UNIT 5 – 2 MARKS

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 theMIME

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

SSL	TLS
In SSL , the minor version is zero and themajor version is 3	In TLS, the major version is 3 and the minor version is 1
SSL use HMAC algorithm, except that the padding bytes concatenation	Make use of the same algorithm
SSL supports 12 various alert codes	It supports all of the alert codes defined in SSL3 with the exception of no-certificate.

5. **What are the services provided by PGP services.**

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

6. **Explain the reasons for using PGP?**

- It is available free worldwide versions that run on a variety of platforms,including DOS/Windows, UNIX, Macintosh and many more
- It is based on algorithms that have survived extensive public review and are considered extremely secure (eg). RSA,DSS
- It has a wide range of applicability from corporations that wish to select andenforce a standardized scheme for encrypting files and communication
- It was not developed by nor and is it controlled by any government or standard organization.

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.

8. **Name any cryptographic keys used in PGP?**

- One time session conventional keys
- Public keys

- Private keys
- Pass phrase based conventional keys.

9. **List out the features of SET.**

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

10. **What is security association?**

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

11. **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 forVirtual Private Networks (VPNs) negotiations and network access to random hosts.

12. **List out the IKE hybrid protocol dependence.**

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

13. **What does IKE hybrid protocol mean?**

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

14. **What are the two security services provided by IPSec?**

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

15. **What are the fields available in AH header?**

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

16. **What is virtual private network?**

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

17. **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.

18. **What is Behavior-Blocking Software (BBS)?**

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

19. **List password selection strategies.**

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

20. List out the applications of IPsec

- Secure branch office connectivity over the Internet
- Secure remote access over the Internet
- Establishing extranet and intranet connectivity with partners
- Enhancing electronic commerce security

21. Write down the benefits of IPsec

• When IPsec is implemented in a firewall or router, it provides strong security that can be applied to all traffic crossing the perimeter. Traffic within a company or workgroup does not incur the overhead of security-related processing.

• IPsec in a firewall is resistant to bypass if all traffic from the outside must use IP and the firewall is the only means of entrance from the Internet into the organization.

• IPsec is below the transport layer (TCP, UDP) and so is transparent to applications. There is no need to change software on a user or server system when IPsec is implemented in the firewall or router. Even if IPsec is implemented in end systems, upper-layer software, including applications, is not affected.

• IPsec can be transparent to end users. There is no need to train users on security mechanisms, issue keying material on a per-user basis, or revoke keying material when users leave the organization.

• IPsec can provide security for individual users if needed. This is useful for offsite workers and for setting up a secure virtual subnetwork within an organization for sensitive applications.

22. Differentiate Transport mode and Tunnel mode

Transport mode	**Tunnel mode**
Provide the protection from upper layer between 2 hosts	Provide the protection for entire IP Packet
ESP in this mode encrypts and optionally authenticates IP Payload but not IP headers	ESP in this mode encrypt authenticate the entire IP packet
AH in this mode authenticate the IP payload and select the portion of IP header	AH in this mode authenticate the entire IP packet plus selected portion of outer IP header

23. List services provided by IPsec?

• Access control
• Connectionless integrity
• Data origin authentication
• Rejection of replayed packets (a form of partial sequence integrity)
• Confidentiality (encryption)
• Limited traffic flow confidentiality

15 MARKS

1. How IPSec ESP does provide transport and Tunnel Mode operation? Explain with a neat sketch. (16)
2. What is the need for security in IP networks? Describe the IPv6 authentication header.(16)
3. What is PGP? Show the message format of PGP(8)
4. Explain the operational description of PGP(10)
5. Describe about the PKI. (8)
6. Identify the fields in ISAKMP and explain it.(8)
7. Evaluate the different protocols of SSL. Explain Handshake protocol in detail.(16)
8. Describe the phases of Internet key exchange in detail. (16)
9. Explain in detail about S/MIME. (8)