Free Questions for 212-81 by actualtestdumps

Shared by Case on 09-08-2024

For More Free Questions and Preparation Resources

Check the Links on Last Page

Question 1

Question Type: MultipleChoice

Which one of the following best describes a process that splits the block of plaintext into two separate blocks, then applies the round function to one half, and finally swaps the two halves?

Options:

A- Block ciphers

B- Symmetric cryptography

C- Feistel cipher

D- Substitution cipher

Answer:

C

Explanation:

Correct answer:

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

Feistel cipher (also known as Luby--Rackoff block cipher) is a symmetric structure used in the construction of block ciphers, named after the German-born physicist and cryptographer Horst Feistel who did pioneering research while working for IBM (USA); it is also commonly known as a Feistel network. A large proportion of block ciphers use the scheme, including the US Data Encryption Standard, the Soviet-developed GOST and the more recent Blowfish and Twofish ciphers. In a Feistel cipher, encryption and decryption are very similar operations, and both consist of iteratively running a function called a 'round function' a fixed number of times.

Incorrect answers:

Symmetric cryptography - Symmetric-key algorithms are algorithms for cryptography that use the same cryptographic keys for both encryption of plaintext and decryption of ciphertext. The keys may be identical or there may be a simple transformation to go between the two keys.

Substitution cipher - is a method of encrypting by which units of plaintext are replaced with ciphertext, according to a fixed system; the 'units' may be single letters (the most common), pairs of letters, triplets of letters, mixtures of the above, and so forth. The receiver deciphers the text by performing the inverse substitution.

Block ciphers - block cipher is a deterministic algorithm operating on fixed-length groups of bits, called blocks. It uses an unvarying transformation, that is, it uses a symmetric key. They are specified elementary components in the design of many cryptographic protocols and are widely used to implement the encryption of large amounts of data, including data exchange protocols.

Question 2

Question Type: MultipleChoice

If the round function is a cryptographically secure pseudorandom function, then ___rounds is sufficient to make it a "strong" pseudorandom permutation.

Options:

A- 15

B- 16

C- 3

D- 4

Answer:

D

Explanation:

4

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

Michael Luby and Charles Rackoff analyzed the Feistel cipher construction, and proved that if the round function is a cryptographically secure pseudorandom function, with Ki used as the seed, then 3 rounds are sufficient to make the block cipher a pseudorandom permutation, while 4 rounds are sufficient to make it a 'strong' pseudorandom permutation (which means that it remains pseudorandom even to an adversary who gets oracle access to its inverse permutation). Because of this very important result of Luby and Rackoff, Feistel ciphers are sometimes called Luby--Rackoff block ciphers.

Question 3

Question Type: **MultipleChoice**

What is the basis for the FISH algorithm?

Options:

A- The Lagged Fibonacci generator

B- Prime number theory

C- Equations that describe an ellipse

D- The difficulty in factoring numbers

Answer:

A

Explanation:

The Lagged Fibonacci generator

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

The FISH (FIbonacci SHrinking) stream cipher is a fast software based stream cipher using Lagged Fibonacci generators, plus a concept from the shrinking generator cipher. It was published by Siemens in 1993. FISH is quite fast in software and has a huge key length. However, in the same paper where he proposed Pike, Ross Anderson showed that FISH can be broken with just a few thousand bits of known plaintext.

Question 4

Question Type: MultipleChoice

If you use substitution alone, what weakness is present in the resulting cipher text?

Options:

A- It is the same length as the original text

B- It is easily broken with modern computers

C- It maintains letter and word frequency

D- It is too simple

Answer:

C

Explanation:

It maintains letter and word frequency

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

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.

Frequency analysis is based on the fact that, in any given stretch of written language, certain letters and combinations of letters occur with varying frequencies. Moreover, there is a characteristic distribution of letters that is roughly the same for almost all samples of that language. For instance, given a section of English language, E, T, A and O are the most common, while Z, Q, X and J are rare. Likewise, TH, ER, ON, and AN are the most common pairs of letters (termed bigrams or digraphs), and SS, EE, TT, and FF are the most

common repeats. The nonsense phrase 'ETAOIN SHRDLU' represents the 12 most frequent letters in typical English language text.

In some ciphers, such properties of the natural language plaintext are preserved in the ciphertext, and these patterns have the potential to be exploited in a ciphertext-only attack.

Question 5

Question Type: **MultipleChoice**

Juanita is attempting to hide some text into a jpeg file. Hiding messages inside another medium is referred to as which one of the following?

Options:

A- Cryptography

B- Steganalysis

C- Cryptology

D- Steganography

Answer:

D

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'.

Incorrect answers:

Cryptography, or cryptology, is the practice and study of techniques for secure communication in the presence of third parties called adversaries.

Steganalysis - is the study of detecting messages hidden using steganography; this is analogous to cryptanalysis applied to cryptography.

Question 6

Question Type: MultipleChoice

A simple algorithm that will take the initial key and from that generate a slightly different key each round.

