1. \_\_\_\_\_\_\_\_\_\_\_ is widely used today for protecting data in transit in a variety of applications such as data transfer on the Internet, and on cellular phone networks.  
a) Encryption  
b) Data mining  
c) Internet Security  
d) Architectural security

Answer: a  
Explanation: Encryption is also used to carry out other tasks, such as authentication.

2. In a database where the encryption is applied the data is cannot be handled by the unauthorised user without  
a) Encryption key  
b) Decryption key  
c) Primary key  
d) Authorised key

Answer: b  
Explanation: Even if the message is intercepted by an enemy, the enemy, not knowing the key, will not be able to decrypt and understand the message.

3. Which of the following is not a property of good encryption technique?  
a) Relatively simple for authorized users to encrypt and decrypt data  
b) Decryption key is extremely difficult for an intruder to determine  
c) Encryption depends on a parameter of the algorithm called the encryption key  
d) None of the mentioned

Answer: d  
Explanation: Here a, b and c are the properties have to be present in a good design of an encryption technique.

4. In which of the following encryption key is used to encrypt and decrypt the data?  
a) Public key  
b) Private key  
c) Symmetric key  
d) Asymmetric key

Answer: c  
Explanation: In public-key (also known as asymmetric-key) encryption techniques, there are two different keys, the public key and the private key, used to encrypt and decrypt the data.

5. Encryption of small values, such as identifiers or names, is made complicated by the possibility of \_\_\_\_\_\_\_\_\_\_  
a) Dictionary attacks  
b) Database attacks  
c) Minor attacks  
d) Random attacks

Answer: a  
Explanation: This happens when particularly if the encryption key is publicly available.

6. Which one of the following uses a 128bit round key to encrypt the data using XOR and use it in reverse to decrypt it?  
a) Round key algorithm  
b) Public key algorithm  
c) Advanced Encryption Standard  
d) Asymmetric key algorithm

Answer: c  
Explanation: The standard is based on the Rijndael algorithm.

7. Which of the following requires no password travel across the internet?  
a) Readable system  
b) Manipulation system  
c) Challenge–response system  
d) Response system

Answer: c  
Explanation: The database system sends a challenge string to the user. The user encrypts the challenge string using a secret password as encryption key and then returns the result. The database system can verify the authenticity of the user by decrypting the string with the same secret password and checking the result with the original challenge string.

8. Assymmetric Encryption: Why can a message encrypted with the Public Key only be decrypted with the receiver’s appropriate Private Key?  
a) Not true, the message can also be decrypted with the Public Key  
b) A so called “one way function with back door” is applied for the encryption  
c) The Public Key contains a special function which is used to encrypt the message and which can only be reversed by the appropriate Private Key  
d) The encrypted message contains the function for decryption which identifies the Private Key

Answer: b  
Explanation: An one-way function is a function which a computer can calculate quickly, but whose reversal would last months or years. An one-way function with back door can be reversed with the help of a couple of additional information (the back door), but scarcely without this information. The information for the back door is contained in the private Key.

9. Which is the largest disadvantage of symmetric Encryption?  
a) More complex and therefore more time-consuming calculations  
b) Problem of the secure transmission of the Secret Key  
c) Less secure encryption function  
d) Isn’t used any more

Answer: b  
Explanation: As there is only one key in the symmetrical encryption, this must be known by both sender and recipient and this key is sufficient to decrypt the secret message. Therefore it must be exchanged between sender and receiver in such a manner that an unauthorized person can in no case take possession of it.

10. Which is the principle of the encryption using a key?  
a) The key indicates which function is used for encryption. Thereby it is more difficult to decrypt an intercepted message as the function is unknown  
b) The key contains the secret function for encryption including parameters. Only a password can activate the key  
c) All functions are public, only the key is secret. It contains the parameters used for the encryption resp. decryption  
d) The key prevents the user of having to reinstall the software at each change in technology or in the functions for encryption

Answer: b  
Explanation: The encoding of a message is calculated by an algorithm. If always the same algorithm would be used, it would be easy to crack intercepted messages. However, it isn’t possible to invent a new algorithm whenever the old one was cracked, therefore the possibility to parameterize algorithms is needed and this is the assignment of the key.