to breach the cryptographic security systems.

PGP - Pretty Good Privacy: PGP, written by Phil Zimmermann is a data encryption and decryption program that provides cryptographic privacy and authentication for data. Still isn't the right answer though. Read more here about PGP.

The following reference(s) was used to create this question:

To get more info on this QUESTION NO: s or any QUESTION NO: s of Security+, subscribe to the CCCure Holistic Security+ CBT available at:
http://www.cccure.tv
http://users.telenet.be/d.rijmenants/en/otp.htm
http://en.wikipedia.org/wiki/One-time_pad
http://searchsecurity.techtarget.com/definition/one-time-pad

QUESTION 668

Which of the following answers is described as a random value used in cryptographic algorithms to ensure that patterns are not created during the encryption process?

A. IV - Initialization Vector
B. Stream Cipher
C. OTP - One Time Pad
D. Ciphertext

Correct Answer: A
Explanation:
The basic power in cryptography is randomness. This uncertainty is why encrypted data is unusable to someone without the key to decrypt.

Initialization Vectors are a used with encryption keys to add an extra layer of randomness to encrypted data. If no IV is used the attacker can possibly break the keyspace because of patterns resulting in the encryption process. Implementation such as DES in Code Book Mode (CBC) would allow frequency analysis attack to take place.

In cryptography, an initialization vector (IV) or starting variable (SV)is a fixed-size input to a cryptographic primitive that is typically required to be random or pseudorandom. Randomization is crucial for encryption schemes to achieve semantic security, a property whereby repeated usage of the scheme under the same key does not allow an attacker to infer relationships between segments of the encrypted message. For block ciphers, the use of an IV is described by so-called modes of operation. Randomization is also required for other primitives, such as universal hash functions and message authentication codes based thereon.

It is define by TechTarget as:
An initialization vector (IV) is an arbitrary number that can be used along with a secret key for data encryption. This number, also called a nonce, is employed only one time in any session. The use of an IV prevents repetition in data encryption, making it more difficult for a hacker using a dictionary attack to find patterns and break a cipher. For example, a sequence might appear twice or more within the body of a message. If there are repeated sequences in encrypted data, an attacker could assume that the corresponding sequences in the message were also identical. The IV prevents the appearance of corresponding duplicate character sequences in the ciphertext.

The following answers are incorrect:

Stream Cipher: This isn't correct. A stream cipher is a symmetric key cipher where plaintext digits are combined with pseudorandom key stream to product cipher text.

OTP - One Time Pad: This isn't correct but OTP is made up of random values used as key material. (Encryption key) It is considered by most to be unbreakable but must be changed with a new key after it is used which makes it impractical for common use.

Ciphertext: Sorry, incorrect answer. Ciphertext is basically text that has been encrypted with key material (Encryption key)

The following reference(s) was used to create this question:

For more details on this TOPIC and other QUESTION NO: s of the Security+ CBK, subscribe to our Holistic Computer Based Tutorial (CBT) at
http://www.cccure.tv
whatis.techtarget.com/definition/initialization-vector-IV
en.wikipedia.org/wiki/Initialization_vector

QUESTION 669
Which of the following encryption algorithms does not deal with discrete logarithms?

A. El Gamal
B. Diffie-Hellman
C. RSA
D. Elliptic Curve

Correct Answer: C
Explanation:
The security of the RSA system is based on the assumption that factoring the product into two original large prime numbers is difficult
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 159).
Shon Harris, CISSP All-in-One Examine Guide, Third Edition, McGraw-Hill Companies, August 2005, Chapter 8: Cryptography, Page 636 - 639

QUESTION 670
The Data Encryption Algorithm performs how many rounds of substitution and permutation?

A. 4
B. 16
C. 54
D. 64

Correct Answer: B
Explanation:
Source: TIPTON, Hal, (ISC)2, Introduction to the CISSP Exam presentation.

