Chapter 2 security +

When a cryptographic system is used to protect the confidentiality of data what is actually protected? Unauthorized users are prevented from viewing or accessing the resource

Which of the following is not a valid example of steganography? Encrypting a data file with an encryption key

By definition which security concept ensures that only authorized parties can access data? Confidentiality

What is the cryptography mechanism which hides secret communication within various forms of data? Steganography

Which of the following encryption methods combines a random value with the plaintext to produce a cipher text? one-time pad

You create a new document and save it to the hard drive on a file server on your company’s network. Then you employ an encryption tool to encrypt the file using AES. This activity is an example of accomplishing what security goal? confidentiality

By definition, which security concept uses the ability to prove that a sender sent an encrypted message ? Non-repudiation

When two different messages produce the same hash value what has occurred? collision

Your computer system is a participant in an asymmetric cryptography system. You’ve crafted a message to be sent to another user. Before transmission you hash the message then encrypt the hash using your private

key. You then attach this encrypted hash into your message as a digital signature before sending it to the other user. In this example what protection does the hashing activity provide? Integrity

Which of the following best describes high amplification when applied to hashing algorithms? A small change in the message results in a big change in the hashing value

Which of the following has the weakest hashing algorithm? MD-5

Which of the following has the strongest hashing algorithm? SHA-1

You have just downloaded a file. You create a hash of the file and compare it to the hash posted on the website. The two hashes match. What do you know about this file? Your copy is the same as the copy posted on the website

Hashing algorithms are used to perform what activity? Create a message digest

Which of the following is used to verify a downloaded file has not been altered? hash

What form of cryptography is best suited for bulk encryption because it’s so fast? symmetric cryptography

You want to encrypt data on a removable storage device. Which encryption method would you choose to use the strongest method possible? AES

What type of key or keys are used in symmetric cryptography? a shared private key

Which of the following algorithms are used in symmetric encryption? 3DESBlowfishAES

How many keys are used with symmetric key cryptography? one

Which of the following is the weakest encryption method? DES

Which of the following is not true concerning symmetric key cryptography? key management is easy when implemented on a large scale.

Which of the following generates the key pair us in asymmetric cryptography? CSP

Which of the following is employment of two separate key pairs in order to separate the security functions of confidentiality and integrity of a communications system? dual key pair

Certificates can be invalidated by the trusted third-party that originally issued the certificate. What is the name of the mechanism that is used to distribute information about invalid certificates? CRL

Which of the following identifies someone who can retrieve private keys from storage? Recovery Agent

Which of the following is an entity that accepts and validates information contained within a request for a certificate? Registration Authority

Which of the following protocols are most likely used with a digital signature? ECCRSA

Which aspect of certificates makes them a reliable and useful mechanism for proving the identity of a person system or service on the internet? Trusted third party

Which of the following would you find on a CPS? A declaration of the security that the organization is implementing for all certificates

Which of the following items are contained in a digital certificate? Validity keypublic key

What is the most obvious means of providing non-repudiation in a cryptography system? Digital signatures

Above all else, what must be protected to maintain the security and benefit of an asymmetric cryptographic solution especially if it is widely used for digital certificates? Private keys

Which of the following conditions does not result in a certificate being added to the certificate revocation list? certificate expiration

What is a PKI? a hierarchy of computers for issuing certificates

Which standard is most widely used for certificates ? X. 509

In the certificate authority trust model known as hierarchy where does trust start? Root CA

What is the purpose of key escrow? To provide a means for legal authorities to access confidential data

In what form of key management solution is key recovery possible? Centralized

Which of the following best describes the contents of the CRL? A list of all revoked certificates

When protection of the content of a message is required which of the following cryptography solutions should be employed? symmetric encryption

An SSL client has determined the certificate authority (CA) issuing a server’s certificate is on its list of trusted CA’s. What is the next step in verifying the servers identity? The CA’s public key must validate the CA’s digital signature on the server certificate

What technology was developed to help improve the efficiency and reliability of checking the validity status of certificates in large complex environments? Online Certificate Status Protocol

You have lost the private key that you have used to encrypt files. You need to get a copy of the private key open some encrypted files. Who should you contact? recovery agent

Which of the following functions are performed by TPM? Create a hash of system components

Which of the following statements is true when comparing symmetric and asymmetric cryptography? Asymmetric key cryptography is used to distribute symmetric keys

A private key has been stolen. What action should be taken to deal with the crisis? Add a digital certificate to the CRL

You want to protect data on hard drives for users with laptops. You want the drive to be encrypted and you want to prevent the laptops from booting unless a special USB drive is instated. In addition the system should not boot if a change is detected in any of the boot files. What should you do? Implement BitLocker with a TPM

Mary wants to send a message to Sam so that only Sam can read it. Which key should be used to encrypt the message? Sam’s public key

Which of the following security measures encrypts the entire contents of data? DriveLock

Which of the following security solutions would prevent a user from reading a file which she did not create? EFS

Certificate revocation should occur under all but which of the following conditions? The certificate owner had held the certificate beyond the established lifetime timer

You have a web server that will be used for secure transactions for customers who access the web site over the internet. The web server

requires a certificate to support SSL . Which method would you use to get a certificate to a server? Obtain a certificate from a public PKI

Which of the following is the best countermeasure for the man-in-the-middle attack? Public Key Infrastructure (PKI)

You are concerned that if a private key is lost all documents encrypted using your private key will be inaccessible. What service should you use to solve this problem? key escrow

You want a security solution that protects the entire hard drive preventing access even when its moved to another system. What solution should you choose? BitLocker

