The security of the Diffie-Hellman key exchange lies in the fact that, while it is relatively easy to calculate exponentials modulo a prime, it is very easy to calculate discrete logarithms.

True

Correct answer:

False

**Results for question 2.**

2

1 / 1 point

Private key encryption is used to produce digital signatures which provide an enhanced form of message authentication.

True

Correct answer:

False

**Results for question 3.**

3

1 / 1 point

The \_\_\_\_\_\_\_\_\_\_ algorithm accepts the ciphertext and the matching key and produces the original plaintext.

Correct answer:

decryption

**Results for question 4.**

4

1 / 1 point

The most important hash function is \_\_\_\_\_\_\_\_.



OWH

, Not Selected



MAC

, Not Selected

Correct answer:



SHA



ECB

, Not Selected

**Results for question 5.**

5

1 / 1 point

In addition to providing authentication, a message digest also provides data integrity and performs the same function as a frame check sequence.

Correct answer:

True

False

**Results for question 6.**

6

1 / 1 point

Message encryption alone provides a secure form of authentication.

True

Correct answer:

False

**Results for question 7.**

7

1 / 1 point

Bob uses his own private key to encrypt the message. When Alice receives the ciphertext she finds that she can decrypt it with Bob's public key, thus proving that the message must have been encrypted by Bob. No one else has Bob's private key and therefore no one else could have created a ciphertext that could be decrypted with Bob's public key. Therefore the entire encrypted message serves as a \_\_\_\_\_\_\_\_\_ .

Correct answer:

digital signature

**Results for question 8.**

8

0 / 1 point

Using an algorithm that is designed to provide only the digital signature function, the \_\_\_\_\_\_\_\_\_ makes use of the SHA-1 and cannot be used for encryption or key exchange.

Incorrect answer:

DSA

Correct Answer:Digital Signature Standard, DSS

**Results for question 9.**

9

1 / 1 point

The key exchange protocol is vulnerable to a man-in-the-middle attack because it does not authenticate the participants.

Correct answer:

True

False

**Results for question 10.**

10

1 / 1 point

As with symmetric encryption, there are two approaches to attacking a secure hash function: brute-force attack and \_\_\_\_\_\_\_\_\_\_\_ .

Correct answer:

cryptanalysis

The purpose of a \_\_\_\_\_\_\_\_\_\_\_ is to produce a "fingerprint" of a file, message, or other block of data.



cipher encryption

, Not Selected



public key

, Not Selected



message authentication

, Not Selected

Correct answer:



hash function

### Results for question 2.

2

0 / 1 point

The \_\_\_\_\_\_\_\_\_\_ approach has two advantages: it provides a digital signature as well as message authentication and it does not require the distribution of keys to communicating parties.

Incorrect answer:

public key

Correct Answer:public-key

### Results for question 3.

3

1 / 1 point

As with symmetric encryption, there are two approaches to attacking a secure hash function: brute-force attack and \_\_\_\_\_\_\_\_\_\_\_ .

Correct answer:

cryptanalysis

### Results for question 4.

4

1 / 1 point

Using an algorithm that is designed to provide only the digital signature function, the \_\_\_\_\_\_\_\_\_ makes use of the SHA-1 and cannot be used for encryption or key exchange.

Correct answer:

DSS

### Results for question 5.

5

1 / 1 point

The most widely accepted and implemented approach to public-key encryption, \_\_\_\_\_\_\_\_\_ is a block cipher in which the plaintext and ciphertext are integers between 0 and n - 1 for some n.

Correct answer:



RSA



CTR

, Not Selected



SHA

, Not Selected



MD5

, Not Selected

### Results for question 6.

6

1 / 1 point

The security of the Diffie-Hellman key exchange lies in the fact that, while it is relatively easy to calculate exponentials modulo a prime, it is very easy to calculate discrete logarithms.

True

Correct answer:

False

### Results for question 7.

7

1 / 1 point

Public key algorithms are useful in the exchange of conventional encryption keys.

Correct answer:

True

False

### Results for question 8.

8

1 / 1 point

If the message includes a \_\_\_\_\_\_\_\_\_ the receiver is assured that the message has not been delayed beyond that normally expected for network transit.



error detection code

, Not Selected



shared key

, Not Selected



sequence number

, Not Selected

Correct answer:



timestamp

### Results for question 9.

9

1 / 1 point

The purpose of the \_\_\_\_\_\_\_\_\_ algorithm is to enable two users to exchange a secret key securely that then can be used for subsequent encryption of messages and depends on the difficulty of computing discrete logarithms for its effectiveness.



DSS

, Not Selected



RSA

, Not Selected



Rivest-Adleman

, Not Selected

Correct answer:



Diffie-Hellman

### Results for question 10.

10

1 / 1 point

\_\_\_\_\_\_\_\_ protects against passive attacks (eavesdropping).

Correct answer:



Encryption



SCR

, Not Selected



Message authentication

, Not Selected



Obfuscation

Public key algorithms are useful in the exchange of conventional encryption keys.

Correct answer:

True

False

### Results for question 2.

2

1 / 1 point

The key algorithmic ingredients of \_\_\_\_\_\_\_\_\_\_ are the AES encryption algorithm, the CTR mode of operation, and the CMAC authentication algorithm.

Correct answer:

CCM

### Results for question 3.

3

1 / 1 point

The \_\_\_\_\_\_\_\_\_\_ property is the "one-way" property and is important if the authentication technique involves the use of a secret value.

Correct answer:

preimage resistant

### Results for question 4.

4

0 / 1 point

Protection against active attacks (falsification of data and transactions) is known as \_\_\_\_\_\_\_\_\_\_\_ .

Incorrect answer:

Message authentication

Correct Answer:message authentication

### Results for question 5.

5

1 / 1 point

In addition to providing authentication, a message digest also provides data integrity and performs the same function as a frame check sequence.

Correct answer:

True

False

### Results for question 6.

6

0 / 1 point

Like the MAC, a \_\_\_\_\_\_\_\_\_\_ accepts a variable size message M as input and produces a fixed size message digest H(M) as output. Unlike the MAC, it does not take a secret key as input.

Incorrect answer:

Hash function

Correct Answer:hash function

### Results for question 7.

7

1 / 1 point

Public key cryptography is \_\_\_\_\_\_\_\_\_\_.



one key

, Not Selected



bit patterned

, Not Selected



symmetric

, Not Selected

Correct answer:



asymmetric

### Results for question 8.

8

1 / 1 point

Because of the mathematical properties of the message authentication code function it is less vulnerable to being broken than encryption.

Correct answer:

True

False

### Results for question 9.

9

1 / 1 point

Bob uses his own private key to encrypt the message. When Alice receives the ciphertext she finds that she can decrypt it with Bob's public key, thus proving that the message must have been encrypted by Bob. No one else has Bob's private key and therefore no one else could have created a ciphertext that could be decrypted with Bob's public key. Therefore the entire encrypted message serves as a \_\_\_\_\_\_\_\_\_ .

Correct answer:

digital signature

### Results for question 10.

10

1 / 1 point

In the ECB mode of encryption if an attacker reorders the blocks of ciphertext then each block will still decrypt successfully, however, the reordering may alter the meaning of the overall data sequence.

Correct answer:

True

False