Multiple Choice Questions Chapter 3:

1. The strength of a Hash function against brute force attack depends on
2. Key used.
3. Length of Hash Code.
4. Strength of the algorithm.
5. Message Digest.

Answer – b) Length of Hash Code.

Reason – The strength of a hash function against brute-force attacks depends solely on

the length of the hash code produced by the algorithm. For a hash code of length *n*,

the level of effort required is proportional to the following:

Preimage resistant 2*n*

Second preimage resistant 2*n*

Collision resistant 2*n*/2

1. In RSA, bits in ‘e’ and ‘d’ should be larger because
2. Makes algorithm simpler.
3. Makes encryption process faster.
4. Increases Security of the algorithm.
5. Obeys the requirements of the algorithm.

Answer – c) Increases security of the algorithm.

Reason – When the values of bits in ‘e’ and ‘d’ are larger it makes the algorithm more secure since it increases the complexity of brute force attack and makes brute force attack almost impossible thus making the algorithm more secure.

1. The security of Dellfie Hellman Key exchange lies in the fact that
2. It uses Discrete Logarithms.
3. Keys are exchanged.
4. Uses Large values for keys.
5. Complex algorithm to decrypt.

Answer – a) It uses Discrete Logarithms.

Reason – The Dellfie Hellman Key exchange algorithm uses Discrete Logarithms to decrypt the Ciphertext. For large values it is very difficult to solve Dicrete Logarithms and hence makes it difficult to decrypt thereby increasing the security.