EC-COUNCIL.212-81.v2023-03-10.q76

Exam Code:	212-81
Exam Name:	Certified Encryption Specialist
Certification Provider:	EC-COUNCIL
Free Question Number:	76
Version:	v2023-03-10
# of views:	1045
# of Questions views:	760
https://www.freepdfdumps.com/EC-COUNCIL.212-81.v2023-03-10.q76.html	

NEW QUESTION: 1
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
Answer: (SHOW ANSWER)
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.

NEW QUESTION: 2
Algorithm that was chosen for the Data Encryption Standard, which was altered and renamed Data Encryption Algorithm.
A. Blowfish
B. Rijndael
C. Lucifer
D. El Gamal
Answer: (SHOW ANSWER)
Lucifer

https://en.wikipedia.org/wiki/Lucifer_(cipher)
Lucifer was a direct precursor to the Data Encryption Standard. One version, alternatively named DTD-1.

NEW QUESTION: 3
In 1977 researchers and MIT described what asymmetric algorithm?
A. DH
B. RSA
C. AES
D. EC
Answer: B (LEAVE A REPLY)
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.

NEW QUESTION: 4
Hash. Created by Ronald Rivest. Replaced MD4. 128 bit output size, 512 bit block size, 32 bit word size, 64 rounds. Infamously compromised by Flame malware in 2012.
A. Keccak
B. MD5
C. SHA-1
D. TIGER
Answer: B (LEAVE A REPLY)
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:
TIGER - hash. Created by Ross Anderson and Eli Baham. 192/160/128 bit output size, 512 bit block size, 53 bit word size, 24 rounds.
SHA-1 - Secure Hashing Algorithm. Designed by NSA. 160 bit output size, 512 bit block size, 40 bit word size, 80 rounds.
Keccak - SHA-3 (Secure Hash Algorithm 3) is the latest member of the Secure Hash Algorithm family of standards, released by NIST on August 5, 2015. SHA-3 is a subset of the broader cryptographic primitive family Keccak, designed by Guido Bertoni, Joan Daemen, Michael Peeters, and Gilles Van Assche, building upon RadioGatun.

NEW QUESTION: 5
The reverse process from encoding - converting the encoded message back into its plaintext format.
A. Substitution
B. Whitening
C. Encoding
D. Decoding
Answer: (SHOW ANSWER)
Decoding
Decoding - reverse process from encoding,converting the encoded message back into its plaintext format.

NEW QUESTION: 6
Denis is looking at an older system that uses DES encryption. A colleague has told him that DES is insecure due to a small key size. What is the key length used for DES?
A. 128
B. 256
C. 56
D. 64
Answer: C (LEAVE A REPLY)
56
https://en.wikipedia.org/wiki/DES
The Data Encryption Standard 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.

NEW QUESTION: 7
The greatest weakness with symmetric algorithms is _____.
A. They are less secure than asymmetric
B. The problem of key exchange
C. The problem of generating keys
D. They are slower than asymmetric
Answer: (SHOW ANSWER)
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).

NEW QUESTION: 8
Which of the following is assured by the use of a hash?
A. Confidentiality
B. Availability
C. Authentication
D. Integrity
Answer: D (LEAVE A REPLY)
Integrity
https://en.wikipedia.org/wiki/Cryptographic_hash_function#Verifying_the_integrity_of_messages_and_files
An important application of secure 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.

NEW QUESTION: 9
Which one of the following uses three different keys, all of the same size?
A. 3DES
B. AES
C. RSA
D. DES
Answer: (SHOW ANSWER)
3DES
https://en.wikipedia.org/wiki/Triple_DES
Triple DES (3DES or TDES), officially the Triple Data Encryption Algorithm (TDEA or Triple DEA), is a symmetric-key block cipher, which applies the DES cipher algorithm three times to each data block.

NEW QUESTION: 10
Fred is using an operating system that stores all passwords as an MD5 hash. What size is an MD5 message digest (hash)?
A. 160
B. 512
C. 256
D. 128
Answer: D (LEAVE A REPLY)
128
https://en.wikipedia.org/wiki/MD5
The MD5 message-digest algorithm is a widely used hash function producing a 128-bit hash value.

NEW QUESTION: 11

Created in 1977 by Ron Rivest, Adi Shamir, and Leonard Adleman at MIT. Most widely used public key cryptography algorithm. Based on relationships with prime numbers. This algorithm is secure because it is difficult to factor a large integer composed of two or more large prime factors.

A. PKI

B. DES

C. RSA

D. Diffie-Helmann

Answer: C (LEAVE A REPLY)

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.

Incorrect answers:

Diffie-Helmann - The first publicly described asymmetric algorithm. A cryptographic protocol that allows two parties to establish a shared key over an insecure channel. Often used to allow parties to exchange a symmetric key through some unsecure medium, such as the Internet. It was developed by Whitfield Diffie and Martin Helmann in 1976.

DES - The Data Encryption Standard 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.

Developed in the early 1970s at IBM and based on an earlier design by Horst Feistel, the algorithm was submitted to the National Bureau of Standards (NBS) following the agency's invitation to propose a candidate for the protection of sensitive, unclassified electronic government data. In 1976, after consultation with the National Security Agency (NSA), the NBS selected a slightly modified version (strengthened against differential cryptanalysis, but weakened against brute-force attacks), which was published as an official Federal Information Processing Standard (FIPS) for the United States in 1977.

PKI - A public key infrastructure is a set of roles, policies, hardware, software and procedures needed to create, manage, distribute, use, store and revoke digital certificates and manage public-key encryption. The purpose of a PKI is to facilitate the secure electronic transfer of information for a range of network activities such as e-commerce, internet banking and confidential email. It is required for activities where simple passwords are an inadequate authentication method and more rigorous proof is required to confirm the identity of the parties involved in the communication and to validate the information being transferred.

NEW QUESTION: 12

A digital document that contains a public key and some information to allow your system to verify where that key came from. Used for web servers, Cisco Secure phones, E-Commerce.

