Number: 212-81
Passing Score: 800
Time Limit: 120
File Version: 4.0

Exam Code: 212-81

Exam Name: Certified Encryption Specialist

Exam A

QUESTION 1
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

Correct Answer: B, C
Section:
Explanation:
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.

QUESTION 2
Which of the following would be the weakest encryption algorithm?

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

Correct Answer: A
Section:
Explanation:
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.

QUESTION 3
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

Correct Answer: A
Section:
Explanation:
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.

QUESTION 4
A cryptographic hash function which uses a Merkle tree-like structure to allow for immense parallel computation of hashes for very long inputs. Authors claim a performance of 28 cycles per byte for MD6-256 on an Intel Core 2 Duo and provable resistance against differential cryptanalysis.

A. TIGER
B. GOST
C. MD5
D. MD6

Correct Answer: D
Section:
Explanation:
MD6
https://en.wikipedia.org/wiki/MD6
The MD6 Message-Digest Algorithm is a cryptographic hash function. It uses a Merkle tree-like structure to allow for immense parallel computation of hashes for very long inputs. Authors claim a performance of 28 cycles per byte for MD6-256 on an Intel Core 2 Duo and provable resistance against differential cryptanalysis.[2] The source code of the reference implementation was released under MIT license.
Speeds in excess of 1 GB/s have been reported to be possible for long messages on 16-core CPU architecture.
In December 2008, Douglas Held of Fortify Software discovered a buffer overflow in the original MD6 hash algorithm's reference implementation. This error was later made public by Ron Rivest on 19 February 2009, with a release of a corrected reference implementation in advance of the Fortify Report.

QUESTION 5
What size block does FORK256 use?

A. 64
B. 512
C. 256
D. 128

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

QUESTION 6
Which of the following algorithms uses three different keys to encrypt the plain text?

A. Skipjack
B. AES
C. Blowfish
D. 3DES

Correct Answer: D
Section:
Explanation:
3DES
https://en.wikipedia.org/wiki/Triple_DES
Triple DES (3DES) has a three different keys with same size (56-bit).
Incorrect answers:
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.
Blowfish. Blowfish has a 64-bit block size and a variable key length from 32 bits up to 448 bits.
Skipjack. Skipjack uses an 80-bit key to encrypt or decrypt 64-bit data blocks.

QUESTION 7
Original, unencrypted information is referred to as ____.

A. text
B. plaintext
C. ciphertext
D. cleartext

Correct Answer: B
Section:
Explanation:
plaintext
https://en.wikipedia.org/wiki/Plaintext
In cryptography, plaintext usually means unencrypted information pending input into cryptographic algorithms, usually encryption algorithms. Cleartext usually refers to data that is transmitted or stored unencrypted ('in clear').

QUESTION 8
Which of the following is a block cipher?

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

Correct Answer: A
Section:
Explanation:
AES
https://en.wikipedia.org/wiki/Advanced_Encryption_Standard
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
Incorrect answers:

RC4. RC4 (Rivest Cipher 4 also known as ARC4 or ARCFOUR meaning Alleged RC4, see below) is a stream cipher.
DH. Diffie--Hellman key exchange is a method of securely exchanging cryptographic keys over a public channel and was one of the first public-key protocols as conceived by Ralph Merkle and named after Whitfield Diffie and Martin Hellman.
RSA. RSA (Rivest--Shamir--Adleman) is one of the first public-key cryptosystems and is widely used for secure data transmission.

QUESTION 9
What is the name of the attack where the attacker obtains the ciphertexts corresponding to a set of plaintexts of his own choosing?

A. Chosen plaintext
B. Differential cryptanalysis
C. Known-plaintext attack
D. Kasiski examination

Correct Answer: A
Section:
Explanation:
Chosen plaintext
https://en.wikipedia.org/wiki/Chosen-plaintext_attack
A chosen-plaintext attack (CPA) is an attack model for cryptanalysis which presumes that the attacker can obtain the ciphertexts for arbitrary plaintexts. The goal of the attack is to gain information that reduces the security of the encryption scheme.
Incorrect answers:
Differential cryptanalysis - is a general form of cryptanalysis applicable primarily to block ciphers, but also to stream ciphers and cryptographic hash functions. In the broadest sense, it is the study of how differences in information input can affect the resultant difference at the output. In the case of a block cipher, it refers to a set of techniques for tracing differences through the network of transformation, discovering where the cipher exhibits non-random behavior, and exploiting such properties to recover the secret key (cryptography key).
Known-plaintext attack - (KPA) is an attack model for cryptanalysis where the attacker has access to both the plaintext (called a crib), and its encrypted version (ciphertext). These can be used to reveal further secret information such as secret keys and code books.
Kasiski examination - (also referred to as Kasiski's test or Kasiski's method) is a method of attacking polyalphabetic substitution ciphers, such as the Vigenre cipher. It was first published by Friedrich Kasiski in 1863, but seems to have been independently discovered by Charles Babbage as early as 1846. In polyalphabetic substitution ciphers where the substitution alphabets are chosen by the use of a keyword, the Kasiski examination allows a cryptanalyst to deduce the length of the keyword. Once the length of the keyword is discovered, the cryptanalyst lines up the ciphertext in n columns, where n is the length of the keyword. Then each column can be treated as the ciphertext of a monoalphabetic substitution cipher. As such, each column can be attacked with frequency analysis.