QUESTION 671
Which of the following services is NOT provided by the digital signature standard (DSS)?

A. Encryption
B. Integrity

C. Digital signature
D. Authentication

Correct Answer: A
Explanation:
DSS provides Integrity, digital signature and Authentication, but does not provide Encryption.
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 160).

QUESTION 672
Complete the blanks. When using PKI, I digitally sign a message using my ______ key. The recipient verifies my signature using my ______ key.

A. Private / Public
B. Public / Private
C. Symmetric / Asymmetric
D. Private / Symmetric

Correct Answer: A
Explanation:
When we encrypt messages using our private keys which are only available to us. The person who wants to read and decrypt the message need only have our public keys to do so.
The whole point to PKI is to assure message integrity, authentication of the source, and to provide secrecy with the digital encryption.

See below a nice walktrough of Digital Signature creation and verification from the Comodo web site:

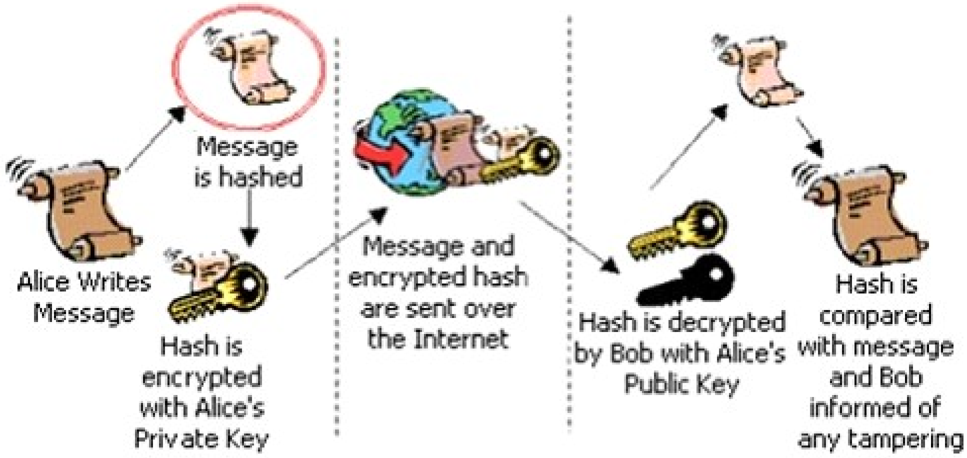
Digital Signatures apply the same functionality to an e-mail message or data file that a handwritten signature does for a paper-based document. The Digital Signature vouches for the origin and integrity of a message, document or other data file.
How do we create a Digital Signature?

The creation of a Digital Signature is a complex mathematical process. However as the complexities of the process are computed by the computer, applying a Digital Signature is no more difficult that creating a handwritten one!

The following text illustrates in general terms the processes behind the generation of a Digital Signature:

1. Alice clicks 'sign' in her email application or selects which file is to be signed.
2. Alice's computer calculates the 'hash' (the message is applied to a publicly known mathematical hashing function that coverts the message into a long number referred to as the hash).
3. The hash is encrypted with Alice's Private Key (in this case it is known as the Signing Key) to create the Digital Signature.
4. The original message and its Digital Signature are transmitted to Bob.
5. Bob receives the signed message. It is identified as being signed, so his email application knows which actions need to be performed to verify it.
6. Bob's computer decrypts the Digital Signature using Alice's Public Key.
7. Bob's computer also calculates the hash of the original message (remember - the mathematical function used by Alice to do this is publicly known).
8. Bob's computer compares the hashes it has computed from the received message with the now decrypted hash received with Alice's message.

