Cryptography & NW Security

Unit 1

→ Basic Cryptographic Techniques
→ Computational complexity
→ finite fields
→ Number Theory
→ DES & AES
→ Public key cryptosystem.
→ Traffic Confidentiality
→ Cryptanalysis
→ Intractable (hard) problems
→ Hash functions
→ OSI Security Architecture Privacy of Data.

Basic Cryptographic techniques

The basic function of Cryptography are encryption, decryption & cryptographic hashing.
Cryptography can be used to provide message Confidentiality & Integrity & Sender verification
In order to encrypt & decrypt msg. the Sender & recipient need to share a secret. It's like a Key, i.e. used to by the cryptographic algorithm.
The Key is used by the sender to encrypt the message (transform it into Cipher text) & by the recipient to decrypt the msg (reverse the Cipher text back to clear text). This process can be done on a fixed msg, such as an e-mail

or a Communications Stream, such as TCP / IP Connection.

Cryptographic hashing is the process of generating a fixed length string from a message of arbitary length.
Modern cryptographic systems are based on complex mathematical relⁿ e processes.

Computational Complexity

It's the study of the minimal Resources needed to solve computational problems. In particular, it aims to distinguish blw those problems that possess efficient algorithm (the "easy" problems) & those that are inherently intractable (the "hard" problems)

Types of Attack:

Active Attack: An Active attack attempts to alter system Resources or affect their Operation.
Here modification of original message is done.
This attack can't be prevented easily.
Active Attacks are of 3 types
1-) Interruption
2-) Modification
3-) Fabrication. (denial of service attack)

Passive Attack: In this the attackers aims to obtain the information. The attacker doesnot pretend or perform any modification in data. i.e. they are harder to detect.
There are 2 type of passive Attack
1. Release of message Content to other
2. Traffic analysis
In traffic analysis → hacker try to analyse ~~patt~~ message using a pattern that provide some clues regarding the communication.

DES

Data Encryption Standard is an outdated Symmetric-Key method of data encryption.

DES works by using the same key to encrypt & decrypt a message, so both the sender & the Receiver must know & use the same private key.
DES is a Symmetric-Key block cipher published by the ~~NIST~~ NIST.

Q: what is Cipher?
A: These earlier crypto systems are also known as Ciphers.
In general, a cipher is simply just a set of steps for performing encryption & Decryption

Nowad rely

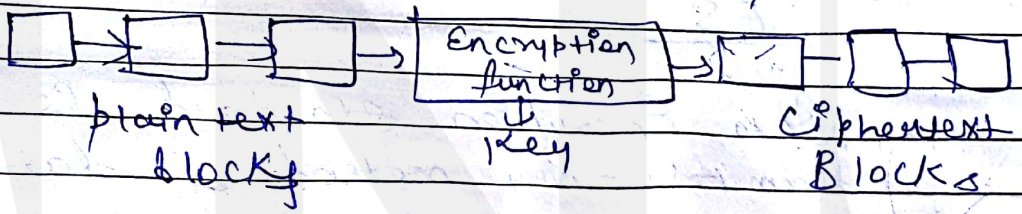
Page No.
Date:

Block ciphers & Stream ciphers

In this scheme, the plain binary text is processed in blocks of bits at a time; i.e. a block of plaintext bits is selected, a series of operations is performed on this block to generate a block of ciphertext bits & ~~a block of plaintext bits is selected, a series of operations is performed on this block.~~

The number of bits in a block is fixed.

for eg: the schemes DES & AES have block sizes of 64 & 128 respectively.



