

14.5
15

B030

Bhatt Pranjal Deepak

CSS Assignment - 2

Date : / /

Page No. :

Assignment 2

2-4-25

Q1 Discuss RSA is 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 numbers 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:

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

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:

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

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

Advantages:

① Proven security.

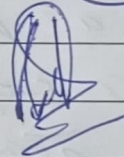
③ Evaluate the findings

Once the vulnerabilities have been identified, you need to carefully evaluate the impact these vulnerabilities should be prioritized according to its 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.

$$\frac{14.5}{15}$$



3-4-25