Multiple Choice Questions Chapter 2:

1. Which one of the following Symmetric Encryption Cipher is the most secure?
2. Caesar Cipher.
3. Monoalphabetic Cipher.
4. Transposition Cipher.
5. Block Cipher.

Answer – d) Block Cipher.

Reason – The other 3 options are less secure for the following reasons:

Caesar Cipher can have only 26 possible ciphers, hence anybody can break the cipher with brute force. Monoalphabetic Cipher do not change relative letter frequencies so they are easy to decrypt. Transposition Ciphers can be recognized since they have the same frequency distribution as the original text. Block Cipher is secure because they provide confidentiality and authentication by means of encryptions standards like DES, Triple DES and AES.

1. The main reason for using Triple DES over DES is
2. Brute force is impossible in Triple DES.
3. Triple DES uses multiple DES encryptions.
4. Triple DES uses Transposition.
5. Triple DES uses longer length keys.

Answer – b) Triple DES uses multiple encryptions.

Reason – DES uses only layer of encryption with only one kind of key. This makes DES less secure even though attacks like brute force are impossible on DES. In Triple DES there are multiple layers of encryptions. There are basically 3 distinct keys used which makes it more secure as compared to DES.

1. Which of the following is one of the secure methods of Key Distribution?
2. If A and B each have an encrypted connection to a third party C, C could deliver a key on the encrypted links to A and B.
3. A sends the key to B over an unknown third party channel.
4. A sends the key to B through a public platform.
5. A sends a key which was previously used and known to everybody and asks B to use it.

Answer – a) If A and B each have an encrypted connection

to a third party C, C could deliver a key on the

encrypted links to A and B.

Reason – In symmetric encryption both the parties share the same key. Hence the key should be distributed securely otherwise if the key is compromised then all the communication between the two parties is compromised. In options b), c) and d) the keys are distributed in an unsecure way whereas in option a) the key is distributed in a secure way by using an encrypted third party connection between A and B.