A. Registration Authority

B. Payload
C. OCSP
D. Digital Certificate
Answer: D (LEAVE A REPLY)
Digital Certificate
https://en.wikipedia.org/wiki/Public_key_certificate
A public key certificate, also known as a digital certificate or identity certificate, is an electronic document used to prove the ownership of a public key. The certificate includes information about the key, information about the identity of its owner (called the subject), and the digital signature of an entity that has verified the certificate's contents (called the issuer).
Incorrect answers:
OCSP - Provides certificate validation in real time and will let you know if it is valid or has been revoked.
Registration Authority (RA) - component of PKI that validates the identity of an entity requesting a digital certificate.
Payload - In computing and telecommunications, the payload is the part of transmitted data that is the actual intended message. Headers and metadata are sent only to enable payload delivery. In the steganography - information to be concealed and sent secretly, or the data covertly communicated;

NEW QUESTION: 13
How can rainbow tables be defeated?
A. Lockout accounts under brute force password cracking attempts
B. All uppercase character passwords
C. Use of non-dictionary words
D. Password salting
Answer: D (LEAVE A REPLY)
Password salting
https://en.wikipedia.org/wiki/Salt_(cryptography)#Benefits
Salts also combat the use of hash tables and rainbow tables for cracking passwords. A hash table is a large list of pre-computed hashes for commonly used passwords. For a password file without salts, an attacker can go through each entry and look up the hashed password in the hash table or rainbow table. If the look-up is considerably faster than the hash function (which it often is), this will considerably speed up cracking the file. However, if the password file is salted, then the hash table or rainbow table would have to contain "salt . password" pre-hashed. If the salt is long enough and sufficiently random, this is very unlikely. Unsalted passwords chosen by humans tend to be vulnerable to dictionary attacks since they have to be both short and meaningful enough to be memorized. Even a small dictionary (or its hashed equivalent, a hash table) is significant help cracking the most commonly used passwords. Since salts do not have to be memorized by humans they can make the size of the rainbow table required for a successful attack prohibitively large without placing a burden on the users.

NEW QUESTION: 14

Changing some part of the plain text for some matching part of cipher text. Historical algorithms typically use this.

A. Decoding

B. Substitution

C. Transposition

D. Collision

Answer: B (LEAVE A REPLY)

Substitution

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

In cryptography, a substitution cipher is a 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.

Incorrect answers:

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

Collision - occurs when a hash function generates the same output for different inputs.

Transposition - a method of encryption by which the positions held by units of plaintext (which are commonly characters or groups of characters) are shifted according to a regular system, so that the ciphertext constitutes a permutation of the plaintext. That is, the order of the units is changed (the plaintext is reordered). Mathematically a bijective function is used on the characters' positions to encrypt and an inverse function to decrypt.

NEW QUESTION: 15

Which of the following was a multi alphabet cipher widely used from the 16th century to the early 20th century?

A. Atbash

B. Caesar

C. Scytale

D. Vigenere

Answer: D (LEAVE A REPLY)

Vigenere

https://en.wikipedia.org/wiki/Vigen%C3%A8re_cipher

The Vigenere cipher is a 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.

First described by Giovan Battista Bellaso in 1553, the cipher is easy to understand and implement, but it resisted all attempts to break it until 1863, three centuries later. This earned it the description le chiffre indechiffrable (French for 'the indecipherable cipher'). Many people have tried to implement encryption schemes that are essentially Vigenere ciphers. In 1863, Friedrich Kasiski was the first to publish a general method of deciphering Vigenere ciphers.

Incorrect answers:

Caesar - 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.
Atbash - Single substitution monoalphabetic cipher that substitutes each letter with its reverse (a and z, b and y, etc).
Scytale - Transposition cipher. A staff with papyrus or letter wrapped around it so edges would line up. There would be a stream of characters which would show you your message. When unwound it would be a random string of characters. Would need an identical size staff on other end for other individuals to decode message.

NEW QUESTION: 16
A _____ refers to a situation where two different inputs yield the same output.
A. Convergence
B. Collision
C. Transposition
D. Substitution
Answer: B (LEAVE A REPLY)
Collision
https://en.wikipedia.org/wiki/Collision_(computer_science)
A collision or clash is a situation that occurs when two distinct pieces of data have the same hash value, checksum, fingerprint, or cryptographic digest.

NEW QUESTION: 17
A _____ is a function is not reversible.
A. Stream cipher
B. Asymmetric cipher
C. Hash
D. Block Cipher
Answer: C (LEAVE A REPLY)
Hash
https://en.wikipedia.org/wiki/Hash_function
Hash functions are irreversible. This is actually required for them to fulfill their function of determining whether someone possesses an uncorrupted copy of the hashed data. This brings susceptibility to brute force attacks, which are quite powerful these days, particularly against MD5.

NEW QUESTION: 18
Which of the following is the standard for digital certificates?
A. 509
https://en.wikipedia.org/wiki/X.509
B. CRL
C. 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.
D. X.509
E. CA
F. RFC 2298
Answer: (SHOW ANSWER)

NEW QUESTION: 19
A non-secret binary vector used as the initializing input algorithm for encryption of a plaintext block sequence to increase security by introducing additional cryptographic variance.
A. IV
B. Salt
C. L2TP
D. Nonce
Answer: A (LEAVE A REPLY)
IV
https://en.wikipedia.org/wiki/Initialization_vector
In cryptography, an initialization vector (IV) or starting variable (SV) is a fixed-size input to a cryptographic primitive that is typically required to be random or pseudorandom. Randomization is crucial for encryption schemes to achieve semantic security, a property whereby repeated usage of the scheme under the same key does not allow an attacker to infer relationships between segments of the encrypted message. For block ciphers, the use of an IV is described by the modes of operation. Randomization is also required for other primitives, such as universal hash functions and message authentication codes based thereon.
Incorrect answers:
L2TP - PPTP combined with L2F (Layer 2 Forwarding) (Cisco proprietary protocol) - Uses EAP, CHAP, MS-CHAP, PAP, or S-PAP for authentication. IPSec is used to provide encryption.
Salt - random bits of data intermixed with the message that is to be hashed.

Nonce - 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. They can also be useful as initialization vectors and in cryptographic hash functions.

NEW QUESTION: 20
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.
A. Whitening
B. Key Exchange
C. Key Schedule
D. Key Clustering
Answer: A (LEAVE A REPLY)
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.

