Eccouncil

212-81 Exam

Certified Encryption Specialist

Thank you for Downloading 212-81 exam PDF Demo

You can also try our 212-81 Full Version Download

https://www.certkillers.net/Exam/212-81

Version: 5.0

Question: 1

What is Kerchoff's principle?

A. A minimum of 15 rounds is needed for a Feistel cipher to be secure
B. Only the key needs to be secret, not the actual algorithm
C. Both algorithm and key should be kept secret
D. A minimum key size of 256 bits is necessary for security

Answer: B

Explanation:

Only the key needs to be secret, not the actual algorithm
https://en.wikipedia.org/wiki/Kerckhoffs%27s_principle
Kerckhoffs's principle of cryptography was stated by Netherlands born cryptographer Auguste Kerckhoffs in the 19th century: A cryptosystem should be secure even if everything about the system, except the key, is public knowledge.

Question: 2

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 _____.

A. Mersenne's number
B. Fermat's number
C. Euler's totient
D. Fermat's prime

Answer: C

Explanation:

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 = 2^2^n+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 = 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.

Question: 3

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?

A. Blowfish
B. Twofish
C. Skipjack
D. Serpent

Answer: C

Explanation:

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).

Question: 4

Which of the following is an asymmetric cipher?

A. RSA
B. AES
C. DES
D. RC4

Answer: A

Explanation:

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.

Question: 5

Juanita has been assigned the task of selecting email encryption for the staff of the insurance company she works for. The various employees often use diverse email clients. Which of the following methods is available as an add-in for most email clients?

A. Caesar cipher
B. RSA
C. PGP
D. DES

Answer: C

Explanation:

PGP
https://en.wikipedia.org/wiki/Pretty_Good_Privacy
Pretty Good Privacy (PGP) is an encryption program that provides cryptographic privacy and authentication for data communication. PGP is used for signing, encrypting, and decrypting texts, e-mails, files, directories, and whole disk partitions and to increase the security of e-mail

communications. Phil Zimmermann developed PGP in 1991.

Thank You for trying 212-81 PDF Demo

To try our 212-81 Full Version Download visit link below

https://www.certkillers.net/Exam/212-81

Start Your 212-81 Preparation

Use Coupon "**CKNET**" for Further discount on the purchase of Full Version Download. Test your 212-81 preparation with actual exam questions.