14.5
15

B030

Bhatt Pranjal Deepak

Date : / /

Page No. :

CSS Assignment -2

Assignment 2

3-4-25

Q1 Discuss RSA as a digital signature algorithm

→ RSA (Rivest -Shamir -Adleman) is a widely used public key cryptographic algorithm that can be used both for encryption & digital signature. When used as a digital signature algorithm, RSA provides authentication, data integrity & non repudiation

How RSA Digital signatures work.

① Key Generation:

A user generates two keys:

Private key (d,n) : Kept secret

Public key (e,n) : Shared with others

The keys are generated by selecting two large prime number and computing $n = p * q$ & then deriving e & d

② Signing Process:

The sender creates a hash of the message. The hash is then encrypted using the sender's private key:

Signature = $(\text{Hash})^{d} \bmod n$

This signature is sent along with the message

③ Verification Process:

The receiver computes the hash of the received message. The receiver decrypts the received signature using the sender's public key:

Decrypted Hash = $(\text{Signature})^{e} \bmod n$

If Decrypted Hash matches the computed message hash, the signature is valid..

Advantages:

① Proven security

Supervisor's Sign. :

Bhatt Pranjal
B030

③ Evaluate the findings
Once the valnerabilities have been idenbified, you noed to carefully evaluate the impact those vuln-orability should bie prioritized according to is impact

④ Fix the findings
The findings from penetration testing are then fixed in order of their impact Fixing the finding is a crucial step to ensure that the attacker cannot exploit them.

14.5
15

3-4-25