Exam Report: 3.4.3 Practice Questions - Section 3.4

Date: 11/24/2015 1:56:59 pm
Time Spent: 0:08

Candidate: Belskis, Tomas
Login: t0mas9lt

Overall Performance

Your Score: 0%

Passing Score: 80%

Certification Ranking

Within your class: Within your school: Nationally:

View results by: Objective Analysis Individual Responses

Individual Responses

Question 1: Incorrect

How many keys are used with asymmetric or public key cryptography?

- One
- Two
- Three
- Four

Explanation

Public Key or Asymmetric Cryptography uses two keys: one is referred to as the public key, and the other the private key. This key pair overcomes the difficulties associated with the secure distribution of private keys. The communicating parties do not need to share secret information: only the public keys are shared. Public keys are associated with users through authentication, usually through a mutually trusted directory such as a certificate authority. The sender transmits a confidential message using only the recipient's public key. The message can only be decrypted with the associated private key possessed solely by the recipient. Public Key Cryptography provides not only encryption, but is the basis for authentication technologies such as digital signatures.

References

LabSim for Security Pro, Section 3.4.
[Questions.exm SP02_4-1 [84]]

Question 2: Incorrect

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?

- Sender's private key
- Receiver's private key
- Receiver's public key

- Sender's public key

Explanation

Digital signatures are created using the sender's private key. Thus, only the sender's *public* key can be used to verify and open any data encrypted with the sender's private key. The recipient's private and public keys are not involved in this type of cryptography situation. Often the hashing value of a message is protected by the sender's private key (i.e. their digital signature). The recipient must extract the original hashing value.

References

LabSim for Security Pro, Section 3.4.
[Questions.exm SP02_4-2 [21]]

Question 3: Incorrect

Which of the follow are characteristics of ECC? (Select two.)

- [ ] Asymmetric encryption
- [ ] Uses a finite set of values within an algebraic field
- [ ] Symmetric encryption
- [ ] Uses multiplication of large prime numbers

Explanation

Elliptic curve cryptography (ECC) is an approach to cryptography that uses a finite set of values within an elliptic curve (an algebraic set of numbers). ECC is an asymmetric encryption algorithm.

RSA is an asymmetric algorithm that uses the multiplication of large prime numbers for encryption.

References

LabSim for Security Pro, Section 3.4.
[Questions.exm SP08_5-3 2]

Question 4: Incorrect

Which of the following algorithms are used in asymmetric encryption? (Select two.)

- [ ] Blowfish
- [ ] AES
- [ ] Diffie-Hellman
- [ ] RSA
- [ ] Twofish

Explanation

RSA and Diffie-Hellman are asymmetric algorithms. RSA, one of the earliest encryption algorithms, can also be used for digital signatures. The Diffie-Hellman protocol was created in

1976, but is still in use today in such technologies such as SSL, SSH, and IPSec.

References

LabSim for Security Pro, Section 3.4.
[Questions.exm SP02_4-4 [85]]

Question 5: Incorrect

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?

- Public keys
- Cryptographic algorithm
- Private keys
- Hash values

Explanation

The strength of an asymmetric cryptographic system lies in the secrecy and security of its private keys. A digital certificate and a digital signature are little more than unique applications of a private key. If the private keys are compromised for a single user, for a secured network, or for a digital certificate authority, the entire realm of trust is destroyed.

References

LabSim for Security Pro, Section 3.4.
[Questions.exm SP02_4-5 [21]]

Question 6: Incorrect

Which of the following generates the key pair used in asymmetric cryptography?

- CRL
- CPS
- CA
- OCSP
- CSP

Explanation

A Cryptographic Service Provider (CSP) resides on the client and generates the key pair. This is a software program that can generate keys using a specific algorithm.

The Certificate Authority (CA) is an entity trusted to issue, store, and revoke digital certificates. The Certificate Practice Statement (CPS) is a declaration of the security that the organization is implementing for all certificates issued by the CA holding the CPS.

The Certificate Revocation List (CRL) resides at the CA and consists of a list of certificates that have been previously revoked. The Online Certificate Status Protocol (OCSP) is a protocol used for checking the status of an individual digital certificate to verify if it is good or has been revoked.

References

LabSim for Security Pro, Section 3.4.
[Questions.exm SP08_5-5 5]

Question 7: Incorrect

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

- Sam's public key
- Mary's public key
- Sam's private key

Explanation

Use Sam's public key to encrypt the message. Only the corresponding private key, which only Sam has, can be used to decrypt the message.

