100% Pass Guaranteed Free 212-81 Exam Dumps Dec 27, 2022 [Q42-Q57

100% Pass Guaranteed Free 212-81 Exam Dumps Dec 27, 2022
Verified & Latest 212-81 Dump Q&As with Correct Answers

NO.42 Changes to one character in the plain text affect multiple characters in the cipher text, unlike in historical algorithms where each plain text character only affect one cipher text character.
* Substitution
* Avalanche
* Confusion
* Diffusion
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.[2] 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.

Incorrect answers:

Confusion – Confusion means that each binary digit (bit) of the ciphertext should depend on several parts of the key, obscuring the connections between the two.

The property of confusion hides the relationship between the ciphertext and the key.

This property makes it difficult to find the key from the ciphertext and if a single bit in a key is changed, the calculation of the values of most or all of the bits in the ciphertext will be affected.

Confusion increases the ambiguity of ciphertext and it is used by both block and stream ciphers.

Avalanche – the desirable property of cryptographic algorithms, typically block ciphers and cryptographic hash functions, wherein if an input is changed slightly (for example, flipping a single bit), the output changes significantly (e.g., half the output bits flip). In the case of high-quality block ciphers, such a small change in either the key or the plaintext should cause a drastic change in the ciphertext.

Substitution – method of encrypting by which units of plaintext are replaced with ciphertext, according to a fixed system; the “units” may be single letters (the most common), pairs of letters, triplets of letters, mixtures of the above, and so forth. The receiver deciphers the text by performing the inverse substitution.

NO.43 What is the formula me %n related to?
* Encrypting with EC
* Decrypting with RSA
* Generating Mersenne primes
* Encrypting with RSA

Encrypting with RSA

https://en.wikipedia.org/wiki/RSA_(cryptosystem)

RSA Encrypting a message m (number) with the public key (n, e) is calculated:

M’ := me %n

Incorrect answers:

Decrypting with RSA:

M” := md %n

Generation Mersenne primes:

Mn = 2n – 1

Encrypting with Elliptic Curve (EC):

y2 = x3 + ax + b

NO.44 When learning algorithms, such as RSA, it is important to understand the mathematics being used. In RSA, the number of positive integers less than or equal to some number is critical in key generation. The number of positive integers less than or equal to n that are coprime to n is called _____.
* Mersenne’s number
* Fermat’s number
* Euler’s totient
* Fermat’s prime

Euler’s totient

https://en.wikipedia.org/wiki/Euler%27s_totient_function

In number theory, Euler’s totient function counts the positive integers up to a given integer n that are relatively prime to n.

Incorrect answers:

Fibonacci number – 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.

Fermat’s number – named after Pierre de Fermat, who first studied them, is 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, …

Mersenne prime – prime number that is one less than a power of two. That is, it is a prime number of the form Mn = 2n – 1 for some integer n. They are named after Marin Mersenne, a French Minim friar, who studied them in the early 17th century.

NO.45 Which service in a PKI will vouch for the identity of an individual or company?
* CA
* CR
* KDC
* CBC

CA

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

A certificate authority or certification authority (CA) is an entity that issues digital certificates. A digital certificate certifies the ownership of a public key by the named subject of the certificate. This allows others (relying parties) to rely upon signatures or on assertions made about the private key that corresponds to the certified public key. A CA acts as a trusted third party-trusted both by the subject (owner) of the certificate and by the party relying upon the certificate. The format of these certificates is specified by the X.509 or EMV standard.

NO.46 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?
* Finding any method that is more efficient than brute force
* Uncovering the algorithm used
* Rendering the cypher no longer useable

* Decoding the key
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 2128 encryptions; an attack requiring 2110 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.”

NO.47 Cylinder tool. Wrap leather around to decode. The diameter is the key. Used in 7th century BC by greek poet Archilochus.
* Cipher disk
* Caesar cipher
* Scytale
* Enigma machine
Scytale

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

A scytale is a tool used to perform a transposition cipher, consisting of a cylinder with a strip of parchment wound around it on which is written a message. The ancient Greeks, and the Spartans in particular, are said to have used this cipher in 7th century BC to communicate during military campaigns.

