A. ECC (Elliptic Curve Cryptosystem)
B. RSA
C. SHA
D. RC4

Correct Answer: A
Explanation:
As it provides much of the same functionality that RSA provides: digital signatures, secure key distribution,and encryption. One differing factor is ECC's efficiency. ECC is more efficient that RSA and any other asymmetric algorithm.

The following answers are incorrect because:

RSA is incorrect as it is less efficient than ECC to be used in handheld devices.
SHA is also incorrect as it is a hashing algorithm.
RC4 is also incorrect as it is a symmetric algorithm.

Reference:
Shon Harris AIO v3, Chapter-8: Cryptography, Page: 631 , 638.

QUESTION 755
What is the main problem of the renewal of a root CA certificate?

A. It requires key recovery of all end user keys
B. It requires the authentic distribution of the new root CA certificate to all PKI participants
C. It requires the collection of the old root CA certificates from all the users
D. It requires issuance of the new root CA certificate

Correct Answer: B
Explanation:
The main task here is the authentic distribution of the new root CA certificate as new trust anchor to all the PKI participants (e.g. the users).

In some of the rollover-scenarios there is no automatic way, often explicit assignment of trust from each user is needed, which could be very costly.

Other methods make use of the old root CA certificate for automatic trust establishment (see PKIX-reference), but these solutions works only well for scenarios with currently valid root CA certificates (and not for emergency cases e.g. compromise of the current root CA certificate).

The rollover of the root CA certificate is a specific and delicate problem and therefore are often ignored during PKI deployment.

Reference:
Camphausen, I.; Petersen, H.; Stark, C.: Konzepte zum Root CA Zertifikatswechsel, conference Enterprise Security 2002, March 26-27, 2002, Paderborn; RFC 2459 : Internet X.509 Public Key Infrastructure Certificate and CRL Profile.

QUESTION 756
Which of the following algorithms is used today for encryption in PGP?

A. RSA
B. IDEA
C. Blowfish
D. RC5

Correct Answer: B
Explanation:
The Pretty Good Privacy (PGP) email encryption system was developed by Phil Zimmerman. For encrypting messages, it actually uses AES with up to 256-bit keys, CAST, TripleDES, IDEA and Twofish. RSA is also used in PGP, but only for symmetric key exchange and for digital signatures, but not for 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 (pages 154, 169).
More info on PGP can be found on their site at
http://www.pgp.com/display.php?pageID=29.

QUESTION 757
Which of the following is NOT a property of a one-way hash function?

A. It converts a message of a fixed length into a message digest of arbitrary length.
B. It is computationally infeasible to construct two different messages with the same digest.
C. It converts a message of arbitrary length into a message digest of a fixed length.
D. Given a digest value, it is computationally infeasible to find the corresponding message.

Correct Answer: A
Explanation:
An algorithm that turns messages or text into a fixed string of digits, usually for security or data management purposes. The "one way" means that it's nearly impossible to derive the original text from the string.

A one-way hash function is used to create digital signatures, which in turn identify and authenticate the sender and message of a digitally distributed message.

A cryptographic hash function is a deterministic procedure that takes an arbitrary block of data and returns a fixed-size bit string, the (cryptographic) hash value, such that an accidental or intentional change to the data will change the hash value. The data to be encoded is often called the "message," and the hash value is sometimes called the message digest or simply digest.

The ideal cryptographic hash function has four main or significant properties:

It is easy (but not necessarily quick) to compute the hash value for any given message it is infeasible to generate a message that has a given hash it is infeasible to modify a message without changing the hash it is infeasible to find two different messages with the same hash.

Cryptographic hash functions have many information security applications, notably in digital signatures, message authentication codes (MACs), and other forms of authentication. They can also be used as ordinary hash functions, to index data in hash tables, for fingerprinting, to detect duplicate data or uniquely identify files, and as checksums to detect accidental data corruption. Indeed, in information security contexts, cryptographic hash values are sometimes called (digital) fingerprints, checksums, or just hash values, even though all these terms stand for functions with rather different properties and purposes.

Source:
TIPTON, Hal, (ISC)2, Introduction to the CISSP Exam presentation.
http://en.wikipedia.org/wiki/Cryptographic_hash_function

QUESTION 758
Which of the following statements is true about data encryption as a method of protecting data?

A. It should sometimes be used for password files
B. It is usually easily administered
C. It makes few demands on system resources
D. It requires careful key management

Correct Answer: D
Explanation:
In cryptography, you always assume the "bad guy" has the encryption algorithm (indeed, many algorithms such as DES, Triple DES, AES, etc. are public domain). What the bad guy lacks is the key used to complete that algorithm and encrypt/decrypt information. Therefore, protection of the key, controlled distribution, scheduled key change, timely destruction, and several other factors require careful consideration. All of these factors are covered under the umbrella term of "key management".

Another significant consideration is the case of "data encryption as a method of protecting data" as the question states. If that data is to be stored over a long period of time (such as on backup), you must ensure that your key management scheme stores old keys for as long as they will be needed to decrypt the information they encrypted.

The other answers are not correct because:

"It should sometimes be used for password files." - Encryption is often used to encrypt passwords stored within password files, but it is not typically effective for the password file itself. On most systems, if a user cannot access the contents of a password file, they cannot authenticate. Encrypting the entire file prevents that access.

"It is usually easily administered." - Developments over the last several years have made cryptography significantly easier to manage and administer. But it remains a significant challenge. This is not a good answer.

