d = \frac{1+192}{35} = \frac{193}{35}$	$d = \frac{1+192\times2}{35}$
		$= \frac{1+384}{35}$
		$d = 11$

$d = 11$

Scanned with CamScanner

Sunil
DATE
PAGE
"Rough 'n' Fair"

Qw. In RSA Algorithm if p = 7, q = 11 & e = 13 find d

p = 7
q = 11
e = 13

$n = p \times q = 7 \times 11$

$\boxed{n = 77}$

$\phi(n) = 6 \times 10 = \boxed{60}$

e = 13

$d = \frac{1 + k\phi(n)}{e}$

13 x 6.

k = 0 $d = \frac{1}{13}$	k = 1. $d = \frac{1+60}{13}$ $d = \frac{61}{13}$	k = 2 $d = \frac{1+120}{13}$ $= \frac{121}{13}$
k = 3. $d = \frac{1+180}{13}$ $= \frac{181}{13}$	k = 4 $d = \frac{1+240}{13}$ $d = \frac{241}{13}$	k = 5 $d = \frac{1+300}{13}$ $= \frac{301}{13}$
k = 6 $d = \frac{361}{13}$	k = 7 $d = \frac{421}{13}$	k = 8 $d = \frac{481}{13}$ d = 37.

$\boxed{d = 37}$

Sunil
DATE
PAGE
"Rough 'n' Fair"

Qu In a system an RSA Algo with p = 5, q = 11 is implemented for data security what is the value of decryption key if the value of encryption key is 27.

Soln

$p = 5 \quad q = 11$

$n = p \times q = 5 \times 11 = 55$

$\phi(n) = 4 \times 10 = 40$

$e = 27$

$d = \frac{1 + k(\phi(n))}{e}$

$k = 0$
$d = \frac{1}{27}$

$k = 1$
$d = \frac{1+40}{27}$
$= \frac{41}{27}$

$k = 2$
$d = \frac{1+80}{27} = \frac{81}{27} = 3$

$d = 3$

27
×3
81

Qu In RSA crypto system Tom uses 2 prime no. 3 & 11 to generate his private key of 7 what is the value of Tom's public key.

Sunil
DATE
PAGE
"Rough 'n' Fair"

$p = 3 \quad q = 11$

$n = p \times q = 3 \times 11 = 33$

$\phi(n) = 2 \times 10 = 20$

$d = 7$

$d = \frac{1 + k(\phi(n))}{e} \quad \Rightarrow \quad e = \frac{1 + k(\phi(n))}{d}$