QUESTION 10
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

Correct Answer: B
Section:
Explanation:
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, Michal Peeters, and Gilles Van Assche, building upon RadioGatn.

QUESTION 11
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

Correct Answer: A
Section:
Explanation:
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.

QUESTION 12
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

Correct Answer: C
Section:
Explanation:
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.

QUESTION 13
What is the largest key size that AES can use?

A. 256
B. 56
C. 512
D. 128

Correct Answer: A
Section:
Explanation:
256
https://en.wikipedia.org/wiki/Advanced_Encryption_Standard
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 14
Terrance oversees the key escrow server for his company. All employees use asymmetric cryptography to encrypt all emails. How many keys are needed for asymmetric cryptography?

A. 2
B. 4
C. 3
D. 1

Correct Answer: A
Section:
Explanation:
:
2
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.

QUESTION 15
Which of the following encryption algorithms relies on the inability to factor large prime numbers?

A. RSA
B. MQV
C. EC
D. AES

Correct Answer: A
Section:
Explanation:
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).

QUESTION 16
If you XOR 10111000 with 10101010, what is the result?

A. 10111010
B. 10101010
C. 11101101
D. 00010010

Correct Answer: D
Section:
Explanation:
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

QUESTION 17
Which one of the following is a symmetric key system using 64-bit blocks?

A. DES
B. PGP
C. DSA
D. RSA

Correct Answer: A
Section:
Explanation:
DES
https://en.wikipedia.org/wiki/Data_Encryption_Standard
DES is the archetypal block cipher---an algorithm that takes a fixed-length string of plaintext bits and transforms it through a series of complicated operations into another ciphertext bitstring of the same length. In the case of DES, the block size is 64 bits. DES also uses a key to customize the transformation, so that decryption can supposedly only be performed by those who know the particular key used to encrypt. The key ostensibly consists of 64 bits; however, only 56 of these are actually used by the algorithm. Eight bits are used solely for checking parity, and are thereafter discarded. Hence the effective key length is 56 bits.

Incorrect answers:
PGP - 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.
RSA - 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.
DSA - The Digital Signature Algorithm (DSA) is a Federal Information Processing Standard for digital signatures, based on the mathematical concept of modular exponentiation and the discrete logarithm problem. DSA is a variant of the Schnorr and ElGamal signature schemes.

QUESTION 18
Ferris has been assigned the task of selecting security for his company's wireless network. It is important that he pick the strongest form of wireless security. Which one of the following is the strongest wireless security?

A. WEP
B. WPA
C. WPA2
D. TKIP

Correct Answer: C
Section:
Explanation:
WPA2
https://en.wikipedia.org/wiki/Wi-Fi_Protected_Access
WPA (sometimes referred to as the draft IEEE 802.11i standard) became available in 2003. The Wi-Fi Alliance intended it as an intermediate measure in anticipation of the availability of the more secure and complex WPA2, which became available in 2004 and is a common shorthand for the full IEEE 802.11i (or IEEE 802.11i-2004) standard.

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

Correct Answer: A
Section:
Explanation:
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.

QUESTION 20
A list of certificates that have been revoked.

A. CA
B. CRL
C. PCBC
D. OCSP

Correct Answer: B
Section:
Explanation:
CRL
https://en.wikipedia.org/wiki/Certificate_revocation_list
In cryptography, a certificate revocation list (or 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'.
Incorrect answers:
PCBC - the propagating cipher block chaining or plaintext cipher-block chaining mode was designed to cause small changes in the ciphertext to propagate indefinitely when decrypting, as well as when encrypting. In PCBC mode, each block of plaintext is XORed with both the previous plaintext block and the previous ciphertext block before being encrypted. As with CBC mode, an initialization vector is used in the first block.
CA - certificate authority or certification authority is an entity that issues digital certificates.
OCSP - The Online Certificate Status Protocol (OCSP) is an Internet protocol used for obtaining the revocation status of an X.509 digital certificate. It is described in RFC 6960 and is on the Internet standards track. It was created as an alternative to certificate revocation lists (CRL), specifically addressing certain problems associated with using CRLs in a public key infrastructure (PKI).

QUESTION 21
Which of the following is generally true about key sizes?

