Chapter 3 MCQS

C. encrypts the key and the message
The Hashed Message Authentication Code (HMAC) _____.
A. encrypts only the message
B. encrypts only the key
C. encrypts the key and the message
D. encrypts the DHE key only

B. SHA-3
What is the latest version of the Secure Hash Algorithm?
A. SHA-2
B. SHA-3
C. SHA-4
D. SHA-5

C. ROT13
Alexei was given a key to a substitution cipher. The key showed that the entire alphabet was rotated 13 steps. What type of cipher is this?
A. AES
B. XAND13
C. ROT13
D. Alphabetic

C. 0
Abram was asked to explain to one of his coworkers the XOR cipher. He showed his coworker an example of adding two bits, 1 and 1. What is the result of this sum?
A. 2
B. 1
C. 0
D. 16

C. Diffie-Hellman (DH)
Which of the following key exchanges uses the same keys each time?
A. Diffie-Hellman-RSA (DHRSA)
B. Diffie-Hellman Ephemeral (DHE)
C. Diffie-Hellman (DH)
D. Elliptic Curve Diffie-Hellman (ECDH)

B. perfect forward secrecy
Public key systems that generate random public keys that are different for each session are called _____.
A. Public Key Exchange (PKE)
B. perfect forward secrecy
C. Elliptic Curve Diffie-Hellman (ECDH)
D. Diffie-Hellman (DH)

B. plaintext
What is data called that is to be encrypted by inputting it into a cryptographic algorithm?
A. opentext
B. plaintext
C. cleartext
D. ciphertext

B. risk loss
Which of these is NOT a basic security protection for information that cryptography can provide?
A. authenticity
B. risk loss
C. integrity
D. confidentiality

D. in the directory structure of the file system
Which areas of a file cannot be used by steganography to hide data?
A. in areas that contain the content data itself
B. in the file header fields that describe the file
C. in data that is used to describe the content or structure of the actual data
D. in the directory structure of the file system

A. non-repudiation
Proving that a user sent an email message is known as _____.
A. non-repudiation
B. repudiation
C. integrity
D. availability

C. digest
A(n) _____ is not decrypted but is only used for comparison purposes.
A. key
B. stream
C. digest
D. algorithm

A. Collisions should be rare.
Which of these is NOT a characteristic of a secure hash algorithm?
A. Collisions should be rare.
B. A message cannot be produced from a predefined hash.
C. The results of a hash function should not be reversed.
D. The hash should always be the same fixed size.

B. confusion
Alyosha was explaining to a friend the importance of protecting a cryptographic key from cryptoanalysis. He said that the key should not relate in a simple way to the cipher text. Which protection is Alyosha describing?
A. diffusion
B. confusion
C. integrity
D. chaos

C. Advanced Encryption Standard
Which of these is the strongest symmetric cryptographic algorithm?
A. Data Encryption Standard
B. Triple Data Encryption Standard
C. Advanced Encryption Standard
D. RC 1

C. Alice's public key
If Bob wants to send a secure message to Alice using an asymmetric cryptographic algorithm, which key does he use to encrypt the message?
A. Alice's private key
B. Bob's public key
C. Alice's public key
D. Bob's private key

C. verify the receiver
Egor wanted to use a digital signature. Which of the following benefits will the digital signature not provide?
A. verify the sender
B. prove the integrity of the message
C. verify the receiver
D. enforce nonrepudiation

D. RSA
Illya was asked to recommend the most secure asymmetric cryptographic algorithm to his supervisor. Which of the following did he choose?
A. SHA-2
B. ME-312

C. BTC-2
D. RSA

C. It would be essentially impossible to keep its location a secret from everyone.
At a staff meeting one of the technicians suggested that the enterprise protect its new web server by hiding it and not telling anyone where it is located. Iosif raised his hand and said that security through obscurity was a poor idea. Why did he say that?
A. It is an unproven approach and has never been tested.
B. It would be too costly to have one isolated server by itself.
C. It would be essentially impossible to keep its location a secret from everyone.
D. It depends too heavily upon non-repudiation in order for it to succeed.

A. It provides cryptographic services in hardware instead of software
What is a characteristic of the Trusted Platform Module (TPM)?
A. It provides cryptographic services in hardware instead of software
B. It allows the user to boot a corrupted disk and repair it
C. It is available only on Windows computers running BitLocker
D. It includes a pseudorandom number generator (PRNG)

B. Hardware Security Module (HSM)
Which of these has an onboard key generator and key storage facility, as well as accelerated symmetric and asymmetric encryption, and can back up sensitive material in encrypted form?
A. Trusted Platform Module (TPM)
B. Hardware Security Module (HSM)
C. self-encrypting hard disk drives (SED)
D. encrypted hardware-based USB devices

Chapter 4

D. Variability
Which of the following is NOT a method for strengthening a key?
A. Randomness
B. Cryptoperiod
C. Length
D. Variability

D. Cipher Block Chaining (CBC)
Which of the following block ciphers XORs each block of plaintext with the previous block of ciphertext before being encrypted?
A. Electronic Code Book (ECB)
B. Galois/Counter (GCM)
C. Counter (CTR)
D. Cipher Block Chaining (CBC)
D. Crypto service provider

What entity calls in crypto modules to perform cryptographic tasks?
A. Certificate Authority (CA)
B. OCSP Chain
C. Intermediate CA
D. Crypto service provider

B. Session keys
_____ are symmetric keys to encrypt and decrypt information exchanged during the session and to verify its integrity.
A. Encrypted signatures
B. Session keys
C. Digital certificates
D. Digital digests

A. TLS v1.2
Which of these is considered the strongest cryptographic transport protocol?
A. TLS v1.2
B. TLS v1.0
C. SSL v2.0
D. SSL v2.0