$k = 0$	$k = 1$
$e = \frac{1}{7}$	$e = \frac{1+20}{7} = \frac{21}{7} = 3$

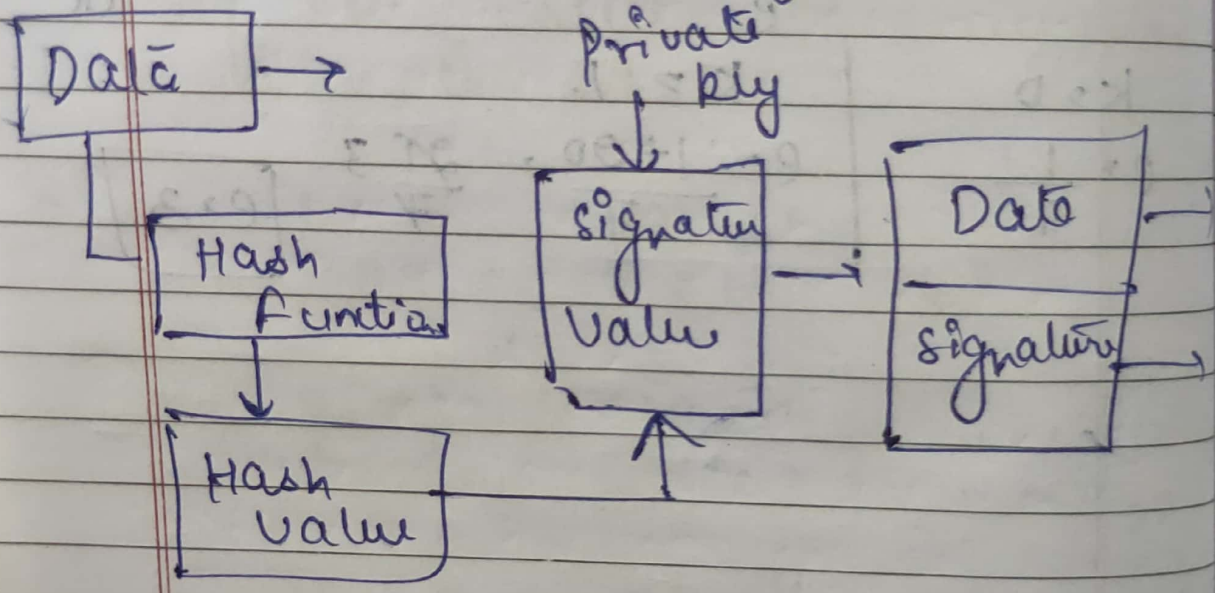
$\boxed{e = 3}$

26/4/22

UNIT-3

Model of Digital signature

Digital signature scheme is based on public key cryptography & model is as follows

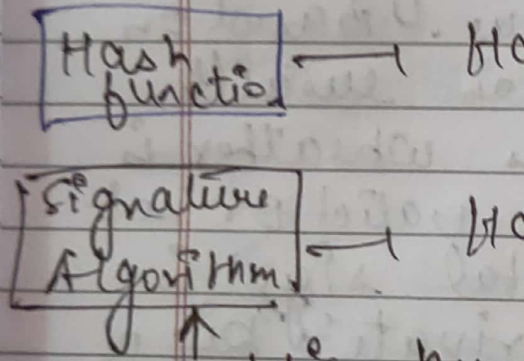


(i)

1. Each person adopted this key has a public key pair
2. The key pair used for encryption & decryption & signing & verifying are different. The private key used for signing is referred to as signature key & the public key as the verification key.

Sunil
DATE
PAGE
"Rough 'n' Fair"

Assignment → Indian Acts for wireless communication



(3) Signer feds the data to the hash function & generate hash value of data

(4) Hash value & signature key are then fed to signature Algo which produces the digital signature on given hash value. signature is appended to data & then both are sent to the verifier.

(5) verifier feds the digital signature & verification key into verification Algo.

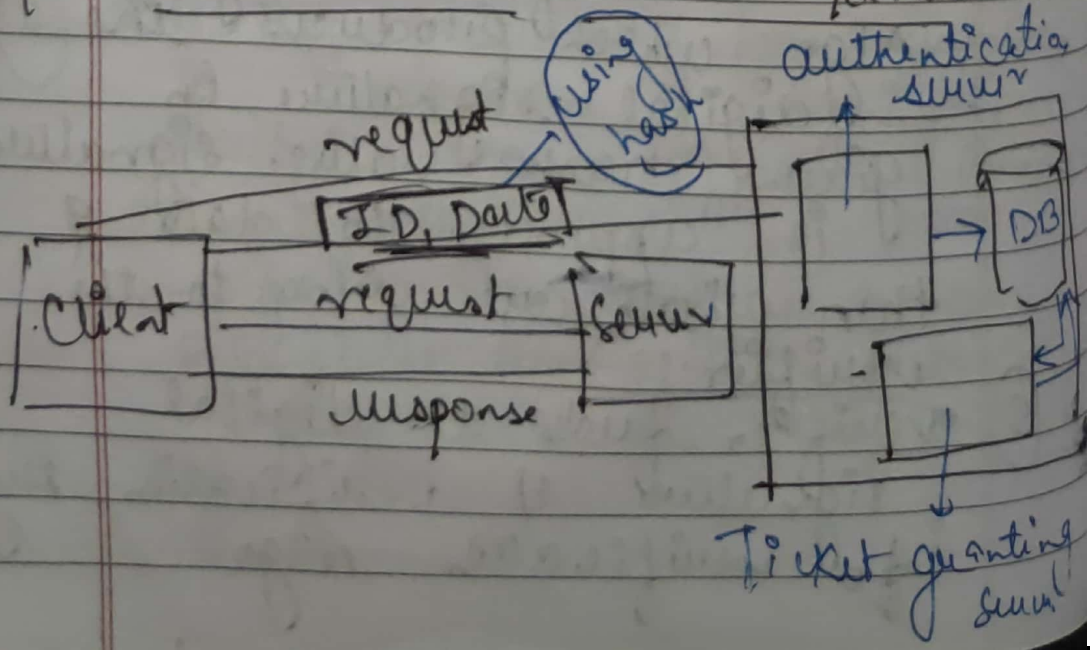
verification algo gives some value as output