NEW QUESTION: 21
WPA2 uses AES for wireless data encryption at which of the following encryption levels?
A. 128 bit and CRC
B. 128 bi and TKIP
C. 128 bit and CCMP
D. 64 bit and CCMP
Answer: (SHOW ANSWER)
128 bit and CCMP

Counter Mode with Cipher Block Chaining Message Authentication Code Protocol (CCMP) is an encryption protocol that forms part of the 802.11i standard for wireless local area networks (WLANs), particularly those using WiMax technology. CCMP employs 128-bit keys and a 48-bit initialization vector that minimizes vulnerability to replay attacks.

NEW QUESTION: 22
Which of the following equations is related to EC?
A. P = Cd%n
B. Me%n
C. y^2 = x^3 + Ax + B
D. Let m = (p-1)(q-1)
Answer: C (LEAVE A REPLY)
y^2 = x^3 + Ax + B
https://en.wikipedia.org/wiki/Elliptic-curve_cryptography
For current cryptographic purposes, an elliptic curve is a plane curve over a finite field (rather than the real numbers) which consists of the points satisfying the equation:

NEW QUESTION: 23
If you XOR 10111000 with 10101010, what is the result?
A. 10111010
B. 10101010
C. 11101101
D. 00010010
Answer: (SHOW ANSWER)
00010010
https://en.wikipedia.org/wiki/XOR_cipher
1 0 1 1 1 0 0 0
1 0 1 0 1 0 1 0

_____
0 0 0 1 0 0 1 0

NEW QUESTION: 24
Which of the following uses an 80 bit key on 64 bit blocks?
A. Skipjack
B. Twofish
C. DES
D. AES
Answer: A (LEAVE A REPLY)
Skipjack
https://en.wikipedia.org/wiki/Skipjack_(cipher)

Skipjack uses an 80-bit key to encrypt or decrypt 64-bit data blocks. It is an unbalanced Feistel network with 32 rounds.
Incorrect answers:
Twofish - is a symmetric key block cipher with a block size of 128 bits and key sizes up to 256 bits. It was one of the five finalists of the Advanced Encryption Standard contest, but it was not selected for standardization. Twofish is related to the earlier block cipher Blowfish.
AES - 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.
DES - Data Encryption Standard 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.

NEW QUESTION: 25
Which of the following is an asymmetric algorithm that was first publically described in 1977?
A. Elliptic Curve
B. Twofish
C. DESX
D. RSA
Answer: (SHOW ANSWER)
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.
Incorrect answers:
Elliptic Curve - Elliptic-curve cryptography (ECC) is an approach to public-key cryptography based on the algebraic structure of elliptic curves over finite fields. ECC allows smaller keys compared to non-EC cryptography (based on plain Galois fields) to provide equivalent security.
Twofish - is a symmetric key block cipher with a block size of 128 bits and key sizes up to 256 bits. It was one of the five finalists of the Advanced Encryption Standard contest, but it was not selected for standardization. Twofish is related to the earlier block cipher Blowfish.
DESX - is a variant on the DES (Data Encryption Standard) symmetric-key block cipher intended to increase the complexity of a brute-force attack using a technique called key whitening.

NEW QUESTION: 26
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 (LEAVE A REPLY)

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.

NEW QUESTION: 27
Ciphers that write message letters out diagonally over a number of rows then read off cipher row by row. Also called zig-zag cipher.
A. Rail Fence Cipher
B. Null Cipher
C. Vigenere Cipher
D. ROT-13
Answer: A (LEAVE A REPLY)
Rail Fence Cipher
https://en.wikipedia.org/wiki/Rail_fence_cipher
The rail fence cipher (also called a zigzag cipher) is a form of transposition cipher. It derives its name from the way in which it is encoded.
Incorrect answers:
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.
Vigenere cipher - is a 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.
ROT13 - ("rotate by 13 places", sometimes hyphenated ROT-13) is a simple letter substitution cipher that replaces a letter with the 13th letter after it, in the alphabet. ROT13 is a special case of the Caesar cipher which was developed in ancient Rome.

NEW QUESTION: 28
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 (LEAVE A REPLY)
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).

NEW QUESTION: 29
A protocol for key aggreement based on Diffie-Hellman. Created in 1995. Incorporated into the public key standard IEEE P1363.
A. Blum Blum Shub
B. Elliptic Curve
C. Menezes-Qu-Vanstone
D. Euler's totient
Answer: C (LEAVE A REPLY)
Menezes-Qu-Vanstone
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).
MQV was initially proposed by Alfred Menezes, Minghua Qu and Scott Vanstone in 1995. It was modified with Law and Solinas in 1998.
Incorrect answers:
Elliptic Curve - an approach to public-key cryptography based on the algebraic structure of elliptic curves over finite fields. ECC allows smaller keys compared to non-EC cryptography (based on plain Galois fields) to provide equivalent security.
Euler's totient - function counts the positive integers up to a given integer n that are relatively prime to n.
Blum Blum Shub - a pseudorandom number generator proposed in 1986 by Lenore Blum, Manuel Blum and Michael Shub that is derived from Michael
O. Rabin's one-way function.

NEW QUESTION: 30
Asymmetric encryption method developed in 1984. It is used in PGP implementations and GNU Privacy Guard Software. Consists of 3 parts: key generator, encryption algorithm, and decryption algorithm.

A. Tiger
B. GOST
C. RIPEMD
D. ElGamal
Answer: D (LEAVE A REPLY)
ElGamal
https://en.wikipedia.org/wiki/ElGamal_encryption
the ElGamal encryption system is an asymmetric key encryption algorithm for public-key cryptography which is based on the Diffie-Hellman key exchange. It was described by Taher Elgamal in 1985. ElGamal encryption is used in the free GNU Privacy Guard software, recent versions of PGP, and other cryptosystems. The Digital Signature Algorithm (DSA) is a variant of the ElGamal signature scheme, which should not be confused with ElGamal encryption.
Incorrect answers:
Tiger - is a cryptographic hash function designed by Ross Anderson and Eli Biham in 1995 for efficiency on 64-bit platforms. The size of a Tiger hash value is 192 bits. Truncated versions (known as Tiger/128 and Tiger/160) can be used for compatibility with protocols assuming a particular hash size. Unlike the SHA-2 family, no distinguishing initialization values are defined; they are simply prefixes of the full Tiger/192 hash value.
GOST - hash function, defined in the standards GOST R 34.11-94 and GOST 34.311-95 is a 256-bit cryptographic hash function. It was initially defined in the Russian national standard GOST R 34.11-94 Information Technology - Cryptographic Information Security - Hash Function. The equivalent standard used by other member-states of the CIS is GOST 34.311-95.
RIPEMD - is a family of cryptographic hash functions developed in 1992 (the original RIPEMD) and 1996 (other variants). There are five functions in the family: RIPEMD, RIPEMD-128, RIPEMD-160, RIPEMD-256, and RIPEMD-320, of which RIPEMD-160 is the most common.

