Free Questions for 212-81 by braindumpscollection

Shared by Greene on 29-01-2024

For More Free Questions and Preparation Resources

Check the Links on Last Page

Question 1

Question Type: MultipleChoice

Basic information theory is the basis for modern symmetric ciphers. Understanding the terminology of information theory is, therefore, important. Changes to one character in the plaintext affect multiple characters in the ciphertext. What is this referred to?

Options:

A- Avalanche

B- Confusion

C- Scrambling

D- Diffusion

Answer:

D

Explanation:

Diffusion

https://en.wikipedia.org/wiki/Confusion_and_diffusion

Diffusion means that if we change a single bit of the plaintext, then (statistically) half of the bits in the ciphertext should change, and similarly, if we change one bit of the ciphertext, then approximately one half of the plaintext bits should change. Since a bit can have only two states, when they are all re-evaluated and changed from one seemingly random position to another, half of the bits will have changed state.

The idea of diffusion is to hide the relationship between the ciphertext and the plain text.

This will make it hard for an attacker who tries to find out the plain text and it increases the redundancy of plain text by spreading it across the rows and columns; it is achieved through transposition of algorithm and it is used by block ciphers only

Incorrect answers:

Confusion

Confusion means that each binary digit (bit) of the ciphertext should depend on several parts of the key, obscuring the connections between the two.

The property of confusion hides the relationship between the ciphertext and the key.

This property makes it difficult to find the key from the ciphertext and if a single bit in a key is changed, the calculation of the values of most or all of the bits in the ciphertext will be affected.

Confusion increases the ambiguity of ciphertext and it is used by both block and stream ciphers.

Avalanchehttps://en.wikipedia.org/wiki/Avalanche_effect

An avalanche effect is the desirable property of cryptographic algorithms, typically block ciphers and cryptographic hash functions, wherein if an input is changed slightly (for example, flipping a single bit), the output changes significantly (e.g., half the output bits flip). In the case of high-quality block ciphers, such a small change in either the key or the plaintext should cause a drastic change in the ciphertext.

If a block cipher or cryptographic hash function does not exhibit the avalanche effect to a significant degree, then it has poor randomization, and thus a cryptanalyst can make predictions about the input, being given only the output. This may be sufficient to partially or completely break the algorithm. Thus, the avalanche effect is a desirable condition from the point of view of the designer of the cryptographic algorithm or device.

Constructing a cipher or hash to exhibit a substantial avalanche effect is one of the primary design objectives, and mathematically the construction takes advantage of the butterfly effect. This is why most block ciphers are product ciphers. It is also why hash functions have large data blocks. Both of these features allow small changes to propagate rapidly through iterations of the algorithm, such that every bit of the output should depend on every bit of the input before the algorithm terminates.

Question 2

Question Type: **MultipleChoice**

Which component of IPsec performs protocol-level functions that are required to encrypt and decrypt the packets?

Options:

A- IPsec Policy Agent

B- Internet Key Exchange (IKE)

C- Oakley

D- IPsec driver

Answer:

B

Explanation:

Internet Key Exchange (IKE)

https://en.wikipedia.org/wiki/Internet_Key_Exchange

Internet Key Exchange (IKE, sometimes IKEv1 or IKEv2, depending on version) is the protocol used to set up a security association (SA) in the IPsec protocol suite. IKE builds upon the Oakley protocol and ISAKMP. IKE uses X.509 certificates for authentication either pre-shared or distributed using DNS (preferably with DNSSEC) and a Diffie--Hellman key exchange to set up a shared session secret from which cryptographic keys are derived.

Incorrect answers:

Oakley -the Oakley Key Determination Protocol is a key-agreement protocol that allows authenticated parties to exchange keying material across an insecure connection using the Diffie--Hellman key exchange algorithm. The protocol was proposed by Hilarie K. Orman in 1998, and formed the basis for the more widely used Internet Key Exchange protocol.