(6) verifier also runs some hash function on received data

(7) to generate hash value.
for verification this hash value & output of verification algo are compare. Based on the comparison result, verifier decides wheather is digital sign is valid or not

(8) since digital sign is created by private key of signer & no one is can have this key the signer cannot repudiate signing the data in future

Authentication Server — Kerberos



DATE
PAGE
"Rough 'n' Fair"

Kerberos provide a synchronised authentication server whose function is to authenticate users to servers & server to users. In Kerberos authentication server & database is used for client authentication Kerberos runs as 3rd party trusted server known as the Key distribution Center (KDC)

Each user & service on network is a principle. The main component of Kerberos are

(1) Authentication server :- It performs the initial authentication & Tickets for Ticket granting service.

(2) Database :- The authentication server verifies the access rights of user in database.

(3) Ticket granting server (TGS)
↓
issues the Tickets for servers.

Sunil
DATE
PAGE
"Rough 'n' Fair"

Authentication Application - X.509

X.509 is digital certificate i.e been on top of the widely trusted standard in which the format of PKI certificate is defined

X.509 digital certificate is a certificate based authentication security framework that can be used for providing secure transaction & private info. These are primarily used for handling the security & identity in computer network & internet based comm. generally the certificate includes various elements such as

1. Version No.
2. Serial No.
3. Issuer Name
4. Period of validity
5. Subject Name
6. Subject's public key information
7. Signature certificate

etc

UNIT-4.

28/4/22

Cyber laws | Internet laws

cyber laws are also known as internet laws which is the part of the overall legal system that is related to legal informatics & supervises the digital circulation of information e-commerce, software & info. security. It is associated with legal info. & electronic element including computer, software, hardware etc it covers many area such as access to the usage of internet & online privacy.

Cyber laws helps to reduce or prevent people for cyber criminal activity on a large scale with the help of protecting info. assets from unauthorised user, guarantees freedom to speech privacy, email comm. website, hardware & software such as data storing device. As internet traffic is increasing rapidly occuring higher rate of legal issue world wide.

Cyber law offers legal protection for the people who are using internet as well as running bussiness online. it is most imp. for internet user to known about the local area & cyber laws of their country.

4. The computer fraud & abuse act was the 1st law of cyber that was implemented in 1983. According to this law any authorised person cannot access other users computer. this Act discribes the stage of ~~conti~~ punishment the range of penalty imposed.

Areas involves in Cyber laws

(1) Fraud Cyber laws are performed to prevent financial crimes such as identity threat credit card threat, ~~creating~~ prevailing online

ownership

Sunil
DATE
PAGE
"Rough 'n' Fair"

(2) copyright issue: strict rules are defined in cyber law if any one goes against copyright that protect the creativity of any individual or company.

(3) Online insult of character degradation.

There are multiple online social media that are the best resource that share your mind with everyone fully but their are some laws in cyber law if you speak, defame someone

→ Racialism → gender inequality

(4) Online harassment & stalking

Harassment is a big issue in cyber space because it is violating both criminal & civil laws.

Sunil
DATE
PAGE
"Rough 'n' Fair"

How to protect yourself from Internet

(1) **Verify data is intercepted**

when you are sending any confidential info such as debit card no., credit card no., user name or password send these info very carefully in the internet browser look for a small lock to verify this security.