NEW QUESTION: 31
Which of the following is an asymmetric algorithm related to the equation y^2 = x^3 + Ax + B?
A. Blowfish
B. Elliptic Curve
C. AES
D. RSA
Answer: (SHOW ANSWER)
Elliptic Curve
https://en.wikipedia.org/wiki/Elliptic-curve_cryptography
For current cryptographic purposes, an elliptic curve is a plane curve over a finite field (rather than the real numbers) which consists of the points satisfying the equation:

NEW QUESTION: 32
A 160-bit hash algorithm developed by Hans Dobbertin, Antoon Bosselaers, and Bart Preneel for which there are 128, 256 and 320-bit versions is called what?
A. SHA1
B. MD5
C. FORK
D. RIPEMD
Answer: D (LEAVE A REPLY)
RIPEMD
https://en.wikipedia.org/wiki/RIPEMD
RIPEMD (RIPE Message Digest) is a family of cryptographic hash functions developed in 1992 (the original RIPEMD) and 1996 (other variants). There are five functions in the family: RIPEMD, RIPEMD-128, RIPEMD-160, RIPEMD-256, and RIPEMD-320, of which RIPEMD-160 is the most common.
The original RIPEMD, as well as RIPEMD-128, is not considered secure because 128-bit result is too small and also (for the original RIPEMD) because of design weaknesses. The 256- and 320-bit versions of RIPEMD provide the same level of security as RIPEMD-128 and RIPEMD-160, respectively; they are designed for applications where the security level is sufficient but longer hash result is necessary.

NEW QUESTION: 33
Created by D. H. Lehmer. It is a classic example of a Linear congruential generator. A PRNG type of linear congruential generator (LCG) that operates in multiplicative group of integers modulo n. The basic algorithm is $X_{i+1}=(aX_i + c) \bmod m$, with $0 \le X_i \le m$.
A. Lehmer Random Number Generator
B. Lagged Fibonacci Generator
C. Linear Congruential Generator
D. Blum Blum Shub
Answer: A (LEAVE A REPLY)
Lehmer Random Number Generator
https://en.wikipedia.org/wiki/Lehmer_random_number_generator
The Lehmer random number generator (named after D. H. Lehmer), sometimes also referred to as the Park-Miller random number generator (after Stephen K. Park and Keith W. Miller), is a type of linear congruential generator (LCG) that operates in multiplicative group of integers modulo n. The general formula is:

where the modulus m is a prime number or a power of a prime number, the multiplier a is an element of high multiplicative order modulo m (e.g., a primitive root modulo n), and the seed X0 is coprime to m. Other names are multiplicative linear congruential generator (MLCG) and multiplicative congruential generator (MCG).

NEW QUESTION: 34
Protocol suite provides a method of setting up a secure channel for protected data exchange between two devices.
A. CLR
B. OCSP
C. TLS
D. IPSec
Answer: D (LEAVE A REPLY)
IPSec
https://en.wikipedia.org/wiki/IPsec
Internet Protocol Security (IPsec) is a secure network protocol suite that authenticates and encrypts the packets of data to provide secure encrypted communication between two computers over an Internet Protocol network. It is used in virtual private networks (VPNs).
Incorrect answers:
OCSP - Online Certificate Status Protocol (OCSP) is an Internet protocol used for obtaining the revocation status of an X.509 digital certificate.
CRL - is a list of digital certificates that have been revoked by the issuing certificate authority (CA) before their scheduled expiration date and should no longer be trusted.
TLS - Transport Layer Security, 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.

NEW QUESTION: 35
What is the basis for the difficulty in breaking RSA?
A. Hashing
B. The birthday paradox
C. Equations that describe an elliptic curve
D. Factoring numbers
Answer: (SHOW ANSWER)
Factoring numbers
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.

NEW QUESTION: 36
MD5 can best be described as which one of the following?
A. Asymmetric algorithm
B. Hashing algorithm
C. Digital signature
D. Symmetric algorithm
Answer: B (LEAVE A REPLY)
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.

NEW QUESTION: 37
A cryptanalysis success where the attacker discovers additional plain texts (or cipher texts) not previously known.
A. Total Break
B. Distinguishing Algorithm
C. Instance Deduction
D. Information Deduction
Answer: C (LEAVE A REPLY)
Instance Deduction
https://en.wikipedia.org/wiki/Cryptanalysis
The results of cryptanalysis can also vary in usefulness. For example, cryptographer Lars Knudsen (1998) classified various types of attack on block ciphers according to the amount and quality of secret information that was discovered:
Total break - the attacker deduces the secret key.
Global deduction - the attacker discovers a functionally equivalent algorithm for encryption and decryption, but without learning the key.
Instance (local) deduction - the attacker discovers additional plaintexts (or ciphertexts) not previously known.

Information deduction - the attacker gains some Shannon information about plaintexts (or ciphertexts) not previously known.
Distinguishing algorithm - the attacker can distinguish the cipher from a random permutation.

NEW QUESTION: 38
John is responsible for VPNs at his company. He is using IPSec because it has two different modes. He can choose the mode appropriate for a given situation. What are the two modes of IPSec? (Choose two)
A. Encrypt mode
B. Transport mode
C. Tunnel mode
D. Decrypt mode
Answer: B,C (LEAVE A REPLY)
Correct answers: Transport mode and Tunnel mode
https://en.wikipedia.org/wiki/IPsec#Modes_of_operation
The IPsec protocols AH and ESP can be implemented in a host-to-host transport mode, as well as in a network tunneling mode.

