



SSCP^{Q&As}

System Security Certified Practitioner (SSCP)

Pass ISC SSCP Exam with 100% Guarantee

Free Download Real Questions & Answers **PDF** and **VCE** file from:

<https://www.pass4itsure.com/sscp.html>

100% Passing Guarantee
100% Money Back Assurance

Following Questions and Answers are all new published by ISC Official Exam Center

-  **Instant Download** After Purchase
-  **100% Money Back** Guarantee
-  **365 Days** Free Update
-  **800,000+** Satisfied Customers



**QUESTION 1**

Which of the following biometric characteristics cannot be used to uniquely authenticate an individual's identity?

- A. Retina scans
- B. Iris scans
- C. Palm scans
- D. Skin scans

Correct Answer: D

The following are typical biometric characteristics that are used to uniquely authenticate an individual's identity:
Fingerprints
Retina scans

Iris scans

Facial scans

Palm scans

Hand geometry

Voice

Handwritten signature dynamics

Source: KRUTZ, Ronald L. and VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, 2001, John Wiley and Sons, Page 39.

And: HARRIS, Shon, All-In-One CISSP Certification guide, McGraw-Hill/Osborne, 2002, chapter 4: Access Control (pages 127-131).

QUESTION 2

Kerberos depends upon what encryption method?

- A. Public Key cryptography.
- B. Secret Key cryptography.
- C. El Gamal cryptography.
- D. Blowfish cryptography.

Correct Answer: B

Kerberos depends on Secret Keys or Symmetric Key cryptography. Kerberos a third party authentication protocol. It was designed and developed in the mid 1980's by MIT. It is considered open source but is



copyrighted and owned by MIT. It relies on the user's secret keys. The password is used to encrypt and decrypt the keys.

This question asked specifically about encryption methods. Encryption methods can be SYMMETRIC (or secret key) in which encryption and decryption keys are the same, or ASYMMETRIC (aka 'Public Key') in which encryption and decryption keys differ.

'Public Key' methods must be asymmetric, to the extent that the decryption key CANNOT be easily derived from the encryption key. Symmetric keys, however, usually encrypt more efficiently, so they lend themselves to encrypting large amounts of data. Asymmetric encryption is often limited to ONLY encrypting a symmetric key and other information that is needed in order to decrypt a data stream, and the remainder of the encrypted data uses the symmetric key method for performance reasons. This does not in any way diminish the security nor the ability to use a public key to encrypt the data, since the symmetric key method is likely to be even MORE secure than the asymmetric method.

For symmetric key ciphers, there are basically two types: BLOCK CIPHERS, in which a fixed length block is encrypted, and STREAM CIPHERS, in which the data is encrypted one 'data unit' (typically 1 byte) at a time, in the same order it was received in.

The following answers are incorrect:

Public Key cryptography. Is incorrect because Kerberos depends on Secret Keys or Symmetric Key cryptography and not Public Key or Asymmetric Key cryptography.

El Gamal cryptography. Is incorrect because El Gamal is an Asymmetric Key encryption algorithm.

Blowfish cryptography. Is incorrect because Blowfish is a Symmetric Key encryption algorithm.

References:

OIG CBK Access Control (pages 181 - 184)

AIOv3 Access Control (pages 151 - 155)

Wikipedia http://en.wikipedia.org/wiki/Blowfish_%28cipher%29 ; http://en.wikipedia.org/wiki/El_Gamal

<http://www.mrp3.com/encrypt.html>

QUESTION 3

Which of the following should be emphasized during the Business Impact Analysis (BIA) considering that the BIA focus is on business processes?



