**Cryptography test questions**

**You should answer at least 15 questions. Choose all answers that apply.**

**1**-What is Diffie-Hellman most commonly used for?

**A.** Symmetric encryption key exchange

**B.** Signing digital contracts

**C.** Secure e-mail

**D.** Storing encrypted passwords

**2**-What is Diffie-Hellman most commonly used for?

**A.** Symmetric encryption key exchange

**B.** Signing digital contracts

**C.** Secure e-mail

**D.** Storing encrypted passwords

**3.** What does a hash function do?

**A.** Creates a secure tunnel

**B.** Breaks encryption by trying every possible key

**C.** Multiplies two very large primes

**D.** Creates a unique digest of a message

**4**-How do hash functions provide integrity?

**A.** If the message is edited, the hash will no longer match.

**B.** The hash makes the message uneditable.

**C.** Hashing encrypts the message so that only the private key holder can read it.

**D.** Hashing destroys the message so it cannot be read by anyone.

**5.** How is 3DES an improvement over normal DES?

**A.** It uses public and private keys.

**B.** It hashes the message before encryption.

**C.** It uses three keys and multiple encryption and/or decryption sets.

**D.** It is faster than DES.

**6.** What kinds of encryption does a digital signature use?

**A.** Hashing and asymmetric

**B.** Asymmetric and symmetric

**C.** Hashing and symmetric

**7.** What does differential cryptanalysis require?

**A.** The key

**B.** Large amounts of plaintext and ciphertext

**C.** Just large amounts of ciphertext

**D.** Computers able to guess at key values faster than a billion times per second

**8**-What is a brute-force attack?

**A.** Feeding certain plaintext into the algorithm to deduce the key

**B.** Capturing ciphertext with known plaintext values to deduce the key

**C.** Sending every key value at the algorithm to find the key

**D.** Sending two large men to the key owner’s house to retrieve the key

**9.** Why is integrity important to cryptographic messages?

**A.** To ensure that the message is properly formatted for decryption

**B.** To protect the keys from exposure

**C.** To show that a message has not been edited in transit

**D.** To show that no one has read the message

**10**-What is the purpose of a digital certificate?

**A.** It binds a CA to a user’s identity.

**B.** It binds a CA’s identity to the correct RA.

**C.** It binds an individual to an RA.

**D.** It binds an individual to a public key.

**11.** Why would a company implement a key archiving and recovery system within

their organization?

**A.** To make sure all data encryption keys are available for the company if and

when it needs them

**B.** To make sure all digital signature keys are available for the company if and

when it needs them

**C.** To create session keys for users to be able to access when they need to

encrypt bulk data

**D.** To back up the RA’s private key for retrieval purposes

**12.** Within a PKI environment, where does the majority of the trust actually lie?

**A.** All users and devices within an environment trust the RA, which allows them

to indirectly trust each other.

**B.** All users and devices within an environment trust the CA, which allows

them to indirectly trust each other.

**C.** All users and devices within an environment trust the CRL, which allows

them to indirectly trust each other.

**D.** All users and devices within an environment trust the CPS, which allows

them to indirectly trust each other.

**13.** Which of the following is not a valid field that could be present in an X.509

version 3 digital certificate?

**A.** Validity dates

**B.** Serial number

**C.** Extensions

**D.** Symmetric key

**14.** What does a certificate path pertain to?

**A.** All of the digital certificates that need to be validated before a received

certificate can be fully validated and trusted

**B.** All of the digital certificates that need to be validated before a sent certificate

can be properly encrypted

**C.** All of the digital certificates that need to be validated before a user trusts

their own trust anchor

**D.** All of the digital certificates that need to be validated before a received

certificate can be destroyed

**15.** Which of the following certificate characteristics was expanded upon with

version 3 of the X.509 standard?

**A.** Subject

**B.** Extensions

**C.** Digital signature

**D.** Serial number

**16.** Which of the following properly describes what a public key infrastructure

(PKI) actually is?

**A.** A protocol written to work with a large subset of algorithms, applications,

and protocols

**B.** An algorithm that creates public/private key pairs

**C.** A framework that outlines specific technologies and algorithms that must be

used

**D.** A framework that does not specify any technologies, but provides a

foundation for confidentiality, integrity, and availability services

**17.** Once an individual validates another individual’s certificate, what is the use of

the public key that is extracted from this digital certificate?

**A.** The public key is now available to use to create digital signatures.

**B.** The user can now encrypt session keys and messages with this public key and

can validate the sender’s digital signatures.

**C.** The public key is now available to encrypt future digital certificates that need

to be validated.

**D.** The user can now encrypt private keys that need to be transmitted securely.

**18.** Why would a digital certificate be added to a certificate revocation list (CRL)?

**A.** If the public key had become compromised in a public repository

**B.** If the private key had become compromised

**C.** If a new employee joined the company and received a new certificate

**D.** If the certificate expired

**19.** When would a certificate be suspended, and where is that information posted?

**A.** It would be suspended when an employee leaves the company. It is posted

on the CRL.

**B.** It would be suspended when an employee changes their last name. It is

posted on the CA.

**C.** It would be suspended when an employee goes on vacation. It is posted on

the CRL.

**D.** It would be suspended when a private key is compromised. It is posted on

the CRL.

**20.** What does cross certification pertain to in a PKI environment?

**A.** When a company uses an outsourced service provider, it needs to modify its

CPS to allow for cross certification to take place between the RA and CA.

**B.** When two end-entities need to communicate in a PKI, they need to exchange

certificates.

**C.** When two or more CAs need to trust each other so that their end-entities can

communicate, they will create certificates for each other.

**D.** A RA needs to perform a cross certification with a user before the certificate

registration is terminated.