Free Questions for 212-81

Shared by Mack on 04-10-2024

For More Free Questions and Preparation Resources

Check the Links on Last Page

Question 1

Question Type: MultipleChoice

Early attempt to make substitution ciphers more robust, masks letter frequencies, plain text letters map to multiple cipher text symbols.

Options:

A- Scytale Cipher

B- Playfair Cipher

C- Homophonic Substitution

D- ADFVGX Cipher

Answer:

C

Explanation:

Homophonic Substitution

https://en.wikipedia.org/wiki/Substitution_cipher#Homophonic_substitution

An early attempt to increase the difficulty of frequency analysis attacks on substitution ciphers was to disguise plaintext letter frequencies by homophony. In these ciphers, plaintext letters map to more than one ciphertext symbol. Usually, the highest-frequency plaintext symbols are given more equivalents than lower frequency letters. In this way, the frequency distribution is flattened, making analysis more difficult.

Incorrect answers:

Playfair Cipher - (Playfair square or Wheatstone-Playfair cipher) is a manual symmetric encryption technique and was the first literal digram substitution cipher. The scheme was invented in 1854 by Charles Wheatstone, but bears the name of Lord Playfair for promoting its use.

Scytale Cipher - is a tool used to perform a transposition cipher, consisting of a cylinder with a strip of parchment wound around it on which is written a message. The ancient Greeks, and the Spartans in particular, are said to have used this cipher to communicate during military campaigns.

ADFVGX Cipher - cipher was a field cipher used by the German Army on the Western Front during World War I. ADFGVX was in fact an extension of an earlier cipher called ADFGX. Invented by Lieutenant Fritz Nebel (1891--1977) and introduced in March 1918, the cipher was a fractionating transposition cipher which combined a modified Polybius square with a single columnar transposition.

Question 2

Question Type: **MultipleChoice**

Storing private keys with a third party is referred to as what?

Options:

A- Key caching

B- Key storage

C- Key banking

D- Key escrow

Answer:

D

Explanation:

Key escrow

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

Key escrow (also known as a "fair" cryptosystem) is an arrangement in which the keys needed to decrypt encrypted data are held in escrow so that, under certain circumstances, an authorized third party may gain access to those keys. These third parties may include businesses, who may want access to employees' secure business-related communications, or governments, who may wish to be able to view the contents of encrypted communications (also known as exceptional access).

Question 3

Question Type: MultipleChoice

Hash algortihm created by the Russians. Produces a fixed length output of 256bits. Input message is broken up into 256 bit blocks. If block is less than 256 bits then it is padded with 0s.

Options:

A- TIGER

B- GOST

C- BEAR

D- FORK-256

Answer:

B

Explanation:

GOST

https://en.wikipedia.org/wiki/GOST_(hash_function)

The GOST hash function, defined in the standards GOST R 34.11-94 and GOST 34.311-95 is a 256-bit cryptographic hash function. It was initially defined in the Russian national standard GOST R 34.11-94 Information Technology -- Cryptographic Information Security -- Hash Function. The equivalent standard used by other member-states of the CIS is GOST 34.311-95.

Incorrect answers:

BEAR - BEAR block cipher was invented by Ross Anderson and Eli Biham by combining a stream cipher and a cryptographic hash function.

TIGER - is a cryptographic hash function designed by Ross Anderson and Eli Biham in 1995 for efficiency on 64-bit platforms. The size of a Tiger hash value is 192 bits. Truncated versions (known as Tiger/128 and Tiger/160) can be used for compatibility with protocols assuming a particular hash size. Unlike the SHA-2 family, no distinguishing initialization values are defined; they are simply prefixes of the full Tiger/192 hash value.

FORK-256 - is a hash algorithm designed in response to security issues discovered in the earlier SHA-1 and MD5 algorithms. After substantial cryptanalysis, the algorithm is considered broken.

Question 4

Question Type: **MultipleChoice**

A number that is used only one time, then discarded is called what?

Options:

A- IV

B- Nonce

C- Chain

D- Salt

Answer:

B

Explanation:

Nonce

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

A nonce is an arbitrary number that can be used just once in a cryptographic communication. It is similar in spirit to a nonce word, hence the name. It is often a random or pseudo-random number issued in an authentication protocol to ensure that old communications cannot be reused in replay attacks.

Question 5

Question Type: MultipleChoice

Which of the following equations is related to EC?

Options:

A- P = Cd%n

B- Me%n

C- y^2 = x^3 + Ax + B

D- Let m = (p-1)(q-1)

Answer:

C

Explanation:

y^2 = x^3 + Ax + B

https://en.wikipedia.org/wiki/Elliptic-curve_cryptography

For current cryptographic purposes, an elliptic curve is a plane curve over a finite field (rather than the real numbers) which consists of the points satisfying the equation:

Question 6

Question Type: **MultipleChoice**

Algorithm that was chosen for the Data Encryption Standard, which was altered and renamed Data Encryption Algorithm.

Options:

A- Blowfish

B- Rijndael

C- Lucifer

D- El Gamal

Answer:

C

Explanation:

Lucifer

https://en.wikipedia.org/wiki/Lucifer_(cipher)

Lucifer was a direct precursor to the Data Encryption Standard. One version, alternatively named DTD-1.