NEW QUESTION: 39
Which analysis type is based on the statistics of the numbers of unique colors and close-color pairs in a 24-bit image, a method that analyzes the pairs of colors created by LSB embedding?
A. Differential Analysis
B. Discrete Cosine Transform
C. Raw Quick Pair
D. Chi squared analysis
Answer: (SHOW ANSWER)
Raw Quick Pair
https://www.cs.auckland.ac.nz/courses/compsci725s2c/archive/termpapers/yy.pdf Du and Long2 (2000) introduced Raw Quick Pairs detecting method of Stego-images (the images that contain the steganographic message). The underlying principle of the method is that the number of close color pairs of Stego-images will be larger compare with the number of close color pairs of normal images. In contrast, Fridrich and Goljan (2001) pointed out that RQP method only works if the number of unique colors is relatively low; and the method can not be applied to grayscale images. However, this paper will outline the core principle of RQP method; and evaluate such critical comments in details. In addition, this paper suggests potential improvement of RQP method and provides one possible alternative.
Incorrect answers:
Chi squared analysis - https://en.wikipedia.org/wiki/Chi-squared_test
Differential Analysis - https://en.wikipedia.org/wiki/Differential_cryptanalysis Discrete Cosine Transform - https://en.wikipedia.org/wiki/Discrete_cosine_transform

NEW QUESTION: 40
A _____ is a function that takes a variable-size input m and returns a fixed-size string.

A. Feistel
B. Asymmetric cipher
C. Symmetric cipher
D. Hash
Answer: D (LEAVE A REPLY)
Hash
https://en.wikipedia.org/wiki/Hash_function
A hash function is any function that can be used to map data of arbitrary size to fixed-size values.

NEW QUESTION: 41
DES has a key space of what?
A. 2^128
B. 2^192
C. 2^64
D. 2^56
Answer: D (LEAVE A REPLY)
2^56
https://en.wikipedia.org/wiki/Data_Encryption_Standard
The Data Encryption Standard (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.

NEW QUESTION: 42
Bob's password is hashed, and so is John's. Even though they used different passwords, the hash is the same. What is this called?
A. A collision
B. A mistake
C. Convergence
D. Transposition
Answer: (SHOW ANSWER)
A collision
https://en.wikipedia.org/wiki/Collision_(computer_science)
A collision or clash is a situation that occurs when two distinct pieces of data have the same hash value, checksum, fingerprint, or cryptographic digest.

NEW QUESTION: 43
Which algorithm was U. S. Patent 5,231,668, filed on july 26, 1991, attributed to David W. Kravitz, and adopted by the U. S. government in 1993 with FIPS 186?
A. DSA
B. AES
C. RC4

D. RSA

Answer: A (LEAVE A REPLY)

DSA

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

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. This patent was given to "The United States of America as represented by the Secretary of Commerce, Washington, D.C.", and NIST has made this patent available worldwide royalty-free. Claus

P. Schnorr claims that his U.S. Patent 4,995,082 (also now expired) covered DSA; this claim is disputed.

NEW QUESTION: 44

Which one of the following attempts to hide data in plain view?

A. Cryptography

B. Substitution

C. Steganography

D. Asymmetric cryptography

Answer: C (LEAVE A REPLY)

Steganography

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

Steganography is the practice of concealing a file, message, image, or video within another file, message, image, or video. The word steganography comes from Greek steganographia, which combines the words steganos , meaning "covered or concealed", and -graphia meaning "writing".

NEW QUESTION: 45

Manipulating individuals so that they will divulge confidential information, rather than by breaking in or using technical cracking techniques.

A. Linear cryptanalysis

B. Replay attack

C. Side-channel attack

D. Social engineering attack

Answer: D (LEAVE A REPLY)

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.

NEW QUESTION: 46
In 2007, this wireless security algorithm was rendered useless by capturing packets and discovering the passkey in a matter of seconds. This security flaw led to a network invasion of TJ Maxx and data theft through a technique known as wardriving.
Which Algorithm is this referring to?
A. Wired Equivalent Privacy (WEP)
B. Wi-Fi Protected Access 2 (WPA2)
C. Wi-Fi Protected Access (WPA)
D. Temporal Key Integrity Protocol (TKIP)
Answer: (SHOW ANSWER)
Wired Equivalent Privacy (WEP)
https://en.wikipedia.org/wiki/Wired_Equivalent_Privacy#Weak_security
In 2007, Erik Tews, Andrei Pychkine, and Ralf-Philipp Weinmann were able to extend Klein's 2005 attack and optimize it for usage against WEP. With the new attack it is possible to recover a 104-bit WEP key with probability 50% using only 40,000 captured packets. For 60,000 available data packets, the success probability is about 80% and for 85,000 data packets about 95%. Using active techniques like deauth and ARP re-injection, 40,000 packets can be captured in less than one minute under good conditions. The actual computation takes about 3 seconds and 3 MB of main memory on a Pentium-M 1.7 GHz and can additionally be optimized for devices with slower CPUs. The same attack can be used for 40-bit keys with an even higher success probability.

NEW QUESTION: 47

Which service in a PKI will vouch for the identity of an individual or company?
A. CA
B. CR
C. KDC
D. CBC
Answer: A (LEAVE A REPLY)
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.

NEW QUESTION: 48
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?
A. Pegasus
B. Blowfish
C. SHA1
D. AES
Answer: A (LEAVE A REPLY)
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.

NEW QUESTION: 49
What size key does Skipjack use?
A. 56 bit
B. 256 bit
C. 128 bit
D. 80 bit
Answer: (SHOW ANSWER)

NEW QUESTION: 50
How did the ATBASH cipher work?
A. By substituting each letter for the letter from the opposite end of the alphabet (i.e. A becomes Z, B becomes Y, etc.)

B. By rotating text a given number of spaces
C. By Multi alphabet substitution
D. By shifting each letter a certain number of spaces
Answer: A (LEAVE A REPLY)
By substituting each letter for the letter from the opposite end of the alphabet (i.e. A becomes Z, B becomes Y, etc.)
https://en.wikipedia.org/wiki/Atbash
The Atbash cipher is a particular type of monoalphabetic cipher formed by taking the alphabet (or abjad, syllabary, etc.) and mapping it to its reverse, so that the first letter becomes the last letter, the second letter becomes the second to last letter, and so on.

NEW QUESTION: 51
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
E. 509
Answer: D (LEAVE A REPLY)
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.
Incorrect answers:
RSA - (Rivest-Shamir-Adleman) is a public-key cryptosystem that is widely used for secure data transmission.
ElGamal - asymmetric key encryption algorithm for public-key cryptography which is based on the Diffie-Hellman key exchange. It was described by Taher Elgamal in 1985.
PAP - used to authenticate users, but is no longer used because the information was sent in cleartext.

