



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.passapply.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

The RSA Algorithm uses which mathematical concept as the basis of its encryption?

- A. Geometry
- B. 16-round ciphers
- C. PI (3.14159...)
- D. Two large prime numbers

Correct Answer: D

Source: TIPTON, et. al, Official (ISC)2 Guide to the CISSP CBK, 2007 edition, page 254.

And from the RSA web site, <http://www.rsa.com/rsalabs/node.asp?id=2214> :

The RSA cryptosystem is a public-key cryptosystem that offers both encryption and digital signatures (authentication). Ronald Rivest, Adi Shamir, and Leonard Adleman developed the RSA system in 1977 [RSA78]; RSA stands for the first letter in each of its inventors' last names.

The RSA algorithm works as follows: take two large primes, p and q , and compute their product $n = pq$; n is called the modulus. Choose a number, e , less than n and relatively prime to $(p-1)(q-1)$, which means e and $(p-1)(q-1)$ have no common factors except 1. Find another number d such that $(ed - 1)$ is divisible by $(p-1)(q-1)$. The values e and d are called the public and private exponents, respectively. The public key is the pair (n, e) ; the private key is (n, d) . The factors p and q may be destroyed or kept with the private key. It is currently difficult to obtain the private key d from the public key (n, e) . However if one could factor n into p and q , then one could obtain the private key d . Thus the security of the RSA system is based on the assumption that factoring is difficult. The discovery of an easy method of factoring would "break" RSA (see Question 3.1.3 and Question 2.3.3).

Here is how the RSA system can be used for encryption and digital signatures (in practice, the actual use is slightly different; see Questions 3.1.7 and 3.1.8):

Encryption

Suppose Alice wants to send a message m to Bob. Alice creates the ciphertext c by exponentiating: $c = me \pmod n$, where e and n are Bob's public key. She sends c to Bob. To decrypt, Bob also exponentiates: $m = cd \pmod n$; the relationship between e and d ensures that Bob correctly recovers m . Since only Bob knows d , only Bob can decrypt this message.

Digital Signature

Suppose Alice wants to send a message m to Bob in such a way that Bob is assured the message is both authentic, has not been tampered with, and from Alice. Alice creates a digital signature s by exponentiating: $s = md \pmod n$, where d and n are Alice's private key. She sends m and s to Bob. To verify the signature, Bob exponentiates and checks that the message m is recovered: $m = se \pmod n$, where e and n are Alice's public key.

Thus encryption and authentication take place without any sharing of private keys: each person uses only another's public key or their own private key. Anyone can send an encrypted message or verify a signed message, but only someone in possession of the correct private key can decrypt or sign a message.

QUESTION 2



What is called an exception to the search warrant requirement that allows an officer to conduct a search without having the warrant in-hand if probable cause is present and destruction of the evidence is deemed imminent?

- A. Evidence Circumstance Doctrine
- B. Exigent Circumstance Doctrine
- C. Evidence of Admissibility Doctrine
- D. Exigent Probable Doctrine

Correct Answer: B

An Exigent Circumstance is an unusual and time-sensitive circumstance that justifies conduct that might not be permissible or lawful in other circumstances.

For example, exigent circumstances may justify actions by law enforcement officers acting without a warrant such as a mortal danger to a young child. Examples of other exigent circumstances include protecting evidence or property from imminent destruction.

In *US v Martinez*, Justice Thomas of the United States Court of Appeal used these words:

"As a general rule, we define exigent circumstances as those circumstances that would cause a reasonable person to believe that entry was necessary to prevent physical harm to the officers or other persons, the destruction of relevant evidence, the escape of the suspect, or some other consequence improperly frustrating legitimate law enforcement efforts."

In *Alvarado*, Justice Blackburn of the Court of Appeals of Georgia referred to exigent circumstances in the context of a drug bust: "The exigent circumstance doctrine provides that when probable cause has been established to believe that evidence will be removed or destroyed before a warrant can be obtained, a warrantless search and seizure can be justified. As many courts have noted, the need for the exigent circumstance doctrine is particularly compelling in narcotics cases, because contraband and records can be easily and quickly destroyed while a search is progressing. Police officers relying on this exception must demonstrate an objectively reasonable basis for deciding that immediate action is required."

All of the other answers were only detractors made up and not legal terms.