Options:

A- Key Schedule

B- Feistel Network

C- SHA-2

D- Diffie-Helman

Answer:

A

Explanation:

Key Schedule

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

In cryptography, the so-called product ciphers are a certain kind of cipher, where the (de-)ciphering of data is typically done as an iteration of rounds. The setup for each round is generally the same, except for round-specific fixed values called a round constant, and round-specific data derived from the cipher key called a round key. A key schedule is an algorithm that calculates all the round keys from

the key.

Incorrect answers:

Feistel Network - (also known as Luby--Rackoff block cipher) is a symmetric structure used in the construction of block ciphers, named after the German-born physicist and cryptographer Horst Feistel who did pioneering research while working for IBM (USA).

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.

Diffie--Hellman - key exchange is a method of securely exchanging cryptographic keys over a public channel and was one of the first public-key protocols as conceived by Ralph Merkle and named after Whitfield Diffie and Martin Hellman.

Question 7

Question Type: MultipleChoice

3DES can best be classified as which one of the following?

Options:

A- Digital signature

B- Symmetric algorithm

C- Asymmetric algorithm

D- Hashing algorithm

Answer:

B

Explanation:

Symmetric algorithm

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

Triple DES (3DES or TDES), officially the Triple Data Encryption Algorithm (TDEA or Triple DEA), is a symmetric-key block cipher, which applies the DES cipher algorithm three times to each data block. The Data Encryption Standard's (DES) 56-bit key is no longer considered adequate in the face of modern cryptanalytic techniques and supercomputing power. However, an adapted version of DES, Triple DES (3DES), uses the same algorithm to produce a more secure encryption.

Question 8

Question Type: MultipleChoice

Represents the total number of possible values of keys in a cryptographic algorithm or other security measure, such as a password.

Options:

A- Key Schedule

B- Key Clustering

C- Key Space

D- Key Exchange

Answer:

C

Explanation:

Key Space

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

Algorithm's key space refers to the set of all possible permutations of a key.

To prevent an adversary from using a brute-force attack to find the key used to encrypt a message, the key space is usually designed to be large enough to make such a search infeasible. On average, half the key space must be searched to find the solution.

Another desirable attribute is that the key must be selected truly randomly from all possible key permutations. Should this not be the case, and the attacker is able to determine some factor that may influence how the key was selected, the search space (and hence also the search time) can be significantly reduced. Humans do not select passwords randomly, therefore attackers frequently try a dictionary attack before a brute force attack, as this approach can often produce the correct answer in far less time than a systematic brute force search of all possible character combinations.

Question 9

Question Type: MultipleChoice

Widely used, particularly with Microsoft operating systems. Created by MIT and derives its name from the mythical three headed dog. The is a great deal of verification for the tickets and the tickets expire quickly. Client authenticates to the Authentication Server once using a long term shared secret and receives back a Ticket-Granting Server. Client can reuse this ticket to get additional tickets without reusing the shared secret. These tickets are used to prove authentication to the Service Server.

Options:

A- Diffie-Hellman

B- Yarrow

C- Kerberos

D- ElGamal

Answer:

C

Explanation:

Kerberos

https://en.wikipedia.org/wiki/Kerberos_(protocol)

Kerberos is a computer-network authentication protocol that works on the basis of tickets to allow nodes communicating over a non-secure network to prove their identity to one another in a secure manner. The protocol was named after the character Kerberos (or Cerberus) from Greek mythology, the ferocious three-headed guard dog of Hades. Its designers aimed it primarily at a client--server model and it provides mutual authentication---both the user and the server verify each other's identity. Kerberos protocol messages are protected against eavesdropping and replay attacks.

Kerberos builds on symmetric key cryptography and requires a trusted third party, and optionally may use public-key cryptography during certain phases of authentication. Kerberos uses UDP port 88 by default.

Incorrect answers:

ElGamal - ElGamal encryption system is an asymmetric key encryption algorithm for public-key cryptography which is based on the Diffie--Hellman key exchange. It was described by Taher Elgamal in 1985. ElGamal encryption is used in the free GNU Privacy Guard software, recent versions of PGP, and other cryptosystems. The Digital Signature Algorithm (DSA) is a variant of the ElGamal signature scheme, which should not be confused with ElGamal encryption.

Diffie-Hellman - Diffie--Hellman key exchange is a method of securely exchanging cryptographic keys over a public channel and was one of the first public-key protocols as conceived by Ralph Merkle and named after Whitfield Diffie and Martin Hellman.[1][2] DH is one of the earliest practical examples of public key exchange implemented within the field of cryptography. Published in 1976 by Diffie and Hellman, this is the earliest publicly known work that proposed the idea of a private key and a corresponding public key.

Yarrow - algorithm is a family of cryptographic pseudorandom number generators (CPRNG) devised by John Kelsey, Bruce Schneier, and Niels Ferguson and published in 1999. The Yarrow algorithm is explicitly unpatented, royalty-free, and open source; no license is required to use it. Yarrow is incorporated in iOS and macOS for their /dev/random devices, and was in FreeBSD (where it is superseded by Fortuna).

Question 10

Question Type: **MultipleChoice**

In 1977 researchers and MIT described what asymmetric algorithm?

Options:

A- DH

B- RSA

C- AES

D- EC

Answer:

B

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.