NEW QUESTION: 52
Represents the total number of possible values of keys in a cryptographic algorithm or other security measure, such as a password.

A. Key Schedule
B. Key Clustering
C. Key Space
D. Key Exchange
Answer: (SHOW ANSWER)
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.

NEW QUESTION: 53
Used to take the burden off of a CA by handling verification prior to certificates being issued. Acts as a proxy between user and CA.
Receives request, authenticates it and forwards it to the CA.
A. PKI (Public Key Infrastructure)
B. TTP (Trusted Third Party)
C. RA (Registration Authority)
D. CP (Certificate Policy)
Answer: C (LEAVE A REPLY)
RA (Registration Authority)
https://en.wikipedia.org/wiki/Registration_authority
Registration authorities exist for many standards organizations, such as ANNA (Association of National Numbering Agencies for ISIN), the Object Management Group, W3C, IEEE and others. In general, registration authorities all perform a similar function, in promoting the use of a particular standard through facilitating its use. This may be by applying the standard, where appropriate, or by verifying that a particular application satisfies the standard's tenants. Maintenance agencies, in contrast, may change an element in a standard based on set rules - such as the creation or change of a currency code when a currency is created or revalued (i.e. TRL to TRY for Turkish lira). The Object Management Group has an additional concept of certified provider, which is deemed an entity permitted to perform some functions on behalf of the registration authority, under specific processes and procedures documented within the standard for such a role.
Incorrect answers:

TTP (Trusted Third Party) - is an entity which facilitates interactions between two parties who both trust the third party; the Third Party reviews all critical transaction communications between the parties, based on the ease of creating fraudulent digital content. In TTP models, the relying parties use this trust to secure their own interactions. TTPs are common in any number of commercial transactions and in cryptographic digital transactions as well as cryptographic protocols, for example, a certificate authority (CA) would issue a digital identity certificate to one of the two parties in the next example. The CA then becomes the Trusted-Third-Party to that certificates issuance. Likewise transactions that need a third party recordation would also need a third-party repository service of some kind or another.
CP (Certificate Policy) - is a document which aims to state what are the different entities of a public key infrastructure (PKI), their roles and their duties. This document is published in the PKI perimeter.
When in use with X.509 certificates, a specific field can be set to include a link to the associated certificate policy. Thus, during an exchange, any relying party has an access to the assurance level associated with the certificate, and can decide on the level of trust to put in the certificate.
PKI (Public Key Infrastructure) - is a set of roles, policies, hardware, software and procedures needed to create, manage, distribute, use, store and revoke digital certificates and manage public-key encryption. The purpose of a PKI is to facilitate the secure electronic transfer of information for a range of network activities such as e-commerce, internet banking and confidential email. It is required for activities where simple passwords are an inadequate authentication method and more rigorous proof is required to confirm the identity of the parties involved in the communication and to validate the information being transferred.

NEW QUESTION: 54
If you use substitution alone, what weakness is present in the resulting cipher text?
A. It is the same length as the original text
B. It is easily broken with modern computers
C. It maintains letter and word frequency
D. It is too simple
Answer: (SHOW ANSWER)
It maintains letter and word frequency
https://en.wikipedia.org/wiki/Frequency_analysis
Frequency analysis (also known as counting letters) is the study of the frequency of letters or groups of letters in a ciphertext. The method is used as an aid to breaking classical ciphers.
Frequency analysis is based on the fact that, in any given stretch of written language, certain letters and combinations of letters occur with varying frequencies. Moreover, there is a characteristic distribution of letters that is roughly the same for almost all samples of that language. For instance, given a section of English language, E, T, A and O are the most common, while Z, Q, X and J are rare. Likewise, TH, ER, ON, and AN are the most common pairs of letters (termed bigrams or digraphs), and SS, EE, TT, and FF are the most common repeats. The nonsense phrase "ETAOIN SHRDLU" represents the 12 most frequent letters in typical English language text.
In some ciphers, such properties of the natural language plaintext are preserved in the ciphertext, and these patterns have the potential to be exploited in a ciphertext-only attack.

NEW QUESTION: 55
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?
A. CRL
B. RFC 2298
C. 509
https://en.wikipedia.org/wiki/X.509
D. CA
E. 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.
F. X.509
Answer: F (LEAVE A REPLY)

NEW QUESTION: 56
A cipher is defined as what
A. The algorithm(s) needed to encrypt and decrypt a message
B. Encrypted text
C. The key used to encrypt a message
D. Any algorithm used in cryptography
Answer: A (LEAVE A REPLY)
The algorithm(s) needed to encrypt and decrypt a message
https://en.wikipedia.org/wiki/Cipher
In cryptography, a cipher (or cypher) is an algorithm for performing encryption or decryption-a series of well-defined steps that can be followed as a procedure. An alternative, less common term is encipherment. To encipher or encode is to convert information into cipher or code. In common parlance, "cipher" is synonymous with "code", as they are both a set of steps that encrypt a message; however, the concepts are distinct in cryptography, especially classical cryptography.

NEW QUESTION: 57
During the process of encryption and decryption, what keys are shared?
A. Public keys
B. Public and private keys
C. User passwords

D. Private keys

Answer: A (LEAVE A REPLY)

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.

NEW QUESTION: 58

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

Answer: A (LEAVE A REPLY)

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.
Incorrect answers:
SPAP - Shiva Password Authentication Protocol, PAP with encryption for the usernames/passwords that are transmitted.
CHAP - calculates a hash, shares the hash with the client system, the hash is periodically validated to ensure nothing has changed.
Kerberos - computer-network authentication protocol that works on the basis of tickets to allow nodes communicating over a non-secure network to prove their identity to one another in a secure manner. Its designers aimed it primarily at a client-server model and it provides mutual authentication-both the user and the server verify each other's identity. Kerberos protocol messages are protected against eavesdropping and replay attacks.
Kerberos builds on symmetric key cryptography and requires a trusted third party, and optionally may use public-key cryptography during certain phases of authentication.