The recipient uses a rod of the same diameter on which the parchment is wrapped to read the message. It has the advantage of being fast and not prone to mistakes-a necessary property when on the battlefield. It can, however, be easily broken. Since the strip of parchment hints strongly at the method, the ciphertext would have to be transferred to something less suggestive, somewhat reducing the advantage noted.

Incorrect answers:

Cipher disk – is an enciphering and deciphering tool developed in 1470 by the Italian architect and author Leon Battista Alberti. He constructed a device, (eponymously called the Alberti cipher disk) consisting of two concentric circular plates mounted one on top of the other. The larger plate is called the “stationary” and the smaller one the “moveable” since the smaller one could move on top of the “stationary”.

Enigma machine – is an encryption device developed and used in the early- to mid-20th century to protect commercial, diplomatic and military communication. It was employed extensively by Nazi Germany during World War II, in all branches of the German military.

Caesar cipher – (also known as Caesar’s cipher, the shift cipher, Caesar’s code or Caesar shift) is one of the simplest and most widely known encryption techniques. It is a type of substitution cipher in which each letter in the plaintext is replaced by a letter some fixed number of positions down the alphabet. For example, with a left shift of 3, D would be replaced by A, E would become B, and so on. The method is named after Julius Caesar, who used it in his private correspondence.

NO.48 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.

NO.49 Bruce Schneier is a well-known and highly respected cryptographer. He has developed several pseudo random number generators as well as worked on teams developing symmetric ciphers. Which one of the following is a symmetric block cipher designed in 1993 by Bruce Schneier team that is unpatented?
* Pegasus
* Blowfish
* SHA1
* AES
Blowfish

https://en.wikipedia.org/wiki/Blowfish_(cipher)

Blowfish is a symmetric-key block cipher, designed in 1993 by Bruce Schneier and included in many cipher suites and encryption products.

NO.50 A number that is used only one time, then discarded is called what?
* IV
* Nonce
* Chain
* Salt
Nonce

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

A nonce is an arbitrary number that can be used just once in a cryptographic communication. It is similar in spirit to a nonce word, hence the name. It is often a random or pseudo-random number issued in an authentication protocol to ensure that old communications cannot be reused in replay attacks.

NO.51 Represents the total number of possible values of keys in a cryptographic algorithm or other security measure, such as a password.
* Key Schedule
* Key Clustering
* Key Space
* Key Exchange
Key Space

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

Algorithm’s key space refers to the set of all possible permutations of a key.

To prevent an adversary from using a brute-force attack to find the key used to encrypt a message, the key space is usually designed to be large enough to make such a search infeasible. On average, half the key space must be searched to find the solution.

Another desirable attribute is that the key must be selected truly randomly from all possible key permutations. Should this not be the case, and the attacker is able to determine some factor that may influence how the key was selected, the search space (and hence also the search time) can be significantly reduced. Humans do not select passwords randomly, therefore attackers frequently try a dictionary attack before a brute force attack, as this approach can often produce the correct answer in far less time than a systematic brute force search of all possible character combinations.

NO.52 A technique used to increase the security of block ciphers. It consists of steps that combine the data with portions of the key (most commonly using a simple XOR) before the first round and after the last round of encryption.
* Whitening
* Key Exchange
* Key Schedule
* Key Clustering

Whitening

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

In cryptography, key whitening is a technique intended to increase the security of an iterated block cipher. It consists of steps that combine the data with portions of the key.

The most common form of key whitening is xor-encrypt-xor — using a simple XOR before the first round and after the last round of encryption.

The first block cipher to use a form of key whitening is DES-X, which simply uses two extra 64-bit keys for whitening, beyond the normal 56-bit key of DES. This is intended to increase the complexity of a brute force attack, increasing the effective size of the key without major changes in the algorithm. DES-X’s inventor, Ron Rivest, named the technique whitening.