digital signature creation and verification

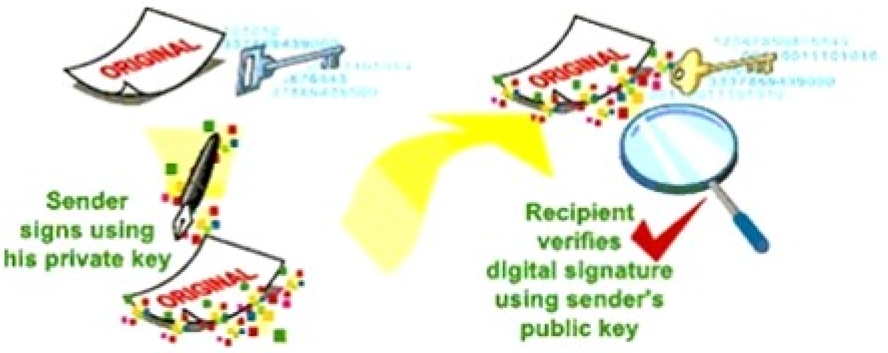

Message is hashed
Alice Writes Message
Hash is encrypted with Alice's Private Key
Message and encrypted hash are sent over the Internet
Hash is decrypted by Bob with Alice's Public Key
Hash is compared with message and Bob informed of any tampering

If the message has remained integral during its transit (i.e. it has not been tampered with), when compared the two hashes will be identical.

However, if the two hashes differ when compared then the integrity of the original message has been compromised. If the original message is tampered with it will result in Bob's computer calculating a different hash value. If a different hash value is created, then the original message will have been altered. As a result the verification of the Digital Signature will fail and Bob will be informed.
Origin, Integrity, Non-Repudiation, and Preventing Men-In-The-Middle (MITM) attacks

Eve, who wants to impersonate Alice, cannot generate the same signature as Alice because she does not have Alice's Private Key (needed to sign the message digest). If instead, Eve decides to alter the content of the message while in transit, the tampered message will create a different message digest to the original message, and Bob's computer will be able to detect that. Additionally, Alice cannot deny sending the message as it has been signed using her Private Key, thus ensuring non-repudiation.

creating and validating a digital signature


ORIGINAL
Sender signs using his private key
ORIGINAL
ORIGINAL
Recipient verifies digital signature using sender's public key

Due to the recent Global adoption of Digital Signature law, Alice may now sign a transaction, message or piece of digital data, and so long as it is verified successfully it is a legally permissible means of proof that Alice has made the transaction or written the message.

The following answers are incorrect:

Public / Private: This is the opposite of the right answer.
Symmetric / Asymmetric: Not quite. Sorry. This form of crypto is asymmetric so you were almost on target.
Private / Symmetric: Well, you got half of it right but Symmetric is wrong.

The following reference(s) was used to create this question:

The CCCure Holistic Security+ CBT, you can subscribe at:
http://www.cccure.tv
http://www.comodo.com/resources/small-business/digital-certificates3.php

QUESTION 673
What can be defined as a digital certificate that binds a set of descriptive data items, other than a public key, either directly to a subject name or to the identifier of another certificate that is a public-key certificate?

A. A public-key certificate
B. An attribute certificate
C. A digital certificate
D. A descriptive certificate

Correct Answer: B
Explanation:
The Internet Security Glossary (RFC2828) defines an attribute certificate as a digital certificate that binds a set of descriptive data items, other than a public key, either directly to a subject name or to the identifier of another certificate that is a public-key certificate. A public-key certificate binds a subject name to a public key value, along with information needed to perform certain cryptographic functions. Other attributes of a subject, such as a security clearance, may be certified in a separate kind of digital certificate, called an attribute certificate. A subject may have multiple attribute certificates associated with its name or with each of its public-key certificates.
Source: SHIREY, Robert W., RFC2828: Internet Security Glossary, may 2000.

QUESTION 674
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
Explanation:
Reference: HARRIS, Shon, All-In-One CISSP Certification Exam Guide, 2001, McGraw-Hill/Osborne, page 467; SMITH, Richard E., Internet Cryptography, 1997, Addison-Wesley Pub Co.