Stream ciphers: In this schemes, the plaintext is processed one bit at a time i.e. 1 bit of plaintext is taken & a series of operations is performed on it to generate 1 bit of ciphertext

Feistel cipher: It's not a specific scheme of block cipher. It's a design model from which many different block ciphers are derived.
DES is just one Eg. of a feistel cipher

eg. DES

from which many types of ciphers are derived

of 3 types

secure attac

DES & AES

block ciphers

The DES algorithm

The main parts of the algorithm are as follows:

- fractioning of the text into 64-bit (8-octet) blocks
- Initial permutation of blocks
- Breakdown of the blocks into 2 parts: left & right, named L & R;
- Permutation & Substitution steps repeated 16 times
- Re-joining of the left & right parts then inverse initial permutation

Basic principle of DES: It's a symmetric encryption system that uses 64-bit blocks, 8-bit of which are used for parity check. Each of the key parity bits is used to check one of the key's octet by odd parity, that is, each of the parity bits is adjusted to have an odd number of 1's in the octet it belongs to. The key therefore has a "useful" length of 56 bits, which means that only 56 bits are usually used in the algorithm.

AES (Advanced Encryption Standard)

Nowadays, AES is used more commonly than DES

128 bits treated as 16 bytes arranged in 4 rows & 4 columns

AES performs all its computations on bytes rather than bits. Hence, AES treats the 128 bits of a plaintext block as 16 bytes. These 16 bytes are arranged in 4 columns & 4 rows for processing.

Unlike DES, the number of rounds in AES is variable & depends on the length of the key.

AES uses 10 rounds for 128-bits keys, 12 rounds for 192-bit keys & 14 rounds for 256-bit keys.

(10 → 128 bits, 12 → 192 bits, 14 → 256 bits)

AES security is assured only if it's correctly implemented & good key management is employed.

* Asymetric Cryptography → also known as public key cryptosystem, uses public & private keys to encrypt & decrypt data. Either of the keys can be used to encrypt a message the opposite key from the I used to encrypt the message is used for decryption

* Cryptanalysis: refers to the study of ciphers, ciphertext or cryptosystems with a view to finding weakness in them that will permit retrieval of the plaintext from the ciphertext, without necessarily

Cryptographers: develops algorithms ... Cipher text & [illegible] to encrypt sensitive information. The [illegible] ential info. eg: In military.

Knowing the key or algorithm.

Below are some of the most common types of attacks:

→ Known-plaintext analysis: With this procedure the cryptanalyst has knowledge of a portion of the plaintext from the ciphertext.

→ Chosen plaintext analysis: The cryptanalyst is able to have any plaintext encrypted with a key & obtain the resulting ciphertext, but the key can't be analyzed itself. Here entire ciphertext is compared with original plaintext (to obtain cipher text).

(margin: can't analyze key)

→ Ciphertext-only analysis: The cryptanalyst has no knowledge of the plaintext & must work only from the ciphertext. This requires accurate guesswork as to how a message could be worded.

→ Man-in-the middle attack: It differs from other by involving tricking individuals into surrending their keys. Here cryptanalyst places him in the communication channel b/w 2 parties who wish to exchange their keys for secure communication. Then cryptanalyst perform a key exchange with each party, with the orignal party, making them believe that they are exchanging key with each other. The 2 parties end up using keys that are

① —— K1
② , K2 → K3

Known to the cryptanalyst.

Unit-2

Differential cryptanalysis → It's a general form of cryptanalysis applicable primarily to block cipher.
It's study of how differences in i/p can affect the output.

Q→ What is hash function? Process of generating fixed-length string from a message

A→ It's useful in almost all information security applications.
It's a mathematical function that converts a numerical i/p value into another compressed numerical value.
Value returned by a hash function are called msg digest.

Q→ What is Triple DES?

A→ Before using 3TDES, user 1st generate & distribute a 3TDES key K, which consists of 3 different DES keys K1, K2 & K3.
This mean that the actual 3TDES key has length 3×56 = 168 bits.

how encryption done

The encryption-decryption process is as follows:

- Encrypt the plaintext blocks using single DES with key K1
- Now decrypt the output of step 1 using single DES with key K2.
- finally, encrypt the output of

step 2: using single DES with key K2.
step 3: The output of step 3 is the ciphertext.
Decryption of a ciphertext is a reverse process. User first decrypt using K3, then encrypt with K2, & finally decrypt with K1.

key decryption performed

Triple DES systems are significantly more secure than single DES, but these are slow compared to DES due to following steps increased.