Reference(s) used for this question:

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 313.

and

<http://www.duhaime.org/LegalDictionary/E/ExigentCircumstances.aspx>

QUESTION 3

Risk reduction in a system development life-cycle should be applied:

- A. Mostly to the initiation phase.
- B. Mostly to the development phase.
- C. Mostly to the disposal phase.



D. Equally to all phases.

Correct Answer: D

Risk is defined as the combination of the probability that a particular threat source will exploit, or trigger, a particular information system vulnerability and the resulting mission impact should this occur. Previously, risk avoidance was a common IT security goal. That changed as the nature of the risk became better understood. Today, it is recognized that elimination of all risk is not cost-effective. A cost-benefit analysis should be conducted for each proposed control. In some cases, the benefits of a more secure system may not justify the direct and indirect costs. Benefits include more than just prevention of monetary loss; for example, controls may be essential for maintaining public trust and confidence. Direct costs include the cost of purchasing and installing a given technology; indirect costs include decreased system performance and additional training. The goal is to enhance mission/business capabilities by managing mission/ business risk to an acceptable level.

Source: STONEBURNER, Gary and al, National Institute of Standards and Technology (NIST), NIST Special Publication 800-27, Engineering Principles for Information Technology Security (A Baseline for Achieving Security), June 2001 (page 8).

QUESTION 4

In an online transaction processing system (OLTP), which of the following actions should be taken when erroneous or invalid transactions are detected?

- A. The transactions should be dropped from processing.
- B. The transactions should be processed after the program makes adjustments.
- C. The transactions should be written to a report and reviewed.
- D. The transactions should be corrected and reprocessed.

Correct Answer: C

In an online transaction processing system (OLTP) all transactions are recorded as they occur. When erroneous or invalid transactions are detected the transaction can be recovered by reviewing the logs.

As explained in the ISC2 OIG:

OLTP is designed to record all of the business transactions of an organization as they occur. It is a data processing system facilitating and managing transaction-oriented applications. These are characterized as a system used by many concurrent users who are actively adding and modifying data to effectively change real-time data.

OLTP environments are frequently found in the finance, telecommunications, insurance, retail, transportation, and travel industries. For example, airline ticket agents enter data in the database in real-time by creating and modifying travel reservations, and these are increasingly joined by users directly making their own reservations and purchasing tickets through airline company Web sites as well as discount travel Web site portals. Therefore, millions of people may be accessing the same flight database every day, and dozens of people may be looking at a specific flight at the same time.

The security concerns for OLTP systems are concurrency and atomicity.

Concurrency controls ensure that two users cannot simultaneously change the same data, or that one user cannot make changes before another user is finished with it. In an airline ticket system, it is critical for an agent processing a reservation to complete the transaction, especially if it is the last seat available on the plane.



Atomicity ensures that all of the steps involved in the transaction complete successfully. If one step should fail, then the other steps should not be able to complete. Again, in an airline ticketing system, if the agent does not enter a name into the name data field correctly, the transaction should not be able to complete. OLTP systems should act as a monitoring system and detect when individual processes abort, automatically restart an aborted process, back out of a transaction if necessary, allow distribution of multiple copies of application servers across machines, and perform dynamic load balancing.

A security feature uses transaction logs to record information on a transaction before it is processed, and then mark it as processed after it is done. If the system fails during the transaction, the transaction can be recovered by reviewing the transaction logs.

Checkpoint restart is the process of using the transaction logs to restart the machine by running through the log to the last checkpoint or good transaction. All transactions following the last checkpoint are applied before allowing users to access the data again.

Wikipedia has nice coverage on what is OLTP:

Online transaction processing, or OLTP, refers to a class of systems that facilitate and manage transaction-oriented applications, typically for data entry and retrieval transaction processing. The term is somewhat ambiguous; some understand a "transaction" in the context of computer or database transactions, while others (such as the Transaction Processing Performance Council) define it in terms of business or commercial transactions.

OLTP has also been used to refer to processing in which the system responds immediately to user requests. An automatic teller machine (ATM) for a bank is an example of a commercial transaction processing application.

The technology is used in a number of industries, including banking, airlines, mailorder, supermarkets, and manufacturing. Applications include electronic banking, order processing, employee time clock systems, e-commerce, and eTrading.