NEW QUESTION: 59
Which method of password cracking takes the most time and effort?
A. Dictionary attack
B. Shoulder surfing
C. Brute force
D. Rainbow tables
Answer: C (LEAVE A REPLY)
Brute force
https://en.wikipedia.org/wiki/Brute-force_attack
A brute-force attack consists of an attacker submitting many passwords or passphrases with the hope of eventually guessing correctly. The attacker systematically checks all possible passwords and passphrases until the correct one is found. Alternatively, the attacker can attempt to guess the key which is typically created from the password using a key derivation function. This is known as an exhaustive key search.
A brute-force attack is a cryptanalytic attack that can, in theory, be used to attempt to decrypt any encrypted data (except for data encrypted in an information-theoretically secure manner). Such an attack might be used when it is not possible to take advantage of other weaknesses in an encryption system (if any exist) that would make the task easier.
Incorrect answers:
Rainbow tables - is a precomputed table for caching the output of cryptographic hash functions, usually for cracking password hashes. Tables are usually used in recovering a key derivation function (or credit card numbers, etc.) up to a certain length consisting of a limited set of characters.
Dictionary attack - is a form of brute force attack technique for defeating a cipher or authentication mechanism by trying to determine its decryption key or passphrase by trying thousands or millions of likely possibilities, such as words in a dictionary or previously used passwords, often from lists obtained from past security breaches.

Shoulder surfing - is a type of social engineering technique used to obtain information such as personal identification numbers (PINs), passwords and other confidential data by looking over the victim's shoulder, either from keystrokes on a device or sensitive information being spoken and heard, also known as eavesdropping.

NEW QUESTION: 60
What must occur in order for a cipher to be considered 'broken'?
A. Uncovering the algorithm used
B. Decoding the key
C. Finding any method that is more efficient than brute force
D. Rendering the cipher no longer useable
Answer: C (LEAVE A REPLY)
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."

NEW QUESTION: 61
Electromechanical rotor-based cipher used in World War II
A. ROT13 Cipher
B. Cipher Disk
C. Enigma Machine
D. Rail Fence Cipher
Answer: C (LEAVE A REPLY)
Enigma Machine
https://en.wikipedia.org/wiki/Enigma_machine
The 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.
Enigma has an electromechanical rotor mechanism that scrambles the 26 letters of the alphabet.
Incorrect answers:
Rail Fence Cipher - a form of transposition cipher. In the rail fence cipher, the plain text is written downwards and diagonally on successive "rails" of an imaginary fence, then moving up when the bottom rail is reached. When the top rail is reached, the message is written downwards again until the whole plaintext is written out. The message is then read off in rows.
Cipher Disk - 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". The first incarnation of the disk had plates made of copper and featured the alphabet, in order, inscribed on the

outer edge of each disk in cells split evenly along the circumference of the circle. This enabled the two alphabets to move relative to each other creating an easy to use key. Rather than using an impractical and complicated table indicating the encryption method, one could use the much simpler cipher disk. This made both encryption and decryption faster, simpler and less prone to error.
ROT13 Cipher - ("rotate by 13 places", sometimes hyphenated ROT-13) is a simple letter substitution cipher that replaces a letter with the 13th letter after it, in the alphabet. ROT13 is a special case of the Caesar cipher which was developed in ancient Rome.

NEW QUESTION: 62
Which one of the following best describes a process that splits the block of plaintext into two separate blocks, then applies the round function to one half, and finally swaps the two halves?
A. Block ciphers
B. Symmetric cryptography
C. Feistel cipher
D. Substitution cipher
Answer: (SHOW ANSWER)
Correct answer:
https://en.wikipedia.org/wiki/Feistel_cipher
Feistel cipher (also known as Luby-Rackoff block cipher) is a symmetric structure used in the construction of block ciphers, named after the German-born physicist and cryptographer Horst Feistel who did pioneering research while working for IBM (USA); it is also commonly known as a Feistel network. A large proportion of block ciphers use the scheme, including the US Data Encryption Standard, the Soviet-developed GOST and the more recent Blowfish and Twofish ciphers. In a Feistel cipher, encryption and decryption are very similar operations, and both consist of iteratively running a function called a "round function" a fixed number of times.
Incorrect answers:
Symmetric cryptography - 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.
Substitution cipher - is a 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.

Block ciphers - block cipher is a deterministic algorithm operating on fixed-length groups of bits, called blocks. It uses an unvarying transformation, that is, it uses a symmetric key. They are specified elementary components in the design of many cryptographic protocols and are widely used to implement the encryption of large amounts of data, including data exchange protocols.

NEW QUESTION: 63
In steganography, _____ is the data to be covertly communicated (in other words, it is the message you wish to hide).
A. Carrier
B. Signal
C. Payload
D. Channel
Answer: C (LEAVE A REPLY)
Payload
https://en.wikipedia.org/wiki/Steganography
The payload is the data covertly communicated. The carrier is the signal, stream, or data file that hides the payload, which differs from the channel, which typically means the type of input, such as a JPEG image. The resulting signal, stream, or data file with the encoded payload is sometimes called the package, stego file, or covert message. The proportion of bytes, samples, or other signal elements modified to encode the payload is called the encoding density and is typically expressed as a number between 0 and 1.

NEW QUESTION: 64
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?
A. Finding any method that is more efficient than brute force
B. Uncovering the algorithm used
C. Rendering the cypher no longer useable
D. Decoding the key
Answer: A (LEAVE A REPLY)
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 2^128 encryptions; an attack requiring 2^110 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."

NEW QUESTION: 65
Modern symmetric ciphers all make use of one or more s-boxes. Both Feistel and non-Feistel ciphers use these s-boxes. What is an s-box?

A. A substitution box where input bits are replaced
B. A black box for the algorithm implementation
C. A shifting box where input bits are shifted
D. Another name for the round function
Answer: A (LEAVE A REPLY)
Substitution box where input bits are replaced
https://en.wikipedia.org/wiki/S-box
In cryptography, an S-box (substitution-box) is a basic component of symmetric key algorithms which performs substitution. In block ciphers, they are typically used to obscure the relationship between the key and the ciphertext - Shannon's property of confusion.

NEW QUESTION: 66
What does Output feedback (OFB) do:
A. The message is divided into blocks and each block is encrypted separately. This is the most basic mode for symmetric encryption
B. The cipher text from the current round is XORed with the plaintext from the previous round
C. 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
D. The cipher text from the current round is XORed with the plaintext for the next round
Answer: (SHOW ANSWER)
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.

NEW QUESTION: 67
What is the solution to the equation 8 mod 3?
A. 1
B. 4
C. 3
D. 2
Answer: D (LEAVE A REPLY)
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.