Q. What is Additive ciphers?

A. Additive ciphers is simplest code. Mathematically, it can be expressed like this

$$c = (p + a) \bmod 26$$

where p is position of the plaintext letter, a is the key, & c is the position of the resulting ciphertext letter.

Q. What is Affine cipher?

A. Here each letter in an alphabet is mapped to its numeric equivalent, encrypted using a simple mathematical function, & converted back to letters.

mathematically represented as $(ax + b) \bmod 26$, where b is magnitude of the shift.

What is playfair cipher?

In this Scheme, pairs of letters are

Page No.
Date:

encrypted, instead of single letters as did the.
Here key table of 5x5 grid is created that consists of alphabets that acts as the key for encrypting the plaintext. Each of plaintext must be unique letters of the alphabet is omitted from the table as we need only 25 alphabets instead of 26.

Date:

Cyber forensics

Cyber forensic is also known as Computer forensics. It's the applic^n of investigation & analysis techniques to gather & preserve evidence from a particular computing device in a way i.e suitable for presentation in a court of law.
The goal of Computer forensics is to perform a structured investigation while maintaining a documented chain of evidence to find out exactly what happened on a computing device & who was responsible for it.
Ethical hacking is key to strengthening n/w security & it's one of the most desired skill for any IT security professional. They have knowledge in problem-solving strategies for security breaches & can collect & analyze data to monitor & interpret weakness.

Comparison Chart for AES & DES

	DES	AES
Basic:	Data block is divided into 2 halves	Entire data block is processed as a single matrix.
	DES work on Feistal Cipher Structure	AES works on Substitution & permutation principle
	plaintext is of 64 bits	plaintext can be of 128, 192, 256 bits.
	has smaller Key compared to AES	AES has larger Key size

Page No.
Date:

DES	AES
★ 16 rounds	★ 10 round for 128
	12 " " 192
	14 " " 256
★ Less Secure	★ Larger secret key & Hence secure
★ Speed is Slower	★ AES is fast

RSA Cryptosystem

→ public-key algorithm — Key K1 – Encryption
Key K2 – Decryption

→ Encryption & Decryption use modular exponential
→ Discovered by Rivest, Shamir, Adleman

Algorithm

1. Choose 2 large prime no. $P \& Q$ such that $P \neq Q$.
2. Calculate $N \leftarrow P \times Q$.
3. Choose E (public key) such that E is not factor of $(P-1)$ & $(Q-1)$
4. Choose D (private key) such that $(D \times E) \bmod (P-1)(Q-1) = 1$
5. Ciphertext $(C.T) = (P.T)^E \bmod N$
6. Plain text $(P.T) = (C.T)^D \bmod N$

Eg:

(5), Alice — Bob.

1. $P = 7$, $Q = 11$
2. $N = 7 \times 11 = 77$
3. $(P-1)(Q-1) = 6 \times 10 = 60$
   $\boxed{E = 13}$
4. $(D \times E) \bmod (P-1)(Q-1) = 1$
   i.e $(D \times 13) \bmod 60 = 1$
   $\boxed{D = 37}$
5. $C.T = (P)^{13} \bmod 77$
   $C.T = 26$. ⟶
6. $(C.T)^D \bmod N$
   $(26)^{37} \bmod 77$
   $= 5$

