1. In cryptography, what is cipher?  
a) algorithm for performing encryption and decryption  
b) encrypted message  
c) both algorithm for performing encryption and decryption and encrypted message  
d) decrypted message

Answer: a  
Explanation: Cipher is a method to implement encryption and decryption of messages travelling in a network. It’s used to increase the confidentiality of the messages.

2. In asymmetric key cryptography, the private key is kept by \_\_\_\_\_\_\_\_\_\_  
a) sender  
b) receiver  
c) sender and receiver  
d) all the connected devices to the network

Answer: b  
Explanation: The private key is kept only by the receiver of the message. Its aim is to make sure that only the intended receiver can decipher the message.

3. Which one of the following algorithm is not used in asymmetric-key cryptography?  
a) rsa algorithm  
b) diffie-hellman algorithm  
c) electronic code book algorithm  
d) dsa algorithm

Answer: c  
Explanation: Electronic code book algorithm is a block cipher method in which each block of text in an encrypted message corresponds to a block of data. It is not feasible for block sizes smaller than 40 bits.

4. In cryptography, the order of the letters in a message is rearranged by \_\_\_\_\_\_\_\_\_\_  
a) transpositional ciphers  
b) substitution ciphers  
c) both transpositional ciphers and substitution ciphers  
d) quadratic ciphers

Answer: a  
Explanation: In transposition ciphers, the order of letters in a plaintext message is shuffled using a pre-defined method. Some of such ciphers are Rail fence cipher and Columnar transposition.

5. What is data encryption standard (DES)?  
a) block cipher  
b) stream cipher  
c) bit cipher  
d) byte cipher

Answer: a  
Explanation: DES is a symmetric key block cipher in which the block size is 64 bits and the key size is 64 bits. It is vulnerable to some attacks and is hence not that popularly used.

6. Cryptanalysis is used \_\_\_\_\_\_\_\_\_\_  
a) to find some insecurity in a cryptographic scheme  
b) to increase the speed  
c) to encrypt the data  
d) to make new ciphers

Answer: a  
Explanation: Cryptanalysis is a field of study in which a cryptographic scheme is intentionally tried to breach in order to find flaws and insecurities. It is used to make sure that the scheme is least vulnerable to attacks.

7. Which one of the following is a cryptographic protocol used to secure HTTP connection?  
a) stream control transmission protocol (SCTP)  
b) transport layer security (TLS)  
c) explicit congestion notification (ECN)  
d) resource reservation protocol

Answer: b  
Explanation: TLS has strong message authentication and key-material generation to prevent eavesdropping, tampering and message forgery. It has been used since the year 1996.

8. Voice privacy in GSM cellular telephone protocol is provided by \_\_\_\_\_\_\_  
a) A5/2 cipher  
b) b5/4 cipher  
c) b5/6 cipher  
d) b5/8 cipher

Answer: a  
Explanation: The A5/2 cipher was published in the year 1996 and was cryptanalysed in the same year within a month. It’s use was discontinued from the year 2006 as it was really weak.

9. ElGamal encryption system is \_\_\_\_\_\_\_\_\_\_  
a) symmetric key encryption algorithm  
b) asymmetric key encryption algorithm  
c) not an encryption algorithm  
d) block cipher method

Answer: b  
Explanation: The ELGamal encryption system was made by Taher Elgamal in the year 1985 and is an asymmetric key algorithm. It is popularly used in PGP and other systems.

10. Cryptographic hash function takes an arbitrary block of data and returns \_\_\_\_\_\_\_\_\_  
a) fixed size bit string  
b) variable size bit string  
c) both fixed size bit string and variable size bit string  
d) variable sized byte string

Answer: a  
Explanation: Cryptographic hash functions are used in digital signatures and message authentication codes. The only issue with it is that it returns the same hash value every time for a message making it vulnerable to attackers to evaluate and break the cipher.