- A. Composition
- B. Priorities
- C. Dependencies
- D. Service levels

Correct Answer: C

The Business Impact Analysis (BIA) identifies time-critical aspects of the critical business processes, and determines their maximum tolerable downtime. The BIA helps to identify organization functions, the capabilities of each organization unit to handle outages, and the priority and sequence of functions and applications to be recovered, identify resources required for recovery of those areas and interdependencies

In performing the Business Impact Analysis (BIA) it is very important to consider what the dependencies are. You cannot bring a system up if it depends on another system to be operational. You need to look at not only internal dependencies but external as well. You might not be able to get the raw materials for your business so dependencies are very important aspect of a BIA.

The BIA committee will not truly understand all business processes, the steps that must take place, or the resources and supplies these processes require. So the committee must gather this information from the people who do know-- department managers and specific employees throughout the organization. The committee starts by identifying the people who will be part of the BIA data-gathering sessions. The committee needs to identify how it will collect the data from the selected employees, be it through surveys, interviews, or workshops. Next, the team needs to collect the information by actually conducting surveys, interviews, and workshops. Data points obtained as part of the information gathering will be used later during analysis. It is important that the team members ask about how different tasks-- whether processes, transactions, or services, along with any relevant dependencies-- get accomplished within the organization.

The following answers are incorrect:

composition This is incorrect because it is not the best answer. While the make up of business may be important, if you have not determined the dependencies first you may not be able to bring the critical business processes to a ready state or have the materials on hand that are needed.

priorities This is incorrect because it is not the best answer. While the priorities of processes are important, if you have not determined the dependencies first you may not be able to bring the critical business processes to a ready state or have the materials on hand that are needed.

service levels This is incorrect because it is not the best answer. Service levels are not as important as dependencies.

Reference(s) used for this question:

Schneider, Andrew (2013-04-15). Official (ISC)2 Guide to the CISSP CBK, Third Edition : Business Continuity and Disaster Recovery Planning (Kindle Locations 188-191). . Kindle Edition.

and

Harris, Shon (2012-10-25). CISSP All-in-One uide, 6th Edition (Kindle Locations 18562-18568). McGraw-Hill. Kindle Edition.

QUESTION 4

Which of the following is the most important consideration in locating an alternate computing facility during the



development of a disaster recovery plan?

- A. It is unlikely to be affected by the same disaster.
- B. It is close enough to become operational quickly.
- C. It is close enough to serve its users.
- D. It is convenient to airports and hotels.

Correct Answer: A

You do not want the alternate or recovery site located in close proximity to the original site because the same event that create the situation in the first place might very well impact that site also.

From NIST: "The fixed site should be in a geographic area that is unlikely to be negatively affected by the same disaster event (e.g., weather-related impacts or power grid failure) as the organization's primary site.

The following answers are incorrect:

It is close enough to become operational quickly. Is incorrect because it is not the best answer. You'd want the alternate site to be close but if it is too close the same event could impact that site as well.

It is close enough to serve its users. Is incorrect because it is not the best answer. You'd want the alternate site to be close to users if applicable, but if it is too close the same event could impact that site as well It is convenient to airports and hotels. Is incorrect because it is not the best answer, it is more important that the same event does not impact the alternate site then convenience.

References:

OIG CBK Business Continuity and Disaster Recovery Planning (pages 368 - 369)

NIST document 800-34 pg 21

QUESTION 5

Which encryption algorithm is BEST suited for communication with handheld wireless devices?

- A. ECC (Elliptic Curve Cryptosystem)
- B. RSA
- C. SHA
- D. RC4

Correct Answer: A

As it provides much of the same functionality that RSA provides: digital signatures, secure key distribution, and encryption. One differing factor is ECC's efficiency. ECC is more efficient than RSA and any other asymmetric algorithm.



The following answers are incorrect because :

RSA is incorrect as it is less efficient than ECC to be used in handheld devices.

SHA is also incorrect as it is a hashing algorithm.

RC4 is also incorrect as it is a symmetric algorithm.

Reference : Shon Harris AIO v3 , Chapter-8 : Cryptography , Page : 631 , 638.

[Latest SSCP Dumps](#)

[SSCP Study Guide](#)

[SSCP Braindumps](#)