1. A symmetric encryption scheme has five ingredients: plaintext, encryption algorithm, ciphertext, decryption algorithm and secret key.

2. Cryptanalysis is the process of attempting to discover the plaintext or key.

3. A block cipher processes the input one block of elements at a time, producing an output block for each input block.

4. A stream cipher processes the input elements continuously, producing output one element at a time as it goes along.

5. An encryption scheme is computationally secure if the cost of breaking the cipher exceeds the value of the encrypted information and/or the time required to break the cipher exceeds the useful lifetime of the information.

6. The AES was issued as a federal information-processing standard and is intended to replace DES and 3DES with an algorithm that is more secure and efficient.

7. RC4 was designed in 1987 by Ron Rivest and is a variable key-size stream cipher with byte-oriented operations.

8. “The input to the encryption algorithm is the XOR of the next 64 bits of plaintext and the preceding 64 bits of ciphertext” is a description of the CBC mode of operation.

9. Unlike ECB and CBC modes, CTR mode requires only the implementation of the encryption algorithm and not the decryption algorithm.

10. The most powerful, and most common, approach to countering the threats to network security is encryption.

11. With end-to-end encryption the encryption process is carried out at the two end systems.

12. With link encryption each vulnerable communications link is equipped on both ends with an encryption device.

13. For symmetric encryption to work the two parties to an exchange must share the same key, which must be protected from access by others.

14. All encryption algorithms are based on two general principles: substitution and transposition.

15. The three most important symmetric block ciphers are: 3DES, AES, and DES.