(2) **Use a safe password**

like online Banking site or any other website that contains confidential info, password should be very strong that cannot be predicted easily

(3) **Keep your software & operating system up to date**

to protect yourself on internet it is better to update yourself OS regularly because many

Sunil
DATE
PAGE
"Rough 'n' Fair"

updats are released by develop. that are related to comp. security

(4) If available always enable 2-factor authentication.

(5) Always be cautious of email links & attachments.

(6) Be aware of fishing scams

(7) Use caution when accepting or agree to any prompts.

Advantage of cyber laws

(1) Organization are now able to carry out e-commerce using legal infrastructure provided by various acts.

(2) Digital sign have been given legal recognization & validity in the act.

(3) It has opened the doors for the entry of corporate company

for issuing digital sign certificate

(4) It allows govt to issue notification on the web

(5) IT act also addrss the imp. issue of security which are also critical to the success of electronic transactions.

25/4/22 Amit

DATE
PAGE
"Rough 'n' Fair"

left work of UNIT-3.

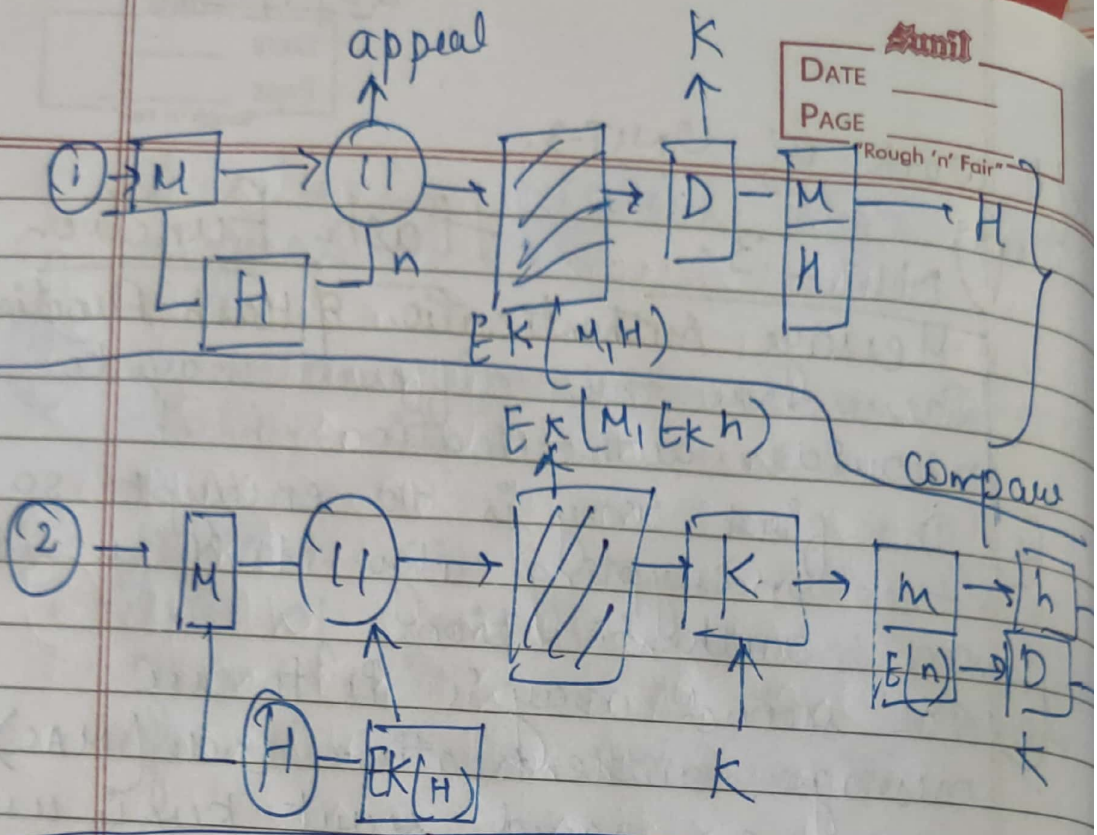
UNIT-3. Hash Function

Message Authentication & Hash Function

There are three different ways to provide authentication.

