2 Marks

① Define S-DES with key generation concept?

Ⓐ The S-DES decryption algorithm takes an 8-bit block of ciphertext and the same 10 bit key can develop that ciphertext as input and makes the initial 8-bit block of plaintext.

② List the steps involved in the process of Block ciphers modes of operation?

Ⓐ Five modes of operations in the process of Block ciphers

- Electronic codebook mode (ECB)
- Ciphers block chaining mode (CBC)
- output feedback mode (OFB)
- Ciphers feedback mode (CFB)
- counter mode (CTR)

③ Give the applications of point of vulnerability?

Ⓐ * The LAN that the workstation is attached
* The wiring closet: tapping the wires
* communications links out of the wiring closet: invasive or inductive tapping
* processors along the path to the outside: modifying the hardware or Software, etc.

④ Analyze the issues in Traffic confidentiality?

Ⓐ Various issues arising in the placement of traffic flow confidentiality service and encipherment, traffic padding, and routing control security mechanisms in the open system interconnection OSI model are presented.

⑤ Generalize in detail about key distribution?

Ⓐ Key distribution is a major cryptographic component to Secure communication. For privacy data must be encryp with keys which are distributed Securely.

⑥ Define Randomness?

Ⓐ Randomness (entropy) is the cornestone of cryptography as it is used to generate session keys. the more random the numbers, the more secure the cryptographics System.

⑦ Evaluate the major tasks of pseudo random numbers?

Ⓐ The random numbers are difficult and hard to find we use algo algorithm techniques (Sequence of numbers) If the algorithm is good it will cause for radomness.

⑧ Formulate what is BBS generator?

Ⓐ The Blum-Blum-Shub (BBS) generator is one of the first and best known cryptographically Secure pseudo-random bit generators.

* If p and q are primes and $n = pq$

$$P \equiv q \equiv 3$$

$$x_0 = s_2 \bmod n$$

$$x_i = (x_i - 1)^2 \bmod n \quad B_i = x_i \bmod 2$$

⑨ Distinguish between end to end and link encryption?

Link Encryption	End to End Encryption
1. performed by service provider not user	1. performed by end-user
2. Encrypts all data along a communication path	2. Data remains encrypted in transmit to remote end
3. Encrypts routing data	3. Routing information is not encrypted.

⑩ Explain the principle elements in KDC element?

Ⓐ The KDC has three main components:

- An authentication server that perform the initial authentication and issues ticket-granting tickets for users
- A ticket granting server that issues service tickets that are based on the initial ticket-granting tickets.
- A principals database of secret keys for all the users and services that it maintains.