A→

Q.13 Using Rivest, Shamir, Adleman cryptosystem with P=7 and q=9, Encrypt M=24 to find ciphertext. The ciphertext is.

A→

Q.14 RSA algorithm is —— cryptography algorithm

A→

Q.15 Private key algorithm is used for - encryption and public key algorithm is used for — + — encryption.

A→

Section - B

Q.1 What are the disadvantages of asymmetric cryptography.

A→
- It is slow process compared to symmetric cryptography
- If an individual loses his private key, he can't decrypt the messages he receives.

- If a malicious actor identifies a person's private key, the attacker can read that individuals message.
- Public key's are not authenticated, no one can ensure a public key belongs to the person specified Consequently, users must verify that their public keys belong to them.

Q.2 Mention any one technique of attacking RSA.

A→ Plain Text Attack :-
Plain text attacks are classified into three categories.
1) short message attack
2) Cycling attack
3) Unconcealed message attack.

Q.3 What primitive operations is used in RC5?

A→ There are Three primitive operations:
1) integer addition
2) bitwise XOR - (exclusive -or)
3) variable rotations

Q.4 What are the properties a digital signatures should have?

A→ 1) Authenticity
2) Unforgeability
3) Non-re-usability
4) Non-repudiation
5) Integrity

Q.5 Differentiate between Asymmetric Cryptography and Symmetric Cryptography.

A-> Symmetric Cryptography	Asymmetric Cryptography
1) There is only one key is used between sender and receiver.	There are a group of pair is used between sender and receiver (public and private key)
2) It is effective as this technique is recommended for high amount of data.	It is inefficient as this technique is used for short message
3) The length of key used is frequently 128 or 256 bits, based on the security level.	The length of the key much higher such as the recommended RSA key size is 2048 bits or higher.
4) It is also known as symmetric key/secret key cryptography	It is also known as public key or conventional public system.

Section - C

Q.1 What is the Real crux of RSA?

A→ The Real crux of RSA algorithm is:

→ The knowledge of the public key does not reveal the secret key.

Q.2 What is the important aspect that establishes trust in digital signatures.

A→ A digital signature - a type of electronic signature - is a mathematical algorithm routinely used to validate the authenticity and integrity of a message. Digital signatures create a virtual fingerprint that is unique to a person or entity and are used to identify users and project information in digital messages or documents.

Integrity:-

The digital signature preserves the integrity of a message because, if any malicious attack intercepts a message and Partially or totally changes it then the decrypted message would be impossible.

Authentication:-

we can use the following reasoning to show how the message is authenticated. if a intruder (user X) sends a message pretending that it is coming from someone else (user A), user X uses her own private key to encrypt the message. The message is decrypted by using the public key of user A. Therefore this makes the message unreadable

Non-Repudiation:-

Digital signature also provides non-repudiation. if the sender denies sending the message, then her private key corresponding to her public key is tested on the plaintext. if the decrypted message is the same as the original message, then we know that the sender has sent the message.

Q.3 Which two type of key does asymmetric Cryptography use.