Computer Networks

Assessment - II

B. Krishna Sai
III - I , IT-B
2107 1A1272

1. Explain RSA Algorithm:

RSA (Rivest - Shamir - Adleman) is a widely used asymmetric cryptographic algorithm for secure data transmission. It involves key-pairs - a public key used for encryption and a private key for decryption. The Algorithm relies on the difficulty of factoring the product of two large prime numbers.

(i) Key generation:

⇒ Choose two large prime numbers p and q.

⇒ Compute $n = pq$, where n is part of the public key.

⇒ Compute $\phi(n) = (p-1)(q-1)$ where $\phi$ is Euler's totient function.

⇒ Select an integer e such that $1 < e < \phi(n)$ and e is coprime with $\phi(n)$. e becomes the public exponent.

⇒ Calculate d, the modular multiplicative inverse of $e \pmod{\phi(n)}$. d becomes the private exponent.

(ii) Public Key:

⇒ The public key is (n, e). n is used as the modulus for both the public and private keys.

(iii) Private Key:

⇒ The private key is (n, d)

(iv) Encryption:

⇒ Sender obtains the receipient's public key (n, e).

⇒ Convert the plaintext messages to a numeric value m.

⇒ Compute the ciphertext $c = m^e \pmod{n}$.

(V) Decryption:-

⇒ Recipient uses their private key $(n, d)$.

⇒ Compute $m = c^d \pmod{n}$ to obtain the original plaintext.

The security of RSA relies on the difficulty of factoring the product of two large primes, making it secure against attacks based on current algorithms. However it is important to use sufficiently large key sizes to withstand advancement in computing power.

Write short notes on above security service.

a) Message confidentiality.

b) Message Integrity.

c) Message Authentication.

d) Digital Signature

e) Entity Authentication.

f) Key Management.

a) Message confidentiality :-

⇒ Ensures that the content of a message remains private and accessible only to authorised users.

⇒ Achieved through encryption techniques, where the message is encoded to prevent unauthorised access.

b) Message Integrity :-

⇒ Ensures that the content of a message remains unchanged during transmission.

⇒ Involves using hashing or checksum techniques to create a unique value for a message, sent along with the message

c) Message Authentication:

⇒ verifies the origin of a message, confirming the identity of sender.

⇒ Utilizes authentication codes or protocols to ensure that a message is indeed sent by the claimed source.

d) Digital Signature:

⇒ Provides a way to verify the authentication and integrity of a digital message.

⇒ Involves the use of a private key to create a unique signature, which can be verified using the corresponding public key, confirming the sender's identity and that the message has not taken tampered with.

e) Entity Authentication:

⇒ Validates the identity of entities participating in network communication.

⇒ Employs methods such as password, digital certificates or biometrics to ensure that entities are who they claim to be.

f) Key management in Computer Networks:

⇒ Encompasses the generation, distribution, storage and revocation of cryptographic keys.

⇒ Crucial for maintaining the security of networked systems ensuring that keys are handled securely throughout their lifecycle to prevent unauthorised access or compromise. Proper key management is vital for secure communication and data protection in computer networks.