There are two security concerns for OLTP system: Concurrency and Atomicity

ATOMICITY In database systems, atomicity (or atomicness) is one of the ACID transaction properties. In an atomic transaction, a series of database operations either all occur, or nothing occurs. A guarantee of atomicity prevents updates to the database occurring only partially, which can cause greater problems than rejecting the whole series outright.

The etymology of the phrase originates in the Classical Greek concept of a fundamental and indivisible component; see atom.

An example of atomicity is ordering an airline ticket where two actions are required: payment, and a seat reservation. The potential passenger must either:

both pay for and reserve a seat; OR

neither pay for nor reserve a seat.

The booking system does not consider it acceptable for a customer to pay for a ticket without securing the seat, nor to reserve the seat without payment succeeding.

CONCURRENCY

Database concurrency controls ensure that transactions occur in an ordered fashion.

The main job of these controls is to protect transactions issued by different users/applications from the effects of each other. They must preserve the four characteristics of database transactions ACID test: Atomicity, Consistency, Isolation, and Durability. Read <http://en.wikipedia.org/wiki/ACID> for more details on the ACID test.



Thus concurrency control is an essential element for correctness in any system where two database transactions or more, executed with time overlap, can access the same data, e.g., virtually in any general-purpose database system. A well established concurrency control theory exists for database systems: serializability theory, which allows to effectively design and analyze concurrency control methods and mechanisms. Concurrency is not an issue in itself, it is the lack of proper concurrency controls that makes it a serious issue.

The following answers are incorrect:

The transactions should be dropped from processing. Is incorrect because the transactions are processed and when erroneous or invalid transactions are detected the transaction can be recovered by reviewing the logs.

The transactions should be processed after the program makes adjustments. Is incorrect because the transactions are processed and when erroneous or invalid transactions are detected the transaction can be recovered by reviewing the logs.

The transactions should be corrected and reprocessed. Is incorrect because the transactions are processed and when erroneous or invalid transactions are detected the transaction can be recovered by reviewing the logs.

References:

Hernandez CISSP, Steven (2012-12-21). Official (ISC)2 Guide to the CISSP CBK, Third Edition ((ISC)2 Press) (Kindle Locations 12749-12768). Auerbach Publications. Kindle Edition.

and

http://en.wikipedia.org/wiki/Online_transaction_processing

and

<http://databases.about.com/od/administration/g/concurrency.htm>

QUESTION 5

As a result of a risk assessment, your security manager has determined that your organization needs to implement an intrusion detection system that can detect unknown attacks and can watch for unusual traffic behavior, such as a new service appearing on the network. What type of intrusion detection system would you select?

- A. Protocol anomaly based
- B. Pattern matching
- C. Stateful matching
- D. Traffic anomaly-based

Correct Answer: D

Traffic anomaly-based is the correct choice. An anomaly based IDS can detect unknown attacks. A traffic anomaly based IDS identifies any unacceptable deviation from expected behavior based on network traffic.

Protocol anomaly based is not the best choice as while a protocol anomaly based IDS can identify unknown attacks, this type of system is more suited to identifying deviations from established protocol standards such as HTTP. This type of IDS faces problems in analyzing complex or custom protocols.

Pattern matching is not the best choice as a pattern matching IDS cannot identify unknown attacks. This type of system



can only compare packets against signatures of known attacks.

Stateful matching is not the best choice as a statful matching IDS cannot identify unknown attacks. This type of system works by scanning traffic streams for patterns or signatures of attacks.

Reference:

Official guide to the CISSP CBK. pages 198 to 201

QUESTION 6

The following is NOT a security characteristic we need to consider while choosing a biometric identification systems:

- A. data acquisition process
- B. cost
- C. enrollment process
- D. speed and user interface

Correct Answer: B

Cost is a factor when considering Biometrics but it is not a security characteristic.

All the other answers are incorrect because they are security characteristics related to Biometrics.

data acquisition process can cause a security concern because if the process is not fast and efficient it can discourage individuals from using the process.

enrollment process can cause a security concern because the enrollment process has to be quick and efficient. This process captures data for authentication.

speed and user interface can cause a security concern because this also impacts the users acceptance rate of biometrics. If they are not comfortable with the interface and speed they might sabotage the devices or otherwise attempt to circumvent them.