Mary cannot use Sam's private key because only Sam has that key. Anything encrypted with the private key can be decrypted by anyone with the public key. Encrypting using Mary's private key would mean that anyone could read the data using Mary's public key. Encrypting with Mary's public key would mean that only Mary would be able to decrypt it using her private key.

References

LabSim for Security Pro, Section 3.4.
[Questions.exm SP08_5-5 1]

Question 8: Incorrect

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

- Sam's private key
- Mary's private key
- Sam's public key
- Mary's public key

Explanation

Use Mary's private key to create the digital signature. This proves that only Mary could have sent the message, because only Mary has access to her private key. Sam would use Mary's public key to verify the digital signature.

Use Sam's public key to encrypt a message that only Sam should be able to read. Only the corresponding private key, which only Sam has, can be used to decrypt the message.

Mary cannot use Sam's private key because only Sam has that key. Anything encrypted with the private key can be decrypted by anyone with the public key. Encrypting with Mary's public key would mean that only Mary would be able to decrypt it using her private key, but could not prove where the message came from because anyone has access to Mary's public key.

References

LabSim for Security Pro, Section 3.4.
[Questions.exm SP08_5-5 2]

Question 9: Incorrect

The strength of a cryptosystem is dependent upon which of the following?

- Secrecy of the key
- Complexity of the cipher text
- Integrity of the individuals who created the cryptosystem
- Secrecy of the algorithm

Explanation

The strength of an asymmetric encryption system lies in the secrecy and security of its private keys. The strength of a cryptosystem should not be in the secrecy of the algorithm. This means that the algorithm is usually published and can be scrutinized for weaknesses.

References

LabSim for Security Pro, Section 3.4.
[Questions.exm NEW [162]]

Question 10: Incorrect

Which form of asymmetric cryptography is based upon Diffie-Hellman?

- El Gamal
- Merkle-Hellman Knapsack
- ECC
- RSA

Explanation

El Gamal is based upon Diffie-Hellman.

References

LabSim for Security Pro, Section 3.4.
[Questions.exm SP [299]]

Question 11: Incorrect

Which cryptography system generates encryption keys that could be used with DES, AES, IDEA, RC5 or any other symmetric cryptography solution?

- Merkle-Hellman Knapsack
- RSA
- Elliptical Curve
- Diffie-Hellman

Explanation

Diffie-Hellman is the only key generation system in this list of options. Diffie-Hellman produces a number which can be used as a key in any symmetric cryptography solution assuming the

number is within the algorithm's keyspace.

Merkle-Hellman Knapsack is not a key generation system, instead it is an insecure concept that pre-dates public key encryption. Elliptical curve is not a key generation system, instead it is a method of applying other systems to gain greater strength from smaller keys. RSA is not a key generation system, instead it is an asymmetric cryptography system which can be used for encryption, key exchange, and digital signatures.

References

LabSim for Security Pro, Section 3.4.
[Questions.exm CP [315]]

Question 12: Incorrect

Match each public-key cryptography key management mechanism on the left with the corresponding description on the right. Each mechanism may be used once, more than once, or not at all.

Implements the Diffie-Hellman key exchange protocol using elliptic curve cryptography

[ ] ECDH

Exist only for the lifetime of a specific communication session

[ ] Ephemeral keys

Uses no deterministic algorithm when generating public keys

[ ] Perfect forward secrecy

Can be reused by multiple communication sessions

[ ] Static keys

Explanation

Public-key cryptography can use a variety of mechanisms to manage encryption keys, including the following:

- *Ephemeral keys* are generated every time the key establishment process is executed and only exist for the lifetime of a specific communication session. As such, these keys have a relatively short lifespan.
- *Static keys* can be reused by multiple communication sessions. As such, these keys remain in use for a relatively long period of time.
- *Perfect forward secrecy* can be implemented in public-key cryptography system such that random public keys are generated for each session. No deterministic algorithm is used when generating the public keys.
- *Elliptic curve Diffie-Hellman* (ECDH) is an implementation of the Diffie-Hellman key exchange protocol using elliptic curve cryptography. It allows two parties, each having their own elliptic curve public/private key pair, to generate symmetric keys simultaneously over a non-secure channel.

References

LabSim for Security Pro, Section 3.4.
[Questions.exm RT-3.4-1]