212-81$^{\text{Q\&As}}$

EC-Council Certified Encryption Specialist (ECES)

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

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

QUESTION 1

If you XOR 10111000 with 10101010, what is the result?

A. 10111010

B. 10101010

C. 11101101

D. 00010010

Correct Answer: D

https://en.wikipedia.org/wiki/XOR_cipher 1 0 1 1 1 0 0 0 1 0 1 0 1 0 1 0

0 0 0 1 0 0 1 0

QUESTION 2

Network of trusted certificate authority servers. Use asymmetric key pairs and combines software, encryption and services to provide a means of protecting security of business communication and transactions.

A. PKI

B. GOST

C. CA

D. PIKE

Correct Answer: A

PKI https://en.wikipedia.org/wiki/Public_key_infrastructure A public key infrastructure (PKI) is a set of roles, policies, hardware, software and procedures needed to create, manage, distribute, use, store and revoke digital certificates and manage public-key encryption. The purpose of a PKI is to facilitate the secure electronic transfer of information for a range of network activities such as e-commerce, internet banking and confidential email. It is required for activities where simple passwords are an inadequate authentication method and more rigorous proof is required to confirm the identity of the parties involved in the communication and to validate the information being transferred.

QUESTION 3

What is the basis for the difficulty in breaking RSA?

A. Hashing

B. The birthday paradox

C. Equations that describe an elliptic curve

D. Factoring numbers

Correct Answer: D

Factoring numbers

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. 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.

In a public-key cryptosystem, the encryption key is public and distinct from the decryption key, which is kept secret (private). An RSA user creates and publishes a public key based on two large prime numbers, along with an auxiliary value.

The prime numbers are kept secret. Messages can be encrypted by anyone, via the public key, but can only be decoded by someone who knows the prime numbers.

QUESTION 4

What must occur in order for a cipher to be considered `broken\\'?

A. Uncovering the algorithm used

B. Decoding the key

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

D. Rendering the cipher no longer useable

Correct Answer: C

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."

QUESTION 5

A ______ refers to a situation where two different inputs yield the same output.

A. Convergence

B. Collision

C. Transposition

D. Substitution

Correct Answer: B

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.