References:

OIG Access Control (Biometrics) (pgs 165-167)

From: TIPTON, Harold F. and KRAUSE, MICKI, Information Security Management Handbook, 4th Edition, Volume 1, Pages 5-6.

in process of correction

QUESTION 7

Which of the following statements pertaining to PPTP (Point-to-Point Tunneling Protocol) is incorrect?

- A. PPTP allow the tunnelling of any protocols that can be carried within PPP.
- B. PPTP does not provide strong encryption.



- C. PPTP does not support any token-based authentication method for users.
- D. PPTP is derived from L2TP.

Correct Answer: D

PPTP is an encapsulation protocol based on PPP that works at OSI layer 2 (Data Link) and that enables a single point-to-point connection, usually between a client and a server. While PPTP depends on IP to establish its connection. As currently implemented, PPTP encapsulates PPP packets using a modified version of the generic routing encapsulation (GRE) protocol, which gives PPTP to the flexibility of handling protocols other than IP, such as IPX and NETBEUI over IP networks. PPTP does have some limitations:

It does not provide strong encryption for protecting data, nor does it support any token-based methods for authenticating users.

L2TP is derived from L2F and PPTP, not the opposite.

QUESTION 8

Which of the following teams should NOT be included in an organization's contingency plan?

- A. Damage assessment team
- B. Hardware salvage team
- C. Tiger team
- D. Legal affairs team

Correct Answer: C

According to NIST's Special publication 800-34, a capable recovery strategy will require some or all of the following functional groups: Senior management official, management team, damage assessment team, operating system administration team, systems software team, server recovery team, LAN/WAN recovery team, database recovery team, network operations recovery team, telecommunications team, hardware salvage team, alternate site recovery coordination team, original site restoration/salvage coordination team, test team, administrative support team, transportation and relocation team, media relations team, legal affairs team, physical/personal security team, procurements team. Ideally, these teams would be staffed with the personnel responsible for the same or similar operation under normal conditions. A tiger team, originally a U.S. military jargon term, defines a team (of sneakers) whose purpose is to penetrate security, and thus test security measures. Used today for teams performing ethical hacking.

Source: SWANSON, Marianne, and al., National Institute of Standards and Technology (NIST), NIST Special Publication 800-34, Contingency Planning Guide for Information Technology Systems, December 2001 (page 23).

QUESTION 9

Which of the following is NOT a correct notation for an IPv6 address?

- A. 2001:0db8:0:0:0:0:1428:57ab
- B. ABCD:EF01:2345:6789:ABCD:EF01:2345:6789



C. ::1

D. 2001:DB8::8:800::417A

Correct Answer: D

This is not a correct notation for an IPv6 address because the the ":" can only appear once in an address. The use of "::" is a shortcut notation that indicates one or more groups of 16 bits of zeros. ::1 is the loopback address using the special notation Reference: IP Version 6 Addressing Architecture <http://tools.ietf.org/html/rfc4291#section-2.1>

QUESTION 10

Which of the following is not a DES mode of operation?

A. Cipher block chaining

B. Electronic code book

C. Input feedback

D. Cipher feedback

Correct Answer: C

Output feedback (OFB) is a DES mode of operation, not input feedback.

Source: KRUTZ, Ronald L. and VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, John Wiley and Sons, 2001, Chapter 4: Cryptography (page 149).

QUESTION 11

Public Key Infrastructure (PKI) uses asymmetric key encryption between parties. The originator encrypts information using the intended recipient's "public" key in order to get confidentiality of the data being sent. The recipients use their own "private" key to decrypt the information. The "Infrastructure" of this methodology ensures that:

A. The sender and recipient have reached a mutual agreement on the encryption key exchange that they will use.

B. The channels through which the information flows are secure.

C. The recipient's identity can be positively verified by the sender.

D. The sender of the message is the only other person with access to the recipient's private key.

Correct Answer: C

Through the use of Public Key Infrastructure (PKI) the recipient's identity can be positively verified by the sender.

The sender of the message knows he is using a Public Key that belongs to a specific user. He can validate through the Certification Authority (CA) that a public key is in fact the valid public key of the receiver and



the receiver is really who he claims to be. By using the public key of the recipient, only the recipient using the matching private key will be able to decrypt the message. When you wish to achieve confidentiality, you encrypt the message with the recipient public key.