A. Larger key sizes increase security
B. Key size is irrelevant to security
C. Key sizes must be more than 256 bits to be secure
D. Smaller key sizes increase security

Correct Answer: A
Section:
Explanation:
Larger key sizes increase security
https://en.wikipedia.org/wiki/Key_size
Key length defines the upper-bound on an algorithm's security (i.e. a logarithmic measure of the fastest known attack against an algorithm), since the security of all algorithms can be violated by brute-force attacks. Ideally, the lower-bound on an algorithm's security is by design equal to the key length (that is, the security is determined entirely by the keylength, or in other words, the algorithm's design doesn't detract from the degree of security inherent in the key length). Indeed, most symmetric-key algorithms are designed to have security equal to their key length. However, after design, a new attack might be discovered. For instance, Triple DES was designed to have a 168 bit key, but an attack of complexity 2112 is now known (i.e. Triple DES now only has 112 bits of security, and of the 168 bits in the key the attack has rendered 56 'ineffective' towards security). Nevertheless, as long as the security (understood as 'the amount of effort it would take to gain access') is sufficient for a particular application, then it doesn't matter if key length and security coincide. This is important for asymmetric-key algorithms, because no such algorithm is known to satisfy this property; elliptic curve cryptography comes the closest with an effective security of roughly half its key length.

QUESTION 22
The next number is derived from adding together the prior two numbers (1, 1, 2, 3, 5, 8, 13, 21, 34, 55, 89).

A. Odd numbers
B. Fibonacci Sequence
C. Fermat pseudoprime
D. Prime numbers

Correct Answer: B
Section:
Explanation:
Fibonacci Sequence
https://en.wikipedia.org/wiki/Fibonacci_number
In mathematics, the Fibonacci numbers, commonly denoted Fn, form a sequence, called the Fibonacci sequence, such that each number is the sum of the two preceding ones, starting from 0 and 1. That is,
F0 = 0, F1=1, Fn = Fn-1 + Fn-2; for n > 1.
The beginning of the sequence is thus:
0,1, 1, 2, 3, 5, 8, 13, 21, 34, 55, 89, 144...
Incorrect answers:
Prime numbers - numbers that have only 2 factors: 1 and themselves. 2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43, 47...
Fermat numbers - a positive integer of the form Fn = 2^2^n +1; where n is a non-negative integer. The first few Fermat numbers are: 3, 5, 17, 257, 65537, 4294967297, 18446744073709551617, ...
Odd numbers - any number which cannot be divided by two 1, 3, 5, 7, 9, 11, 13, 15 ...

QUESTION 23
In a Feistel cipher, the two halves of the block are swapped in each round. What does this provide?

A. Diffusion
B. Confusion
C. Avalanche
D. Substitution

Correct Answer: C
Section:
Explanation:
Confusion
https://en.wikipedia.org/wiki/Confusion_and_diffusion#Definition
Confusion means that each binary digit (bit) of the ciphertext should depend on several parts of the key, obscuring the connections between the two.
The property of confusion hides the relationship between the ciphertext and the key.
This property makes it difficult to find the key from the ciphertext and if a single bit in a key is changed, the calculation of the values of most or all of the bits in the ciphertext will be affected.
Confusion increases the ambiguity of ciphertext and it is used by both block and stream ciphers.
Incorrect answer:
Avalanche - The avalanche effect is the desirable property of cryptographic algorithms, typically block ciphers and cryptographic hash functions, wherein if an input is changed slightly (for example, flipping a single bit), the output changes significantly (e.g., half the output bits flip). In the case of high-quality block ciphers, such a small change in either the key or the plaintext should cause a drastic change in the ciphertext. The actual term was first used by Horst Feistel, although the concept dates back to at least Shannon's diffusion.
Diffusion - Diffusion means that if we change a single bit of the plaintext, then (statistically) half of the bits in the ciphertext should change, and similarly, if we change one bit of the ciphertext, then approximately one half of the plaintext bits should change.[2] Since a bit can have only two states, when they are all re-evaluated and changed from one seemingly random position to another, half of the bits will have changed state.
Substitution - Substitution technique is a classical encryption technique where the characters present in the original message are replaced by the other characters or numbers or by symbols.

QUESTION 24
What size key does Skipjack use?

A. 128 bit
B. 56 bit
C. 80 bit
D. 256 bit

Correct Answer: C
Section:

QUESTION 25
A _____ is a function is not reversible.

A. Stream cipher
B. Asymmetric cipher
C. Hash
D. Block Cipher

Correct Answer: C
Section:
Explanation:
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.

QUESTION 26
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

Correct Answer: C
Section:
Explanation:
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.

QUESTION 27
What size block does AES work on?

A. 64
B. 128
C. 192
D. 256

Correct Answer: B
Section:
Explanation:

128
https://en.wikipedia.org/wiki/Advanced_Encryption_Standard
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 28
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

Correct Answer: B
Section:
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 29
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

Correct Answer: C
Section:
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 30
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

Correct Answer: C
Section:
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 31
Which of the following is an asymmetric cipher?

