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

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

Basic information theory is the basis for modern symmetric ciphers. Understanding the terminology of information theory is, therefore, important. Changes to one character in the plaintext affect multiple characters in the ciphertext. What is this referred to?

A. Avalanche

B. Confusion

C. Scrambling

D. Diffusion

Correct Answer: D

Diffusion https://en.wikipedia.org/wiki/Confusion_and_diffusion Diffusion means that if we change a single bit of the plaintext, then (statistically) half of the bits in the ciphertext should change, and similarly, if we change one bit of the ciphertext, then approximately one half of the plaintext bits should change. Since a bit can have only two states, when they are all re-evaluated and changed from one seemingly random position to another, half of the bits will have changed state. The idea of diffusion is to hide the relationship between the ciphertext and the plain text. This will make it hard for an attacker who tries to find out the plain text and it increases the redundancy of plain text by spreading it across the rows and columns; it is achieved through transposition of algorithm and it is used by block ciphers only

QUESTION 2

_____ uses at least two different shifts, changing the shift with different letters in the plain text.

A. Caesar cipher

B. multi-alphabet encryption

C. Scytale

D. Atbash

Correct Answer: B

multi-alphabet encryption https://en.wikipedia.org/wiki/Polyalphabetic_cipher Two different shifts create two different alphabets. For +1 and +2 Plaintext alphabet A B C D E F G H I J K L M N O P Q R S T U V W X Y Z 2 ciphertext alphabets B C D E F G H I J K L M N O P Q R S T U V W X Y Z A C D E F G H I J K L M N O P Q R S T U V W X Y Z A B

QUESTION 3

You are explaining basic mathematics to beginning cryptography students. You are covering the basic math used in RSA. A prime number is defined as

A. Odd numbers with no divisors

B. Odd numbers

C. Any number only divisible by odd numbers

D. Any number only divisible by one and itself

Correct Answer: C

Any number only divisible by one and itself https://en.wikipedia.org/wiki/Prime_number A prime number (or a prime) is a natural number greater than 1 that is not a product of two smaller natural numbers. A natural number greater than 1 that is not prime is called a composite number. For example, 5 is prime because the only ways of writing it as a product, 1 ?5 or 5 ?1, involve 5 itself. However, 4 is composite because it is a product (2 ?2) in which both numbers are smaller than 4. Primes are central in number theory because of the fundamental theorem of arithmetic: every natural number greater than 1 is either a prime itself or can be factorized as a product of primes that is unique up to their order.

QUESTION 4

A _______ product refers to an NSA-endorsed classified or controlled cryptographic item for classified or sensitive U. S. government information, including cryptographic equipment, assembly, or component classified or certified by NSA for encrypting and decrypting classified and sensitive national security information when appropriately keyed

A. 1

B. 4

C. 2

D. 3

Correct Answer: A

Type 1 https://en.wikipedia.org/wiki/NSA_cryptography#Type_1_Product A Type 1 Product refers to an NSA endorsed classified or controlled cryptographic item for classified or sensitive U.S. government information, including cryptographic equipment, assembly or component classified or certified by NSA for encrypting and decrypting classified and sensitive national security information when appropriately keyed.

QUESTION 5

If Bob is using asymmetric cryptography and wants to send a message to Alice so that only she can decrypt it, what key should he use to encrypt the message?

A. Alice\\'s private key

B. Bob\\'s private key

C. Alice\\'s public key

D. Bob\\'s public key

Correct Answer: C

Alice\\'s public key https://en.wikipedia.org/wiki/Diffie%E2%80%93Hellman_key_exchange In asymmetric (public key) cryptography, both communicating parties (i.e. both Alice and Bob) have two keys of their own -- just to be clear, that\\'s four keys total. Each party has their own public key, which they share with the world, and their own private key which they ... well, which they keep private, of course but, more than that, which they keep as a closely guarded secret. The magic of public key cryptography is that a message encrypted with the public key can only be decrypted with the private key. Alice will encrypt her message with Bob\\'s public key, and even though Eve knows she used Bob\\'s public key, and even though Eve knows Bob\\'s public key herself, she is unable to decrypt the message. Only Bob, using his secret key, can decrypt the message ... assuming he\\'s kept it secret, of course.

QUESTION 6

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 7

The reverse process from encoding - converting the encoded message back into its plaintext format.

A. Substitution

B. Whitening

C. Encoding

D. Decoding

Correct Answer: D

Decoding

Decoding - reverse process from encoding,converting the encoded message back into its plaintext format.

QUESTION 8

Which one of the following is an authentication method that sends the username and password in cleartext?

A. PAP

B. CHAP

C. Kerberos

D. SPAP

Correct Answer: A

PAP https://en.wikipedia.org/wiki/Password_Authentication_Protocol Password Authentication Protocol (PAP) is a password-based authentication protocol used by Point to Point Protocol (PPP) to validate users. Almost all network operating system remote servers support PAP. PAP is specified in RFC 1334. PAP is considered a weak authentication scheme (weak schemes are simple and have lighter computational overhead but are much more vulnerable to attack; while weak schemes may have limited application in some constrained environments, they are avoided in general). Among PAP\\'s deficiencies is the fact that it transmits unencrypted passwords (i.e. in plain-text) over the network. PAP is therefore used only as a last resort when the remote server does not support a stronger scheme such as CHAP or EAP.

QUESTION 9

Jane is looking for an algorithm to ensure message integrity. Which of following would be an acceptable choice?

A. RSA

B. AES

C. RC4

D. SHA-1

Correct Answer: D

Integrity. In information security, data integrity means maintaining and assuring the accuracy and completeness of data over its entire lifecycle. This means that data cannot be modified in an unauthorized or undetected manner. An important application of hashes is verification of message integrity. Comparing message digests (hash digests over the message) calculated before, and after, transmission can determine whether any changes have been made to the message or file. SHA-1 https://en.wikipedia.org/wiki/SHA-1 SHA-1 (Secure Hash Algorithm 1) is a cryptographic hash function which takes an input and produces a 160-bit (20-byte) hash value known as a message digest ?typically rendered as a hexadecimal number, 40 digits long. It was designed by the United States National Security Agency, and is a U.S. Federal Information Processing Standard.

QUESTION 10

Which of the following is the standard for digital certificates?

A. RFC 2298

B. X.509

C. CRL

D. CA

Correct Answer: B

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.

QUESTION 11

In a ______ the attacker discovers a functionally equivalent algorithm for encryption and decryption, but without learning the key.

A. Information deduction

B. Total break

C. Instance deduction

D. Global deduction

Correct Answer: D

Global deduction https://en.wikipedia.org/wiki/Cryptanalysis Global deduction -- the attacker discovers a functionally equivalent algorithm for encryption and decryption, but without learning the key.

QUESTION 12

What does the OCSP protocol provide?

A. Revoked certificates

B. Hashing

C. VPN connectivity

D. Encryption

Correct Answer: A

Revoked certificates https://en.wikipedia.org/wiki/Online_Certificate_Status_Protocol The Online Certificate Status Protocol (OCSP) is an Internet protocol used for obtaining the revocation status of an X.509 digital certificate.It is described in RFC 6960 and is on the Internet standards track. It was created as an alternative to certificate revocation lists (CRL), specifically addressing certain problems associated with using CRLs in a public key infrastructure (PKI). Messages communicated via OCSP are encoded in ASN.1 and are usually communicated over HTTP. The "request/response" nature of these messages leads to OCSP servers being termed OCSP responders.

QUESTION 13

A transposition cipher invented 1918 by Fritz Nebel, used a 36 letter alphabet and a modified Polybius square with a single columnar transposition.

A. ADFVGX Cipher

B. ROT13 Cipher

C. Book Ciphers

D. Cipher Disk

Correct Answer: A

ADFVGX Cipher https://en.wikipedia.org/wiki/ADFGVX_cipher ADFGVX cipher was a field cipher used by the German Army on the Western Front during World War I. ADFGVX was in fact an extension of an earlier cipher called ADFGX. Invented by Lieutenant Fritz Nebel (1891?977) and introduced in March 1918, the cipher was a fractionating transposition cipher which combined a modified Polybius square with a single columnar transposition.

QUESTION 14

The most widely used digital certificate standard. First issued July 3, 1988. It is a digital document that contains a public key signed by the trusted third party, which is known as a Certificate Authority, or CA. Relied on by S/MIME. Contains your name, info about you, and a signature of a person who issued the certificate.

A. ElGamal

B. RSA

C. PAP

D. X.509

Correct Answer: D

https://en.wikipedia.org/wiki/X.509 In cryptography, 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.

QUESTION 15

An authentication method that periodically re-authenticates the client by establishing a hash that is then resent from the client is called ______.

A. CHAP

B. SPAP

C. PAP

D. EAP

Correct Answer: A

CHAP https://en.wikipedia.org/wiki/Challenge-Handshake_Authentication_Protocol Challenge-Handshake Authentication Protocol (CHAP) is an identity verification protocol that does not rely on sending a shared secret between the access-requesting party and the identity-verifying party (the authenticator). CHAP is based on a shared secret, but in order to authenticate, the authenticator sends a "challenge" message to the access-requesting party, which responds with a value calculated using a "one-way hash" function that takes as inputs the challenge and the shared secret. The authenticator checks the response against its own calculation of the expected hash value. If the values match, the authentication succeeds, otherwise it fails. Following the establishment of an authenticated connection, the authenticator may send a challenge to the access-requesting party at random intervals, to which the access-requesting party will have to produce the correct response.