# 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**

Collision resistance is an important property for any hashing algorithm. Joan wants to find a cryptographic hash that has strong collision resistance. Which one of the following is the most collisionresistant?

A. SHA2

B. MD5

C. MD4

D. PIKE

Correct Answer: A

SHA2 https://en.wikipedia.org/wiki/Collision_resistance Collision resistance is a property of cryptographic hash functions: a hash function H is collision-resistant if it is hard to find two inputs that hash to the same output; that is, two inputs a and b where a b but H(a) = H(b). The pigeonhole principle means that any hash function with more inputs than outputs will necessarily have such collisions; the harder they are to find, the more cryptographically secure the hash function is. Due to the Birthday Problem, for a hash function that produces an output of length n bits, the probability of getting a collision is 1/2^n/2. So, just looking for a hash function with larger "n". 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 2**

How did the ATBASH cipher work?

A. By substituting each letter for the letter from the opposite end of the alphabet (i.e. A becomes Z, B becomes Y, etc.)

B. By rotating text a given number of spaces

C. By Multi alphabet substitution

D. By shifting each letter a certain number of spaces

Correct Answer: A

By substituting each letter for the letter from the opposite end of the alphabet (i.e. A becomes Z, B becomes Y, etc.)

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

The Atbash cipher is a particular type of monoalphabetic cipher formed by taking the alphabet (or abjad, syllabary, etc.) and mapping it to its reverse, so that the first letter becomes the last letter, the second letter becomes the second to last

letter, and so on.

**QUESTION 3**

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.

**QUESTION 4**

John works as a cryptography consultant. He finds that people often misunderstand the reality of breaking a cipher. What is the definition of breaking a cipher?

A. Finding any method that is more efficient than brute force

B. Uncovering the algorithm used

C. Rendering the cypher no longer useable

D. Decoding the key

Correct Answer: A

Finding any method that is more efficient than brute force.

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

Bruce Schneier notes that even computationally impractical attacks can be considered breaks: "Breaking a cipher simply means finding a weakness in the cipher that can be exploited with a complexity less than brute force. Never mind that

brute-force might require 2^128 encryptions; an attack requiring 2^110 encryptions would be considered a break...simply put, a break can just be a certificational weakness: evidence that the cipher does not perform as advertised."

**QUESTION 5**

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?

A. Block ciphers

B. Symmetric cryptography

C. Feistel cipher

D. Substitution cipher

Correct Answer: C