# Eccouncil 212-81 ECES Practice Questions

**Shared by Moreno on 17-08-2026**

**For More Free Questions and Preparation Resources**

Check the Links on Last Page

## Question 1

Question Type: MultipleChoice

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

### Options:

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



### Answer:

D

### 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 2

Question Type: MultipleChoice

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

### Options:

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

### Answer:

C

### 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 3

Question Type: MultipleChoice

What is the basis for the FISH algorithm?

### Options:

A- The Lagged Fibonacci generator
B- Prime number theory
C- Equations that describe an ellipse
D- The difficulty in factoring numbers

### Answer:

A

### Explanation:

The Lagged Fibonacci generator

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.

## Question 4

Question Type: MultipleChoice

Encryption of the same plain text with the same key results in the same cipher text. Use of an IV that is XORed with the first block of plain text solves this problem.

## Options:

A- CFB
B- GOST
C- ECB
D- RC4

## Answer:

C

## Explanation:

ECB

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

The simplest of the encryption modes is the electronic codebook (ECB) mode (named after conventional physical codebooks). The message is divided into blocks, and each block is encrypted separately.

The disadvantage of this method is a lack of diffusion. Because ECB encrypts identical plaintext blocks into identical ciphertext blocks, it does not hide data patterns well. ECB is not recommended for use in cryptographic protocols.

ECB mode can also make protocols without integrity protection even more susceptible to replay attacks, since each block gets decrypted in exactly the same way.

Incorrect answers:

RC4 - stream symmetric cipher that was created by Ron Rivest of RSA. Used in SSL and WEP.

GOST - the GOST block cipher (Magma), defined in the standard GOST 28147-89 (RFC 5830), is a Soviet and Russian government standard symmetric key block cipher with a block size of 64 bits. The original standard, published in 1989, did not give the cipher any name, but the most recent revision of the standard, GOST R 34.12-2015, specifies that it may be referred to as Magma. The GOST hash function is based on this cipher. The new standard also specifies a new 128-bit block cipher called Kuznyechik.

CFB - the process wherein the ciphertext block is encrypted then the ciphertext produced is XOR'd back with the plaintext to produce the current ciphertext block.

## Question 5

Question Type: MultipleChoice

Software for maintaining an on-the-fly-encrypted volume. Data is automatically encrypted right before it is saved, then decrypted right after it is loaded, all w/o user intervention.

### Options:

A- VPN
B- PGP
C- Cryptool
D- VeraCrypt



### Answer:

D

### Explanation:

VeraCrypt

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

VeraCrypt is a source-available freeware utility used for on-the-fly encryption (OTFE). It can create a virtual encrypted disk within a file or encrypt a partition or (in Windows) the entire storage device with pre-boot authentication.

Incorrect answers:

PGP - designed by Phil Zimmerman as a freeware e-mail security program and was released in 1991. It was the first widespread public key encryption program.

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

Cryptool - an open-source project that focuses on the free e-learning software CrypTool illustrating cryptographic and cryptanalytic concepts. According to 'Hakin9', CrypTool is worldwide the most widespread e-learning software in the field of cryptology.

## Question 6

Question Type: MultipleChoice

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

### Options:

A- PKI
B- DES
C- RSA
D- Diffie-Helmann

### Answer:

C

### 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.

Incorrect answers:

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

DES - The Data Encryption Standard is a symmetric-key algorithm for the encryption of digital data. Although its short key length of 56 bits makes it too insecure for applications, it has been highly influential in the advancement of cryptography.

Developed in the early 1970s at IBM and based on an earlier design by Horst Feistel, the algorithm was submitted to the National Bureau of Standards (NBS) following the agency's invitation to propose a candidate for the protection of sensitive, unclassified electronic government data. In 1976, after consultation with the National Security Agency (NSA), the NBS

selected a slightly modified version (strengthened against differential cryptanalysis, but weakened against brute-force attacks), which was published as an official Federal Information Processing Standard (FIPS) for the United States in 1977.

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

## Question 7

Question Type: MultipleChoice

The most widely used digital certificate standard. First issued July 3, 1988. It is a digital document that contains a public key signed by the trusted third party, which is known as a Certificate Authority, or C

### Options:

A- ElGamal
A- Relied on by S/MIME. Contains your name, info about you, and a signature of a person who issued the certificate.
B- RSA
C- PAP
D- X.509
X- 509

https://en.wikipedia.org/wiki/X.509
In cryptography, X.509 is a standard defining the format of public key certificates. X.509 certificates are used in many Internet protocols, including TLS/SSL, which is the basis for HTTPS, the secure protocol for browsing the web. They are also used in offline applications, like electronic signatures. An X.509 certificate contains a public key and an identity (a hostname, or an organization, or an individual), and is either signed by a certificate authority or self-signed. When a certificate is signed by a trusted certificate authority, or validated by other means, someone holding that certificate can rely on the public key it contains to establish secure communications with another party, or validate documents digitally signed by the corresponding private key.
Incorrect answers:
RSA - (Rivest--Shamir--Adleman) is a public-key cryptosystem that is widely used for secure data transmission.
ElGamal - asymmetric key encryption algorithm for public-key cryptography which is based on the Diffie--Hellman key exchange. It was described by Taher Elgamal in 1985.
PAP - used to authenticate users, but is no longer used because the information was sent in

cleartext.

## Answer:

D

## Question 8

Question Type: MultipleChoice

What is the basis for the difficulty in breaking RSA?

## Options:

A- Hashing
B- The birthday paradox
C- Equations that describe an elliptic curve
D- Factoring numbers

## Answer:

D

## Explanation:

Factoring numbers

https://en.wikipedia.org/wiki/RSA_(cryptosystem)

RSA (Rivest--Shamir--Adleman) is a public-key cryptosystem that is widely used for secure data transmission. It is also one of the oldest. The acronym RSA comes from the surnames of Ron Rivest, Adi Shamir, and Leonard Adleman, who publicly described the algorithm in 1977. An equivalent system was developed secretly, in 1973 at GCHQ (the British signals intelligence agency), by the English mathematician Clifford Cocks. That system was declassified in 1997.

In a public-key cryptosystem, the encryption key is public and distinct from the decryption key, which is kept secret (private). An RSA user creates and publishes a public key based on two large prime numbers, along with an auxiliary value. The prime numbers are kept secret. Messages can be encrypted by anyone, via the public key, but can only be decoded by someone who knows the prime numbers.