bit to hide your data. See below a color code for one pixel in binary format. The bits below are not real they are just example for illustration purpose:

RED GREEN BLUE
0101 0101 1100 1011 1110 0011
MSB LSB MSB LSB MSB LSB

Let's say that I would like to hide the letter A uppercase within the pixels of the picture. If we convert the letter "A" uppercase to a decimal value it would be number 65 within the ASCII table , in binary format the value 65 would translet to 01000001

You can break the 8 bits of character A uppercase in group of two bits as follow: 01 00 00 Using the pixel above we will hide those bits within the last two bits of each of the color as follow:

RED GREEN BLUE
0101 0101 1100 1000 1110 0000
MSB LSB MSB LSB MSB LSB

As you can see above, the last two bits of RED was already set to the proper value of 01, then we move to the GREEN value and we changed the last two bit from 11 to 00, and finally we changed the last two bits of blue to 00. One pixel allowed us to hide 6 bits of data. We would have to use another pixel to hide the remaining two bits.

The following answers are incorrect:

ADS - Alternate Data Streams: This is almost correct but ADS is different from steganography in that ADS hides data in streams of communications or files while Steganography hides data in a single file.

Encryption: This is almost correct but Steganography isn't exactly encryption as much as using space in a file to store another file.

NTFS ADS: This is also almost correct in that you're hiding data where you have space to do so. NTFS, or New Technology File System common on Windows computers has a feature where you can hide files where they're not viewable under normal conditions. Tools are required to uncover the ADS-hidden files.

The following reference(s) was used to create this question:
The CCCure Security+ Holistic Tutorial
at http://www.cccure.tv
Steganography tool
http://en.wikipedia.org/wiki/Steganography

QUESTION 798
Which of the following statements pertaining to message digests is incorrect?

A. The original file cannot be created from the message digest.
B. Two different files should not have the same message digest.
C. The message digest should be calculated using at least 128 bytes of the file.
D. Messages digests are usually of fixed size.

Correct Answer: C
Explanation:
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 799
Which of the following was developed in order to protect against fraud in electronic fund transfers (EFT) by ensuring the message comes from its claimed originator and that it has not been altered in transmission?

A. Secure Electronic Transaction (SET)
B. Message Authentication Code (MAC)
C. Cyclic Redundancy Check (CRC)
D. Secure Hash Standard (SHS)

Correct Answer: B
Explanation:
In order to protect against fraud in electronic fund transfers (EFT), the Message Authentication Code (MAC), ANSI X9.9, was developed. The MAC is a check value, which is derived from the contents of the message itself, that is sensitive to the bit changes in a message. It is similar to a Cyclic Redundancy Check (CRC).

The aim of message authentication in computer and communication systems is to verify that he message comes from its claimed originator and that it has not been altered in transmission. It is particularly needed for EFT Electronic Funds Transfer). The protection mechanism is generation of a Message Authentication Code (MAC), attached to the message, which can be recalculated by the receiver and will reveal any alteration in transit. One standard method is described in (ANSI, X9.9). Message authentication mechanisms an also be used to achieve non-repudiation of messages.

The Secure Electronic Transaction (SET) was developed by a consortium including MasterCard and VISA as a means of preventing fraud from occurring during electronic payment.

The Secure Hash Standard (SHS), NIST FIPS 180, available at http://www.itl.nist.gov/fipspubs/fip180-1.htm, specifies the Secure Hash Algorithm (SHA-1).

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 170)

also see:
http://luizfirmino.blogspot.com/2011/04/message-authentication-code-mac.html
http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.22.2312&rep=rep1&type=pdf

QUESTION 800
Which type of algorithm is considered to have the highest strength per bit of key length of any of the asymmetric algorithms?

A. Rivest, Shamir, Adleman (RSA)
B. El Gamal
C. Elliptic Curve Cryptography (ECC)
D. Advanced Encryption Standard (AES)

Correct Answer: C
Explanation:
The other answers are not correct because:

"Rivest, Shamir, Adleman (RSA)" is incorrect because RSA is a "traditional" asymmetric algorithm. While it is reasonably strong, it is not considered to be as strong as ECC based systems.

"El Gamal" is incorrect because it is also a "traditional" asymmetric algorithm and not considered as strong as ECC based systems.

"Advanced Encryption Standard (AES)" is incorrect because the question asks specifically about asymmetric algorithms and AES is a symmetric algorithm.

References:
Official ISC2 Guide page: 258
All in One Third Edition page: 638
The RSA Crypto FAQ: http://www.rsa.com/rsalabs/node.asp?id=2241

QUESTION 801
Which of the following is more suitable for a hardware implementation?

A. Stream ciphers
B. Block ciphers
C. Cipher block chaining
D. Electronic code book

Correct Answer: A
Explanation:
A stream cipher treats the message as a stream of bits or bytes and performs mathematical functions on them individually. The key is a random value input into the stream cipher, which it uses to ensure the randomness of the keystream data. They are more suitable for hardware implementations, because they encrypt and decrypt one bit at a time. They are intensive because each bit must be manipulated, which works better at the silicon level. Block ciphers operate a the block level, dividing the message into blocks of bits. Cipher Block chaining (CBC) and Electronic Code Book (ECB) are operation modes of DES, a block encryption algorithm.
Source: WALLHOFF, John, CBK#5 Cryptography (CISSP Study Guide), April 2002 (page 2).

QUESTION 802
Which of the following can be best defined as computing techniques for inseparably embedding unobtrusive marks or labels as bits in digital data and for detecting or extracting the marks later?