"It makes few demands on system resources." - Cryptography is, essentially, a large complex mathematical algorithm. In order to encrypt and decrypt information, the system must perform this algorithm hundreds, thousands, or even millions/billions/trillions of times. This becomes system resource intensive, making this a very bad answer.

Reference:
Official ISC2 Guide page: 266 (poor explanation)
All in One Third Edition page: 657 (excellent explanation)
Key Management - Page 732, All in One Fourth Edition

QUESTION 759
Which of the following cryptographic attacks describes when the attacker has a copy of the

plaintext and the corresponding ciphertext?

A. known plaintext
B. brute force
C. ciphertext only
D. chosen plaintext

Correct Answer: A
Explanation:
The goal to this type of attack is to find the cryptographic key that was used to encrypt the message. Once the key has been found, the attacker would then be able to decrypt all messages that had been encrypted using that key.

The known-plaintext attack (KPA) or crib is an attack model for cryptanalysis where the attacker has samples of both the plaintext and its encrypted version (ciphertext), and is at liberty to make use of them to reveal further secret information such as secret keys and code books. The term "crib" originated at Bletchley Park, the British World War II decryption operation

In cryptography, a brute force attack or exhaustive key search is a strategy that can in theory be used against any encrypted data by an attacker who is unable to take advantage of any weakness in an encryption system that would otherwise make his task easier. It involves systematically checking all possible keys until the correct key is found. In the worst case, this would involve traversing the entire key space, also called search space.

In cryptography, a ciphertext-only attack (COA) or known ciphertext attack is an attack model for cryptanalysis where the attacker is assumed to have access only to a set of ciphertexts.

The attack is completely successful if the corresponding plaintexts can be deduced, or even better, the key. The ability to obtain any information at all about the underlying plaintext is still considered a success. For example, if an adversary is sending ciphertext continuously to maintain traffic-flow security, it would be very useful to be able to distinguish real messages from nulls. Even making an informed guess of the existence of real messages would facilitate traffic analysis.

In the history of cryptography, early ciphers, implemented using pen-and-paper, were routinely broken using ciphertexts alone. Cryptographers developed statistical techniques for attacking ciphertext, such as frequency analysis. Mechanical encryption devices such as Enigma made these attacks much more difficult (although, historically, Polish cryptographers were able to mount a successful ciphertext-only cryptanalysis of the Enigma by exploiting an insecure protocol for indicating the message settings).

Every modern cipher attempts to provide protection against ciphertext-only attacks. The vetting process for a new cipher design standard usually takes many years and includes exhaustive testing of large quantities of ciphertext for any statistical departure from random noise. See: Advanced Encryption Standard process. Also, the field of steganography evolved, in part, to develop methods like mimic functions that allow one piece of data to adopt the statistical profile of another. Nonetheless poor cipher usage or reliance on home- grown proprietary algorithms that have not been subject to thorough scrutiny has resulted in many computer-age encryption systems that are still subject to ciphertext-only attack.
Examples include:

Early versions of Microsoft's PPTP virtual private network software used the same RC4 key for the sender and the receiver (later versions had other problems). In any case where a stream cipher like RC4 is used twice with the same key it is open to ciphertext-only attack.
See: stream cipher attack

Wired Equivalent Privacy (WEP), the first security protocol for Wi-Fi, proved vulnerable to several attacks, most of them ciphertext-only.

A chosen-plaintext attack (CPA) is an attack model for cryptanalysis which presumes that the attacker has the capability to choose arbitrary plaintexts to be encrypted and obtain the corresponding ciphertexts. The goal of the attack is to gain some further information which reduces the security of the encryption scheme. In the worst case, a chosen-plaintext attack could reveal the scheme's secret key.

This appears, at first glance, to be an unrealistic model; it would certainly be unlikely that an attacker could persuade a human cryptographer to encrypt large amounts of plaintexts of the attacker's choosing. Modern cryptography, on the other hand, is implemented in software or hardware and is used for a diverse range of applications; for many cases, a chosen-plaintext attack is often very feasible. Chosen-plaintext attacks become extremely important in the context of public key cryptography, where the encryption key is public and attackers can encrypt any plaintext they choose.

Any cipher that can prevent chosen-plaintext attacks is then also guaranteed to be secure against known-plaintext and ciphertext-only attacks; this is a conservative approach to security.

Two forms of chosen-plaintext attack can be distinguished:

Batch chosen-plaintext attack, where the cryptanalyst chooses all plaintexts before any of them are encrypted. This is often the meaning of an unqualified use of "chosen-plaintext attack".

Adaptive chosen-plaintext attack, where the cryptanalyst makes a series of interactive queries, choosing subsequent plaintexts based on the information from the previous encryptions.

References:
Source: TIPTON, Harold, Official (ISC)2 Guide to the CISSP CBK (2007), page 271.
Wikipedia at the following links:
http://en.wikipedia.org/wiki/Chosen-plaintext_attack http://en.wikipedia.org/wiki/Known-plaintext_attack
http://en.wikipedia.org/wiki/Ciphertext-only_attack http://en.wikipedia.org/wiki/Brute_force_attack

QUESTION 760
A public key algorithm that does both encryption and digital signature is which of the following?

A. RSA
B. DES
C. IDEA
D. Diffie-Hellman

Correct Answer: A
Explanation:
RSA can be used for encryption, key exchange, and digital signatures.
Key Exchange versus key Agreement

KEY EXCHANGE
Key exchange (also known as "key establishment") is any method in cryptography by which cryptographic keys are exchanged between users, allowing use of a cryptographic algorithm.

If sender and receiver wish to exchange encrypted messages, each must be equipped to encrypt messages to be sent and decrypt messages received. The nature of the equipping they require