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

QUESTION 1

A type of frequency analysis used to attack polyalphabetic substitution ciphers. It\\'s used to try to discover patterns and use that information to decrypt the cipher.

A. Kasiski Method

B. Birthday Attack

C. Information Deduction

D. Integral Cryptanalysis

Correct Answer: A

Kasiski Method https://en.wikipedia.org/wiki/Kasiski_examination In cryptanalysis, Kasiski examination (also referred to as Kasiski\\'s test or Kasiski\\'s method) is a method of attacking polyalphabetic substitution ciphers, such as the Vigen?e cipher. It was first published by Friedrich Kasiski in 1863, but seems to have been independently discovered by Charles Babbage as early as 1846.

QUESTION 2

Which of the following is generally true about key sizes?

A. Larger key sizes increase security

B. Key size is irrelevant to security

C. Key sizes must be more than 256 bits to be secure

D. Smaller key sizes increase security

Correct Answer: A

Larger key sizes increase security https://en.wikipedia.org/wiki/Key_size Key length defines the upper-bound on an algorithm\\'s security (i.e. a logarithmic measure of the fastest known attack against an algorithm), since the security of all algorithms can be violated by brute-force attacks. Ideally, the lower-bound on an algorithm\\'s security is by design equal to the key length (that is, the security is determined entirely by the keylength, or in other words, the algorithm\\'s design doesn\\'t detract from the degree of security inherent in the key length). Indeed, most symmetric-key algorithms are designed to have security equal to their key length. However, after design, a new attack might be discovered. For instance, Triple DES was designed to have a 168 bit key, but an attack of complexity 2112 is now known (i.e. Triple DES now only has 112 bits of security, and of the 168 bits in the key the attack has rendered 56 \\'ineffective\\' towards security). Nevertheless, as long as the security (understood as \\'the amount of effort it would take to gain access\\') is sufficient for a particular application, then it doesn\\'t matter if key length and security coincide. This is important for asymmetric-key algorithms, because no such algorithm is known to satisfy this property; elliptic curve cryptography comes the closest with an effective security of roughly half its key length.

QUESTION 3

In relationship to hashing, the term _____refers to random bits that are used as one of the inputs to the hash. Essentially the _____ is intermixed with the message that is to be hashed

A. Vector

B. Salt

C. Stream

D. IV

Correct Answer: B

Salt

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

A salt is random data that is used as an additional input to a one-way function that hashes data, a password or passphrase. Salts are used to safeguard passwords in storage. Historically a password was stored in plaintext on a system, but

over time additional safeguards were developed to protect a user\\'s password against being read from the system. A salt is one of those methods.

QUESTION 4

Ciphers that write message letters out diagonally over a number of rows then read off cipher row by row. Also called zig-zag cipher.

A. Rail Fence Cipher

B. Null Cipher

C. Vigenere Cipher

D. ROT-13

Correct Answer: A

Rail Fence Cipher https://en.wikipedia.org/wiki/Rail_fence_cipher The rail fence cipher (also called a zigzag cipher) is a form of transposition cipher. It derives its name from the way in which it is encoded.

QUESTION 5

You have been tasked with selecting a digital certificate standard for your company to use. Which one of the following was an international standard for the format and information contained in a digital certificate?

A. CA

B. X.509

C. CRL

D. RFC 2298

Correct Answer: B

X.509 https://en.wikipedia.org/wiki/X.509

X.509 is a standard defining the format of public key certificates. X.509 certificates are used in many Internet protocols, including TLS/SSL, which is the basis for HTTPS, the secure protocol for browsing the web. They are also used in offline applications, like electronic signatures. An X.509 certificate contains a public key and an identity (a hostname, or an organization, or an individual), and is either signed by a certificate authority or self-signed. When a certificate is signed by a trusted certificate authority, or validated by other means, someone holding that certificate can rely on the public key it contains to establish secure communications with another party, or validate documents digitally signed by the corresponding private key.