PGP uses which of the following to encrypt data?

A. An asymmetric encryption algorithm
B. A symmetric encryption algorithm
C. A symmetric key distribution system
D. An X.509 digital certificate

Correct Answer: B
Explanation:
Notice that the question specifically asks what PGP uses to encrypt For this, PGP uses an symmetric key algorithm. PGP then uses an asymmetric key algorithm to encrypt the session key and then send it securely to the receiver. It is an hybrid system where both types of ciphers are being used for different purposes.

Whenever a question talks about the bulk of the data to be sent, Symmetric is always best to choice to use because of the inherent speed within Symmetric Ciphers. Asymmetric ciphers are 100 to 1000 times slower than Symmetric Ciphers.

The other answers are not correct because:

"An asymmetric encryption algorithm" is incorrect because PGP uses a symmetric algorithm to encrypt data.

"A symmetric key distribution system" is incorrect because PGP uses an asymmetric algorithm for the distribution of the session keys used for the bulk of the data.

"An X.509 digital certificate" is incorrect because PGP does not use X.509 digital certificates to encrypt the data, it uses a session key to encrypt the data.

References:
Official ISC2 Guide page: 275
All in One Third Edition page: 664 - 665

QUESTION 682
What principle focuses on the uniqueness of separate objects that must be joined together to perform a task? It is sometimes referred to as "what each must bring" and joined together when getting access or decrypting a file. Each of which does not reveal the other?

A. Dual control
B. Separation of duties
C. Split knowledge
D. Need to know

Correct Answer: C
Explanation:
Split knowledge involves encryption keys being separated into two components, each of which does not reveal the other. Split knowledge is the other complementary access control principle to dual control.

In cryptographic terms, one could say dual control and split knowledge are properly implemented if no one person has access to or knowledge of the content of the complete cryptographic key being protected by the two rocesses.

The sound implementation of dual control and split knowledge in a cryptographic environment

necessarily means that the quickest way to break the key would be through the best attack known for the algorithm of that key. The principles of dual control and split knowledge primarily apply to access to plaintext keys.

Access to cryptographic keys used for encrypting and decrypting data or access to keys that are encrypted under a master key (which may or may not be maintained under dual control and split knowledge) do not require dual control and split knowledge. Dual control and split knowledge can be summed up as the determination of any part of a key being protected must require the collusion between two or more persons with each supplying unique cryptographic materials that must be joined together to access the protected key.

Any feasible method to violate the axiom means that the principles of dual control and split knowledge are not being upheld.

Split knowledge is the unique "what each must bring" and joined together when implementing dual control. To illustrate, a box containing petty cash is secured by one combination lock and one keyed lock. One employee is given the combination to the combo lock and another employee has possession of the correct key to the keyed lock.

In order to get the cash out of the box both employees must be present at the cash box at the same time. One cannot open the box without the other. This is the aspect of dual control.

On the other hand, split knowledge is exemplified here by the different objects (the combination to the combo lock and the correct physical key), both of which are unique and necessary, that each brings to the meeting. Split knowledge focuses on the uniqueness of separate objects that must be joined together.

Dual control has to do with forcing the collusion of at least two or more persons to combine their split knowledge to gain access to an asset. Both split knowledge and dual control complement each other and are necessary functions that implement the segregation of duties in high integrity cryptographic environments.

The following are incorrect answers:
Dual control is a procedure that uses two or more entities (usually persons) operating in concert to protect a system resource, such that no single entity acting alone can access that resource. Dual control is implemented as a security procedure that requires two or more persons to come together and collude to complete a process. In a cryptographic system the two (or more) persons would each supply a unique key, that when taken together, performs a cryptographic process. Split knowledge is the other complementary access control principle to dual control.

Separation of duties - The practice of dividing the steps in a system function among different individuals, so as to keep a single individual from subverting the process. The need-to-know principle requires a user having necessity for access to, knowledge of, or possession of specific information required to perform official tasks or services.

