of-work scheme by a number of cryptocurrencies, such as Litecoin and Dogecoin.

PBKDF2 (Password-Based Key Derivation Function 2) is a key derivation function that is part of RSA Laboratories' Public-Key Cryptography Standards (PKCS) series, specifically PKCS #5 v2.0, also published as Internet Engineering Task Force's RFC 2898. It replaces an earlier standard, PBKDF1, which could only produce derived keys up to 160 bits long.

PBKDF2 applies a pseudorandom function, such as a cryptographic hash, cipher, or HMAC to the input password or passphrase along with a salt value and repeats the process many times to produce a derived key, which can then be used as a cryptographic key in subsequent operations. The added computational work makes password cracking much more difficult, and is known as key stretching. When the standard was written in 2000, the recommended minimum number of iterations was 1000, but the parameter is intended to be increased over time as CPU speeds increase. Having a salt added to the password reduces the ability to use precomputed hashes (rainbow tables) for attacks, and means that multiple passwords have to be tested individually, not all at once. The standard recommends a salt length of at least 64 bits.

The other answers are incorrect:

"It prevents an unauthorized person from trying multiple passwords in one logon attempt." is incorrect because the fact that a password has been hashed does not prevent this type of brute force password guessing attempt.

"It minimizes the amount of storage required for user passwords" is incorrect because hash algorithms always generate the same number of bits, regardless of the length of the input. Therefore, even short passwords will still result in a longer hash and not minimize storage requirements.

"It minimizes the amount of processing time used for encrypting passwords" is incorrect because the processing time to encrypt a password would be basically the same required to produce a one-way has of the same password.

Reference(s) used for this question:

http://en.wikipedia.org/wiki/PBKDF2
http://en.wikipedia.org/wiki/Scrypt
http://en.wikipedia.org/wiki/Bcrypt
Harris, Shon (2012-10-18). CISSP All-in-One Exam Guide, 6th Edition (p. 195) . McGraw- Hill. Kindle Edition.

QUESTION 775
Which of the following is not a one-way hashing algorithm?

A. MD2
B. RC4
C. SHA-1
D. HAVAL

Correct Answer: B
Explanation:
RC4 was designed by Ron Rivest of RSA Security in 1987. While it is officially termed "Rivest Cipher 4", the RC acronym is alternatively understood to stand for "Ron's Code" (see also RC2, RC5 and RC6).
RC4 was initially a trade secret, but in September 1994 a description of it was anonymously

posted to the Cypherpunks mailing list. It was soon posted on the sci.crypt newsgroup, and from there to many sites on the Internet. The leaked code was confirmed to be genuine as its output was found to match that of proprietary software using licensed RC4. Because the algorithm is known, it is no longer a trade secret. The name RC4 is trademarked, so RC4 is often referred to as ARCFOUR or ARC4 (meaning alleged RC4) to avoid trademark problems. RSA Security has never officially released the algorithm; Rivest has, however, linked to the English Wikipedia article on RC4 in his own course notes. RC4 has become part of some commonly used encryption protocols and standards, including WEP and WPA for wireless cards and TLS.

The main factors in RC4's success over such a wide range of applications are its speed and simplicity: efficient implementations in both software and hardware are very easy to develop.

The following answer were not correct choices:
SHA-1 is a one-way hashing algorithms. SHA-1 is a cryptographic hash function designed by the United States National Security Agency and published by the United States NIST as a U.S. Federal Information Processing Standard. SHA stands for "secure hash algorithm".

The three SHA algorithms are structured differently and are distinguished as SHA-0, SHA- 1, and SHA-2. SHA-1 is very similar to SHA-0, but corrects an error in the original SHA hash specification that led to significant weaknesses. The SHA-0 algorithm was not adopted by many applications. SHA-2 on the other hand significantly differs from the SHA- 1 hash function.

SHA-1 is the most widely used of the existing SHA hash functions, and is employed in several widely used security applications and protocols. In 2005, security flaws were identified in SHA-1, namely that a mathematical weakness might exist, indicating that a stronger hash function would be desirable. Although no successful attacks have yet been reported on the SHA-2 variants, they are algorithmically similar to SHA-1 and so efforts are underway to develop improved alternatives. A new hash standard, SHA-3, is currently under development -- an ongoing NIST hash function competition is scheduled to end with the selection of a winning function in 2012.

SHA-1 produces a 160-bit message digest based on principles similar to those used by Ronald L.Rivest of MIT in the design of the MD4 and MD5 message digest algorithms, but has a more conservative design.

MD2 is a one-way hashing algorithms. The MD2 Message-Digest Algorithm is a cryptographic hash function developed by Ronald Rivest in 1989. The algorithm is optimized for 8-bit computers. MD2 is specified in RFC 1319. Although MD2 is no longer considered secure, even as of 2010 it remains in use in public key infrastructures as part of certificates generated with MD2 and RSA.

Haval is a one-way hashing algorithms. HAVAL is a cryptographic hash function. Unlike MD5, but like most modern cryptographic hash functions, HAVAL can produce hashes of different lengths. HAVAL can produce hashes in lengths of 128 bits, 160 bits, 192 bits, 224 bits, and 256 bits. HAVAL also allows users to specify the number of rounds (3, 4, or 5) to be used to generate the hash.

The following reference(s) were used for this question:

SHIREY, Robert W., RFC2828: Internet Security Glossary, may 2000.
https://en.wikipedia.org/wiki/HAVAL
https://en.wikipedia.org/wiki/MD2_%28cryptography%29
https://en.wikipedia.org/wiki/SHA-1

QUESTION 776
The Clipper Chip utilizes which concept in public key cryptography?