1. The first way is to encrypt so the encrypting algo itself provide an authentication.
2. The second way is is to use message authentication code (MAC) where a shared secret key is used to generate message authentication code, which provide message authentiticity
3. The thirtd ways [method] are hash function. Under this a message of variable length 'M' is given to the hash function & this hash function generate a hash value (h). This hash value is known as "message digest". Hash value also provide error detection apart from authentication of message.

⇒ The different scenerios where has funtion can be implemented are

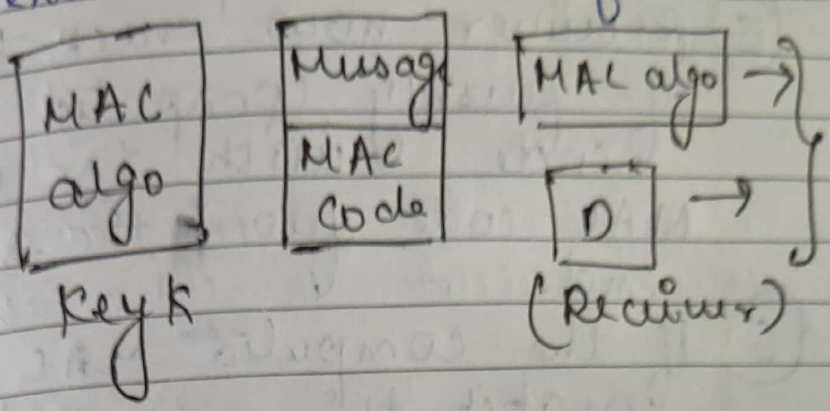


3 M → H → Hash value / message Digest

MAC (Message Authentication Code)

MAC Algorithm is a symmetric Algo to provide message authentication. For establishing MAC process the sender & reciver share a symmetric key. Essentially mac is encrypted checksum generated on the underlying message that is send along with a message to ensure message authenticity

The process of using MAC for authentication is as follows.



MAC - Explanation

1. The sender uses some publically known mac algo & takes the message as input along with the secret key 'K' & produce a mac value.
2. similar to hash, MAC function also have a variable message length but fixed input. The major difference b/w hash & MAC uses secret key but an advanced model of hash function works on public key cryptography.
3. The sender forwards the message along with mac code
4. On receipt of the message, the receiver feds the message &

& share secret key into MAC algo to recompute the MAC value

(5) Receiver now check the equality of freshly computed mac code with the received MAC code from the sender's end.

(6) If the computed MAC doesn't match the MAC sent by the sender, the receiver cannot determine whether it is the message that has been altered or it is the origin that has been falsified.

Hash Function

Takes a group of character or keys & maps it to a value of a certain length known as "hash value". The hash value is the representation of the string of characters but is normally of smaller length than the original message.

=> Hashing is used in encryption & also for indexing &

2/5/22 Imp

17-Oct 2000 Amit

DATE

PAGE

Date

Page No.

locating items in database.

Digital signature

Digital signature are the public key primitives of message authentication in the physical world. It is commanly known as handwritten signature or typed message. Similarly a digital signature is a technique that binds a person to a digital data. This binding can be independently verified by receiver as well as any third party.

Digital signature is a cryptographic value that is calculated from the data and a secret key which is known only to the sender. In real world the receiver of the message needs to assure that the message belongs to

the sender of he should not be able to repudiate (deny sending) the origin of that particular message, This requirement is very crucial in bussiness application, since likelihood of a dispute over exchanged data is very high.

9/5/22 Imp

17-Oct 2000 Sunil

DATE
PAGE
"Rough 'n' Fair"

E-governance & IT Act-2000
7 chp - 90 section

E in goverment stands for electronic goverment refers to lawful rules for management control & administration.
E-goverment needs application of electronic means in the interaction b/w

1. goverment - citizen
   citizen - govt
   Bussiness & govt
   govt - Buniness
   Internal govt. operations

Objective of E-governance

E-governance not only providing info. about various activities & organisation of the govt. but it envolves citizen to communicate with govt & participate in diseion making process

1. Putting govt-rules & regulation online

Sunil
DATE
PAGE
"Rough 'n' Fair"

(2) putting info. related to govt plans, E-budget, expenditure online.