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

Correct Answer: A
Section:
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 32
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

Correct Answer: C
Section:
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.

QUESTION 33
What is a salt?

A. Key whitening
B. Random bits intermixed with a symmetric cipher to increase randomness and make it more secure
C. Key rotation
D. Random bits intermixed with a hash to increase randomness and reduce collisions

Correct Answer: D
Section:
Explanation:
Random bits intermixed with a hash to increase randomness and reduce collisions
https://en.wikipedia.org/wiki/Salt_(cryptography)
Salt is random data that is used as an additional input to a one-way function that hashes data, a password or passphrase. Salts are used to safeguard passwords in storage. Historically a password was stored in plaintext on a system, but over time additional safeguards were developed to protect a user's password against being read from the system. A salt is one of those methods.
Incorrect answers:
Key whitening - 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.
Key rotation - is when you retire an encryption key and replace that old key by generating a new cryptographic key. Rotating keys on a regular basis help meet industry standards and cryptographic best practices.
Random bits intermixed with a symmetric cipher to increase randomness and make it more secure -- Initialization Vector (IV)

QUESTION 34
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

Correct Answer: D
Section:
Explanation:
Vigenere
https://en.wikipedia.org/wiki/Vigen%C3%A8re_cipher
The Vigenre 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 indchiffrable (French for 'the indecipherable cipher'). Many people have tried to implement encryption schemes that are essentially Vigenre ciphers. In 1863, Friedrich Kasiski was the first to publish a general method of deciphering Vigenre 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.

QUESTION 35
A symmetric Stream Cipher published by the German engineering firm Seimans in 1993. A software based stream cipher that uses a Lagged Fibonacci generator along with concepts borrowed from shrinking generator ciphers.

A. DESX
B. FISH
C. Twofish
D. IDEA

Correct Answer: B
Section:
Explanation:
FISH
https://en.wikipedia.org/wiki/FISH_(cipher)
The FISH (FIbonacci SHrinking) stream cipher is a fast software based stream cipher using Lagged Fibonacci generators, plus a concept from the shrinking generator cipher. It was published by Siemens in 1993. FISH is quite fast in software and has a huge key length. However, in the same paper where he proposed Pike, Ross Anderson showed that FISH can be broken with just a few thousand bits of known plaintext.
Incorrect answers:
Twofish - symmetric algorithm. Designed by Bruce Schneier, John Kelsey, Doug Whiting, David Wagner, Chris Hall, and Niels Ferguson. Uses a block size of 128 bits and key sizes of 128, 192, or 256 bits. It is a Feistel cipher.
IDEA - symmetric algorithm. Designed by James Massey and Xuejia Lai. Operates on 64 bit blocks and has a 128 bit key. Consists of 8 identical transformations each round and an output transformation.
DESX - symmetric algorithm. 64 bit key is appended to data, XOR it, and then apply the DES algorithm.

QUESTION 36
What advantage do symmetric algorithms have over asymmetric algorithms

A. It is easier to implement them in software
B. They are more secure
C. They are faster
D. It is easier to exchange keys

Correct Answer: C
Section:
Explanation:
They are faster
Symmetric key encryption is much faster than asymmetric key encryption, because both the sender and the recipient of a message to use the same secret key.

QUESTION 37
Which one of the following is an example of a symmetric key algorithm?

A. ECC
B. Diffie-Hellman
C. RSA
D. Rijndael

Correct Answer: D
Section:

Explanation:
Rijndael
https://en.wikipedia.org/wiki/Advanced_Encryption_Standard
The Advanced Encryption Standard (AES), also known by its original name Rijndael. The algorithm described by AES is a symmetric-key algorithm, meaning the same key is used for both encrypting and decrypting the data.
Incorrect answers:
ECC - Elliptic-curve cryptography 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.
Diffie--Hellman - key exchange is a method of securely exchanging cryptographic keys over a public channel and was one of the first public-key protocols as conceived by Ralph Merkle and named after Whitfield Diffie and Martin Hellman.
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.

QUESTION 38
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

Correct Answer: B
Section:
Explanation:
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).

QUESTION 39
In IPSec, if the VPN is a gateway-gateway or a host-gateway, then which one of the following is true?

A. IPSec does not involve gateways
B. Only transport mode can be used
C. Encapsulating Security Payload (ESP) authentication must be used
D. Only the tunnel mode can be used

Correct Answer: D
Section:
Explanation:
IPSec has two different modes: transport mode and tunnel mode.
Only the tunnel mode can be used
https://en.wikipedia.org/wiki/IPsec
In tunnel mode, the entire IP packet is encrypted and authenticated. It is then encapsulated into a new IP packet with a new IP header. Tunnel mode is used to create virtual private networks for network-to-network communications (e.g. between routers to link sites), host-to-network communications (e.g. remote user access) and host-to-host communications (e.g. private chat).
Incorrect answers:
Encapsulating Security Payload (ESP) authentication must be used. ESP in transport mode does not provide integrity and authentication for the entire IP packet. However, in Tunnel Mode, where the entire original IP packet is encapsulated with a new packet header added, ESP protection is afforded to the whole inner IP packet (including the inner header) while the outer header (including any outer IPv4 options or IPv6 extension headers) remains unprotected.

