B. The Contingency Planning Coordinator should make sure that every employee gets an up-to-date copy of the plan.
C. Strict version control should be maintained.
D. Copies of the plan should be provided to recovery personnel for storage offline at home and office.

Correct Answer: B
Explanation:
Because the contingency plan contains potentially sensitive operational and personnel information, its distribution should be marked accordingly and controlled. Not all employees would obtain a copy, but only those involved in the execution of the plan.
All other statements are correct.

NOTE FROM CLEMENT:
I have received multiple emails stating the explanations contradict the correct answer. It seems many people have a hard time with negative question. In this case the Incorrect choice (the one that is not true) is the correct choice. Be very carefull of such questions, you will get some on the real exam as well.

Reference(s) used for this question:
SWANSON, Marianne, & al., National Institute of Standards and Technology (NIST), NIST Special Publication 800-34, Contingency Planning Guide for Information Technology Systems

QUESTION 660
A prolonged high voltage is a:

A. spike
B. blackout
C. surge
D. fault

Correct Answer: C
Explanation:
A prolonged high voltage is a surge.
From: HARRIS, Shon, All-In-One CISSP Certification Exam Guide, 3rd. Edition McGraw-Hill/Osborne, 2005, page 368.

QUESTION 661
Which of the following assertions is NOT true about pattern matching and anomaly detection in intrusion detection?

A. Anomaly detection tends to produce more data
B. A pattern matching IDS can only identify known attacks
C. Stateful matching scans for attack signatures by analyzing individual packets instead of traffic streams
D. An anomaly-based engine develops baselines of normal traffic activity and throughput, and alerts on deviations from these baselines

Correct Answer: C
Explanation:
This is wrong which makes this the correct choice. This statement is not true as stateful matching scans for attack signatures by analyzing traffic streams rather than individual packets. Stateful matching intrusion detection takes pattern matching to the next level.

As networks become faster there is an emerging need for security analysis techniques that can

keep up with the increased network throughput. Existing network-based intrusion detection sensors can barely keep up with bandwidths of a few hundred Mbps. Analysis tools that can deal with higher throughput are unable to maintain state between different steps of an attack or they are limited to the analysis of packet headers.

The following answers are all incorrect:

Anomaly detection tends to produce more data is true as an anomaly-based IDS produces a lot of data as any activity outside of expected behavior is recorded.

A pattern matching IDS can only identify known attacks is true as a pattern matching IDS works by comparing traffic streams against signatures. These signatures are created for known attacks.

An anomaly-based engine develops baselines of normal traffic activity and throughput, and alerts on deviations from these baselines is true as the assertion is a characteristic of a statistical anomaly-based IDS.

Reference:
Official guide to the CISSP CBK. Pages 198 to 201
http://cs.ucsb.edu/~vigna/publications/2003_vigna_robertson_kher_kemmerer_ACSAC03.pdf

QUESTION 662
What is NOT true with pre shared key authentication within IKE / IPsec protocol?

A. Pre shared key authentication is normally based on simple passwords
B. Needs a Public Key Infrastructure (PKI) to work
C. IKE is used to setup Security Associations
D. IKE builds upon the Oakley protocol and the ISAKMP protocol.

Correct Answer: B
Explanation:
Internet Key Exchange (IKE or IKEv2) is the protocol used to set up a security association (SA) in the IPsec protocol suite. IKE builds upon the Oakley protocol and ISAKMP. IKE uses X.509 certificates for authentication which are either pre-shared or distributed using DNS (preferably with DNSSEC) and a Diffie瑓ellman key exchange to set up a shared session secret from which cryptographic keys are derived.

Internet Key Exchange (IKE) Internet key exchange allows communicating partners to prove their identity to each other and establish a secure communication channel, and is applied as an authentication component of IPSec.

IKE uses two phases:

Phase 1: In this phase, the partners authenticate with each other, using one of the following: Shared Secret: A key that is exchanged by humans via telephone, fax, encrypted e-mail, etc. Public Key Encryption: Digital certificates are exchanged. Revised mode of Public Key Encryption: To reduce the overhead of public key encryption, a nonce (a Cryptographic function that refers to a number or bit string used only once, in security engineering) is encrypted with the communicating partner's public key, and the peer's identity is encrypted with symmetric encryption using the nonce as the key. Next, IKE establishes a temporary security association and secure tunnel to protect the rest of the key exchange. Phase 2: The peers' security associations are established, using the secure tunnel and temporary SA created at the end of phase 1.

