A. RC6
B. Twofish
C. Rijndael
D. Blowfish

Correct Answer: C
Explanation:
On October 2, 2000, NIST announced the selection of the Rijndael Block Cipher, developed by the Belgian cryptographers Dr. Joan Daemen and Dr. Vincent Rijmen, as the proposed AES algorithm. Twofish and RC6 were also candidates. Blowfish is also a symmetric algorithm but wasn't a finalist for a replacement for DES.

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 152).

QUESTION 768
Kerberos depends upon what encryption method?

A. Public Key cryptography.
B. Secret Key cryptography.
C. El Gamal cryptography.
D. Blowfish cryptography.

Correct Answer: B
Explanation:
Kerberos depends on Secret Keys or Symmetric Key cryptography.

Kerberos a third party authentication protocol. It was designed and developed in the mid 1980's by MIT. It is considered open source but is copyrighted and owned by MIT. It relies on the user's secret keys. The password is used to encrypt and decrypt the keys.

This question asked specifically about encryption methods. Encryption methods can be SYMMETRIC (or secret key) in which encryption and decryption keys are the same, or ASYMMETRIC (aka 'Public Key') in which encryption and decryption keys differ.

'Public Key' methods must be asymmetric, to the extent that the decryption key CANNOT be easily derived from the encryption key. Symmetric keys, however, usually encrypt more efficiently, so they lend themselves to encrypting large amounts of data. Asymmetric encryption is often limited to ONLY encrypting a symmetric key and other information that is needed in order to decrypt a data stream, and the remainder of the encrypted data uses the symmetric key method for performance reasons. This does not in any way diminish the security nor the ability to use a public key to encrypt the data, since the symmetric key method is likely to be even MORE secure than the asymmetric method.

For symmetric key ciphers, there are basically two types: BLOCK CIPHERS, in which a fixed length block is encrypted, and STREAM CIPHERS, in which the data is encrypted one 'data unit' (typically 1 byte) at a time, in the same order it was received in.

The following answers are incorrect:

Public Key cryptography. Is incorrect because Kerberos depends on Secret Keys or Symmetric Key cryptography and not Public Key or Asymmetric Key cryptography.

El Gamal cryptography. Is incorrect because El Gamal is an Asymmetric Key encryption algorithm.
Blowfish cryptography. Is incorrect because Blowfish is a Symmetric Key encryption algorithm.

References:
OIG CBK Access Control (pages 181 - 184)
AIOv3 Access Control (pages 151 - 155)

Wikipedia http://en.wikipedia.org/wiki/Blowfish_%28cipher%29;
http://en.wikipedia.org/wiki/El_Gamal
http://www.mrp3.com/encrypt.html

QUESTION 769
What is the RESULT of a hash algorithm being applied to a message ?

A. A digital signature
B. A ciphertext
C. A message digest
D. A plaintext

Correct Answer: C
Explanation:
As when a hash algorithm is applied on a message, it produces a message digest.

The other answers are incorrect because:

A digital signature is a hash value that has been encrypted with a sender's private key. A ciphertext is a message that appears to be unreadable.
A plaintext is a readable data.

Reference:
Shon Harris, AIO v3, Chapter-8: Cryptography, Page: 593-594, 640, 648

QUESTION 770
Which of the following was not designed to be a proprietary encryption algorithm?

A. RC2
B. RC4
C. Blowfish
D. Skipjack

Correct Answer: C
Explanation:
Blowfish is a symmetric block cipher with variable-length key (32 to 448 bits) designed in 1993 by Bruce Schneier as an unpatented, license-free, royalty-free replacement for DES or IDEA. See attributes below:

Block cipher: 64-bit block
Variable key length: 32 bits to 448 bits
Designed by Bruce Schneier
Much faster than DES and IDEA
Unpatented and royalty-free
No license required

Free source code available

Rivest Cipher #2 (RC2) is a proprietary, variable-key-length block cipher invented by Ron Rivest for RSA Data Security, Inc.

Rivest Cipher #4 (RC4) is a proprietary, variable-key-length stream cipher invented by Ron Rivest for RSA Data Security, Inc.
The Skipjack algorithm is a Type II block cipher [NIST] with a block size of 64 bits and a key size of 80 bits that was developed by NSA and formerly classified at the U.S. Department of Defense "Secret" level. The NSA announced on June 23, 1998, that Skipjack had been declassified.

References:
RSA Laboratories
http://www.rsa.com/rsalabs/node.asp?id=2250

RFC 2828 - Internet Security Glossary
http://www.faqs.org/rfcs/rfc2828.html

QUESTION 771
Which of the following algorithms is a stream cipher?

A. RC2
B. RC4
C. RC5
D. RC6

Correct Answer: B
Explanation:
RC2, RC4, RC5 and RC6 were developed by Ronal Rivest from RSA Security.
In the RC family only RC4 is a stream cipher.
RC4 allows a variable key length.
RC2 works with 64-bit blocks and variable key lengths, RC5 has variable block sizes, key length and number of processing rounds.
RC6 was designed to fix a flaw in RC5.
Source: ANDRESS, Mandy, Exam Cram CISSP, Coriolis, 2001, Chapter 6: Cryptography (page 103).

QUESTION 772
Which of the following is NOT an asymmetric key algorithm?