IPSec does not involve gateways. Wrong.
Only transport mode can be used. Transport mode, the default mode for IPSec, provides for end-to-end security. It can secure communications between a client and a server. When using the transport mode, only the IP payload is encrypted.

QUESTION 40
What is the formula m^e %n related to?

A. Encrypting with EC
B. Decrypting with RSA
C. Generating Mersenne primes
D. Encrypting with RSA

Correct Answer: D
Section:
Explanation:
Encrypting with RSA
https://en.wikipedia.org/wiki/RSA_(cryptosystem)
RSA Encrypting a message m (number) with the public key (n, e) is calculated:
M' := m^e %n
Incorrect answers:
Decrypting with RSA:
M'' := m^d %n
Generation Mersenne primes:
Mn = 2^n - 1
Encrypting with Elliptic Curve (EC):
y^2 = x^3 + ax + b

QUESTION 41
A real time protocol for verifying certificates (and a newer method than CRL).

A. Online Certificate Status Protocol (OCSP)
B. Server-based Certificate Validation Protocol (SCVP)
C. Public Key Infrastructure (PKI)
D. Registration Authority (RA)

Correct Answer: A
Section:
Explanation:
Online Certificate Status Protocol (OCSP)
https://en.wikipedia.org/wiki/Online_Certificate_Status_Protocol
The Online Certificate Status Protocol (OCSP) is an Internet protocol used for obtaining the revocation status of an X.509 digital certificate. It is described in RFC 6960 and is on the Internet standards track. It was created as an alternative to certificate revocation lists (CRL), specifically addressing certain problems associated with using CRLs in a public key infrastructure (PKI).
Incorrect answers:
Public Key Infrastructure (PKI) - 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.
Registration Authority (RA) - omponent of PKI that validates the identity of an entity requesting a digital certificate.
Server-based Certificate Validation Protocol (SCVP) - Internet protocol for determining the path between an X.509 digital certificate and a trusted root (Delegated Path Discovery) and the validation of that path (Delegated Path Validation) according to a particular validation policy.

QUESTION 42
Which of the following is not a key size used by AES?

A. 128 bits
B. 192 bits
C. 256 bits
D. 512 b

Correct Answer: D
Section:
Explanation:
512 bits
https://en.wikipedia.org/wiki/Advanced_Encryption_Standard
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 43
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

Correct Answer: A
Section:
Explanation:
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.

QUESTION 44
A _____ is a digital representation of information that identifies you as a relevant entity by a trusted third party.

A. Digital Signature
B. Hash
C. Ownership stamp
D. Digest

Correct Answer: A
Section:
Explanation:
Digital Signature
https://en.wikipedia.org/wiki/Digital_signature
A digital signature is a mathematical scheme for verifying the authenticity of digital messages or documents. A valid digital signature, where the prerequisites are satisfied, gives a recipient very strong reason to believe that the message was created by a known sender (authentication), and that the message was not altered in transit (integrity).

QUESTION 45
You are trying to find a modern method for security web traffic for use in your company's ecommerce web site. Which one of the following is used to encrypt web pages and uses bilateral authentication?

A. AES
B. SSL
C. TLS
D. 3DES

Correct Answer: C
Section:
Explanation:
TLS
https://en.wikipedia.org/wiki/Mutual_authentication
Mutual authentication or two-way authentication refers to two parties authenticating each other at the same time, being a default mode of authentication in some protocols (IKE, SSH) and optional in others (TLS).
By default the TLS protocol only proves the identity of the server to the client using X.509 certificate and the authentication of the client to the server is left to the application layer. TLS also offers client-to-server authentication using client-side X.509 authentication. As it requires provisioning of the certificates to the clients and involves less user-friendly experience, it's rarely used in end-user applications.

QUESTION 46
An authentication method that periodically re-authenticates the client by establishing a hash that is then resent from the client is called _____.

A. CHAP
B. SPAP
C. PAP
D. EAP

Correct Answer: A
Section:
Explanation:
CHAP
https://en.wikipedia.org/wiki/Challenge-Handshake_Authentication_Protocol
Challenge-Handshake Authentication Protocol (CHAP) is an identity verification protocol that does not rely on sending a shared secret between the access-requesting party and the identity-verifying party (the authenticator). CHAP is based on a shared secret, but in order to authenticate, the authenticator sends a ''challenge'' message to the access-requesting party, which responds with a value calculated using a ''one-way hash'' function that takes as inputs the challenge and the shared secret. The authenticator checks the response against its own calculation of the expected hash value. If the values match, the authentication succeeds, otherwise it fails. Following the establishment of an authenticated connection, the authenticator may send a challenge to the access-requesting party at random intervals, to which the access-requesting party will have to produce the correct response.
Incorrect answers:
EAP - A framework that allows for creation of different ways to provide authentication, such as smart cards
SPAP - Shiva Password Authentication Protocol, PAP with encryption for the usernames/passwords that are transmitted.
PAP - Password Authentication Protocol. Used to authenticate users, but is no longer used because the information was sent in cleartext.

