Latest Version: 6.0

Question: 1

Which one of the following are characteristics of a hash function? (Choose two)

A. Fast
B. Symmetric
C. One-way
D. Fixed length output
E. Requires a key

Answer: C,D

Explanation:
https://en.wikipedia.org/wiki/Cryptographic_hash_function
A cryptographic hash function is a mathematical algorithm that maps data of arbitrary size (often called the "message") to a bit array of a fixed size (the "hash value", "hash", or "message digest"). It is a one-way function, that is, a function which is practically infeasible to invert.
Symmetric. Cryptographic algorithms can be categorized into three classes: Hash functions, Symmetric and Asymmetric algorithms. Differences: purpose and main fields of application.
Requires a key. Well, technically, this is the correct answer. But in the hash-function, “key” is input data.
Fast. Fast or slow is a subjective characteristic, there are many different algorithms, and here it is impossible to say this unambiguously like "Symmetric encryption is generally faster than asymmetric encryption."

Question: 2

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

Answer: A

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.

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: 3

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

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

Answer: C

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.
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.
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: 4

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

Explanation:
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.

Question: 5

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

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

Answer: A

Explanation:
https://en.wikipedia.org/wiki/Vigen%C3%A8re_cipher
The Vigenère 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 indéchiffrable (French for 'the indecipherable cipher'). Many people have tried to implement encryption schemes that are essentially Vigenère ciphers. In 1863, Friedrich Kasiski was the first to publish a general method of deciphering Vigenère ciphers.
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: 6

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

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

Answer: C

Explanation:
IPSec has two different modes: transport mode and tunnel mode.
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).
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: 7

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. 3DES
B. SSL
C. TSL
D. AES

Answer: C

Explanation:
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: 8

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

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

Answer: B

Explanation:
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: 9

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. GOST
B. TIGER
C. MD6
D. MD5

Answer: C

Explanation:
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: 10

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

Answer: A

Explanation:
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.
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.