PNS School of Engineering & Technology
Branch: Computer Science & Engineering
6th Semester
Internal Assessment Question & Answer: 2023
Subject : C&NS(Th1)

N.1 (a) What is need for security?

Network needs security against attackers & hackers

Network security includes two basic securities, first is security of data i.e to protect data from unauthorized access & loss during transmission over the internet & second is computer security i.e to protect computer systems from unwanted damages caused due to network.

(b) What is crypt analysis?

It is the technique of decoding messages from a non-readable format back to a readable format.

It is done without knowing how they were initially converted from readable format to non-readable format.

(c) What is cipher text . Give an example.

When plain text is codified(encoded) using any scheme ,the resulting message is called as cipher text.

Eg:- A B C ----- PLAIN TEXT
D E F ------ CIPHER PEXT

(d) Write down polygram substitution cipher with example.

In this substitution cipher one group of characters are substituted by other group of characters.

In this technique one block of plain text are replaced as a block but not character by character.

Eg:- HELLO is replaced by yuqqw
HELL is replaced by tequ

(e) Write short note CA.

Certification Authority(CA) is a trusted agency / entity that issues the digital certificate.

Usually CA is a reputed organization & responsible for the verifying the identity of requesting entity before issuing a certificate & then signs the certificate using its private key . SafeScript ltd. Is an first Indian CA.

No.2

a) Short notes on Digital certificate.

A digital certificate is simply a small computer file. For example, my digital certificate would actually be a computer file with a file name such as name .cer.

The digital certificate is actually quite similar to a passport. As we know every passport has a unique passport number, similarly every digital certificate has a unique serial number. Also gives information of the issuer's name, serial number, public key, validity period, etc.

Digital Certificate is issued by a trusted agency called as CA (Certification Authority).

Another third party called as RA (Registration Authority) acts as a intermediate entity between CA and end user.

Contents of Digital Certificate:

Version: Version of X.509 protocol. Version can be 1,2 or 3

Certificate Serial No.: Contains unique integer which is generated by CA

Signature Algorithm Identifier: Identifies the algorithm used by CA to sign the certificate.

Issuer Name: Identifies the Distinguished Name that created & signed the certificate

Validity: (not before/not after) Contains two date-time values. This value generally specifies the date & time up to seconds or milliseconds.

Subject name: Distinguished Name of the end user (user or organization)

Subject Public key info.: This field can never be blank. Contains public key & algorithm related.

Issuer Unique Identifier: Helps identify a CA uniquely if two or more CAs have used the same Issuer Name over time.

Subject Unique Identifier: Helps identify a subject uniquely if two or more subjects have used the same Subject Name over time.

(b) Write down the advantages of digital signature.

Advantages of digital signature are:

➢ A normal message authentication scheme protects the two communicating parties against attacks from a third party (intruder). However, a secure digital signature scheme protects the two parties against each other also.

Message integrity:

➢ Digital signatures also provide message integrity.

➢ If a message has a digital signature, then any change in the message after the signature is attached will invalidate the signature.

➢ That is, it is not possible to get the same signature if the message is changed. Moreover, there is no efficient way to modify a message and its signature such that a new message with a valid signature is produced.

Non-repudiation:

➢ Digital signatures also ensure non-repudiation.

➢ For example, if A has sent a signed message to B, then in future A cannot deny about the sending of the message. B can keep a copy of the message along with A's signature.

➢ In case A denies, B can use A's public key to generate the original message. If the newly created message is the same as that initially sent by A, it is proved that the message has been sent by A only.

➢ In the same way, B can never create a forged message bearing A's digital signature, because only A can create his or her digital signatures with the help of that private key.

Message confidentiality:

➢ Digital signatures do not provide message confidentiality, because anyone knowing the sender's public key can decrypt the message.