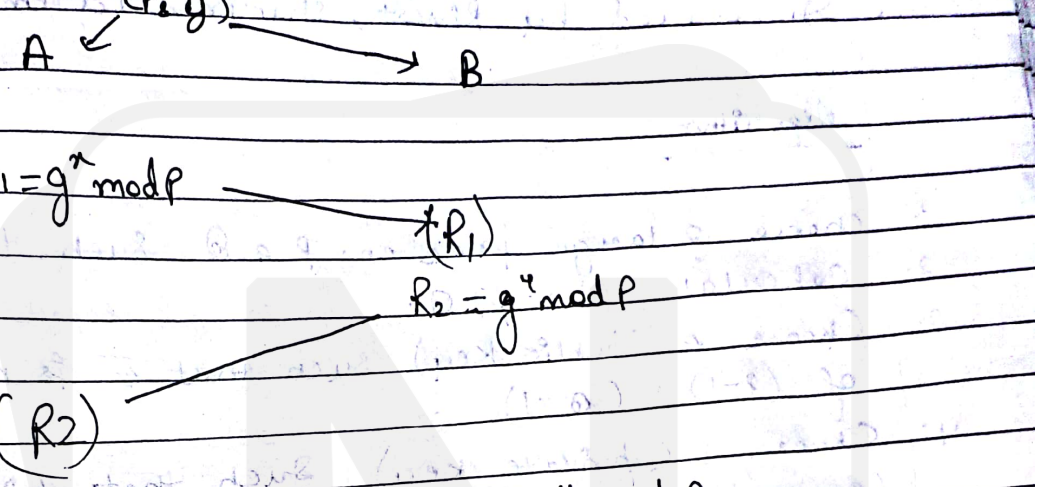
~~(6) RTP = (26)~~

Page No.
Date:

Diffie - Hellman Key Exchange

- Symmetric Key exchange.
  - Single Key for both Encryption / Decryption

Process:



Eg:

Alice — Bob

$g = 7, p = 23$.

A

~~B~~

$x = 3$

$y = 6$

$R_1 = 7^3 \bmod 23$

$= 21$ → 21

$R_2 = g^y \bmod P$

$= 7^6 \bmod 23$

$= 4$

4 ←

$K = (R_2)^x \bmod p$
$= (4)^2 \bmod 23$
$= 18$

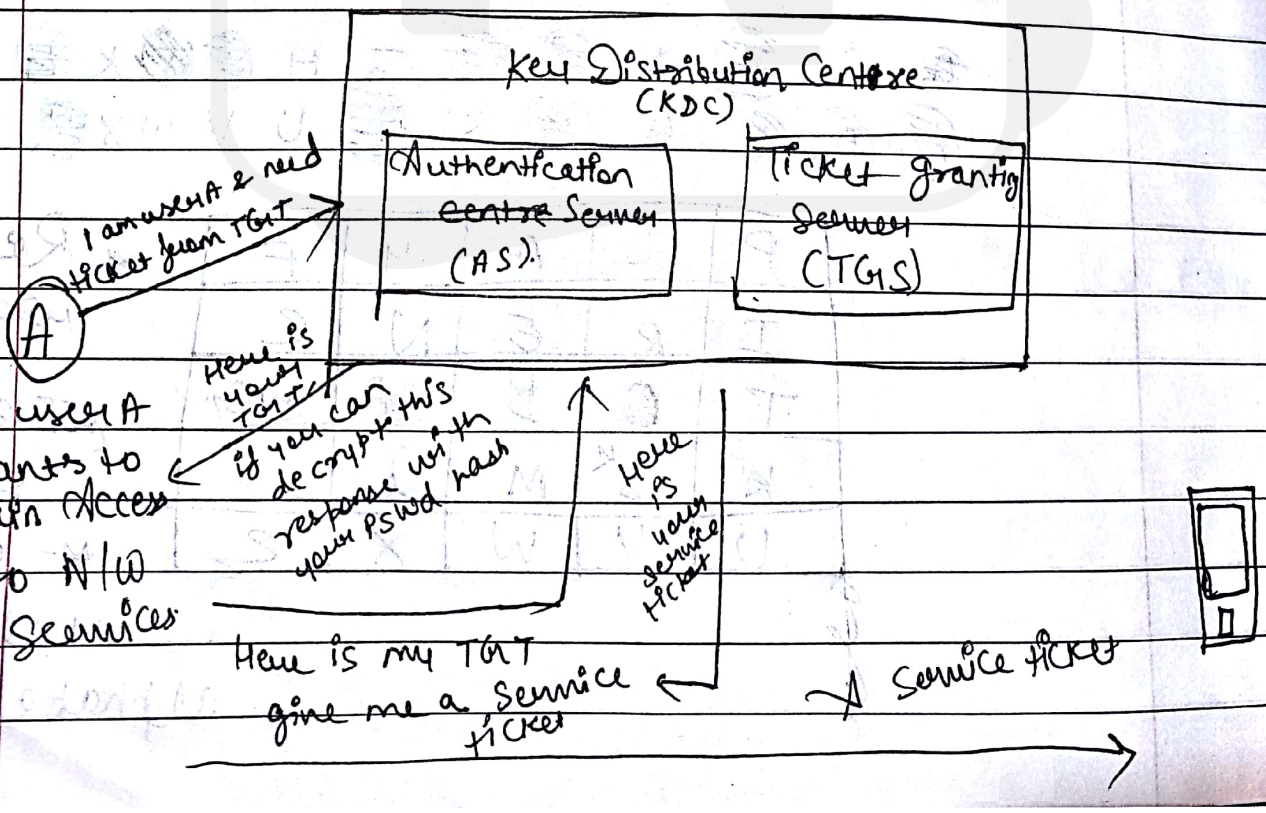
$K = (R_1)^y \bmod p$
$= (21)^6 \bmod 23$
$= 18$