IPsec Policy Agent -service provides end-to-end security between clients and servers on TCP/IP networks, manages IPsec policy settings, starts the Internet Key Exchange (IKE), and coordinates IPsec policy settings with the IP security driver.

IPsec driver -wrong!

Question 3

Question Type: MultipleChoice

This hash function uses 512-bit blocks and implements preset constants that change after each repetition. Each block is hashed into a 256-bit block through four branches that divides each 512 block into sixteen 32-bit words that are further encrypted and rearranged.

Options:

A- SHA-256

B- FORK-256

C- SHA-1

D- RSA

Answer:

B

Explanation:

FORK-256

https://en.wikipedia.org/wiki/FORK-256

FORK-256 was introduced at the 2005 NIST Hash workshop and published the following year.[6]FORK-256 uses 512-bitblocksand implements preset constants that change after each repetition. Each block is hashed into a 256-bit block through four branches that divides each 512 block into sixteen 32-bit words that are further encrypted and rearranged.

Incorrect answers:

SHA1 -(Secure Hash Algorithm 1) is a cryptographic hash function which takes an input and produces a 160-bit (20-byte) hash value known as a message digest -- typically rendered as a hexadecimal number, 40 digits long. It was designed by the United States National Security Agency, and is a U.S. Federal Information Processing Standard.

RSA-(Rivest--Shamir--Adleman) is a public-key cryptosystem that is widely used for secure data transmission. It is also one of the oldest. The acronym RSA comes from the surnames of Ron Rivest, Adi Shamir, and Leonard Adleman, who publicly described the algorithm in 1977. An equivalent system was developed secretly, in 1973 at GCHQ (the British signals intelligence agency), by the

English mathematician Clifford Cocks. That system was declassified in 1997.

SHA-256 -SHA-2 (Secure Hash Algorithm 2) is a set of cryptographic hash functions designed by the United States National Security Agency (NSA) and first published in 2001. They are built using the Merkle--Damgrd structure, from a one-way compression function itself built using the Davies--Meyer structure from a specialized block cipher. SHA-2 includes significant changes from its predecessor, SHA-1. The SHA-2 family consists of six hash functions with digests (hash values) that are 224, 256, 384 or 512 bits: SHA-224, SHA-256, SHA-384, SHA-512, SHA-512/224, SHA-512/256

Question 4

Question Type: **MultipleChoice**

WPA2 uses AES for wireless data encryption at which of the following encryption levels?

Options:

A- 128 bit and CRC

B- 128 bi and TKIP

C- 128 bit and CCMP

D- 64 bit and CCMP

Answer:

C

Explanation:

128 bit and CCMP

Counter Mode with Cipher Block Chaining Message Authentication Code Protocol (CCMP) is an encryption protocol that forms part of the 802.11i standard for wireless local area networks (WLANs), particularly those using WiMax technology. CCMP employs 128-bit keys and a 48-bit initialization vector that minimizes vulnerability to replay attacks.

Question 5

Question Type: **MultipleChoice**

In relationship to hashing, the term _____refers to random bits that are used as one of the inputs to the hash. Essentially the _____ is intermixed with the message that is to be hashed

Options:

A- Vector

B- Salt

C- Stream

D- IV

Answer:

B

Explanation:

Salt

https://en.wikipedia.org/wiki/Salt_(cryptography)

A salt is random data that is used as an additional input to a one-way function that hashes data, a password or passphrase. Salts are used to safeguard passwords in storage. Historically a password was stored in plaintext on a system, but over time additional safeguards were developed to protect a user's password against being read from the system. A salt is one of those methods.

Incorrect answers:

Vector -Wrong!

IV-an initialization vector or starting variable (SV) is a fixed-size input to a cryptographic primitive that is typically required to be random or pseudorandom. Randomization is crucial for encryption schemes to achieve semantic security, a property whereby repeated usage of the scheme under the same key does not allow an attacker to infer relationships between segments of the encrypted message. For block ciphers, the use of an IV is described by the modes of operation. Randomization is also required for other primitives, such as universal hash functions and message authentication codes based thereon.

