End Semester Examination

Name: Mohrish Devaraj

Reg NO: 39110636

Roll NO: 19S115398

Date: 10th May 2022

Subject Name: Network Security

Subject code: SCSA1602

No. of pages: 6

360415522922958

(31) Explain in detail about various substitution techniques with example.

Ans:

Substitution technique is a classical encryption technique where the characters present in the original message are replaced by other characters or numbers or symbols. If the plain text (original message) is considered as the string of bits, then the substitution technique would replace bit pattern of plain text with the bit pattern of cipher text. The substitution techniques can be explained as follows:

a) ~~Ceas~~ Caesar Cipher

b) Monoalphabetic Cipher

c) Polyalphabetic Cipher

d) Playfair Cipher

e) One-Time pad

f) Hill Cipher

a) Caesar Cipher

The Caesar Cipher technique is one of the earliest and simplest method of encryption technique. each letter of a given text is replaced by a letter some fixed number of positions down the alphabet. For example with a shift of 1, A would be replaced by B, B would become C, and so on.

$D_n(x) = (x+n) \mod 26$ [Encryption]

$D_n(x) = (x-n) \mod 26$ [Decryption]

b) Monoalphabetic:

Monoalphabetic cipher is a substitution method in which a given key, the cipher alphabet for each plain alphabet is fixed throughout the encryption process. For example, if 'A' is encrypted as 'D', for any number of occurances in the plaintext, 'A' will always get encrypted to 'D'.

Eg: Message to Send: Hide the money

Secreat word: RICH

Letter position: 17-8-2-7

Adding Sequence: Hide the Money

17-8-2-7 17-8-2 7-17-8-2-7

c) Polyalphabetic Cipher

Alberti Cipher used a mixed alphabet to encrypt the plaintext, but at random points he would change to a different mixed alphabet, indicating the change with an upper case letter in the ciphertext.

Eg: Plain text : lean bat
Ciphertext: rGZJIWVOg

Plaintext: ..tistaa...
Ciphertext: ...gz OYZGGm

d) Playfair Cipher

It was used for tactical purposes by British forces in the second Boer War and in World war I and for the same purpose by the Australians during World war II. This was because Playfair is resonabley faste to use and requires no special ~~element~~ equipment.

Eg: text : Monarchy
Plain text : instruments

in st ru me nt sz
ga tl mz cl rq tx

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

e) One-Time pad:

In cryptography, a one time pad is a system in which a private key generated randomly is used only once to encrypt a message that is then decrypted by the receiver using a matching one-time pad and key. Messages encrypted with key based on randomness have the advantage that there is theortically no way to "break the code" by analysing a succession of messages.

eg:

Plaintext : H! $\xrightarrow[XOR]{}$ 1001000 1101001 0100001

f) <u>Hill Cipher</u>

Hill Cipher is a polygraphic substitution cipher based on linear algebra. Each letter is represented by a number modulo 26. Often the simple scheme A = 0, B = 1, ... Z = 25. is used, but this is not an essential feature of the cipher.

eg:
Input : Plaintext : ACT

key : GYBNQKLRP

Output : Ciphertext : POH

$$\begin{bmatrix} 6 & 24 & 1 \\ 13 & 16 & 10 \\ 20 & 17 & 15 \end{bmatrix} \begin{bmatrix} 0 \\ 2 \\ 9 \end{bmatrix} = \begin{bmatrix} 67 \\ 222 \\ 319 \end{bmatrix} = \begin{bmatrix} 15 \\ 14 \\ 7 \end{bmatrix} (\text{mod } 26)$$

$\downarrow$

'POH'

(34) What is kerberos? Briefly cex the kerberos overview with neat diagram.