Reference(s) used for this question:

Schneiter, Andrew (2013-04-15). Official (ISC)2 Guide to the CISSP CBK, Third Edition. Cryptography (Kindle Locations 1621-1635). . Kindle Edition.
Schneiter, Andrew (2013-04-15). Official (ISC)2 Guide to the CISSP CBK, Third Edition. Cryptography (Kindle Locations 1643-1650). . Kindle Edition.
Shon Harris, CISSP All In One (AIO), 6th Edition , page 126

QUESTION 683

Which of the following can best be defined as a cryptanalysis technique in which the analyst tries to determine the key from knowledge of some plaintext-ciphertext pairs?

A. A known-plaintext attack
B. A known-algorithm attack
C. A chosen-ciphertext attack
D. A chosen-plaintext attack

Correct Answer: A
Explanation:
RFC2828 (Internet Security Glossary) defines a known-plaintext attack as a cryptanalysis technique in which the analyst tries to determine the key from knowledge of some plaintext-ciphertext pairs (although the analyst may also have other clues, such as the knowing the cryptographic algorithm). A chosen-ciphertext attack is defined as a cryptanalysis technique in which the analyst tries to determine the key from knowledge of plaintext that corresponds to ciphertext selected (i.e., dictated) by the analyst. A chosen- plaintext attack is a cryptanalysis technique in which the analyst tries to determine the key from knowledge of ciphertext that corresponds to plaintext selected (i.e., dictated) by the analyst. The other choice is a distracter.

The following are incorrect answers:

A chosen-plaintext attacks
The attacker has the plaintext and ciphertext, but can choose the plaintext that gets encrypted to see the corresponding ciphertext. This gives her more power and possibly a deeper understanding of the way the encryption process works so she can gather more information about the key being used. Once the key is discovered, other messages encrypted with that key can be decrypted.

A chosen-ciphertext attack
In chosen-ciphertext attacks, the attacker can choose the ciphertext to be decrypted and has access to the resulting decrypted plaintext. Again, the goal is to figure out the key. This is a harder attack to carry out compared to the previously mentioned attacks, and the attacker may need to have control of the system that contains the cryptosystem.

A known-algorithm attack
Knowing the algorithm does not give you much advantage without knowing the key. This is a bogus detractor. The algorithm should be public, which is the Kerckhoffs's Principle . The only secret should be the key.

Reference(s) used for this question:
Source: SHIREY, Robert W., RFC2828: Internet Security Glossary, may 2000.
Harris, Shon (2012-10-25). CISSP All-in-One Exam Guide, 6th Edition (p. 866). McGraw- Hill. Kindle Edition.
Kerckhoffs's Principle

QUESTION 684
The Data Encryption Standard (DES) encryption algorithm has which of the following characteristics?

A. 64 bits of data input results in 56 bits of encrypted output
B. 128 bit key with 8 bits used for parity
C. 64 bit blocks with a 64 bit total key length
D. 56 bits of data input results in 56 bits of encrypted output

Correct Answer: C
Explanation:
DES works with 64 bit blocks of text using a 64 bit key (with 8 bits used for parity, so the effective key length is 56 bits).

Some people are getting the Key Size and the Block Size mixed up. The block size is usually a specific length. For example DES uses block size of 64 bits which results in 64 bits of encrypted data for each block. AES uses a block size of 128 bits, the block size on AES can only be 128 as per the published standard FIPS-197.

A DES key consists of 64 binary digits ("0"s or "1"s) of which 56 bits are randomly generated and used directly by the algorithm. The other 8 bits, which are not used by the algorithm, may be used for error detection. The 8 error detecting bits are set to make the parity of each 8-bit byte of the key odd, i.e., there is an odd number of "1"s in each 8-bit byte1. Authorized users of encrypted computer data must have the key that was used to encipher the data in order to decrypt it.

IN CONTRAST WITH AES
The input and output for the AES algorithm each consist of sequences of 128 bits (digits with values of 0 or 1). These sequences will sometimes be referred to as blocks and the number of bits they contain will be referred to as their length. The Cipher Key for the AES algorithm is a sequence of 128, 192 or 256 bits. Other input, output and Cipher Key lengths are not permitted by this standard.

