Free Questions for 212-81 by go4braindumps

Shared by Carroll on 12-12-2023

For More Free Questions and Preparation Resources

Check the Links on Last Page

Question 1

Question Type: MultipleChoice

What does the OCSP protocol provide?

Options:

A- Revoked certificates

B- Hashing

C- VPN connectivity

D- Encryption

Answer:

A

Explanation:

Revoked certificates

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

The Online Certificate Status Protocol (OCSP) is an Internet protocol used for obtaining the revocation status of an X.509 digital certificate.It is described in RFC 6960 and is on the Internet standards track. It was created as an alternative to certificate revocation lists (CRL), specifically addressing certain problems associated with using CRLs in a public key infrastructure (PKI). Messages communicated via OCSP are encoded in ASN.1 and are usually communicated over HTTP. The 'request/response' nature of these messages leads to OCSP servers being termed OCSP responders.

Question 2

Question Type: **MultipleChoice**

Bob's password is hashed, and so is John's. Even though they used different passwords, the hash is the same. What is this called?

Options:

A- A collision

B- A mistake

C- Convergence

D- Transposition

Answer:

A

Explanation:

A collision

https://en.wikipedia.org/wiki/Collision_(computer_science)

A collision or clash is a situation that occurs when two distinct pieces of data have the same hash value, checksum, fingerprint, or cryptographic digest.

Question 3

Question Type: MultipleChoice

Which of the following is an asymmetric algorithm that was first publically described in 1977?

Options:

A- Elliptic Curve

B- Twofish

C- DESX

D- RSA

Answer:

D

Explanation:

RSA

https://en.wikipedia.org/wiki/RSA_(cryptosystem)

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.

Incorrect answers:

Elliptic Curve -Elliptic-curve cryptography (ECC) is an approach to public-key cryptography based on the algebraic structure of elliptic curves over finite fields. ECC allows smaller keys compared to non-EC cryptography (based on plain Galois fields) to provide equivalent security.

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.

DESX -is a variant on the DES (Data Encryption Standard) symmetric-key block cipher intended to increase the complexity of a brute-force attack using a technique called key whitening.

Question 4

Question Type: **MultipleChoice**

This is a 128 bit hash that is specified by RFC 1321. It was designed by Ron Rivest in 1991 to replace an earlier hash function.

Options:

A- SHA1

B- SHA-256

C- RSA

D- MD5

Answer:

D

Explanation:

MD5

https://en.wikipedia.org/wiki/MD5

The MD5 message-digest algorithm is a widely used hash function producing a 128-bit hash value. Although MD5 was initially designed to be used as a cryptographic hash function, it has been found to suffer from extensive vulnerabilities. It can still be used as a checksum to verify data integrity, but only against unintentional corruption. It remains suitable for other non-cryptographic purposes, for example for determining the partition for a particular key in a partitioned database.

MD5 was designed by Ronald Rivest in 1991 to replace an earlier hash function MD4, and was specified in 1992 as RFC 1321.

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 5

Question Type: **MultipleChoice**

Cylinder tool. Wrap leather around to decode. The diameter is the key. Used in 7th century BC by greek poet Archilochus.

Options:

A- Cipher disk

B- Caesar cipher

C- Scytale

D- Enigma machine

Answer:

C

Explanation:

Scytale

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

A scytale 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 in 7th century BC to communicate during military campaigns.

The recipient uses a rod of the same diameter on which the parchment is wrapped to read the message. It has the advantage of being fast and not prone to mistakes---a necessary property when on the battlefield. It can, however, be easily broken. Since the strip of parchment hints strongly at the method, the ciphertext would have to be transferred to something less suggestive, somewhat reducing the advantage noted.

Incorrect answers:

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'.

Enigma machine -is an encryption device developed and used in the early- to mid-20th century to protect commercial, diplomatic and military communication. It was employed extensively by Nazi Germany during World War II, in all branches of the German military.