A. RSA
B. Elliptic Curve Cryptosystem (ECC)
C. El Gamal
D. Data Encryption System (DES)

Correct Answer: D
Explanation:
Data Encryption Standard (DES) is a symmetric key algorithm. Originally developed by IBM, under project name Lucifer, this 128-bit algorithm was accepted by the NIST in 1974, but the key size was reduced to 56 bits, plus 8 bits for parity. It somehow became a national cryptographic standard in 1977, and an American National Standard Institute (ANSI) standard in 1978. DES was later replaced by the Advanced Encryption Standard (AES) by the NIST. All other options are asymmetric algorithms. Source: HARRIS, Shon, All-In-One CISSP Certification Exam Guide,

McGraw- Hill/Osborne, 2002, chapter 8: Cryptography (page 525).
Reference:
DES: http://csrc.nist.gov/publications/fips/fips46-3/fips46-3.pdf

QUESTION 773
The Secure Hash Algorithm (SHA-1) creates:

A. a fixed length message digest from a fixed length input message
B. a variable length message digest from a variable length input message
C. a fixed length message digest from a variable length input message
D. a variable length message digest from a fixed length input message

Correct Answer: C
Explanation:
According to The CISSP Prep Guide, "The Secure Hash Algorithm (SHA-1) computes a fixed length message digest from a variable length input message."
Source: KRUTZ, Ronald L.& VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, John Wiley & Sons, 2001, page 160.
also see:
http://csrc.nist.gov/publications/fips/fips180-2/fips180-2withchangenotice.pdf

QUESTION 774
The primary purpose for using one-way hashing of user passwords within a password file is which of the following?

A. It prevents an unauthorized person from trying multiple passwords in one logon attempt.
B. It prevents an unauthorized person from reading the password.
C. It minimizes the amount of storage required for user passwords.
D. It minimizes the amount of processing time used for encrypting passwords.

Correct Answer: B
Explanation:
The whole idea behind a one-way hash is that it should be just that - one- way. In other words, an attacker should not be able to figure out your password from the hashed version of that password in any mathematically feasible way (or within any reasonable length of time).

Password Hashing and Encryption
In most situations , if an attacker sniffs your password from the network wire, she still has some work to do before she actually knows your password value because most systems hash the password with a hashing algorithm, commonly MD4 or MD5, to ensure passwords are not sent in cleartext.

Although some people think the world is run by Microsoft, other types of operating systems are out there, such as Unix and Linux. These systems do not use registries and SAM databases, but contain their user passwords in a file cleverly called "shadow." Now, this shadow file does not contain passwords in cleartext; instead, your password is run through a hashing algorithm, and the resulting value is stored in this file.

Unixtype systems zest things up by using salts in this process. Salts are random values added to the encryption process to add more complexity and randomness. The more randomness entered into the encryption process, the harder it is for the bad guy to decrypt and uncover your password. The use of a salt means that the same password can be encrypted into several thousand different formats. This makes it much more difficult for an attacker to uncover the right

format for your system.

Password Cracking tools
Note that the use of one-way hashes for passwords does not prevent password crackers from guessing passwords. A password cracker runs a plain-text string through the same one-way hash algorithm used by the system to generate a hash, then compares that generated has with the one stored on the system. If they match, the password cracker has guessed your password.

This is very much the same process used to authenticate you to a system via a password. When you type your username and password, the system hashes the password you typed and compares that generated hash against the one stored on the system - if they match, you are authenticated.

Pre-Computed password tables exists today and they allow you to crack passwords on Lan Manager (LM) within a VERY short period of time through the use of Rainbow Tables. A Rainbow Table is a precomputed table for reversing cryptographic hash functions, usually for cracking password hashes. Tables are usually used in recovering a plaintext password up to a certain length consisting of a limited set of characters. It is a practical example of a space/time trade-off also called a Time-Memory trade off, using more computer processing time at the cost of less storage when calculating a hash on every attempt, or less processing time and more storage when compared to a simple lookup table with one entry per hash. Use of a key derivation function that employs a salt makes this attack unfeasible.

You may want to review "Rainbow Tables" at the links:
http://en.wikipedia.org/wiki/Rainbow_table
http://www.antsight.com/zsl/rainbowcrack/

Today's password crackers:
Meet oclHashcat. They are GPGPU-based multi-hash cracker using a brute-force attack (implemented as mask attack), combinator attack, dictionary attack, hybrid attack, mask attack, and rule-based attack.

This GPU cracker is a fusioned version of oclHashcat-plus and oclHashcat-lite, both very well-known suites at that time, but now deprecated. There also existed a now very old oclHashcat GPU cracker that was replaced w/ plus and lite, which - as said - were then merged into oclHashcat 1.00 again.

This cracker can crack Hashes of NTLM Version 2 up to 8 characters in less than a few hours. It is definitively a game changer. It can try hundreds of billions of tries per seconds on a very large cluster of GPU's. It supports up to 128 Video Cards at once.

I am stuck using Password what can I do to better protect myself? You could look at safer alternative such as Bcrypt, PBKDF2, and Scrypt.

bcrypt is a key derivation function for passwords designed by Niels Provos and David Mazi鏰es, based on the Blowfish cipher, and presented at USENIX in 1999. Besides incorporating a salt to protect against rainbow table attacks, bcrypt is an adaptive function:
over time, the iteration count can be increased to make it slower, so it remains resistant to brute-force search attacks even with increasing computation power.

In cryptography, scrypt is a password-based key derivation function created by Colin Percival, originally for the Tarsnap online backup service. The algorithm was specifically designed to make it costly to perform large-scale custom hardware attacks by requiring large amounts of memory. In 2012, the scrypt algorithm was published by the IETF as an Internet Draft, intended to become an informational RFC, which has since expired. A simplified version of scrypt is used as a proof-