To get a digital certificate and participate in a Public Key Infrastructure (PKI) what must be submitted and where should it be submitted? Identifying data and a certification request to the registration authority (RA)

What action is taken when the private key associated with a digital certificate is compromised? The certificate is revoked and added to the Certificate Revocation List

Mary wants to send a message to Sam. She wants to digitally sign the message to prove she sent it. Which key would Mary use to create a digital signature? Mary’s private key

You use BitLocker to encrypt the hard drive of a laptop. The Laptop stores the startup key in the TPM and a PIN is also required to start the system. Because of a hardware failure, the system will not boot. You want to gain

access to the data of the hard drive. What should you do? Move the hard drive to another system. Use the recovery key to unlock the disk

You would like to implement BitLocker to encrypt data on a hard disk even if its moved to another system. You want the system to boot automatically without providing a startup key on an external USB device. What should you do? Enable the TPM in Bios

Telnet is inherently insecure because its communications is in plain text and easily intercepted. Which of the following is an acceptable alternative to Telnet? SSH

What protocol does HTTPS use to offer greater security in Web transactions? SSL

You want to allow traveling users to connect to your private network through the internet. Users will connect from various locations including airports, hotels and public access points such as coffee shops and libraries. As such you won’t be able to configure the firewalls that might be controlling access to the internet in these locations. Which of the following protocols will be most likely to be allowed through the widest number of firewalls? SSL

Which protocol is used for securely browsing a website? HTTPS

You are purchasing a hard disk over the internet from an online retailer. What does your browser use to ensure that others cannot see your credit card number on the internet? SSL

Which of the following protocols are often added to other protocols to provide secure transmission of data? TLSSSL

The session keys employed by SSL (Secure Sockets Layer) are available in what bit lengths? 128 bit at 40 bit

Which of the following is the best counter measure against man-in-the-middle attacks? IPsec

Which IPsec subprotocol provides data encryption? Encapsulating Security Payload (ESP)

Which of the following technologies is based upon SSL (Secure Socket Layer) ? TLS (Transport Layer Security)

Which of the following protocols can be used to securely manage a network device from a remote connection? SSH

Which of the following protocols can TLS use for key exchange? Diffie-HellmanRSA

What is the primary function of the IKE protocol used with IPsec? Creates a security association between communicating partners

Which of the following can be used to encrypt web email telnet transfer and SNMP traffic ? IPsec

IPsec is implemented through two separate protocols. What are these protocols called? ESPAH

Which of the following network layer protocols provides authentication and encryption services for IP based network traffic? IPsec

SHA-1 uses with of the following bit length hashing algorithmsonly 160 – bit

Which of the following does not or cannot produce a hash value of 128 bitsSHA-1

A birthday attack focuses on what ? hashing algorithms

If two different messages or files produce the same hashing digest, then a collision has occurred. What form of cryptographic attacks exploits this condition? Birthday Attack

If a birthday attack is successful meaning the attacker discovers a password that generates the same hash as that captured from user’s logon credentials which of the following is true? The discovered password will allow the attacker to logon as the user even if its not the same as the user’s password

A collision was discovered

Which of the following are true of Triple DES (3DES)? Is used in IPsecUses a 168 bit key

Which of the following are true concerning the Advanced Encryption Standard (AES) symmetric block cipher? AES uses the Rijindel block cipher

AES uses variable length block key and key length (128-192-, or 256 keys)

Which of the following symmetric block ciphers does not use a variable block length? International Data Encryption Algorithm (IDEA)

Which of the following encryption mechanisms offers the least security because of weak keys? DES

Which version of the River Cipher is a block cipher that supports variable bit length keys and variable bit block sizes? RC5

Bob Jones uses the RC5 cryptosystem to encrypt a sensitive and confidential file on his notebook. He used 32 bit blocks a 64 bit key and he only used the selected key once. He moved the key onto a USB hard drive which was stored in a safety deposit box. Bob’s notebook was stolen. Within a few days Bob discovered the contents of his encrypted file on the Internet. What is the primary reason Bob’s file was opened so quickly? Weak key

What type of key or keys are used in symmetric cryptography? A shared private key

How many keys are used in symmetric key cryptography? one

Which of the following is not true concerning symmetric key cryptography? Key management is easy when implemented on a large scale

Which of the following is classified as a stream cipher? RC4

You want to encrypt data on a removable storage device. Which encryption method would you choose to use the strongest method possible? AES

Which of the following algorithms are used in symmetric encryption? Blowfish3DESAES

You are concerned about the strength of your cryptographic keys so you implement a system that does the following:

The initial key is fed into the input of the bcrypt utility on a Linux workstation

The bcrypt key utility produces an enhanced key that is 128 bits long

The resulting enhanced key is much more difficult to crack than the original key. Which kind of encryption mechanism was used in the scenario?

key stretching

Which of the following is considered an out of band distribution method for private key encryption? copying the key to a USB drive

1. The senders key is sent to a recipient using a Diffie-Hellman key exchange2. The senders key is copied to a USB drive and handed to the recipient3. The senders key is sent to the recipient using public-key cryptography4. The senders key is burned to a CD and handed to the recipient1. In band distribution2. Out of band distribution3. In band distribution4. Out of band distribution

How many keys are used with asymmetric or publicly key cryptography? Two

A receiver wants to verify the integrity of a message received from a sender. A hashing value is contained within the digital signature of the sender. What must the receiver use to access the hashing value to verify the integrity of the transmission? Senders public key

A PKI is a method for managing which type of encryption? Asymmetric

When is the best time to apply for a certificate renewal ? near the end of the certificates valid lifetime