NEW QUESTION: 68
Which of the following encryption algorithms relies on the inability to factor large prime numbers?
A. RSA
B. MQV
C. EC
D. AES
Answer: A (LEAVE A REPLY)
Correct answers: 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.
The security of RSA relies on the practical difficulty of factoring the product of two large prime numbers, the "factoring problem". Breaking RSA encryption is known as the RSA problem. Whether it is as difficult as the factoring problem is an open question. There are no published methods to defeat the system if a large enough key is used.
Incorrect answers:
EC - Elliptic-curve cryptography (ECC) is an approach to public-key cryptography based on the algebraic structure of elliptic curves over finite fields. ECC allows smaller keys compared to non-EC cryptography (based on plain Galois fields) to provide equivalent security.
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.
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.

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).

NEW QUESTION: 69
Which of the following would be the weakest encryption algorithm?
A. DES
B. AES
C. RSA
D. EC
Answer: A (LEAVE A REPLY)
DES
https://en.wikipedia.org/wiki/Data_Encryption_Standard
DES is insecure due to the relatively short 56-bit key size. In January 1999, distributed.net and the Electronic Frontier Foundation collaborated to publicly break a DES key in 22 hours and 15 minutes.
Incorrect answers:
AES - has been adopted by the U.S. government and is now used worldwide. It supersedes the Data Encryption Standard (DES),which was published in 1977. The algorithm described by AES is a symmetric-key algorithm, meaning the same key is used for both encrypting and decrypting the data.
RSA - The security of RSA relies on the practical difficulty of factoring the product of two large prime numbers, the "factoring problem". Breaking RSA encryption is known as the RSA problem. Whether it is as difficult as the factoring problem is an open question. There are no published methods to defeat the system if a large enough key is used.
EC - Elliptic-curve cryptography (ECC) is an approach to public-key cryptography based on the algebraic structure of elliptic curves over finite fields. ECC allows smaller keys compared to non-EC cryptography (based on plain Galois fields) to provide equivalent security.

NEW QUESTION: 70
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
Answer: (SHOW ANSWER)
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 (1891-1977) and introduced in March 1918, the cipher was a fractionating transposition cipher which combined a modified Polybius square with a single columnar transposition.
Incorrect answers:
Book Ciphers - or Ottendorf cipher, is a cipher in which the key is some aspect of a book or other piece of text. Books, being common and widely available in modern times, are more convenient for this use than objects made specifically for cryptographic purposes. It is typically essential that both correspondents not only have the same book, but the same edition.
Cipher Disk - 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" ROT13 Cipher - simple letter substitution cipher that replaces a letter with the 13th letter after it, in the alphabet. ROT13 is a special case of the Caesar cipher which was developed in ancient Rome.

NEW QUESTION: 71
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 (LEAVE A REPLY)
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.

NEW QUESTION: 72
Cryptographic hashes are often used for message integrity and password storage. It is important to understand the common properties of all cryptographic hashes. What is not true about a hash?
A. Few collisions
B. Reversible
C. Variable length input
D. Fixed length output
Answer: B (LEAVE A REPLY)
Reversible
https://en.wikipedia.org/wiki/Hash_function

Hash functions are not reversible.
Incorrect answers:
Fixed length output and Variable length input. Hash function receive variable length input and produce fixed length output Few collisions. Every hash function with more inputs than outputs will necessarily have collisions

NEW QUESTION: 73
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.
A. SHA1
B. SHA-256
C. RSA
D. MD5
Answer: D (LEAVE A REPLY)
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

NEW QUESTION: 74

Ahlen is using a set of pre-calculated hashes to attempt to derive the passwords from a Windows SAM file. What is a set of pre-calculated hashes used to derive a hashed password called?

A. Hash matrix

B. Rainbow table

C. Password table

D. Hash table

Answer: B (LEAVE A REPLY)

Rainbow table

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

A rainbow table is a precomputed table for caching the output of cryptographic hash functions, usually for cracking password hashes. Tables are usually used in recovering a key derivation function (or credit card numbers, etc.) up to a certain length consisting of a limited set of characters. It is a practical example of a space-time tradeoff, using less computer processing time and more storage than a brute-force attack which calculates a hash on every attempt, but more processing time and less storage than a simple key derivation function with one entry per hash. Use of a key derivation that employs a salt makes this attack infeasible.

NEW QUESTION: 75

3DES can best be classified as which one of the following?

A. Digital signature

B. Symmetric algorithm

C. Asymmetric algorithm

D. Hashing algorithm

Answer: B (LEAVE A REPLY)

Symmetric algorithm

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

Triple DES (3DES or TDES), officially the Triple Data Encryption Algorithm (TDEA or Triple DEA), is a symmetric-key block cipher, which applies the DES cipher algorithm three times to each data block. The Data Encryption Standard's (DES) 56-bit key is no longer considered adequate in the face of modern cryptanalytic techniques and supercomputing power. However, an adapted version of DES, Triple DES (3DES), uses the same algorithm to produce a more secure encryption.

NEW QUESTION: 76

Basic information theory is the basis for modern symmetric ciphers. Understanding the terminology of information theory is, therefore, important. If a single change of a single bit in the plaintext causes changes in all the bits of the resulting ciphertext, what is this called?

A. Complete diffusion

B. Complete avalanche

C. Complete scrambling

D. Complete confusion

Answer: (SHOW ANSWER)

Valid 212-81 Dumps shared by Actual4test.com for Helping Passing 212-81 Exam! Actual4test.com now offer the **newest 212-81 exam dumps**, the Actual4test.com 212-81 exam **questions have been updated** and **answers have been corrected** get the **newest** Actual4test.com 212-81 dumps with Test Engine here: https://www.actual4test.com/212-81_examcollection.html (**208** Q&As Dumps, **30%OFF Special Discount: Freepdfdumps**)

Valid 212-81 Dumps shared by Actual4test.com for Helping Passing 212-81 Exam! Actual4test.com now offer the **newest 212-81 exam dumps**, the Actual4test.com 212-81 exam **questions have been updated** and **answers have been corrected** get the **newest** Actual4test.com 212-81 dumps with Test Engine here: https://www.actual4test.com/212-81_examcollection.html (**208** Q&As Dumps, **30%OFF Special Discount: Freepdfdumps**)