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.passapply.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

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 2

A non-secret binary vector used as the initializing input algorithm for encryption of a plaintext block sequence to increase security by introducing additional cryptographic variance.

A. IV

B. Salt

C. L2TP

D. Nonce

Correct Answer: A

IV https://en.wikipedia.org/wiki/Initialization_vector In cryptography, an initialization vector (IV) 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.

QUESTION 3

A linear congruential generator is an example of what?

A. A coprime generator

B. A prime number generator

C. A pseudo random number generator

D. A random number generator

Correct Answer: C

A pseudo random number generator https://en.wikipedia.org/wiki/Linear_congruential_generator A linear congruential generator (LCG) is an algorithm that yields a sequence of pseudo- randomized numbers calculated with a discontinuous piecewise linear equation. The method represents one of the oldest and best-known pseudorandom number generator algorithms. The theory behind them is relatively easy to understand, and they are easily implemented and fast, especially on computer hardware which can provide modular arithmetic by storage-bit truncation.

QUESTION 4

Hash. Created by Ronald Rivest. Replaced MD4. 128 bit output size, 512 bit block size, 32 bit word size, 64 rounds. Infamously compromised by Flame malware in 2012.

A. Keccak

B. MD5

C. SHA-1

D. TIGER

Correct Answer: B

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

QUESTION 5

This algorithm was published by the German engineering firm Seimans in 1993. It is a software based stream cipher using Lagged Fibonacci generator along with a concept borrowed from the shrinking generator ciphers.

A. RC4

B. Blowfish

C. Twofish

D. FISH

Correct Answer: D

FISH

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.