
# Free Questions for ISSAP by dumpshq

## Shared by Mccoy on 29-01-2024

**For More Free Questions and Preparation Resources**

**Check the Links on Last Page**

# Question 1

**Question Type:** MultipleChoice

Single Loss Expectancy (SLE) represents an organization's loss from a single threat. Which of the following formulas best describes the Single Loss Expectancy (SLE)?

## Options:

**A-** SLE = Asset Value (AV) * Exposure Factor (EF)

**B-** SLE = Asset Value (AV) * Annualized Rate of Occurrence (ARO)

**C-** SLE = Annualized Loss Expectancy (ALE) * Annualized Rate of Occurrence (ARO)

**D-** SLE = Annualized Loss Expectancy (ALE) * Exposure Factor (EF)

## Answer:

A

## Explanation:

the occurrence of a risk on an asset. It is mathematically expressed as follows:

Single Loss Expectancy (SLE) = Asset Value (AV) * Exposure Factor (EF)

where the Exposure Factor is represented in the impact of the risk over the asset, or percentage of asset lost. As an example, if the Asset

Value is reduced two thirds, the exposure factor value is .66. If the asset is completely lost, the Exposure Factor is 1.0. The result is a

monetary value in the same unit as the Single Loss Expectancy is expressed.

Answer options D, B, and C are incorrect. These are not valid formulas of SLE.

# Question 2

**Question Type:** **MultipleChoice**

You are responsible for security at a defense contracting firm. You are evaluating various possible encryption algorithms to use. One of the

algorithms you are examining is not integer based, uses shorter keys, and is public key based. What type of algorithm is this?

## Options:

**A-** Symmetric

**B-** None - all encryptions are integer based.

**C-** Elliptic Curve

**D-** RSA

### Answer:

C

### Explanation:

shorter key than integer based algorithms, and still obtains the same level of security.

Answer option B is incorrect. While integer based methods are the most common, they are not the only encryption algorithms.

Answer option D is incorrect. RSA is integer based, it uses the product of two very large prime numbers (i.e. integers).

## Question 3

**Question Type:** **MultipleChoice**

You are the Network Administrator for a bank. In addition to the usual security issues, you are concerned that your customers could be the victim of phishing attacks that use fake bank Web sites. Which of the following would protect against this?

## Options:

**A-** MAC

**B-** Mutual authentication

**C-** Three factor authentication

**D-** Two factor authentication

## Answer:

B

## Explanation:

server. For example some banks now have a user pick an image and a phrase that is stored. When they enter their user name, the bank Web

site will display their pre-selected image and phrase, before the user enters their password. If the user does not see their unique

image/phrase combination, then this is not really the bank Web site.

# Question 4

**Question Type:** MultipleChoice

An access control secures the confidentiality, integrity, and availability of the information and data of an organization. In which of the following categories can you deploy the access control? Each correct answer represents a part of the solution. Choose all that apply.

## Options:

**A-** Detective access control

**B-** Corrective access control

**C-** Administrative access control

**D-** Preventive access control

## Answer:

A, B, D

## Explanation:

Preventive access control: It prevents unwanted or unauthorized activities from happening.

Detective access control: It searches for unwanted or unauthorized activities.

Corrective access control: It helps the systems in getting their normal status after an unwanted or unauthorized activity has occurred.

Answer option C is incorrect. It is a category of implementation of the access control. The administrative access control is a set of policies and

procedures that are defined by an organization's security policy in order to implement an access control.

# Question 5

**Question Type:** MultipleChoice

Which of the following uses public key cryptography to encrypt the contents of files?

## Options:

**A-** EFS

**B-** DFS

**C-** NTFS

**D-** RFS

## Answer:

A

## Explanation:

access to the computer.

EFS is enabled in all versions of Windows meant for professional use from Windows 2000 onwards. However, since significant caveats exist

for its use, no files are encrypted by default and must explicitly be invoked by the user (in organizational settings, encryption can also be

mandated through Group Policy).

Answer option B is incorrect. Distributed File System (DFS) is a set of client and server services that allow an organization utilizing Microsoft

Windows servers to organize many distributed SMB file shares into a distributed file system. DFS provides location transparency and

redundancy to improve data availability in the face of failure or heavy load by allowing shares in multiple different locations to be logically

grouped under one folder, or DFS root.

Answer option C is incorrect. NTFS is an advanced file system designed for use specifically in Windows NT, Windows 2000/2003, and Windows

XP operating systems. It supports file system recovery, large storage media, long file names, and other features.

NTFS offers features such as disk quotas, distributed link tracking, compression, and mounted drives. NTFS also offers security features, such

as encryption and file and folder permissions. These features are not available on FAT volumes.

Answer option D is incorrect. The Reiser file system is the preferred partition type for a Linux-only computer. It is not used in a dual-booting

environment. The Reiser file system allows faster recovery from unexpected problems such as power failure. It uses a faster and more secure

method of writing data to the hard drive.

# Question 6

**Question Type:** **MultipleChoice**

Which of the following encryption methods comes under symmetric encryption algorithm? Each correct answer represents a complete solution. Choose three.

## Options:

**A-** DES

**B-** Blowfish

**C-** RC5

**D-** Diffie-Hellman

## Answer:

A, B, C

## Explanation:

to encrypt and decrypt data. Symmetric encryption algorithms are faster than public key encryption. Therefore, it is commonly used when a

message sender needs to encrypt a large amount of data. Data Encryption Standard (DES) uses symmetric encryption key algorithm to

encrypt data.