The following reference(s) were used for this question:

Hernandez CISSP, Steven (2012-12-21). Official (ISC)2 Guide to the CISSP CBK, Third Edition ((ISC)2 Press) (Kindle Locations 7032-7048). Auerbach Publications. Kindle Edition.
RFC 2409 at http://tools.ietf.org/html/rfc2409
http://en.wikipedia.org/wiki/Internet_Key_Exchange

QUESTION 663
Where parties do not have a shared secret and large quantities of sensitive information must be passed, the most efficient means of transferring information is to use Hybrid Encryption Methods. What does this mean?

A. Use of public key encryption to secure a secret key, and message encryption using the secret key.
B. Use of the recipient's public key for encryption and decryption based on the recipient's private key.
C. Use of software encryption assisted by a hardware encryption accelerator.
D. Use of elliptic curve encryption.

Correct Answer: A
Explanation:
A Public Key is also known as an asymmetric algorithm and the use of a secret key would be a symmetric algorithm.

The following answers are incorrect:

Use of the recipient's public key for encryption and decryption based on the recipient's private key. Is incorrect this would be known as an asymmetric algorithm.
Use of software encryption assisted by a hardware encryption accelerator. This is incorrect, it is a distractor.
Use of Elliptic Curve Encryption. Is incorrect this would use an asymmetric algorithm.

QUESTION 664
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
Explanation:
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 mod n, where e and n are Bob's public key. She sends c to Bob. To decrypt, Bob also exponentiates: m = cd mod 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 mod 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 mod 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 665
Which of the following offers security to wireless communications?

A. S-WAP
B. WTLS
C. WSP
D. WDP

Correct Answer: B
Explanation:
Wireless Transport Layer Security (WTLS) is a communication protocol that allows wireless devices to send and receive encrypted information over the Internet. S- WAP is not defined. WSP (Wireless Session Protocol) and WDP (Wireless Datagram Protocol) are part of Wireless Access Protocol (WAP).
Source: KRUTZ, Ronald L.& VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, John Wiley & Sons, 2001, Chapter 4: Cryptography (page 173).

QUESTION 666
Which of the following would best define a digital envelope?

A. A message that is encrypted and signed with a digital certificate.
B. A message that is signed with a secret key and encrypted with the sender's private key.
C. A message encrypted with a secret key attached with the message. The secret key is encrypted with the public key of the receiver.
D. A message that is encrypted with the recipient's public key and signed with the sender's private key.

Correct Answer: C
Explanation:
A digital envelope for a recipient is a combination of encrypted data and its encryption key in an encrypted form that has been prepared for use of the recipient.
It consists of a hybrid encryption scheme in sealing a message, by encrypting the data and sending both it and a protected form of the key to the intended recipient, so that one else can open the message.
In PKCS #7, it means first encrypting the data using a symmetric encryption algorithm and a secret key, and then encrypting the secret key using an asymmetric encryption algorithm and the public key of the intended recipient.
Source: SHIREY, Robert W., RFC2828: Internet Security Glossary, may 2000.

QUESTION 667
Which type of encryption is considered to be unbreakable if the stream is truly random and is as large as the plaintext and never reused in whole or part?

A. One Time Pad (OTP)
B. One time Cryptopad (OTC)
C. Cryptanalysis
D. Pretty Good Privacy (PGP)

Correct Answer: A
Explanation:
OTP or One Time Pad is considered unbreakable if the key is truly random and is as large as the plaintext and never reused in whole or part AND kept secret.

In cryptography, a one-time pad is a system in which a key generated randomly is used only once to encrypt a message that is then decrypted by the receiver using the matching one-time pad and key. Messages encrypted with keys based on randomness have the advantage that there is theoretically no way to "break the code" by analyzing a succession of messages. Each encryption is unique and bears no relation to the next encryption so that some pattern can be detected.

With a one-time pad, however, the decrypting party must have access to the same key used to encrypt the message and this raises the problem of how to get the key to the decrypting party safely or how to keep both keys secure. One-time pads have sometimes been used when the both parties started out at the same physical location and then separated, each with knowledge of the keys in the one-time pad. The key used in a one- time pad is called a secret key because if it is revealed, the messages encrypted with it can easily be deciphered.

One-time pads figured prominently in secret message transmission and espionage before and during World War II and in the Cold War era. On the Internet, the difficulty of securely controlling secret keys led to the invention of public key cryptography.

The biggest challenge with OTP was to get the pad security to the person or entity you wanted to communicate with. It had to be done in person or using a trusted courrier or custodian. It certainly did not scale up very well and it would not be usable for large quantity of data that needs to be encrypted as we often time have today.

The following answers are incorrect:

One time Cryptopad: Almost but this isn't correct. Cryptopad isn't a valid term in cryptography.

Cryptanalysis: Sorry, incorrect. Cryptanalysis is the process of analyzing information in an effort