Free Questions for 212-81 by certsdeals

Shared by Branch on 22-07-2024

For More Free Questions and Preparation Resources

Check the Links on Last Page

Question 1

Question Type: MultipleChoice

An attack that is particularly successful against block ciphers based on substitution-permutation networks. For a block size b, holds b-k bits constant and runs the other k through all 2k possibilities. For k=1, this is just deferential cryptanalysis, but with k>1 it is a new technique.

Options:

A- Differential Cryptanalysis

B- Linear Cryptanalysis

C- Chosen Plaintext Attack

D- Integral Cryptanalysis

Answer:

D

Explanation:

Integral Cryptanalysis

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

Integral cryptanalysis is a cryptanalytic attack that is particularly applicable to block ciphers based on substitution-permutation networks. It was originally designed by Lars Knudsen as a dedicated attack against Square, so it is commonly known as the Square attack. It was also extended to a few other ciphers related to Square: CRYPTON, Rijndael, and SHARK. Stefan Lucks generalized the attack to what he called a saturation attack and used it to attack Twofish, which is not at all similar to Square, having a radically different Feistel network structure. Forms of integral cryptanalysis have since been applied to a variety of ciphers, including Hierocrypt, IDEA, Camellia, Skipjack, MISTY1, MISTY2, SAFER++, KHAZAD, and FOX (now called IDEA NXT).

Incorrect answers:

Chosen Plaintext Attack - 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.

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.

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).

Question 2

Question Type: MultipleChoice

Uses a formula, M_n = 2^n 1 where n is a prime number, to generate primes. Works for 2, 3, 5, 7 but fails on 11 and on many other n values.

Options:

A- Fibonacci Numbers

B- Co-prime Numbers

C- Even Numbers

D- Mersenne Primes

Answer:

D

Explanation:

Correct answers: Mersenne Primes

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

Mersenne prime 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 2^n 1. Therefore, an equivalent definition of the Mersenne primes is that they are the prime numbers of the form M_p = 2^p 1 for some prime p.

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.

Co-prime Numbers - 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.

Question 3

Question Type: **MultipleChoice**

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?

Options:

A- Alice's private key

B- Bob's private key

C- Alice's public key

D- Bob's public key

Answer:

C

Explanation:

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 4

Question Type: MultipleChoice

Which of the following asymmetric algorithms is described by U.S. Patent 5,231,668 and FIPS 186

Options:

A- AES

B- RC4

C- DSA

D- RSA

Answer:

C

Explanation:

DSA

https://ru.wikipedia.org/wiki/DSA

The National Institute of Standards and Technology (NIST) proposed DSA for use in their Digital Signature Standard (DSS) in 1991, and adopted it as FIPS 186 in 1994.

DSA is covered by U.S. Patent 5,231,668 , filed July 26, 1991 and now expired, and attributed to David W. Kravitz, a former NSA employee.

Question 5

Question Type: MultipleChoice

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

Options:

A- Substitution

B- Whitening

C- Encoding

D- Decoding

Answer:

D

Explanation:

Decoding

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

Question 6

Question Type: MultipleChoice

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

Options:

A- 1

B- 4

C- 2

D- 3

Answer:

A

Explanation:

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.

Incorrect answers:

Type 2 - product refers to an NSA endorsed unclassified cryptographic equipment, assemblies or components for sensitive but unclassified U.S. government information.

Type 3 - unclassified cryptographic equipment, assembly, or component used, when appropriately keyed, for encrypting or decrypting unclassified sensitive U.S. Government or commercial information, and to protect systems requiring protection mechanisms consistent with standard commercial practices. A Type 3 Algorithm refers to NIST endorsed algorithms, registered and FIPS published, for sensitive but unclassified U.S. government and commercial information.

Type 4 - Algorithm refers to algorithms that are registered by the NIST but are not FIPS published. Unevaluated commercial cryptographic equipment, assemblies, or components that are neither NSA nor NIST certified for any Government usage.

Question 7

Question Type: MultipleChoice

The most common way steganography is accomplished is via which one of the following?

Options:

A- rsb

B- lsb

C- msb

D- asb

Answer:

B

Explanation:

lbs

https://en.wikipedia.org/wiki/Bit_numbering#:~:text=In%20computing%2C%20the%20least%20significant,number%20is%20even%20or%20odd.

The least significant bit (LSB) is the bit position in a binary integer giving the units value, that is, determining whether the number is even or odd. The LSB is sometimes referred to as the low-order bit or right-most bit, due to the convention in positional notation of writing less significant digits further to the right. It is analogous to the least significant digit of a decimal integer, which is the digit in the ones (right-most) position.

Question 8

Question Type: MultipleChoice

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.

Options:

A- Key

B- IV

C- Chain

D- Salt

Answer:

A

Explanation:

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.

Question 9

Question Type: MultipleChoice

What is an IV?

Options:

A- Random bits added to a hash

B- The key used for a cryptography algorith

C- A fixed size random stream that is added to a block cipher to increase randomeness

D- The cipher used

Answer:

C

Explanation:

A fixed size random stream that is added to a block cipher to increase randomeness

https://en.wikipedia.org/wiki/Block_cipher_mode_of_operation#Initialization_vector_(IV)

An initialization vector (IV) or starting variable (SV) is a block of bits that is used by several modes to randomize the encryption and hence to produce distinct ciphertexts even if the same plaintext is encrypted multiple times, without the need for a slower re-keying process.

Question 10

Question Type: MultipleChoice

Numbers that have no factors in common with another.

Options:

A- Fibonacci Numbers

B- Even Numbers

C- Co-prime numbers

D- Mersenne Primes

Answer:

C

Explanation:

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 2^n 1. Therefore, an equivalent definition of the Mersenne primes is that they are the prime numbers of the form M_p = 2^p 1 for some prime p.

Question 11

Question Type: MultipleChoice

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?

Options:

A- Changing a message using complex mathematics

B- Applying keys to a message to conceal it

C- Complex mathematics to conceal a message

D- Changing a message so it can only be easily read by the intended recipient

Answer:

D

Explanation:

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.