QUESTION 47
In a _____ the attacker discovers a functionally equivalent algorithm for encryption and decryption, but without learning the key.

A. Information deduction
B. Total break
C. Instance deduction
D. Global deduction

Correct Answer: B
Section:
Explanation:
Global deduction
https://en.wikipedia.org/wiki/Cryptanalysis
Global deduction --- the attacker discovers a functionally equivalent algorithm for encryption and decryption, but without learning the key.
Incorrect answers:
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.
Total break --- the attacker deduces the secret key.

QUESTION 48
Which of the following is a cryptographic protocol that allows two parties to establish a shared key over an insecure channel?

A. Elliptic Curve
B. NMD5
C. RSA
D. Diffie-Hellman

Correct Answer: D
Section:
Explanation:
Diffie-Hellman
https://en.wikipedia.org/wiki/Diffie%E2%80%93Hellman_key_exchange
Diffie-Hellman key exchange is a method of securely exchanging cryptographic keys over a public channel and was one of the first public-key protocols as originally conceptualized by Ralph Merkle and named after Whitfield Diffie and Martin Hellman. DH is one of the earliest practical examples of public key exchange implemented within the field of cryptography.
Incorrect answers:
Elliptic Curve - Asymmetric Key Algorithm, provides encryption, digital signatures, key exchange, based on the idea of using points on a curve to define the public/private key, used in wireless devices and smart cards. The security of the Elliptic Curve cryptography is based on the fact that finding the discrete logarithm of a random elliptic curve element with respect to a publicly known base point is difficult to the point of being impractical to do so. (y2 = x3 + Ax + B) - Developed by Victor Miller and Neil Koblitz in 1985
MD5 - hash function - 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. Not collision resistant - Not Reversible - RFC 1321
RSA - is a public-key cryptosystem that is widely used for secure data transmission.

QUESTION 49
A linear congruential generator is an example of what?

A. A coprime generator
B. A prime number generator
C. A pseudo random number generator
D. A random number generator

Correct Answer: C
Section:
Explanation:
A pseudo random number generator
https://en.wikipedia.org/wiki/Linear_congruential_generator
A linear congruential generator (LCG) is an algorithm that yields a sequence of pseudo-randomized numbers calculated with a discontinuous piecewise linear equation. The method represents one of the oldest and best-known pseudorandom number generator algorithms. The theory behind them is relatively easy to understand, and they are easily implemented and fast, especially on computer hardware which can provide modular arithmetic by storage-bit truncation.

QUESTION 50
DES has a key space of what?

A. 2^128
B. 2^192
C. 2^64
D. 2^56

Correct Answer: D
Section:
Explanation:
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.

QUESTION 51
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

Correct Answer: A
Section:
Explanation:
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.'

QUESTION 52
_____ uses at least two different shifts, changing the shift with different letters in the plain text.

A. Caesar cipher
B. multi-alphabet encryption
C. Scytale

D. Atbash

Correct Answer: B
Section:
Explanation:
multi-alphabet encryption
https://en.wikipedia.org/wiki/Polyalphabetic_cipher
Two different shifts create two different alphabets.
For +1 and +2
Plaintext alphabet
A B C D E F G H I J K L M N O P Q R S T U V W X Y Z
2 ciphertext alphabets
B C D E F G H I J K L M N O P Q R S T U V W X Y Z A
C D E F G H I J K L M N O P Q R S T U V W X Y Z A B
Incorrect answers:
Scytale - transposition cipher
Caesar cipher - monoalphabetic cipher
Atbash - monoalphabetic cipher

QUESTION 53
Jane is looking for an algorithm to ensure message integrity. Which of following would be an acceptable choice?

A. RSA
B. AES
C. RC4
D. SHA-1

Correct Answer: D
Section:
Explanation:
Integrity. In information security, data integrity means maintaining and assuring the accuracy and completeness of data over its entire lifecycle. This means that data cannot be modified in an unauthorized or undetected manner.
An important application of 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.
SHA-1
https://en.wikipedia.org/wiki/SHA-1
SHA-1 (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.
Incorrect answers:
RSA (Rivest--Shamir--Adleman) is one of the first public-key cryptosystems and is widely used for secure data transmission.
RC4 (Rivest Cipher 4 also known as ARC4 or ARCFOUR meaning Alleged RC4, see below) is a stream cipher.
AES (Advanced Encryption Standard) is a subset of the Rijndael block cipher

QUESTION 54
If you wished to see a list of revoked certificates from a CA, where would you look?

