Page No.:
Date: 24/05/21

YOUVA

Mock Test

CSS

AMEY MAHENDRA THAKUR

TE COMPS B-50

TU3F1219127

Q2

Q2 A] RSA $n = 221$ & $e = 5$ $d = ?$

Q2 A] Diffie-Hellman $g = 7$, $P = 23$, $x = 3$, $Y = 5$

Q2 B] Digital Certificate X.509 standard

Q3

Q3 A] ARP Spoofing and Port Scanning

Q3 B] Cross-Site Scripting (XSS) with its types

Q3 B] Virus with its types

6(A)

RSA

$n = 221$, $e = 5$

There are two requirements

- n must be a product of two primes
- e must be relatively prime to $\phi(n)$.

First requirement

$n = 221 = 13 \cdot 17$. 13 and 17 are primes

So this holds.

Second requirement

If $n = p \cdot q$ where p and q are distinct primes. then $\phi(p \cdot q) = (p-1) \cdot (q-1)$

So, $\phi(221) = (13-1) \cdot (17-1) = 12 \cdot 16 = 192$

$e * d \bmod \phi(n) = 1$; $5 * d \bmod 192 = 1$

d is calculated using the following method

We continue till we get an integer

$$d = \frac{[\phi(n) * i] + 1}{e} = \frac{[192 * 1]}{5} = 38.6$$

where, $i = 1$ to 100

SIGNATURE: Amey

For $i = 2$

$$d = \frac{(192 * 2) + 1}{5}$$

$$= \frac{384 + 1}{5}$$

$$= \frac{385}{5}$$

$$\therefore d = 77$$

SIGNATURE: Amey

6 (A)

Diffie - Hellman Protocol

$g = 7$, $p = 23$, $x = 3$, $y = 5$

$R_1 = p^x \bmod g = 23^3 \bmod 7$

$= 12167 \bmod 7$

$R_1 = 1$

$R_2 = p^y \bmod g = 23^5 \bmod 7$

$= 6436343 \bmod 7$

$R_2 = 4$

Secret key 1 $= R_2^x \bmod g$

$= 4^3 \bmod 7$

$= 1$

Secret key 2 $= R_1^y \bmod g$

$= 1^5 \bmod 7$

$= 1$

Secret key 1 = Secret key 2 = 1

∴ Symmetric Key $k = 1$

SIGNATURE: Amey

6 (B)

Digital Certificate X.509 standard

- Digital certificate is an electronic file that is used to identify people and resources over a insecure channel or a network called internet. Digital certificate also enable secure confidential communication between sender and receiver using encryption.
- For example when we travel to another country, our passports provides a way to establish our identity and gain entry. Digital certificate provide similar identification in the electronic world.
- The role of Certification Authority (CA) is to issue certificates with authorized digital signature. Much like the role of the passport office, the role of the CA is to validate the certificate owner's identity and to "sign" the certificate so that it cannot be tampered by unauthorized users.
- Once a CA has signed a certificate, the owner can present their certificate to people, web sites and network resources to prove their identity for confidential communications over insecure channel

SIGNATURE: Amey

- A standard called as X.509 defines structure of digital certificate. The International Telecommunication Union (ITU) permitted this standard in 1998.

The following diagram shows the structure of X.509 digital certificate.

Digital Certificate Contents
Certificate Version Number
Certificate Serial Number
Algorithm for signature identifier
Certificate Issuer Name
Validity Details
Name of the certificate Owner
Public key of Certificate Owner
Issuer Unique Identifier
Owner Unique Identifier
Extentions to certificate
Certificate Authority (CA) Digital signature

Structure of X.509 Digital Signature

- A standard digital certificate typically includes a variety of information pertaining to its owner and to the Certificate Authority (A Trusted Agency that can issue Digital Certificate)

SIGNATURE: Amey

Such as:

1. Certificate Version Number
   - Identifies a particular version of the X.509 Current version is X.509 v3

2. Certificate Serial Number
   - Unique Integer Number generated by certification authority

3. Algorithm for signature Identifier.
   - Identifies algorithm used by the certification authority to sign the certificate

4. Certificate Issuer Name
   - The name of the certification authority that issued the certificate

5. Validity Details
   - The validity period of the certificate

6. Name of the certificate owner
   - The name of the owner and other identification information required for identifying the owner such as email ID and contact details

SIGNATURE: Amey

⑦ Public key of certificate owner
- Certificate owners public key which is used to encrypt confidential information of the certificate owner.

⑧ Issuer Unique Identifier
- Identify the CA uniquely

⑨ Owner Unique Identifier
- Identify the owner uniquely

⑩ Extensions to certificate
- This is an optional field which allows a CA to add additional private information to the certificate

⑪ Certificate Authority (CA) Digital Signature
- In creating the certificate, the information is digitally signed by the issuing CA.

SIGNATURE: Amey