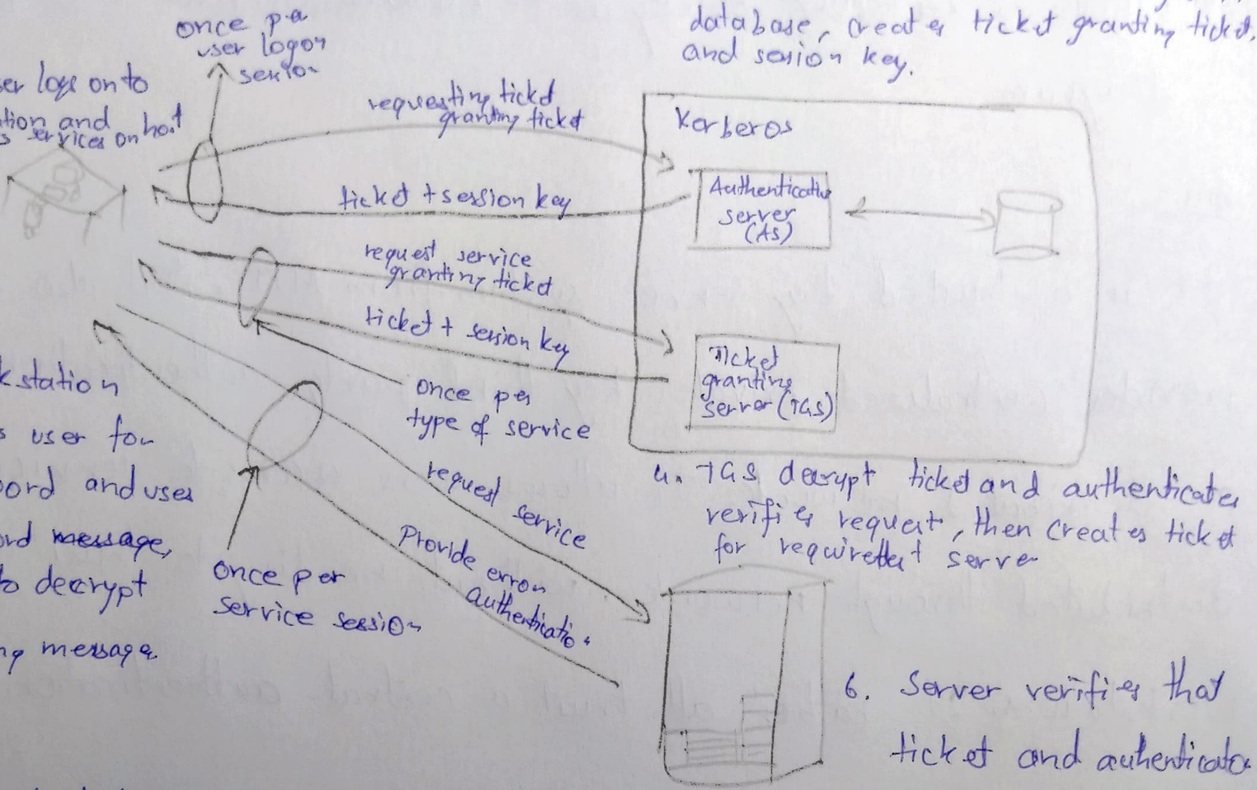
Ans.

It is a trusted key server system from MIT. And also it provides Centralised private-key third-party authentication in a distributed network. It allows users access to services distributed through network, without needing to trust all workstations. It rather all trust a central authentication error.

A basic third-party authentication scheme to have an Authentication Server (AS). The users initially negotiate with AS to identify self. As AS provide a non-Corruptible authentication credential (ticket granting ticket TGT). It have a Ticket ganting Server (TGS) which users subsequently request access to other services from TGS on basis of users TGT.

1. User logs onto workstation and requests services on host

2. AS verifies users access right is database, create ticket granting ticket, and session key.


once per user logon session
requesting ticket granting ticket
Kerberos
ticket + session key
Authentication server (AS)
request service granting ticket
ticket + session key
Ticket granting server (TGS)
once per type of service
request service
Provide server authentication
once per service session

3. Work station prompts user for password and user password message, then to decrypt incoming message

4. TGS decrypt ticket and authenticator verifies request, then creates ticket for requested server

6. Server verifies that ticket and authenticator match, then grants access to service. If manual authentication is required, server returns an authenticator.

5. Work station sends ticket and authentication to server