A. Steganography
B. Digital watermarking
C. Digital enveloping
D. Digital signature

Correct Answer: B
Explanation:
RFC 2828 (Internet Security Glossary) defines digital watermarking as computing techniques for inseparably embedding unobtrusive marks or labels as bits in digital data-text, graphics, images, video, or audio#and for detecting or extracting the marks later. The set of embedded bits (the digital watermark) is sometimes hidden, usually imperceptible, and always intended to be unobtrusive. It is used as a measure to protect intellectual property rights. Steganography involves hiding the very existence of a message. A digital signature is a value computed with a cryptographic algorithm and appended to a data object in such a way that any recipient of the

data can use the signature to verify the data's origin and integrity. A digital envelope is a combination of encrypted data and its encryption key in an encrypted form that has been prepared for use of the recipient.
Source: SHIREY, Robert W., RFC2828: Internet Security Glossary, may 2000.

QUESTION 803
What is used to bind a document to its creation at a particular time?

A. Network Time Protocol (NTP)
B. Digital Signature
C. Digital Timestamp
D. Certification Authority (CA)

Correct Answer: C
Explanation:
While a digital signature binds a document to the possessor of a particular key, a digital timestamp binds a document to its creation at a particular time.

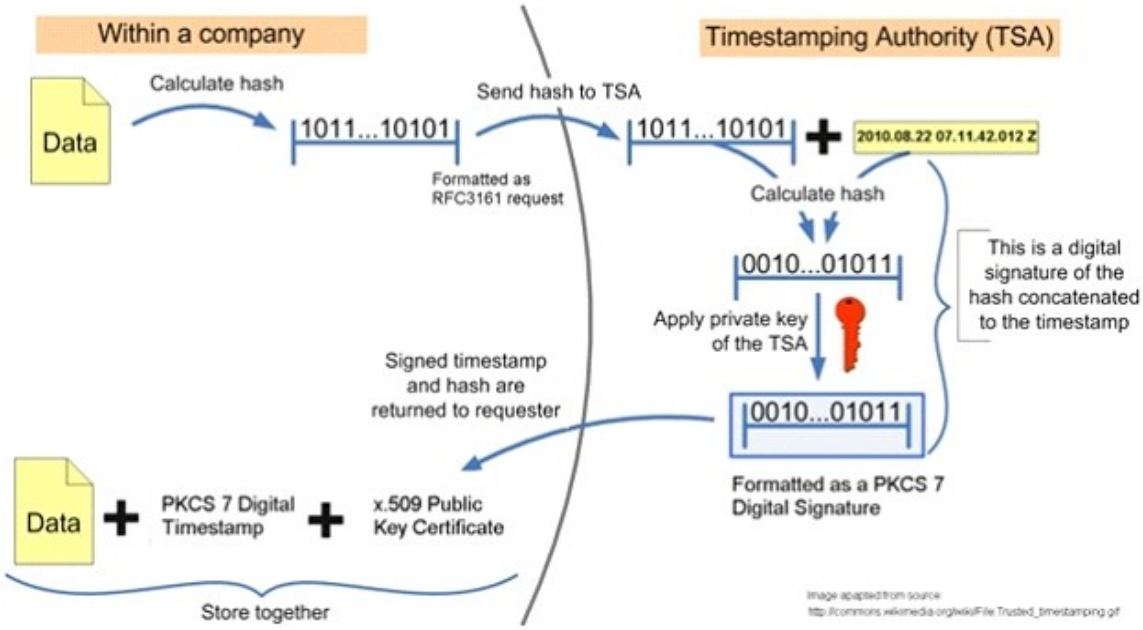
Trusted timestamping is the process of securely keeping track of the creation and modification time of a document. Security here means that no one -- not even the owner of the document -- should be able to change it once it has been recorded provided that the timestamper's integrity is never compromised.

The administrative aspect involves setting up a publicly available, trusted timestamp management infrastructure to collect, process and renew timestamps or to make use of a commercially available time stamping service.

A modern example of using a Digital Timestamp is the case of an industrial research organization that may later need to prove, for patent purposes, that they made a particular discovery on a particular date; since magnetic media can be altered easily, this may be a nontrivial issue. One possible solution is for a researcher to compute and record in a hardcopy laboratory notebook a cryptographic hash of the relevant data file. In the future, should there be a need to prove the version of this file retrieved from a backup tape has not been altered, the hash function could be recomputed and compared with the hash value recorded in that paper notebook.

According to the RFC 3161 standard, a trusted timestamp is a timestamp issued by a trusted third party (TTP) acting as a Time Stamping Authority (TSA). It is used to prove the existence of certain data before a certain point (e.g. contracts, research data, medical records,...) without the possibility that the owner can backdate the timestamps. Multiple TSAs can be used to increase reliability and reduce vulnerability.

The newer ANSI ASC X9.95 Standard for trusted timestamps augments the RFC 3161 standard with data-level security requirements to ensure data integrity against a reliable time source that is provable to any third party. This standard has been applied to authenticating digitally signed data for regulatory compliance, financial transactions, and legal evidence.



Digital TimeStamp

The following are incorrect answers:

Network Time Protocol (NTP) is used to achieve high accuracy time synchronization for computers across a network.
A Certification Authority (CA) is the entity responsible for the issuance of digital certificates. A Digital Signature provides integrity and authentication but does not bind a document to a specific time it was created.

Reference used for this question:

http://en.m.wikipedia.org/wiki/File:Trusted_timestamping.gif
http://en.wikipedia.org/wiki/Trusted_timestamping

QUESTION 804
How many rounds are used by DES?

A. 16
B. 32
C. 64
D. 48

Correct Answer: A
Explanation:
DES is a block encryption algorithm using 56-bit keys and 64-bit blocks that are divided in half and each character is encrypted one at a time. The characters are put through 16 rounds of transposition and substitution functions. Triple DES uses 48 rounds.
Source: WALLHOFF, John, CBK#5 Cryptography (CISSP Study Guide), April 2002 (page 3).