Incorrect answers:

Key Clustering – different encryption keys generated the same ciphertext from the same plaintext message.

Key Schedule – an algorithm for the key that calculates the subkeys for each round that the encryption goes through.

Key Exchange – a method in cryptography by which cryptographic keys are exchanged between two parties, allowing use of a cryptographic algorithm.

NO.53 What is the name of the attack where the attacker obtains the ciphertexts corresponding to a set of plaintexts of his own choosing?
* Chosen plaintext
* Differential cryptanalysis
* Known-plaintext attack
* Kasiski examination

Chosen plaintext

https://en.wikipedia.org/wiki/Chosen-plaintext_attack

A chosen-plaintext attack (CPA) is an attack model for cryptanalysis which presumes that the attacker can obtain the ciphertexts for arbitrary plaintexts. The goal of the attack is to gain information that reduces the security of the encryption scheme.

Incorrect answers:

Differential cryptanalysis – is a general form of cryptanalysis applicable primarily to block ciphers, but also to stream ciphers and cryptographic hash functions. In the broadest sense, it is the study of how differences in information input can affect the resultant difference at the output. In the case of a block cipher, it refers to a set of techniques for tracing differences through the network of transformation, discovering where the cipher exhibits non-random behavior, and exploiting such properties to recover the secret key (cryptography key).

Known-plaintext attack – (KPA) is an attack model for cryptanalysis where the attacker has access to both the plaintext (called a crib), and its encrypted version (ciphertext). These can be used to reveal further secret information such as secret keys and code books.

Kasiski examination – (also referred to as Kasiski’s test or Kasiski’s method) is a method of attacking polyalphabetic substitution ciphers, such as the Vigenere cipher. It was first published by Friedrich Kasiski in 1863, but seems to have been independently discovered by Charles Babbage as early as 1846. In polyalphabetic substitution ciphers where the substitution alphabets are chosen by the use of a keyword, the Kasiski examination allows a cryptanalyst to deduce the length of the keyword. Once the length of the keyword is discovered, the cryptanalyst lines up the ciphertext in n columns, where n is the length of the keyword. Then each column can be treated as the ciphertext of a monoalphabetic substitution cipher. As such, each column can be attacked with frequency analysis.

NO.54 The greatest weakness with symmetric algorithms is _____.
* They are less secure than asymmetric
* The problem of key exchange
* The problem of generating keys
* They are slower than asymmetric

The problem of key exchange

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

Symmetric-key algorithms are algorithms for cryptography that use the same cryptographic keys for both encryption of plaintext and decryption of ciphertext. The keys may be identical or there may be a simple transformation to go between the two keys. The keys, in practice, represent a shared secret between two or more parties that can be used to maintain a private information link. This requirement that both parties have access to the secret key is one of the main drawbacks of symmetric key encryption, in comparison to public-key encryption (also known as asymmetric key encryption).

NO.55 Which of the following techniques is used (other than brute force) to attempt to derive a key?
* Cryptography
* Cryptoanalysis
* Password cracking
* Hacking

Cryptoanalysis

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

Cryptanalysis is the study of analyzing information systems in order to study the hidden aspects of the systems. Cryptanalysis is used to breach cryptographic security systems and gain access to the contents of encrypted messages, even if the cryptographic key is unknown.

NO.56 This hash function uses 512-bit blocks and implements preset constants that change after each repetition. Each block is hashed into a 256-bit block through four branches that divides each 512 block into sixteen 32-bit words that are further encrypted and rearranged.

* SHA-256
* FORK-256
* SHA-1
* RSA

FORK-256

https://en.wikipedia.org/wiki/FORK-256

FORK-256 was introduced at the 2005 NIST Hash workshop and published the following year.[6] FORK-256 uses 512-bit blocks and implements preset constants that change after each repetition. Each block is hashed into a 256-bit block through four branches that divides each 512 block into sixteen 32-bit words that are further encrypted and rearranged.

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

NO.57 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.