SRI VIDYA COLLEGE OF ENGINEERING & TECHNOLOGY

DEPARTMENT OF COMPUTER SCIENCE AND ENGINEERING

QUESTION BANK

Year / Dept / Sem:	**IV / CSE / 07**	**Subject code:**	**CS6701**
Staff Name :	**M.Mohana**	**SubjectName:**	**Cryptography and Network Security**

UNIT-V

PART-A

1. Define key Identifier?

PGP assigns a key ID to each public key that is very high probability unique with a user ID. It is also required for the PGP digital signature. The key ID associated with each public key consists of its least significant 64bits.

2. List the limitations of SMTP/RFC 822?

1. SMTP cannot transmit executable files or binary objects.
2. It cannot transmit text data containing national language characters.
3. SMTP servers may reject mail message over certain size.
4. SMTP gateways cause problems while transmitting ASCII and EBCDIC.
5. SMTP gateways to X.400 E-mail network cannot handle non textual data included in X.400 messages.

3. Define S/MIME?

Secure/Multipurpose Internet Mail Extension(S/MIME) is a security enhancement to the MIME Internet E-mail format standard, based on technology from RSA Data Security.

4. What are the different between SSL version 3 and TLS?

SSL	TLS
* In SSL the minor version is 0 and	* In TLS, the major version is 3 and the minor
major version is 3.	version is 1.
* SSL use HMAC alg., except that the padding bytes concatenation.	* TLS makes use of the same alg.
* SSL supports 12 various alert codes.	* TLS supports all of the alert codes defined in SSL3 with the exception of no _ certificate.

6. What are the services provided by PGP services.

- Digital signature
- Compression
- Segmentation
- Message encryption
- E-mail compatibility

7. Why E-mail compatibility function in PGP needed?

Electronic mail systems only permit the use of blocks consisting of ASCII text. To accommodate this restriction PGP provides the service converting the row 8-bit binary stream to a stream of printable ASCII characters. The scheme used for this purpose is Radix-64 conversion.

5. Name any cryptographic keys used in PGP?

- One-time session conventional keys.
- Public keys.
- Private keys.
- Pass phrase based conventional keys.

6. Define S/MIME.

Secure / Multipurpose Internet Mail Extension(S/MIME) is a security enhancement to the MIME internet E-mail format standard, based on technology from RSA Data security.

7. What are the services provided by PGP services?

- Digital signature
- Compression
- Segmentation
- Message encryption
- E-mail compatibility

8. Name any cryptographic keys used in PGP?

- One time session conventional keys
- Public keys
- Private keys
- Pass phrase based conventional keys.

9. What are the steps involved in SET transaction?

- The customer opens an account.
- The customer receives a certificate
- Merchants have their own certificate
- The customer places an order.
- The merchant requests payment authorization.
- The merchant confirm the order.
- The merchant provides the goods or services.
- The merchant requests payments.

10. List out the features of SET.

- Confidentiality
- Integrity of data
- Cardholder account authentication
- Merchant authentication

11. What is security association?

A security association (SA) is the establishment of shared security attributes between two network entities to support secure communication.

12. What does Internet key management in IPSec?

Internet key exchange (IKE) is a key management protocol standard used in conjunction with the Internet Protocol Security (IPSec) standard protocol. It provides security for Virtual Private Networks (VPNs) negotiations and network access to random hosts.

13. List out the IKE hybrid protocol dependence.

- ISAKMP - Internet Security Association and Key Management Protocols.
- Oakley

14. What does IKE hybrid protocol mean?

Internet Key Exchange (IKE) is a key management protocol standard used in conjunction with the internet protocol security (IPSec) standard protocol. It provides security for Virtual Private Networks (VPNs) negotiations and network access to random hosts.

15. What are the two security services provided by IPSec?

- Authentication Header (AH)
- Encapsulating Security Payload (ESP).

16. What are the fields available in AH header?

- Next header
- Payload length
- Reserved
- Security parameter
- Sequence number Integrity check value

17. What is virtual private network?

VPN means virtual private network, a secure tunnel between two devices.

18. What is ESP?

ESP- encapsulating security payload provides authentication, integrity and confidentiality, which protect against data tempering and provide message content protection. IPSec provides standard algorithms, such as SHA and MD5.

19. What is Behavior-Blocking Software (BBS)?

BBS integrates with the OS of a host computer and monitors program behavior in real time for malicious actions.

20. List password selection strategies.

- User education
- Reactive password checking
- Computer-generated password.
- Proactive password checking.

PART-B

1. Explain the operational description of PGP.
2. Write Short notes on S/MIME.
3. Explain the architecture of IP Security.
4. Write short notes on authentication header and ESP.
5. Explain in detail the operation of Secure Socket Layer in detail.
6. Explain Secure Electronic transaction with neat diagram.
7. Write brief note on E-mail Security.
8. Write brief note on IP Security.
9. Write brief note on Web Security.
10. Explain about PKI in detail.
11. Describe about SSL/TLS Protocol.
12. Explain in detail the operation of Internet Key Exchange with an example.