D. digital certificate
The strongest technology that would assure Alice that Bob is the sender of a message is a(n) _____.
A. digital signature
B. encrypted signature

C. digest
D. digital certificate

B. the user's identity with his public key
A digital certificate associates _____.
A. a user's public key with his private key
B. the user's identity with his public key
C. a user's private key with the public key
D. a private key with a digital signature

A. to verify the authenticity of the Registration Authorizer
Digital certificates can be used for each of these EXCEPT _____.
A. to verify the authenticity of the Registration Authorizer
B. to encrypt channels to provide secure communication between clients and servers
C. to verify the identity of clients and servers on the Web
D. to encrypt messages for secure email communications

C. Certificate Authority (CA)
An entity that issues digital certificates is a _____.
A. Certificate Signatory (CS)
B. Digital Signer (DS)
C. Certificate Authority (CA)
D. Signature Authority (SA)

C. Certificate Repository (CR)
A centralized directory of digital certificates is called a(n) _____.
A. Digital Signature Permitted Authorization (DSPA)
B. Digital Signature Approval List (DSAP)
C. Certificate Repository (CR)
D. Authorized Digital Signature (ADS)

C. Online Certificate Status Protocol (OCSP)
_____ performs a real-time lookup of a digital certificate's status.
A. Certificate Revocation List (CRL)
B. Real-Time CA Verification (RTCAV)
C. Online Certificate Status Protocol (OCSP)
D. CA Registry Database (CARD)

D. salt
12. What is a value that can be used to ensure that hashed plaintext will not consistently result in the same digest?
A. algorithm
B. initialization vector (IV)
C. nonce

D. salt

B. Extended Validation (EV) Certificate
Which digital certificate displays the name of the entity behind the website?
A. Online Certificate Status Certificate
B. Extended Validation (EV) Certificate
C. Session Certificate
D. X.509 Certificate

A. Bridge
Which trust model has multiple CAs, one of which acts as a facilitator?
A. Bridge
B. Hierarchical
C. Distributed
D. Web

A. It is designed for use on a large scale.
Which statement is NOT true regarding hierarchical trust models?
A. It is designed for use on a large scale.
B. The root signs all digital certificate authorities with a single key.
C. It assigns a single hierarchy with one master CA.
D. The master CA is called the root.

C. is the management of digital certificates
Public key infrastructure (PKI) _____.
A. generates public/private keys automatically
B. creates private key cryptography
C. is the management of digital certificates
D. requires the use of an RA instead of a CA

D. certificate policy (CP)
A(n) _____ is a published set of rules that govern the operation of a PKI.
A. signature resource guide (SRG)
B. enforcement certificate (EF)
C. certificate practice statement (CPS)
D. certificate policy (CP)

C. authorization
Which of these is NOT part of the certificate life cycle?
A. expiration
B. revocation
C. authorization
D. creation

B. Key escrow

_____ refers to a situation in which keys are managed by a third party, such as a trusted CA.

A. Key authorization
B. Key escrow
C. Remote key administration
D. Trusted key authority

B. Secure Shell (SSH)

_____ is a protocol for securely accessing a remote computer.

A. Transport Layer Security (TLS)
B. Secure Shell (SSH)
C. Secure Sockets Layer (SSL)
D. Secure Hypertext Transport Protocol (SHTTP)

CHAPTER 7: PREVENTING SYSTEM INTRUSIONS

True/False

2. True
3. False
4. False
5. False

Multiple Choice

1. A
2. E
3. A, B, D
4. D
5. B

True/False

1. True or False? A network intrusion is an authorized penetration of your enterprise's network, or an individual machine address in your assigned domain.
False

2. True or False? In some cases, a network intrusion could be done from the inside by a disgruntled employee looking to hurt the organization or steal company secrets for profit.
True

3. True or False? Most security software products available today have two basic methods of spotting malicious software.
False

4. True or False? Crackers are going to first look for known strengths in the operating system (OS) or any applications you are using.
False

5. True or False? Finding a device, using it in a place (or manner) in which prying eyes can see passwords or data, awareness of hacking tools specifically designed to sniff wireless signals for data, and logging on to unsecured networks, are all potential problem areas with which users need to be familiar
1. False

Multiple Choice

1. Which devices can locate wireless signals within a certain range, where they can siphon off the data being transmitted over the signals?
A. Wireless sniffers
B. Packet sniffers
C. Port scanners
D. Port knocking
E. Keystroke loggers

2. You can expect to have continued problems maintaining good network security awareness. Keep it simple. You need to draft some policies that define your network and its

basic architecture. A good place to start is by asking the following questions, except which one?

A. What kinds of resources need to be protected (user financial or medical data, credit-card information, etc.)?

B. How many users will be accessing the network on the inside (employees, contractors, etc.)?

C. Will there need to be access only at certain times or on a 24/7 basis (and across multiple time zones and/ or internationally)?

D. What kind of budget do I have?

E. Will internal users be accessing the network, and if so, how many?

3. A good IDS detects unauthorized intrusions using three types of models:
A. Anomaly-based B. Signature-based C. Network-based **D. Hybrid detection** E. Host-based

4.For an IPS to be effective, it must also be very good at discriminating between a real threat signature and one that looks like but isn't one (false positive). Once a signature interpreted to be an intrusion is detected, the system must quickly notify the administrator so that the appropriate evasive action can be taken. The following are types of IPS, except one:
A. Network-based B. Rate-based C. Host-based **D. Backdoor-based** E. Content-based

5.The latest trend to emerge in the network intrusion prevention arena is referred to as:
A. Antivirus **B. Unified threat management** C. VPN D. Firewall services E. Antispam