Caesar cipher -(also known as Caesar's cipher, the shift cipher, Caesar's code or Caesar shift) is one of the simplest and most widely known encryption techniques. It is a type of substitution cipher in which each letter in the plaintext is replaced by a letter some fixed number of positions down the alphabet. For example, with a left shift of 3, D would be replaced by A, E would become B, and so on. The method is named after Julius Caesar, who used it in his private correspondence.

Question 6

Question Type: **MultipleChoice**

Which one of the following attempts to hide data in plain view?

Options:

A- Cryptography

B- Substitution

C- Steganography

D- Asymmetric cryptography

Answer:

C

Explanation:

Steganography

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

Steganography is the practice of concealing a file, message, image, or video within another file, message, image, or video. The word steganography comes from Greek steganographia, which combines the words stegans , meaning 'covered or concealed', and -graphia meaning 'writing'.

Question 7

Question Type: **MultipleChoice**

Which service in a PKI will vouch for the identity of an individual or company?

Options:

A- CA

B- CR

C- KDC

D- CBC

Answer:

A

Explanation:

CA

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

A certificate authority or certification authority (CA) is an entity that issues digital certificates. A digital certificate certifies the ownership of a public key by the named subject of the certificate. This allows others (relying parties) to rely upon signatures or on assertions made about the private key that corresponds to the certified public key. A CA acts as a trusted third party---trusted both by the subject (owner) of the certificate and by the party relying upon the certificate. The format of these certificates is specified by the X.509 or EMV standard.

Question 8

Question Type: MultipleChoice

Manipulating individuals so that they will divulge confidential information, rather than by breaking in or using technical cracking techniques.

Options:

A- Linear cryptanalysis

B- Replay attack

C- Side-channel attack

D- Social engineering attack

Answer:

D

Explanation:

Social engineering attack

https://en.wikipedia.org/wiki/Social_engineering_(security)

Social engineering is the psychological manipulation of people into performing actions or divulging confidential information. This differs from social engineering within the social sciences, which does not concern the divulging of confidential information. A type of confidence trick for the purpose of information gathering, fraud, or system access, it differs from a traditional 'con' in that it is often one of many steps in a more complex fraud scheme.

Incorrect answers:

Replay attack -(also known as playback attack) is a form of network attack in which a valid data transmission is maliciously or fraudulently repeated or delayed. This is carried out either by the originator or by an adversary who intercepts the data and re-transmits it, possibly as part of a masquerade attack by IP packet substitution. This is one of the lower tier versions of a 'Man-in-the-middle attack.'

Side-channel attack -is any attack based on information gained from the implementation of a computer system, rather than weaknesses in the implemented algorithm itself (e.g. cryptanalysis and software bugs). Timing information, power consumption, electromagnetic leaks or even sound can provide an extra source of information, which can be exploited.

Linear cryptanalysis -is a general form of cryptanalysis based on finding affine approximations to the action of a cipher. Attacks have been developed for block ciphers and stream ciphers. Linear cryptanalysis is one of the two most widely used attacks on block ciphers; the other being differential cryptanalysis.

Question 9

Question Type: MultipleChoice

_____cryptography uses one key to encrypt a message and a different key to decrypt it.

Options:

A- Secure

B- Asymmetric

C- Stream

D- Symmetric

Answer:

B

Explanation:

Asymmetric

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

Public-key cryptography, or 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.

Question 10

Question Type: MultipleChoice

MD5 can best be described as which one of the following?

Options:

A- Asymmetric algorithm

B- Hashing algorithm

C- Digital signature

D- Symmetric algorithm

Answer:

B

Explanation:

Hashing algorithm

https://en.wikipedia.org/wiki/MD5

The MD5 message-digest algorithm is a widely used hash function producing a 128-bit hash value. Although MD5 was initially designed to be used as a cryptographic hash function, it has been found to suffer from extensive vulnerabilities. It can still be used as a checksum to verify data integrity, but only against unintentional corruption. It remains suitable for other non-cryptographic purposes, for example for determining the partition for a particular key in a partitioned database.