CERTKILLERS

Eccouncil

ECES

EC-Council Certified Encryption Specialist (ECES)

QUESTION & ANSWERS

Question: 1

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. Null Ciphers

B. Playfair Cipher

C. Vigenere Cipher

D. Caesar Cipher

Answer: A

Explanation/Reference:

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.
Vigenère - 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: 2

A transposition cipher invented 1918 by Fritz Nebel, used a 36 letter alphabet and a modified Polybius square with a single columnar transposition.

A. Cipher Disk

B. ROT13 Cipher

C. Book Ciphers

D. ADFVGX Cipher

Answer: D

Explanation/Reference:

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: 3

Collision resistance is an important property for any hashing algorithm. Joan wants to find a cryptographic hash that has strong collision resistance. Which one of the following is the most collisionresistant?

A. MD4

B. PIKE

C. SHA2

D. MD5

Answer: C

Explanation/Reference:

https://en.wikipedia.org/wiki/Collision_resistance
Collision resistance is a property of cryptographic hash functions: a hash function H is collision-resistant if it is hard to find two inputs that hash to the same output; that is, two inputs a and b where a ≠ b but H(a) = H(b). The pigeonhole principle means that any hash function with more inputs than outputs will necessarily have such collisions; the harder they are to find, the more cryptographically secure the hash function is.
Due to the Birthday Problem, for a hash function that produces an output of length n bits, the probability of getting a collision is 1/2^n/2.
So, just looking for a hash function with larger "n".
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.

Question: 4

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

A. Generating Mersenne primes

B. Decrypting with RSA

C. Encrypting with RSA

D. Encrypting with EC

Answer: C

Explanation/Reference:

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: 5

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

A. Symmetric

B. Fast

C. Requires a key

D. Fixed length output

E. One-way

Answer: D,E

Explanation/Reference:

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.
Incorrect answers:
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."