A. RA
B. RFC
C. CRL

D. CA

Correct Answer: C
Section:
Explanation:
CRL
https://ru.wikipedia.org/wiki/Certificate_Revocation_List
Certificate Revocation List (or 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'.
Incorrect answers:
RA - Used to proxy the certificate requests on behalf of the user and validate whether or not they are legitimate instead of having the user go directly to the CA. The RA talks to the subordinate CA on behalf of the user, which makes it harder for the actor to get directly to the certificate authority and do harm.
RFC -- Request for Comments (RFC) is a publication from the Internet Society (ISOC) and its associated bodies, most prominently the Internet Engineering Task Force (IETF), the principal technical development and standards-setting bodies for the Internet.
CA - certificate authority or certification authority is an entity that issues digital certificates

QUESTION 55
Which of the following are valid key sizes for AES (choose three)?

A. 192
B. 56
C. 256
D. 128
E. 512
F. 64

Correct Answer: A, C, D
Section:
Explanation:
Correct answers: 128, 192, 256
https://en.wikipedia.org/wiki/Advanced_Encryption_Standard
The 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.

QUESTION 56
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 scrambling
C. Complete confusion
D. Complete avalanche

Correct Answer: D
Section:

QUESTION 57
This is a proprietary version of PAP. Encrypts username and password as it is sent across network.

A. PPTP VPN
B. S-PAP
C. Kerberos
D. WPA2

Correct Answer: B
Section:
Explanation:
S-PAP
Shiva Password Authentication Protocol (S-PAP) - PAP with encryption for the usernames/passwords that are transmitted.
Incorrect answers:
Kerberos - a 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.
WPA2 -- (Wi-Fi Protected Access II) security certification program developed by the Wi-Fi Alliance to secure wireless computer networks. It includes mandatory support for CCMP, an AES-based encryption mode.
PPTP VPN - works at layer 2 (data link) layer of OSI model. Provides both authentication and encryption. EAP or CHAP is used to provide the authentication for PPTP. MPPE (Microsoft Point to Point Encryption) is used to encrypt the traffic. MPPE - a specific Microsoft implementation of DES. Can only use over a traditional Ethernet network.

QUESTION 58
The ATBASH cipher is best described as what type of cipher?

A. Asymmetric
B. Symmetric
C. Substitution
D. Transposition

Correct Answer: C
Section:
Explanation:
Substitution
https://en.wikipedia.org/wiki/Atbash
Atbash is a monoalphabetic substitution cipher originally used to encrypt the Hebrew alphabet. It can be modified for use with any known writing system with a standard collating order.

QUESTION 59
Developed by Netscape and has been replaced by TLS. It was the preferred method used with secure websites.

A. OCSP
B. VPN
C. CRL
D. SSL

Correct Answer: D
Section:
Explanation:
SSL
https://en.wikipedia.org/wiki/Transport_Layer_Security
Transport Layer Security (TLS), and its now-deprecated predecessor, Secure Sockets Layer (SSL), are cryptographic protocols designed to provide communications security over a computer network. Several versions of the

protocols find widespread use in applications such as web browsing, email, instant messaging, and voice over IP (VoIP). Websites can use TLS to secure all communications between their servers and web browsers.
Netscape developed the original SSL protocols, and Taher Elgamal, chief scientist at Netscape Communications from 1995 to 1998, has been described as the 'father of SSL'. SSL version 1.0 was never publicly released because of serious security flaws in the protocol. Version 2.0, released in February 1995, contained a number of security flaws which necessitated the design of version 3.0. Released in 1996, SSL version 3.0 represented a complete redesign of the protocol produced by Paul Kocher working with Netscape engineers Phil Karlton and Alan Freier, with a reference implementation by Christopher Allen and Tim Dierks of Consensus Development.
Incorrect answers:
CRL - a list of every certificate that has been revoked.
VPN - A virtual private network (VPN) extends a private network across a public network and enables users to send and receive data across shared or public networks as if their computing devices were directly connected to the private network. Applications running across a VPN may therefore benefit from the functionality, security, and management of the private network. Encryption is a common, although not an inherent, part of a VPN connection
OCSP - The Online Certificate Status Protocol (OCSP) is an Internet protocol used for obtaining the revocation status of an X.509 digital certificate. It is described in RFC 6960 and is on the Internet standards track. It was created as an alternative to certificate revocation lists (CRL), specifically addressing certain problems associated with using CRLs in a public key infrastructure (PKI).

QUESTION 60
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

Correct Answer: A
Section:
Explanation:
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.

QUESTION 61
Message hidden in unrelated text. Sender and receiver have pre-arranged to use a pattern to remove certain letters from the message which leaves only the true message behind.