Question 7

Question Type: **MultipleChoice**

With Cipher-block chaining (CBC) what happens?

Options:

A- The block cipher is turned into a stream cipher

B- The message is divided into blocks and each block is encrypted separately. This is the most basic mode for symmetric encryption

C- Each block of plaintext is XORed with the previous ciphertext block before being encrypted

D- The cipher text from the current round is XORed with the plaintext for the next round

Answer:

C

Explanation:

Each block of plaintext is XORed with the previous ciphertext block before being encrypted

https://en.wikipedia.org/wiki/Block_cipher_mode_of_operation#Cipher_block_chaining_(CBC)

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.

Question 8

Question Type: MultipleChoice

Frank is trying to break into an encrypted file... He is attempting all the possible keys that could be used for this algorithm. Attempting to crack encryption by simply trying as many randomly generated keys as possible is referred to as what?

Options:

A- Rainbow table

B- Frequency analysis

C- Brute force

D- Kasiski

Answer:

C

Explanation:

Brute force

https://en.wikipedia.org/wiki/Brute-force_attack

Brute-force attack consists of an attacker submitting many passwords or passphrases with the hope of eventually guessing correctly. The attacker systematically checks all possible passwords and passphrases until the correct one is found. Alternatively, the attacker can

attempt to guess the key which is typically created from the password using a key derivation function. This is known as an exhaustive key search.

Incorrect answers:

Kasiski - Kasiski examination (also referred to as Kasiski's test or Kasiski's method) is a method of attacking polyalphabetic substitution ciphers, such as the Vigenre cipher. It was first published by Friedrich Kasiski in 1863, but seems to have been independently discovered by Charles Babbage as early as 1846.

Rainbow table - is a precomputed table for caching the output of cryptographic hash functions, usually for cracking password hashes. Tables are usually used in recovering a key derivation function (or credit card numbers, etc.) up to a certain length consisting of a limited set of characters. It is a practical example of a space--time tradeoff, using less computer processing time and more storage than a brute-force attack which calculates a hash on every attempt, but more processing time and less storage than a simple key derivation function with one entry per hash. Use of a key derivation that employs a salt makes this attack infeasible.

Frequency analysis - (also known as counting letters) is the study of the frequency of letters or groups of letters in a ciphertext. The method is used as an aid to breaking classical ciphers.

Question 9

Question Type: **MultipleChoice**

Which of the following uses an 80 bit key on 64 bit blocks?

Options:

A- Skipjack

B- Twofish

C- DES

D- AES

Answer:

A

Explanation:

Skipjack

https://en.wikipedia.org/wiki/Skipjack_(cipher)

Skipjack uses an 80-bit key to encrypt or decrypt 64-bit data blocks. It is an unbalanced Feistel network with 32 rounds.

Incorrect answers:

Twofish - is a symmetric key block cipher with a block size of 128 bits and key sizes up to 256 bits. It was one of the five finalists of the Advanced Encryption Standard contest, but it was not selected for standardization. Twofish is related to the earlier block cipher Blowfish.

AES - For AES, NIST selected three members of the Rijndael family, each with a block size of 128 bits, but three different key lengths: 128, 192 and 256 bits.

DES - 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 10

Question Type: **MultipleChoice**

A disk you rotated to encrypt/decrypt. Created by Leon Alberti. Similar technologies were used in the Enigma machine. Considered the forefather of modern encryption.

Options:

A- Chi Square

B- Enigma Machine

C- Cipher Disks

D- Scytale Cipher

Answer:

C

Explanation:

Cipher disks

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

A cipher disk is an enciphering and deciphering tool developed in 1470 by the Italian architect and author Leon Battista Alberti. He constructed a device, (eponymously called the Alberti cipher disk) consisting of two concentric circular plates mounted one on top of the other. The larger plate is called the 'stationary' and the smaller one the 'moveable' since the smaller one could move on top of the 'stationary'.

Question 11

Question Type: MultipleChoice

With Electronic codebook (ECB) what happens:

Options:

A- The message is divided into blocks and each block is encrypted separately. This is the most basic mode for symmetric encryption

B- The cipher text from the current round is XORed with the plaintext from the previous round

C- The block cipher is turned into a stream cipher

D- The cipher text from the current round is XORed with the plaintext for the next round

Answer:

A

Explanation:

The message is divided into blocks and each block is encrypted separately. This is the most basic mode for symmetric encryption

https://en.wikipedia.org/wiki/Block_cipher_mode_of_operation#Electronic_codebook_(ECB)

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

Question 12

Question Type: MultipleChoice

What type of encryption uses different keys to encrypt and decrypt the message?

Options:

A- Asymmetric

B- Symmetric

C- Secure

D- Private key

Answer:

A

Explanation:

Asymmetric

https://en.wikipedia.org/wiki/Public-key_cryptography

Asymmetric cryptography, is a cryptographic system that uses pairs of keys: public keys, which may be disseminated widely, and private keys, which are known only to the owner. The generation of such keys depends on cryptographic algorithms based on mathematical

problems to produce one-way functions. Effective security only requires keeping the private key private; the public key can be openly distributed without compromising security.

To Get Premium Files for 212-81 Visit

https://www.p2pexams.com/products/212-81

For More Free Questions Visit

https://www.p2pexams.com/eccouncil/pdf/212-81