(3) Giving of guidance & receiving feedback from govt.

E govt is a broader concept that deals with the whole spectrum of relationship & network within the govt regarding the usage of app. of ICT (Info. & comm. Technology)

E governance is a narrow concept that deals with the development of online services to the citizen & bussiness such as E-tags, E-transportation etc.

IT Act - 2000

Information Technology Act 2000 also known as IT Act 2000 is act proposed by Indian parliament on 17 Oct 2000. It is the most imp law of india dealing with cyber crimes & e-commerce.

Sunil
DATE
PAGE
"Rough 'n' Fair"

The main objective of this act is to carry lawful & trust worthy electronic digital & online transaction & to reduce online crimes.
This IT Act has 13 chapters & 90 sections. The last 4 sections that starts from section 91-94 deals with the emission to Indian panel court 1860 or ITC 1860.
The IT Act 2000 has 2 schechedules

(1) 1st schedules deals with document to which the Act shall not apply

(2) The second schedule deals with electronic signature & electronic authentication method.

Offensies & punishment in IT Act 2000

(1) Pampering with the computer source document

Sunil
DATE
PAGE
"Rough 'n' Fair"

(2) publishing of info in electronic form

(3) Penality for malicious purposes

(4) penality for publishing digital signature certificate with falls data.

(5) penalty for mis. representation

(6) power of investigating offence

(7) Act to apply for Offence committed outside India

(8) Publication for fraud purpose etc.

Sections & punishments under IT Act 2000 are as follows

(1) Section 43
This section of IT Act 2000 states that any act of destroying, altering, stealing comp system or network

without authorisation of owner of the comp. is liable for the payment or penalty

(2) section 66
Hacking of a computer system with malicious intensions like fraud. will be punished with 3 years imprisonment or & fine of ₹5,00,000 or both.

(3) section 66 E:
This section is for voilating of privacy by transmiting private images of privat videos is punishable with 3 years imprisonment or ₹2,00,000 fine or both

(4) Section 67
This section states publishing obscene info or transmition of obscene content in public is liable for imprisonment upto 5 years or a fine of ₹10,00,000 or both.

UNIT-5

5/5/22 → done intially

DOS (Denial of service)

Denial of service is a cyber attack on and individual computer or website with the intent to deny service to intended user. This purpose is to distrupt an organization network opration by denying excess to its users. DOS is typically accomplished by flooding the targeted machine or resource with sirplus request in an attempt to overload system & prevent some legal user request from being fulfilled.

For Example :- If a bank website can handle 10 users per second. An attacker only has to send 10 fake request per second so that no register user can login.

— Dos attack exploits various weakness in computer network

The may target servers, network routers etc to bog down the network.

The most famous DOS technique is PING OF DEATH ATTACK that works by generating & sending special Network messages that can cause problem at the victim system

Example: Ping ip-address -t 655600

- "Ping" sends the data packet to victim system"
- "ip-address" is the ip-address of the victim"
- "-t" means the data packet should be send until the system or program stops working."
- "655600" specified the data load which is to be diverted to victim system.

Sunil
DATE
PAGE
"Rough 'n' Fair"

Types of DOS Attack

(1) Flooding a network with useless activities so that genuine traffic cannot get services.
TCP/IP SYN & SMURF attack are 2 common example of this

(2) Remotely overloading systems CPU so that valid request cannot be processed.

(3) changing permission or breaking authorization logic to prevent user from logining into a system
One common ex- involve ~~logging~~ triggering a rapid series of false login attempts

(4) Deleting or interfering with specific critical application or services to prevent their normal operation.

Another variant of DOS is smurf attack.
This involves email with automatic response if someone is sending 100 - 1000 email to a random email id & if that random id belongs to some person this can overwhelms that person's acc.

Dos attack can cause diff problem

1. Ineffective Service
2. Inaccessible Service
3. Interruption of Network traffic
4. Connection Interferances

DO attack prevention

Cloud mitigation provider
Firewall
Internet Service Provider (ISP)