A. Caesar Cipher
B. Null Ciphers
C. Vigenere Cipher
D. Playfair Cipher

Correct Answer: B
Section:
Explanation:
Null Ciphers
https://en.wikipedia.org/wiki/Null_cipher
A null cipher, also known as concealment cipher, is an ancient form of encryption where the plaintext is mixed with a large amount of non-cipher material. Today it is regarded as a simple form of steganography, which can be used to hide ciphertext.

Incorrect answers:
Caesar Cipher - Monoalphabetic cipher where letters are shifted one or more letters in either direction. The method is named after Julius Caesar, who used it in his private correspondence.
Vigenre - method of encrypting alphabetic text by using a series of interwoven Caesar ciphers, based on the letters of a keyword. It employs a form of polyalphabetic substitution.
Playfair Cipher - manual symmetric encryption technique and was the first literal digram substitution cipher. The scheme was invented in 1854 by Charles Wheatstone, but bears the name of Lord Playfair for promoting its use.

QUESTION 62
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

Correct Answer: B
Section:
Explanation:
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

QUESTION 63
John is going to use RSA to encrypt a message to Joan. What key should he use?

A. A random key
B. Joan's public key
C. A shared key
D. Joan's private key

Correct Answer: B
Section:
Explanation:
Joan's public key
https://en.wikipedia.org/wiki/RSA_(cryptosystem)
Suppose Joahn uses Bob's public key to send him an encrypted message. In the message, she can claim to be Alice but Bob has no way of verifying that the message was actually from Alice since anyone can use Bob's public key to send him encrypted messages. In order to verify the origin of a message, RSA can also be used to sign a message.
Suppose Alice wishes to send a signed message to Bob. She can use her own private key to do so. She produces a hash value of the message, raises it to the power of d (modulo n) (as she does when decrypting a message), and attaches it as a 'signature' to the message. When Bob receives the signed message, he uses the same hash algorithm in conjunction with Alice's public key. He raises the signature to the power of e (modulo n) (as he does when encrypting a message), and compares the resulting hash value with the message's actual hash value. If the two agree, he knows that the author of the message was in possession of Alice's private key, and that the message has not been tampered with since.

QUESTION 64
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

Correct Answer: D
Section:
Explanation:
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.

QUESTION 65
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

Correct Answer: A
Section:
Explanation:
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.

QUESTION 66
A measure of the uncertainty associated with a random variable.

A. Collision
B. Whitening
C. Diffusion
D. Entropy

Correct Answer: D
Section:
Explanation:
Entropy
https://en.wikipedia.org/wiki/Entropy_(information_theory)
In information theory, the entropy of a random variable is the average level of 'information', 'surprise', or 'uncertainty' inherent in the variable's possible outcomes. The concept of information entropy was introduced by Claude Shannon in his 1948 paper 'A Mathematical Theory of Communication'.
Incorrect answers:
Diffusion - transposition processes used in encryption functions to increase randomness.
Whitening - technique intended to increase the security of an iterated block cipher. It consists of steps that combine the data with portions of the key.
Collision - situation where two different inputs yield the same output.

QUESTION 67

Which of the following is a type of encryption that has two different keys. One key can encrypt the message and the other key can only decrypt it?

A. Block cipher
B. Asymmetric
C. Symmetric
D. Stream cipher

Correct Answer: B
Section:
Explanation:
Asymmetric
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.
Incorrect answers:
Symmetric - Symmetric-key algorithms are algorithms for cryptography that use the same cryptographic keys for both encryption of plaintext and decryption of ciphertext.
Block cipher - A 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.
Stream cipher - A stream cipher is a symmetric key cipher where plaintext digits are combined with a pseudorandom cipher digit stream (keystream). In a stream cipher, each plaintext digit is encrypted one at a time with the corresponding digit of the keystream, to give a digit of the ciphertext stream.

QUESTION 68
Which of the following is a substitution cipher used by ancient Hebrew scholars?

A. Atbash
B. Vigenere
C. Caesar
D. Scytale

Correct Answer: A
Section:
Explanation:
Atbash
https://en.wikipedia.org/wiki/Atbash
Atbash is a monoalphabetic substitution cipher originally used to encrypt the Hebrew alphabet. It can be modified for use with any known writing system with a standard collating order.
Incorrect answers:
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.
Vigenre - 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.
Caesar Cipher - Monoalphabetic cipher where letters are shifted one or more letters in either direction. The method is named after Julius Caesar, who used it in his private correspondence.

QUESTION 69
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.

A. Fibonacci Numbers
B. Co-prime Numbers
C. Even Numbers
D. Mersenne Primes

Correct Answer: D
Section:
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 70
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.

A. Differential Cryptanalysis
B. Linear Cryptanalysis
C. Chosen Plaintext Attack
D. Integral Cryptanalysis

Correct Answer: D
Section:
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).