Kerberos

→ It's a Computer Network authentication protocol which works on the basis of "tickets" to allow nodes communicate over a non-secure NW to prove their identity to one another in a secure manner.

→ Client-Server model
→ Symmetric key model
→ Requires a Trusted 3rd party → Key Distribution Centre (KDC)

(KDC) is database of secret key.
There are 2 types of KDC.
↳ Authentication Server (AS)
↳ Ticket Granting Server (TGS)



Page No.
Date:

Playfair Cipher.

- Invented by Charles wheatstone in 1854.
- 5×5 matrix table is used.
- method to Convert plain text to Cipher text

Algorithm

1. Choose Keyword ("Eg. playfair Encryption")
2. Enter characters of keyword in 5×5 matrix row-wise from left to right.
3. Fill remaining spaces in matrix with rest of English alphabet.
4. Combine I & J in same cell.

Encryption process

1. Broke the PT in gp of 2 alphabet.
2. If both alphabet are same (or only 1 is left), add an X after 1st 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.

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

* Repeated word not used
* I & J in same cell
* write unlyt alphabets

3. If both the alphabet in the pair appear in the same row of matrix, replace them with alphabets to their immediate right resp.
4. If both the alphabet in the pair appear in the same column, replace with alphabets immediately below them resp.
5. If the alphabet are not in same row or column, replace them with alphabets in the same row resp, but at other pair of corners.

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

eg: LY → AF
EM → BW
IO → TR

eg. NAME → NA → YE
ME → WB.

Encryption will be EYWB.

HIDE MONEYZ.

Page No.
Date:

Eg: As an example, we shall encrypt the plaintext "Hide the gold in the tree stump" using Keyphrase playfair Example.

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

Now we must split the plaintext into digraphs

hi de th eg ol di nt he tr ee st um p

So, now

hi de th eg ol di nt he tr ex es tu mp.

Now check from above table

MB OD ZB XD NA BE KU DM UI XM MO VV IF.

Page No.
Date:

Vernam Cipher

→ Implemented by using 1-time pad (key)
→ Length of I/p ciphertext (1-time pad) is equal to the length of original plaintext.

Algorithm:

1. Write each P.T. alphabet as no. (A=0, B=1, ... Z=25) or (A=1, B=2, ... Z=26)
2. Same for 1-time pad.
3. Add P.T. alphabet No. to 1 time pad no.
4. If Sum > 26, subtract 26 from it.
5. Convert each no. of sum to alphabet.

P.T → HELLO.

H	E	L	L	O
7	4	11	11	14] P.T

Key can be used any

X	M	C	K	L
23	12	2	10	11] Key

7	4	11	11	14 (P.T)
23	12	2	10	11 (Key)

30	16	13	21	25] P.T + Key
-26	↓	↓	↓	↓
4	16	13	21	25

E Q N V Z → receiver

* How to reverse back

4 16 13 21 25 (C.T)
23 12 2 10 11 (key)
-19 4 11 11 14

add 26 for -ve no.

7 4 11 11 14
H E L L O