algorithms - SHA-1, SHA-224, SHA-256, SHA- 384, and SHA-512 for federal use in the US; the standard was also widely adopted by the information technology industry and commercial companies.

The MD5 Message-Digest Algorithm is a widely used cryptographic hash function that produces a 128-bit (16-byte) hash value. Specified in RFC 1321, MD5 has been employed in a wide variety of security applications, and is also commonly used to check data integrity. MD5 was designed by Ron Rivest in 1991 to replace an earlier hash function, MD4. An MD5 hash is typically expressed as a 32-digit hexadecimal number.

However, it has since been shown that MD5 is not collision resistant; as such, MD5 is not suitable for applications like SSL certificates or digital signatures that rely on this property. In 1996, a flaw was found with the design of MD5, and while it was not a clearly fatal weakness, cryptographers began recommending the use of other algorithms, such as SHA- 1 - which has since been found also to be vulnerable. In 2004, more serious flaws were discovered in MD5, making further use of the algorithm for security purposes questionable - specifically, a group of researchers described how to create a pair of files that share the same MD5 checksum. Further advances were made in breaking MD5 in 2005, 2006, and 2007. In December 2008, a group of researchers used this technique to fake SSL certificate validity, and US-CERT now says that MD5 "should be considered cryptographically broken and unsuitable for further use." and most U.S. government applications now require the SHA-2 family of hash functions.

NIST CRYPTOGRAPHIC HASH PROJECT
NIST announced a public competition in a Federal Register Notice on November 2, 2007 to develop a new cryptographic hash algorithm, called SHA-3, for standardization. The competition was NIST's response to advances made in the cryptanalysis of hash algorithms.

NIST received sixty-four entries from cryptographers around the world by October 31, 2008, and selected fifty-one first-round candidates in December 2008, fourteen second- round candidates in July 2009, and five finalists - BLAKE, Grøstl, JH, Keccak and Skein, in December 2010 to advance to the third and final round of the competition.

Throughout the competition, the cryptographic community has provided an enormous amount of feedback. Most of the comments were sent to NIST and a public hash forum; in addition, many of the cryptanalysis and performance studies were published as papers in major cryptographic conferences or leading cryptographic journals. NIST also hosted a SHA-3 candidate conference in each round to obtain public feedback. Based on the public comments and internal review of the candidates, NIST announced Keccak as the winner of the SHA-3 Cryptographic Hash Algorithm Competition on October 2, 2012, and ended the five-year competition.

Reference:
Tipton, Harold, et. al., Officical (ISC)2 Guide to the CISSP CBK, 2007 edition, page 261.
https://secure.wikimedia.org/wikipedia/en/wiki/Md5
http://csrc.nist.gov/groups/ST/hash/sha-3/index.html

QUESTION 747
A X.509 public key certificate with the key usage attribute "non repudiation" can be used for which of the following?

A. encrypting messages
B. signing messages
C. verifying signed messages
D. decrypt encrypted messages

Correct Answer: C
Explanation:
References: RFC 2459: Internet X.509 Public Key Infrastructure Certificate and CRL Profile; GUTMANN, P., X.509 style guide.

QUESTION 748
Which of the following is less likely to be used today in creating a Virtual Private Network?

A. L2TP
B. PPTP
C. IPSec
D. L2F

Correct Answer: D
Explanation:
L2F (Layer 2 Forwarding) provides no authentication or encryption. It is a Protocol that supports the creation of secure virtual private dial-up networks over the Internet.
At one point L2F was merged with PPTP to produce L2TP to be used on networks and not only on dial up links.
IPSec is now considered the best VPN solution for IP environments.
Source: HARRIS, Shon, All-In-One CISSP Certification Exam Guide, McGraw- Hill/Osborne, 2002, Chapter 8: Cryptography (page 507).

QUESTION 749
What is the maximum key size for the RC5 algorithm?

A. 128 bits
B. 256 bits
C. 1024 bits
D. 2040 bits

Correct Answer: D
Explanation:
RC5 is a fast block cipher created by Ron Rivest and analyzed by RSA Data Security, Inc.

It is a parameterized algorithm with a variable block size, a variable key size, and a variable number of rounds.

Allowable choices for the block size are 32 bits (for experimentation and evaluation purposes only), 64 bits (for use a drop-in replacement for DES), and 128 bits.

The number of rounds can range from 0 to 255, while the key can range from 0 bits to 2040 bits in size.
Please note that some sources such as the latest Shon Harris book mentions that RC5 maximum key size is of 2048, not 2040 bits. I would definitively use RSA as the authoritative source which specifies a key of 2040 bits. It is an error in Shon's book.

The OIG book says:
RC5 was developed by Ron Rivest of RSA and is deployed in many of RSA's products. It is a very adaptable product useful for many applications, ranging from software to hardware implementations. The key for RC5 can vary from 0 to 2040 bits, the number of rounds it executes can be adjusted from 0 to 255, and the length of the input words can also be chosen from 16-, 32-, and 64-bit lengths.

The following answers were incorrect choices:

All of the other answers were wrong.

Reference(s) used for this question:

Schneiter, Andrew (2013-04-15). Official (ISC)2 Guide to the CISSP CBK, Third Edition. Cryptography (Kindle Locations 1098-1101). . Kindle Edition.

Harris, Shon (2012-10-25). CISSP All-in-One Exam Guide, 6th Edition (Kindle Locations 16744-16747). McGraw-Hill. Kindle Edition.
http://www.rsa.com/rsalabs/node.asp?id=2251, What are RC5 and RC6, RSA The Security Division of EMC.
From Rivest himself, see http://people.csail.mit.edu/rivest/Rivest-rc5rev.pdf Also see the draft IETF IPSEC standard which clearly mention that it is in fact 2040 bits as a MAXIMUM key size: http://www.tools.ietf.org/html/draft-ietf-ipsec-esp-rc5-cbc-00 http://en.wikipedia.org/wiki/RC5, Mention a maximum key size of 2040 as well.