If the sender would wish to prove to the recipient that he is really who he claims to be then the sender would apply a digital signature on the message before encrypting it with the public key of the receiver. This would provide Confidentiality and Authenticity of the message.

A PKI (Public Key Infrastructure) enables users of an insecure public network, such as the Internet, to securely and privately exchange data through the use of public key-pairs that are obtained and shared through a trusted authority, usually referred to as a Certificate Authority.

The PKI provides for digital certificates that can vouch for the identity of individuals or organizations, and for directory services that can store, and when necessary, revoke those digital certificates. A PKI is the underlying technology that addresses the issue of trust in a normally untrusted environment.

The following answers are incorrect:

The sender and recipient have reached a mutual agreement on the encryption key exchange that they will use. Is incorrect because through the use of Public Key Infrastructure (PKI), the parties do not have to have a mutual agreement. They have a trusted 3rd party Certificate Authority to perform the verification of the sender.

The channels through which the information flows are secure. Is incorrect because the use of Public Key Infrastructure (PKI) does nothing to secure the channels.

The sender of the message is the only other person with access to the recipient's private key. Is incorrect because the sender does not have access to the recipient's private key though Public Key Infrastructure (PKI).

Reference(s) used for this question:

OIG CBK Cryptography (pages 253 - 254)

QUESTION 12

Which of the following are suitable protocols for securing VPN connections at the lower layers of the OSI model?

- A. S/MIME and SSH
- B. TLS and SSL



- C. IPsec and L2TP
- D. PKCS#10 and X.509

Correct Answer: C

Reference: HARRIS, Shon, All-In-One CISSP Certification uide, 2001, McGraw- Hill/Osborne, page 467; SMITH, Richard E., Internet Cryptography, 1997, Addison-Wesley Pub Co.

QUESTION 13

A department manager has read access to the salaries of the employees in his/her department but not to the salaries of employees in other departments. A database security mechanism that enforces this policy would typically be said to provide which of the following?

- A. Content-dependent access control
- B. Context-dependent access control
- C. Least privileges access control
- D. Ownership-based access control

Correct Answer: A

When access control is based on the content of an object, it is considered to be content dependent access control.

Content-dependent access control is based on the content itself.

The following answers are incorrect:

context-dependent access control. Is incorrect because this type of control is based on what the context is, facts about the data rather than what the object contains. least privileges access control. Is incorrect because this is based on the least amount of rights needed to perform their jobs and not based on what is contained in the database. ownership-based access control. Is incorrect because this is based on the owner of the data and and not based on what is contained in the database.

References:

OIG CBK Access Control (page 191)

QUESTION 14

A business continuity plan should list and prioritize the services that need to be brought back after a disaster strikes. Which of the following services is more likely to be of primary concern in the context of what your Disaster Recovery Plan would include?

- A. Marketing/Public relations
- B. Data/Telecomm/IS facilities
- C. IS Operations



D. Facilities security

Correct Answer: B

The main concern when recovering after a disaster is data, telecomm and IS facilities. Other services, in descending priority order are: IS operations, IS support services, market structure, marketing/public relations, customer service and systems support, market regulation/surveillance, listing, application development, accounting services, facilities, human resources, facilities security, legal and Office of the Secretary, national sales. Source: BARNES, James C. and ROTHSTEIN, Philip J., A Guide to Business Continuity Planning, John Wiley and Sons, 2001 (page 129).

QUESTION 15

What type of cable is used with 100Base-TX Fast Ethernet?

- A. Fiber-optic cable
- B. Category 3 or 4 unshielded twisted-pair (UTP).
- C. Category 5 unshielded twisted-pair (UTP).
- D. RG-58 cable.

Correct Answer: C

This is the type of cabling recommended for 100Base-TX networks.

Fiber-optic cable is incorrect. Incorrect media type for 100Base-TX -- 100Base-FX would denote fiber optic cabling. "Category 3 or 4 unshielded twisted-pair (UTP)" is incorrect. These types are not recommended for

100Mbps operation. RG-58 cable is incorrect. Incorrect media type for 100Base-TX. References CBK, p. 428 AIO3, p. 455

[Latest SSCP Dumps](#)

[SSCP VCE Dumps](#)

[SSCP Study Guide](#)