212-81 Q&As

EC-Council Certified Encryption Specialist (ECES)

Pass EC-COUNCIL 212-81 Exam with 100% Guarantee

Free Download Real Questions & Answers **PDF** and **VCE** file from:

https://www.geekcert.com/212-81.html

100% Passing Guarantee
100% Money Back Assurance

Following Questions and Answers are all new published by EC-COUNCIL Official Exam Center

- **Instant Download** After Purchase
- **100% Money Back** Guarantee
- **365 Days** Free Update
- **800,000+** Satisfied Customers

QUESTION 1

Which of the following is a key exchange protocol?

A. MQV

B. AES

C. DES

D. RSA

Correct Answer: A

MQV https://en.wikipedia.org/wiki/MQV MQV (Menezes-Qu-Vanstone) is an authenticated protocol for key agreement based on the Diffie-Hellman scheme. Like other authenticated Diffie-Hellman schemes, MQV provides protection against an active attacker. The protocol can be modified to work in an arbitrary finite group, and, in particular, elliptic curve groups, where it is known as elliptic curve MQV (ECMQV).

QUESTION 2

What is the basis for the FISH algorithm?

A. The Lagged Fibonacci generator

B. Prime number theory

C. Equations that describe an ellipse

D. The difficulty in factoring numbers

Correct Answer: A

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 3

You are trying to find a modern method for security web traffic for use in your company\\'s ecommerce web site. Which one of the following is used to encrypt web pages and uses bilateral authentication?

A. AES

B. SSL

C. TLS

D. 3DES

Correct Answer: C

TLS https://en.wikipedia.org/wiki/Mutual_authentication Mutual authentication or two-way authentication refers to two parties authenticating each other at the same time, being a default mode of authentication in some protocols (IKE, SSH) and optional in others (TLS). By default the TLS protocol only proves the identity of the server to the client using X.509 certificate and the authentication of the client to the server is left to the application layer. TLS also offers client-to-server authentication using client-side

X.509 authentication. As it requires provisioning of the certificates to the clients and involves less user-friendly experience, it\\'s rarely used in end-user applications.

QUESTION 4

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?

A. Rainbow table

B. Frequency analysis

C. Brute force

D. Kasiski

Correct Answer: C

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.

QUESTION 5

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

A. Asymmetric

B. Symmetric

C. Secure

D. Private key

Correct Answer: A

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.