QUESTION 750
What can be defined as an instance of two different keys generating the same ciphertext from the same plaintext?

A. Key collision
B. Key clustering
C. Hashing
D. Ciphertext collision

Correct Answer: B
Explanation:
Key clustering happens when a plaintext message generates identical ciphertext messages using the same transformation algorithm, but with different keys.
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 130).

QUESTION 751
Which of the following keys has the SHORTEST lifespan?

A. Secret key
B. Public key
C. Session key
D. Private key

Correct Answer: C
Explanation:
As session key is a symmetric key that is used to encrypt messages between two users. A session key is only good for one communication session between users.

For example, If Tanya has a symmetric key that she uses to encrypt messages between Lance and herself all the time , then this symmetric key would not be regenerated or changed. They would use the same key every time they communicated using encryption. However , using the same key repeatedly increases the chances of the key being captured and the secure communication being compromised. If , on the other hand , a new symmetric key were generated

each time Lance and Tanya wanted to communicate , it would be used only during their dialog and then destroyed. if they wanted to communicate and hour later , a new session key would be created and shared.

The other answers are not correct because :

Public Key can be known to anyone.
Private Key must be known and used only by the owner. Secret Keys are also called as Symmetric Keys, because this type of encryption relies on each user to keep the key a secret and properly protected.

References:
SHON HARRIS, ALL IN ONE THIRD EDITION: Chapter 8: Cryptography, Page: 619-620

QUESTION 752
Which protocol makes USE of an electronic wallet on a customer's PC and sends encrypted credit card information to merchant's Web server, which digitally signs it and sends it on to its processing bank?

A. SSH (Secure Shell)
B. S/MIME (Secure MIME)
C. SET (Secure Electronic Transaction)
D. SSL (Secure Sockets Layer)

Correct Answer: C
Explanation:
As protocol was introduced by Visa and Mastercard to allow for more credit card transaction possibilities. It is comprised of three different pieces of software, running on the customer's PC (an electronic wallet), on the merchant's Web server and on the payment server of the merchant's bank. The credit card information is sent by the customer to the merchant's Web server, but it does not open it and instead digitally signs it and sends it to its bank's payment server for processing.

The following answers are incorrect because :

SSH (Secure Shell) is incorrect as it functions as a type of tunneling mechanism that provides terminal like access to remote computers.
S/MIME is incorrect as it is a standard for encrypting and digitally signing electronic mail and for providing secure data transmissions.
SSL is incorrect as it uses public key encryption and provides data encryption, server authentication, message integrity, and optional client authentication.

Reference:
Shon Harris AIO v3, Chapter-8: Cryptography, Page: 667-669

QUESTION 753
What kind of certificate is used to validate a user identity?

A. Public key certificate
B. Attribute certificate
C. Root certificate
D. Code signing certificate

Correct Answer: A
Explanation:
In cryptography, a public key certificate (or identity certificate) is an electronic document which incorporates a digital signature to bind together a public key with an identity -- information such as the name of a person or an organization, their address, and so forth. The certificate can be used to verify that a public key belongs to an individual.

In a typical public key infrastructure (PKI) scheme, the signature will be of a certificate authority (CA). In a web of trust scheme, the signature is of either the user (a self-signed certificate) or other users ("endorsements"). In either case, the signatures on a certificate are attestations by the certificate signer that the identity information and the public key belong together.

In computer security, an authorization certificate (also known as an attribute certificate) is a digital document that describes a written permission from the issuer to use a service or a resource that the issuer controls or has access to use. The permission can be delegated.

Some people constantly confuse PKCs and ACs. An analogy may make the distinction clear. A PKC can be considered to be like a passport: it identifies the holder, tends to last for a long time, and should not be trivial to obtain. An AC is more like an entry visa: it is typically issued by a different authority and does not last for as long a time. As acquiring an entry visa typically requires presenting a passport, getting a visa can be a simpler process.

A real life example of this can be found in the mobile software deployments by large service providers and are typically applied to platforms such as Microsoft Smartphone (and related), Symbian OS, J2ME, and others.

In each of these systems a mobile communications service provider may customize the mobile terminal client distribution (ie. the mobile phone operating system or application environment) to include one or more root certificates each associated with a set of capabilities or permissions such as "update firmware", "access address book", "use radio interface", and the most basic one, "install and execute". When a developer wishes to enable distribution and execution in one of these controlled environments they must acquire a certificate from an appropriate CA, typically a large commercial CA, and in the process they usually have their identity verified using out-of-band mechanisms such as a combination of phone call, validation of their legal entity through government and commercial databases, etc., similar to the high assurance SSL certificate vetting process, though often there are additional specific requirements imposed on would-be developers/publishers.

Once the identity has been validated they are issued an identity certificate they can use to sign their software; generally the software signed by the developer or publisher's identity certificate is not distributed but rather it is submitted to processor to possibly test or profile the content before generating an authorization certificate which is unique to the particular software release. That certificate is then used with an ephemeral asymmetric key-pair to sign the software as the last step of preparation for distribution. There are many advantages to separating the identity and authorization certificates especially relating to risk mitigation of new content being accepted into the system and key management as well as recovery from errant software which can be used as attack vectors.

References:
HARRIS, Shon, All-In-One CISSP Certification Exam Guide, 2001, McGraw-Hill/Osborne, page 540.
http://en.wikipedia.org/wiki/Attribute_certificate
http://en.wikipedia.org/wiki/Public_key_certificate
QUESTION 754
Which encryption algorithm is BEST suited for communication with handheld wireless devices?