A. Substitution
B. Key Escrow
C. An undefined algorithm
D. Super strong encryption

Correct Answer: B
Explanation:
The Clipper chip is a chipset that was developed and promoted by the U.S. Government as an encryption device to be adopted by telecommunications companies for voice transmission. It was announced in 1993 and by 1996 was entirely defunct.

The heart of the concept was key escrow. In the factory, any new telephone or other device with a Clipper chip would be given a "cryptographic key", that would then be provided to the government in "escrow". If government agencies "established their authority" to listen to a communication, then the password would be given to those government agencies, who could then decrypt all data transmitted by that particular telephone.

The CISSP Prep Guide states, "The idea is to divide the key into two parts, and to escrow two portions of the key with two separate 'trusted' organizations. Then, law enforcement officals, after obtaining a court order, can retreive the two pieces of the key from the organizations and decrypt the message."

References:
http://en.wikipedia.org/wiki/Clipper_Chip

Source: KRUTZ, Ronald L.& VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, John Wiley & Sons, 2001, page 166.

QUESTION 777
What is the primary role of smartcards in a PKI?

A. Transparent renewal of user keys
B. Easy distribution of the certificates between the users
C. Fast hardware encryption of the raw data
D. Tamper resistant, mobile storage and application of private keys of the users

Correct Answer: D
Explanation:
Reference:
HARRIS, Shon, All-In-One CISSP Certification Exam Guide, 2001, McGraw- Hill/Osborne, page 139;

SNYDER, J., What is a SMART CARD?.

Wikipedia has a nice definition at: http://en.wikipedia.org/wiki/Tamper_resistance

Security

Tamper-resistant microprocessors are used to store and process private or sensitive information, such as private keys or electronic money credit. To prevent an attacker from retrieving or modifying the information, the chips are designed so that the information is not accessible

through external means and can be accessed only by the embedded software, which should contain the appropriate security measures.

Examples of tamper-resistant chips include all secure cryptoprocessors, such as the IBM 4758 and chips used in smartcards, as well as the Clipper chip.

It has been argued that it is very difficult to make simple electronic devices secure against tampering, because numerous attacks are possible, including:

physical attack of various forms (microprobing, drills, files, solvents, etc.)

freezing the device

applying out-of-spec voltages or power surges

applying unusual clock signals

inducing software errors using radiation

measuring the precise time and power requirements of certain operations (see power analysis)

Tamper-resistant chips may be designed to zeroise their sensitive data (especially cryptographic keys) if they detect penetration of their security encapsulation or out-of- specification environmental parameters. A chip may even be rated for "cold zeroisation", the ability to zeroise itself even after its power supply has been crippled.

Nevertheless, the fact that an attacker may have the device in his possession for as long as he likes, and perhaps obtain numerous other samples for testing and practice, means that it is practically impossible to totally eliminate tampering by a sufficiently motivated opponent. Because of this, one of the most important elements in protecting a system is overall system design. In particular, tamper-resistant systems should "fail gracefully" by ensuring that compromise of one device does not compromise the entire system. In this manner, the attacker can be practically restricted to attacks that cost less than the expected return from compromising a single device (plus, perhaps, a little more for kudos). Since the most sophisticated attacks have been estimated to cost several hundred thousand dollars to carry out, carefully designed systems may be invulnerable in practice.

QUESTION 778
Which of the following issues is not addressed by digital signatures?

A. nonrepudiation
B. authentication
C. data integrity
D. denial-of-service

Correct Answer: D
Explanation:
A digital signature directly addresses both confidentiality and integrity of the CIA triad. It does not directly address availability, which is what denial-of-service attacks.

The other answers are not correct because:

"nonrepudiation" is not correct because a digital signature can provide for nonrepudiation.
"authentication" is not correct because a digital signature can be used as an authentication

mechanism
"data integrity" is not correct because a digital signature does verify data integrity (as part of nonrepudiation)

References:
Official ISC2 Guide page: 227 & 265
All in One Third Edition page: 648

QUESTION 779
What are the three most important functions that Digital Signatures perform?

A. Integrity, Confidentiality and Authorization
B. Integrity, Authentication and Nonrepudiation
C. Authorization, Authentication and Nonrepudiation
D. Authorization, Detection and Accountability

Correct Answer: B
Explanation:
Reference: TIPTON, Harold F.& KRAUSE, MICKI, Information Security Management Handbook, 4th Edition, Volume 2.

QUESTION 780
Which of the following protocols that provide integrity and authentication for IPSec, can also provide non-repudiation in IPSec?

A. Authentication Header (AH)
B. Encapsulating Security Payload (ESP)
C. Secure Sockets Layer (SSL)
D. Secure Shell (SSH-2)

Correct Answer: A
Explanation:
As per the RFC in reference, the Authentication Header (AH) protocol is a mechanism for providing strong integrity and authentication for IP datagrams. It might also provide non-repudiation, depending on which cryptographic algorithm is used and how keying is performed. For example, use of an asymmetric digital signature algorithm, such as RSA, could provide non-repudiation.

from a cryptography point of view, so we will cover it from a VPN point of view here. IPSec is a suite of protocols that was developed to specifically protect IP traffic. IPv4 does not have any integrated security, so IPSec was developed to bolt onto IP and secure the data the protocol transmits. Where PPTP and L2TP work at the data link layer, IPSec works at the network layer of the OSI model. The main protocols that make up the IPSec suite and their basic functionality are as follows:
A.Authentication Header (AH) provides data integrity, data origin authentication, and protection from replay attacks.
B.Encapsulating Security Payload (ESP) provides confidentiality, data-origin authentication, and data integrity.
C.Internet Security Association and Key Management Protocol (ISAKMP) provides a framework for security association creation and key exchange.
D.Internet Key Exchange (IKE) provides authenticated keying material for use with ISAKMP.

The following are incorrect answers: