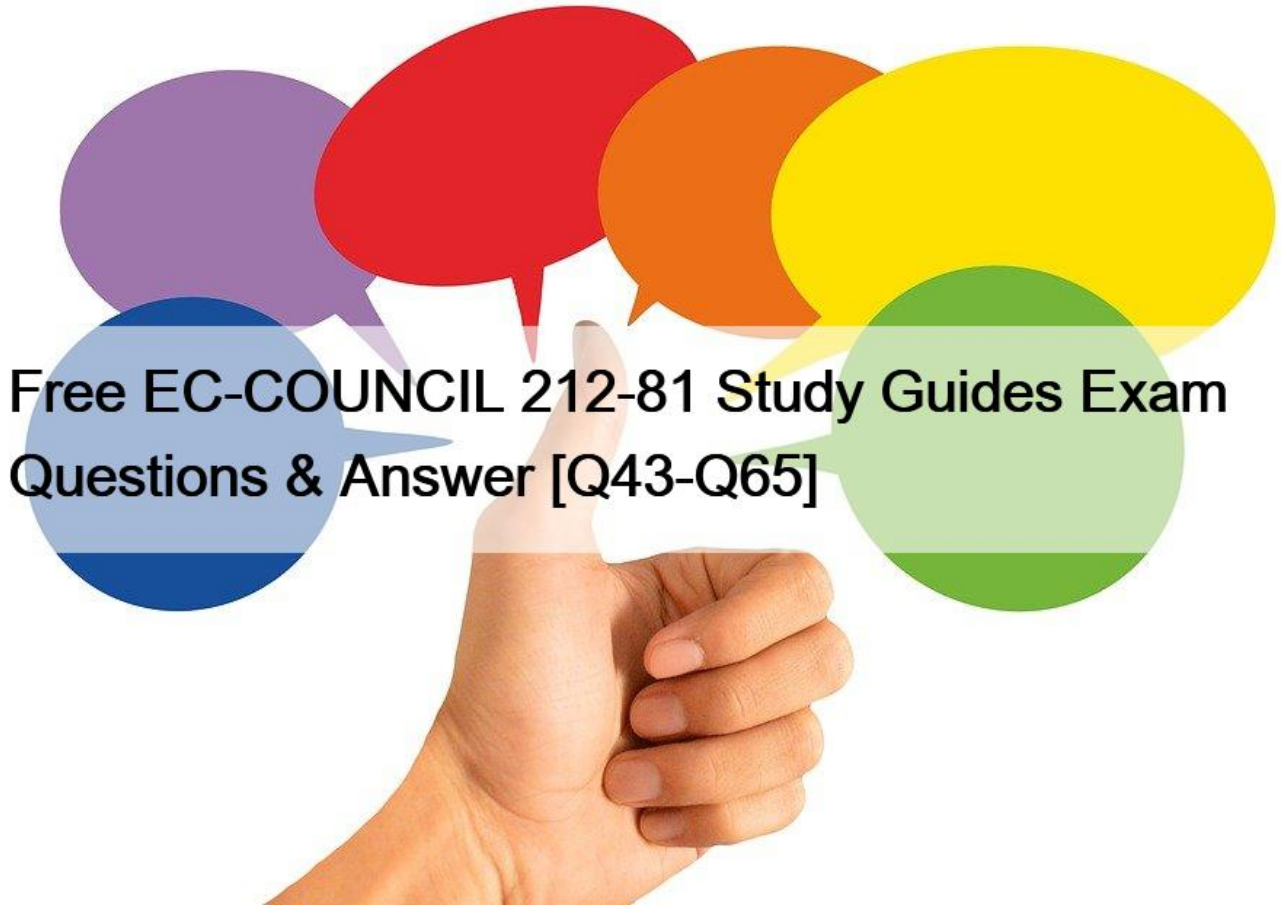
Free EC-COUNCIL 212-81 Study Guides Exam Questions & Answer [Q43-Q65



Free EC-COUNCIL 212-81 Study Guides Exam Questions and Answer
212-81 Exam Dumps, 212-81 Practice Test Questions

Q43. 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?
* CA
* X.509
* CRL
* RFC 2298
* 509

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

Q44. The most widely used asymmetric encryption algorithm is what?
* Vigenere
* Caesar Cipher
* RSA
* DES
RSA

The RSA encryption algorithm is one of the most widely used public key encryption algorithms that have ever been invented. It was created by the three scientists Ronald Rivest, Adi Shamir, and Leonard Adleman in 1977, and today it is increasingly being used in the network area.

Incorrect answers:

Caesar Cipher – Monoalphabetic cipher where letters are shifted one or more letters in either direction. The method is named after Julius Caesar, who used it in his private correspondence.

Vigenere – Multi alphabet cipher Invented by Giovan Battista Bellaso in middle 1553. Vigenere created a stronger version of the cipher. Combining/Weaving Caesar cipher. Not cracked until late 1800s. Widely used from 16th century to early 20th century. It is a cipher square with A to Z across all the columns and rows. You then use a keyword to encrypt the message DES – The Data Encryption Standard is a symmetric-key algorithm for the encryption of digital data.

Q45. Which of the following is an asymmetric cipher?
* RSA
* AES
* DES
* RC4
RSA

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.

Incorrect answers:

DES – is a symmetric-key algorithm for the encryption of digital data. Although its short key length of 56 bits makes it too insecure for applications, it has been highly influential in the advancement of cryptography.

RC4 – RSA (Rivest-Shamir-Adleman) is one of the first public-key cryptosystems and is widely used for secure data transmission (stream cipher).

AES – is a subset of the Rijndael block cipher developed by two Belgian cryptographers, Vincent Rijmen and Joan Daemen,

who submitted a proposal to NIST during the AES selection process. Rijndael is a family of ciphers with different key and block sizes. For AES, NIST selected three members of the Rijndael family, each with a block size of 128 bits, but three different key lengths: 128, 192 and 256 bits.

Q46. Developed by Netscape and has been replaced by TLS. It was the preferred method used with secure websites.
* OCSP
* VPN
* CRL
* SSL
SSL

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

Transport Layer Security (TLS), and its now-deprecated predecessor, Secure Sockets Layer (SSL), are cryptographic protocols designed to provide communications security over a computer network. Several versions of the protocols find widespread use in applications such as web browsing, email, instant messaging, and voice over IP (VoIP). Websites can use TLS to secure all communications between their servers and web browsers.

Netscape developed the original SSL protocols, and Taher Elgamal, chief scientist at Netscape Communications from 1995 to 1998, has been described as the “father of SSL”. SSL version 1.0 was never publicly released because of serious security flaws in the protocol. Version 2.0, released in February 1995, contained a number of security flaws which necessitated the design of version 3.0. Released in 1996, SSL version 3.0 represented a complete redesign of the protocol produced by Paul Kocher working with Netscape engineers Phil Karlton and Alan Freier, with a reference implementation by Christopher Allen and Tim Dierks of Consensus Development.

Incorrect answers:

CRL – a list of every certificate that has been revoked.

VPN – A virtual private network (VPN) extends a private network across a public network and enables users to send and receive data across shared or public networks as if their computing devices were directly connected to the private network. Applications running across a VPN may therefore benefit from the functionality, security, and management of the private network. Encryption is a common, although not an inherent, part of a VPN connection OCSP – 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).

Q47. MD5 can best be described as which one of the following?
* Asymmetric algorithm
* Hashing algorithm
* Digital signature
* Symmetric algorithm
Hashing algorithm

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.

Q48. Which one of the following terms describes two numbers that have no common factors?
* Coprime
* Fermat’s number
* Euler’s totient
* Convergent

Coprime

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

In number theory, two integers a and b are said to be relatively prime, mutually prime, or coprime if the only positive integer (factor) that divides both of them is 1. Consequently, any prime number that divides one of a or b does not divide the other. This is equivalent to their greatest common divisor (gcd) being 1.

Incorrect answers:

Convergent – a series is the sum of the terms of an infinite sequence of numbers.

Euler’s totient function – counts the positive integers up to a given integer n that are relatively prime to n. It is written using the Greek letter phi as ?(n) or ?(n), and may also be called Euler’s phi function. In other words, it is the number of integers k in the range 1 ? k ? n for which the greatest common divisor gcd(n, k) is equal to 1. The integers k of this form are sometimes referred to as totatives of n.

Fermat’s number – named after Pierre de Fermat, who first studied them, is a positive integer of the form where n is a non-negative integer.

Q49. The Clipper chip is notable in the history of cryptography for many reasons. First, it was designed for civilian used secure phones. Secondly, it was designed to use a very specific symmetric cipher. Which one of the following was originally designed to provide built-in cryptography for the Clipper chip?
* Blowfish
* Twofish
* Skipjack
* Serpent

Skipjack

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

The Clipper chip was a chipset that was developed and promoted by the United States National Security Agency (NSA) as an encryption device that secured “voice and data messages” with a built-in backdoor that was intended to “allow Federal, State, and local law enforcement officials the ability to decode intercepted voice and data transmissions.”. It was intended to be adopted by telecommunications companies for voice transmission. Introduced in 1993, it was entirely defunct by 1996.

he Clipper chip used a data encryption algorithm called Skipjack to transmit information and the Diffie-Hellman key exchange-algorithm to distribute the cryptokeys between the peers. Skipjack was invented by the National Security Agency of the U.S. Government; this algorithm was initially classified SECRET, which prevented it from being subjected to peer review from the encryption research community. The government did state that it used an 80-bit key, that the algorithm was symmetric, and that it was similar to the DES algorithm. The Skipjack algorithm was declassified and published by the NSA on June 24, 1998. The initial cost of the chips was said to be $16 (unprogrammed) or $26 (programmed), with its logic designed by Mykotronx, and fabricated by VLSI Technology, Inc (see the VLSI logo on the image on this page).

Q50. What does Output feedback (OFB) do:
* The message is divided into blocks and each block is encrypted separately. This is the most basic mode for symmetric encryption
* The cipher text from the current round is XORed with the plaintext from the previous round
* A block cipher is converted into a stream cipher by generating a keystream blocks, which are then XORed with the plaintext blocks to get the ciphertext
* The cipher text from the current round is XORed with the plaintext for the next round
A block cipher is converted into a stream cipher by generating a keystream blocks, which are then XORed with the plaintext blocks to get the ciphertext

https://en.wikipedia.org/wiki/Block_cipher_mode_of_operation#Output_feedback_(OFB) The output feedback (OFB) mode makes a block cipher into a synchronous stream cipher. It generates keystream blocks, which are then XORed with the plaintext blocks to get the ciphertext. Just as with other stream ciphers, flipping a bit in the ciphertext produces a flipped bit in the plaintext at the same location. This property allows many error-correcting codes to function normally even when applied before encryption.

Q51. Part of understanding cryptography is understanding the cryptographic primitives that go into any crypto system. A(n) _____ is a fixed-size input to a cryptographic primitive that is random or pseudorandom.
* Key
* IV
* Chain
* Salt
Key

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

In cryptography, a key is a piece of information (a parameter) that determines the functional output of a cryptographic algorithm. For encryption algorithms, a key specifies the transformation of plaintext into ciphertext, and vice versa for decryption algorithms. Keys also specify transformations in other cryptographic algorithms, such as digital signature schemes and message authentication codes.

Q52. 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?
* Alice’s private key
* Bob’s private key
* Alice’s public key
* Bob’s public key
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.

Q53. Numbers that have no factors in common with another.
* Fibonacci Numbers
* Even Numbers

* Co-prime numbers
* Mersenne Primes

Correct answers: Co-prime numbers

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

Two integers a and b are said to be relatively prime, mutually prime, or coprime if the only positive integer (factor) that evenly divides both of them is 1. Consequently, any prime number that divides one of a or b does not divide the other. This is equivalent to their greatest common divisor (gcd) being 1.

The numerator and denominator of a reduced fraction are coprime. The numbers 14 and 25 are coprime, since 1 is their only common divisor. On the other hand, 14 and 21 are not coprime, because they are both divisible by 7.

Incorrect answers:

Even Numbers – A formal definition of an even number is that it is an integer of the form n = 2k, where k is an integer; it can then be shown that an odd number is an integer of the form n = 2k + 1 (or alternately, 2k – 1). It is important to realize that the above definition of parity applies only to integer numbers, hence it cannot be applied to numbers like 1/2 or 4.201. See the section “Higher mathematics” below for some extensions of the notion of parity to a larger class of “numbers” or in other more general settings.

Fibonacci Numbers – commonly denoted F_n, form a sequence, called the Fibonacci sequence, such that each number is the sum of the two preceding ones, starting from 0 and 1.

Mersenne Primes – is a prime number that is one less than a power of two. That is, it is a prime number of the form M_n = 2 n – 1 for some integer n. They are named after Marin Mersenne, a French Minim friar, who studied them in the early 17th century. If n is a composite number then so is 2n – 1. Therefore, an equivalent definition of the Mersenne primes is that they are the prime numbers of the form M_p = 2p – 1 for some prime p.

Q54. Message hidden in unrelated text. Sender and receiver have pre-arranged to use a pattern to remove certain letters from the message which leaves only the true message behind.

* Caesar Cipher
* Null Ciphers
* Vigenere Cipher
* Playfair Cipher

Null Ciphers

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

A null cipher, also known as concealment cipher, is an ancient form of encryption where the plaintext is mixed with a large amount of non-cipher material. Today it is regarded as a simple form of steganography, which can be used to hide ciphertext.

Incorrect answers:

Caesar Cipher – Monoalphabetic cipher where letters are shifted one or more letters in either direction. The method is named after Julius Caesar, who used it in his private correspondence.

Vigenere – method of encrypting alphabetic text by using a series of interwoven Caesar ciphers, based on the letters of a keyword. It employs a form of polyalphabetic substitution.

Playfair Cipher – manual symmetric encryption technique and was the first literal digram substitution cipher. The scheme was invented in 1854 by Charles Wheatstone, but bears the name of Lord Playfair for promoting its use.

Q55. Encryption of the same plain text with the same key results in the same cipher text. Use of an IV that is XORed with the first block of plain text solves this problem.
* CFB
* GOST
* ECB
* RC4
ECB

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

The simplest of the encryption modes is the electronic codebook (ECB) mode (named after conventional physical codebooks). The message is divided into blocks, and each block is encrypted separately.

The disadvantage of this method is a lack of diffusion. Because ECB encrypts identical plaintext blocks into identical ciphertext blocks, it does not hide data patterns well. ECB is not recommended for use in cryptographic protocols.

ECB mode can also make protocols without integrity protection even more susceptible to replay attacks, since each block gets decrypted in exactly the same way.

Incorrect answers:

RC4 – stream symmetric cipher that was created by Ron Rivest of RSA. Used in SSL and WEP.

GOST – the GOST block cipher (Magma), defined in the standard GOST 28147-89 (RFC 5830), is a Soviet and Russian government standard symmetric key block cipher with a block size of 64 bits. The original standard, published in 1989, did not give the cipher any name, but the most recent revision of the standard, GOST R 34.12-2015, specifies that it may be referred to as Magma. The GOST hash function is based on this cipher. The new standard also specifies a new 128-bit block cipher called Kuznyechik.

CFB – the process wherein the ciphertext block is encrypted then the ciphertext produced is XOR’d back with the plaintext to produce the current ciphertext block.

Q56. The next number is derived from adding together the prior two numbers (1, 1, 2, 3, 5, 8, 13, 21, 34, 55, 89).
* Odd numbers
* Fibonacci Sequence
* Fermat pseudoprime
* Prime numbers
Fibonacci Sequence

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

In mathematics, the Fibonacci numbers, commonly denoted Fn, form a sequence, called the Fibonacci sequence, such that each number is the sum of the two preceding ones, starting from 0 and 1. That is, F0 = 0, F1=1, Fn = Fn-1 + Fn-2; for n > 1.

The beginning of the sequence is thus:

0,1, 1, 2, 3, 5, 8, 13, 21, 34, 55, 89, 144…

Incorrect answers:

Prime numbers – numbers that have only 2 factors: 1 and themselves. 2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43, 47…

Fermat numbers – a positive integer of the form Fn = 22n +1; where n is a non-negative integer. The first few Fermat numbers are: 3, 5, 17, 257, 65537, 4294967297, 18446744073709551617, …

Odd numbers – any number which cannot be divided by two 1, 3, 5, 7, 9, 11, 13, 15 …

Q57. You are explaining basic mathematics to beginning cryptography students. You are covering the basic math used in RSA. A prime number is defined as
* Odd numbers with no divisors
* Odd numbers
* Any number only divisible by odd numbers
* Any number only divisible by one and itself

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.

Q58. What is the solution to the equation 8 mod 3?
* 1
* 4
* 3
* 2

2

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

The modulo operation returns the remainder or signed remainder of a division, after one number is divided by another (called the modulus of the operation).

Given two positive numbers a and n, a modulo n (abbreviated as a mod n) is the remainder of the Euclidean division of a by n, where a is the dividend and n is the divisor. The modulo operation is to be distinguished from the symbol mod, which refers to the modulus (or divisor) one is operating from.

For example, the expression “5 mod 2” would evaluate to 1, because 5 divided by 2 has a quotient of 2 and a remainder of 1, while “9 mod 3” would evaluate to 0, because the division of 9 by 3 has a quotient of 3 and a remainder of 0; there is nothing to subtract from 9 after multiplying 3 times 3.

Q59. This is a 128 bit hash that is specified by RFC 1321. It was designed by Ron Rivest in 1991 to replace an earlier hash function.
* SHA1
* SHA-256

* RSA
* MD5
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.

Incorrect answers:

SHA1 – (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.

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.

SHA-256 – SHA-2 (Secure Hash Algorithm 2) is a set of cryptographic hash functions designed by the United States National Security Agency (NSA) and first published in 2001. They are built using the Merkle-Damgard structure, from a one-way compression function itself built using the Davies-Meyer structure from a specialized block cipher. SHA-2 includes significant changes from its predecessor, SHA-1. 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

Q60. Which of the following is a key exchange protocol?
* MQV
* AES
* DES
* RSA
MQV

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

MQV (Menezes-Qu-Vanstone) is an authenticated protocol for key agreement based on the Diffie-Hellman scheme. Like other authenticated Diffie-Hellman schemes, MQV provides protection against an active attacker. The protocol can be modified to work in an arbitrary finite group, and, in particular, elliptic curve groups, where it is known as elliptic curve MQV (ECMQV).

Incorrect answers:

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.

AES – Advanced Encryption Standard (AES), also known by its original name Rijndael, is a specification for the encryption

of electronic data established by the U.S. National Institute of Standards and Technology (NIST) in 2001.

DES – Data Encryption Standard is a symmetric-key algorithm for the encryption of digital data.

Q61. With Cipher feedback (CFB) what happens?
* The key is reapplied
* The ciphertext block is encrypted then the ciphertext produced is XOR’d back with the plaintext to produce the current ciphertext block
* The block cipher is turned into a stream cipher
* The message is divided into blocks and each block is encrypted separately. This is the most basic mode for symmetric encryption
The ciphertext block is encrypted then the ciphertext produced is XOR’d back with the plaintext to produce the current ciphertext block

https://en.wikipedia.org/wiki/Block_cipher_mode_of_operation#Cipher_feedback_(CFB) The cipher feedback (CFB) mode, a close relative of CBC, makes a block cipher into a self-synchronizing stream cipher.

Q62. John is trying to explain the basics of cryptography to a group of young, novice, security students. Which one of the following most accurately defines encryption?
* Changing a message using complex mathematics
* Applying keys to a message to conceal it
* Complex mathematics to conceal a message
* Changing a message so it can only be easily read by the intended recipient
Changing a message so it can only be easily read by the intended recipient

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

Encryption is the process of encoding information. This process converts the original representation of the information, known as plaintext, into an alternative form known as ciphertext. Ideally, only authorized parties can decipher a ciphertext back to plaintext and access the original information. Encryption does not itself prevent interference but denies the intelligible content to a would-be interceptor.

Q63. Manipulating individuals so that they will divulge confidential information, rather than by breaking in or using technical cracking techniques.
* Linear cryptanalysis
* Replay attack
* Side-channel attack
* Social engineering attack
Social engineering attack

https://en.wikipedia.org/wiki/Social_engineering_(security)

Social engineering is the psychological manipulation of people into performing actions or divulging confidential information. This differs from social engineering within the social sciences, which does not concern the divulging of confidential information. A type of confidence trick for the purpose of information gathering, fraud, or system access, it differs from a traditional “con” in that it is often one of many steps in a more complex fraud scheme.

Incorrect answers:

Replay attack – (also known as playback attack) is a form of network attack in which a valid data transmission is maliciously or fraudulently repeated or delayed. This is carried out either by the originator or by an adversary who intercepts the data and

re-transmits it, possibly as part of a masquerade attack by IP packet substitution. This is one of the lower tier versions of a “Man-in-the-middle attack.” Side-channel attack – is any attack based on information gained from the implementation of a computer system, rather than weaknesses in the implemented algorithm itself (e.g. cryptanalysis and software bugs). Timing information, power consumption, electromagnetic leaks or even sound can provide an extra source of information, which can be exploited.

Linear cryptanalysis – is a general form of cryptanalysis based on finding affine approximations to the action of a cipher. Attacks have been developed for block ciphers and stream ciphers. Linear cryptanalysis is one of the two most widely used attacks on block ciphers; the other being differential cryptanalysis.

Q64. Which of the following would be the fastest.
* EC
* DH
* RSA
* AES
AES

https://en.wikipedia.org/wiki/Symmetric-key_algorithm

AES – symmetric cipher. Symmetric keys use the same key for both encryption and decryption. Both the sender and receiver of the data must know and share the secret key. For standard encrypt/decrypt functions, symmetric algorithms generally perform much faster than their asymmetrical counterparts. This is due to the fact that asymmetric cryptography is massively inefficient. Symmetric cryptography is designed precisely for the efficient processing of large volumes of data. In other words, symmetric encryption is generally used for speed and performance, e.g. when there’s a large amount of data that needs to be encrypted/protected.

Incorrect answers:

RSA – asymmetric cipher,

DH – Diffie-Hellman key exchange is a method of securely exchanging cryptographic keys over a public channel and was one of the first public-key protocols as conceived by Ralph Merkle and named after Whitfield Diffie and Martin Hellman.

EC – Elliptic-curve cryptography (ECC) is an approach to public-key cryptography based on the algebraic structure of elliptic curves over finite fields.

Q65. During the process of encryption and decryption, what keys are shared?
* Public keys
* Public and private keys
* User passwords
* Private keys
Public keys

https://en.wikipedia.org/wiki/Public-key_cryptography

Public-key cryptography, or asymmetric cryptography, is a cryptographic system that uses pairs of keys: public keys, which may be disseminated widely, and private keys, which are known only to the owner. The generation of such keys depends on cryptographic algorithms based on mathematical problems to produce one-way functions. Effective security only requires keeping the private key private; the public key can be openly distributed without compromising security.

In such a system, any person can encrypt a message using the receiver’s public key, but that encrypted message can only be decrypted with the receiver’s private key.

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.

Alice and Bob do not need to plan anything ahead of time to communicate securely: they generate their public-private key pairs independently, and happily broadcast their public keys to the world at large. Alice can rest assured that only Bob can decrypt the message she sends because she has encrypted it with his public key.