Stream -A stream cipher is a symmetric key cipher where plaintext digits are combined with a pseudorandom cipher digit stream (keystream). In a stream cipher, each plaintext digit is encrypted one at a time with the corresponding digit of the keystream, to give a digit of the ciphertext stream. Since encryption of each digit is dependent on the current state of the cipher, it is also known as state cipher. In practice, a digit is typically a bit and the combining operation is an exclusive-or (XOR).

Question 6

Question Type: **MultipleChoice**

You are explaining the details of the AES algorithm to cryptography students. You are discussing the derivation of the round keys from the shared symmetric key. The portion of AES where round keys are derived from the cipher key using Rijndael's key schedule is called what?

Options:

A- The key expansion phase

B- The round key phase

C- The bit shifting phase

D- The initial round

Answer:

A

Explanation:

The key expansion phase

https://en.wikipedia.org/wiki/Advanced_Encryption_Standard

KeyExpansion -- round keys are derived from the cipher key using the AES key schedule. AES requires a separate 128-bit round key block for each round plus one more.

Question 7

Question Type: MultipleChoice

You have been tasked with selecting a digital certificate standard for your company to use. Which one of the following was an international standard for the format and information contained in a digital certificate?

Options:

A- CA

B- X.509

C- CRL

D- RFC 2298

X- 509
https://en.wikipedia.org/wiki/X.509

X- 509 is a standard defining the format of public key certificates. X.509 certificates are used in many Internet protocols, including TLS/SSL, which is the basis for HTTPS, the secure protocol for browsing the web. They are also used in offline applications, like electronic signatures. An X.509 certificate contains a public key and an identity (a hostname, or an organization, or an individual), and is either signed by a certificate authority or self-signed. When a certificate is signed by a trusted certificate authority, or validated by other means, someone holding that certificate can rely on the public key it contains to establish secure communications with another party, or validate documents digitally signed by the corresponding private key.

Answer:

B

Question 8

Question Type: MultipleChoice

Denis is looking at an older system that uses DES encryption. A colleague has told him that DES is insecure due to a small key size. What is the key length used for DES?

Options:

A- 128

B- 256

C- 56

D- 64

Answer:

C

Explanation:

56

https://en.wikipedia.org/wiki/DES

The Data Encryption Standard is a symmetric-key algorithm for the encryption of digital data. Although its short key length of 56 bits makes it too insecure for applications, it has been highly influential in the advancement of cryptography.

Question 9

Question Type: **MultipleChoice**

The mode makes a block cipher into a synchronous stream cipher. It generates keystream blocks, which are then XORed with the plaintext blocks to get the ciphertext.

Options:

A- Cipher-block chaining (CBC)

B- Electronic codebook (ECB)

C- Output feedback (OFB)

D- Cipher feedback (CFB)

Answer:

C

Explanation:

Output feedback (OFB)

https://en.wikipedia.org/wiki/Block_cipher_mode_of_operation#Output_feedback_(OFB)

The output feedback (OFB) mode makes a block cipher into a synchronous stream cipher. It generates keystream blocks, which are then XORed with the plaintext blocks to get the ciphertext. Just as with other stream ciphers, flipping a bit in the ciphertext produces a flipped bit in the plaintext at the same location. This property allows many error-correcting codes to function normally even when applied before encryption.

Incorrect answers:

Cipher feedback (CFB)- mode, a close relative of CBC, makes a block cipher into a self-synchronizing stream cipher.

Electronic codebook (ECB)- the simplest of the encryption modes (named after conventional physical codebooks). The message is divided into blocks, and each block is encrypted separately.

Cipher-block chaining (CBC)- Ehrsam, Meyer, Smith and Tuchman invented the cipher block chaining (CBC) mode of operation in 1976. In CBC mode, each block of plaintext is XORed with the previous ciphertext block before being encrypted. This way, each ciphertext block depends on all plaintext blocks processed up to that point. To make each message unique, an initialization vector must be used in the first block.