The Advanced Encryption Standard (AES) specifies the Rijndael algorithm, a symmetric block cipher that can process data blocks of 128 bits, using cipher keys with lengths of 128, 192, and 256 bits. Rijndael was designed to handle additional block sizes and key lengths, however they are not adopted in the AES standard.

The AES algorithm may be used with the three different key lengths indicated above, and therefore these different "flavors" may be referred to as "AES-128", "AES-192", and "AES- 256".

The other answers are not correct because:
"64 bits of data input results in 56 bits of encrypted output" is incorrect because while DES does work with 64 bit block input, it results in 64 bit blocks of encrypted output.

"128 bit key with 8 bits used for parity" is incorrect because DES does not ever use a 128 bit key.

"56 bits of data input results in 56 bits of encrypted output" is incorrect because DES always works with 64 bit blocks of input/output, not 56 bits.

Reference(s) used for this question:
Official ISC2 Guide to the CISSP CBK, Second Edition, page: 336-343
http://csrc.nist.gov/publications/fips/fips197/fips-197.pdf
http://csrc.nist.gov/publications/fips/fips46-3/fips46-3.pdf

QUESTION 685
Which of the following is true about digital certificate?

A. It is the same as digital signature proving Integrity and Authenticity of the data
B. Electronic credential proving that the person the certificate was issued to is who they claim to be
C. You can only get digital certificate from Verisign, RSA if you wish to prove the key belong to a specific user.
D. Can't contain geography data such as country for example.

Correct Answer: B
Explanation:
Digital certificate helps others verify that the public keys presented by users are genuine and valid. It is a form of Electronic credential proving that the person the certificate was issued to is who they claim to be.

The certificate is used to identify the certificate holder when conducting electronic transactions. It is issued by a certification authority (CA). It contains the name of an organization or individual, the business address, a serial number, expiration dates, a copy of the certificate holder's public key (used for encrypting messages), and the digital signature of the certificate-issuing authority so that a recipient can verify that the certificate is real. Some digital certificates conform to a standard, X.509. Digital certificates can be kept in registries so that authenticating users can look up other users' public keys.

Digital certificates are key to the PKI process. The digital certificate serves two roles. First, it ensures the integrity of the public key and makes sure that the key remains unchanged and in a valid state. Second, it validates that the public key is tied to the stated owner and that all associated information is true and correct. The information needed to accomplish these goals is added into the digital certificate.

A Certificate Authority (CA) is an entity trusted by one or more users as an authority in a network that issues, revokes, and manages digital certificates. A Registration Authority (RA) performs certificate registration services on behalf of a CA.

The RA, a single purpose server, is responsible for the accuracy of the information contained in a certificate request. The RA is also expected to perform user validation before issuing a certificate request.

A Digital Certificate is not like same as a digital signature, they are two different things, a digital Signature is created by using your Private key to encrypt a message digest and a Digital Certificate is issued by a trusted third party who vouch for your identity.

There are many other third parties which are providing Digital Certifictes and not just Verisign, RSA.

Reference(s) 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 14894-14903). Auerbach Publications. Kindle Edition.

Gregg, Michael; Haines, Billy (2012-02-16). CASP: CompTIA Advanced Security Practitioner Study Guide Authorized Courseware: Exam CAS-001 (p. 24). Wiley. Kindle Edition.

Please refer to http://en.wikipedia.org/wiki/Digital_certificate What is Digital certificate: http://searchsecurity.techtarget.com/sDefinition/0,,sid14_gci211947,00.html another deifination on http://www.webopedia.com/TERM/D/digital_certificate.html

QUESTION 686
The computations involved in selecting keys and in enciphering data are complex, and are not practical for manual use. However, using mathematical properties of modular arithmetic and a method known as "_____," RSA is quite feasible for computer use.

A. computing in Galois fields
B. computing in Gladden fields
C. computing in Gallipoli fields