QUESTION 675
This type of attack is generally most applicable to public-key cryptosystems, what type of attack am I ?

A. Chosen-Ciphertext attack
B. Ciphertext-only attack
C. Plaintext Only Attack
D. Adaptive-Chosen-Plaintext attack

Correct Answer: A
Explanation:
A chosen-ciphertext attack is one in which cryptanalyst may choose a piece of ciphertext and attempt to obtain the corresponding decrypted plaintext. This type of attack is generally most applicable to public-key cryptosystems.

A chosen-ciphertext attack (CCA) is an attack model for cryptanalysis in which the cryptanalyst gathers information, at least in part, by choosing a ciphertext and obtaining its decryption under an unknown key. In the attack, an adversary has a chance to enter one or more known ciphertexts into the system and obtain the resulting plaintexts. From these pieces of information the adversary can attempt to recover the hidden secret key used for decryption.

A number of otherwise secure schemes can be defeated under chosen-ciphertext attack. For example, the El Gamal cryptosystem is semantically secure under chosen-plaintext attack, but this semantic security can be trivially defeated under a chosen-ciphertext attack. Early versions of RSA padding used in the SSL protocol were vulnerable to a sophisticated adaptive chosen-ciphertext attack which revealed SSL session keys. Chosen-ciphertext attacks have implications for some self-synchronizing stream ciphers as well. Designers of tamper-resistant cryptographic smart cards must be particularly cognizant of these attacks, as these devices may be completely under the control of an adversary, who can issue a large number of chosen-ciphertexts in an attempt to recover the hidden secret key.

According to RSA:
Cryptanalytic attacks are generally classified into six categories that distinguish the kind of information the cryptanalyst has available to mount an attack. The categories of attack are listed here roughly in increasing order of the quality of information available to the cryptanalyst, or, equivalently, in decreasing order of the level of difficulty to the cryptanalyst. The objective of the cryptanalyst in all cases is to be able to decrypt new pieces of ciphertext without additional information. The ideal for a cryptanalyst is to extract the secret key.

A ciphertext-only attack is one in which the cryptanalyst obtains a sample of ciphertext, without the plaintext associated with it. This data is relatively easy to obtain in many scenarios, but a successful ciphertext-only attack is generally difficult, and requires a very large ciphertext sample. Such attack was possible on cipher using Code Book Mode where frequency analysis was being used and even thou only the ciphertext was available, it was still possible to eventually collect enough data and decipher it without having the key.

A known-plaintext attack is one in which the cryptanalyst obtains a sample of ciphertext and the corresponding plaintext as well. 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.

A chosen-plaintext attack is one in which the cryptanalyst is able to choose a quantity of plaintext

and then obtain the corresponding encrypted ciphertext. 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, is a special case of chosen-plaintext attack in which the cryptanalyst is able to choose plaintext samples dynamically, and alter his or her choices based on the results of previous encryptions. The cryptanalyst makes a series of interactive queries, choosing subsequent plaintexts based on the information from the previous encryptions.

Non-randomized (deterministic) public key encryption algorithms are vulnerable to simple "dictionary"-type attacks, where the attacker builds a table of likely messages and their corresponding ciphertexts. To find the decryption of some observed ciphertext, the attacker simply looks the ciphertext up in the table. As a result, public-key definitions of security under chosen-plaintext attack require probabilistic encryption (i.e., randomized encryption). Conventional symmetric ciphers, in which the same key is used to encrypt and decrypt a text, may also be vulnerable to other forms of chosen-plaintext attack, for example, differential cryptanalysis of block ciphers.

An adaptive-chosen-ciphertext is the adaptive version of the above attack. A cryptanalyst can mount an attack of this type in a scenario in which he has free use of a piece of decryption hardware, but is unable to extract the decryption key from it.

An adaptive chosen-ciphertext attack (abbreviated as CCA2) is an interactive form of chosen-ciphertext attack in which an attacker sends a number of ciphertexts to be decrypted, then uses the results of these decryptions to select subsequent ciphertexts. It is to be distinguished from an indifferent chosen-ciphertext attack (CCA1).

The goal of this attack is to gradually reveal information about an encrypted message, or about the decryption key itself. For public-key systems, adaptive-chosen-ciphertexts are generally applicable only when they have the property of ciphertext malleability -- that is, a ciphertext can be modified in specific ways that will have a predictable effect on the decryption of that message.

A Plaintext Only Attack is simply a bogus detractor. If you have the plaintext only then there is no need to perform any attack.

References:
RSA Laboratories FAQs about today's cryptography: What are some of the basic types of

cryptanalytic attack?

also see:
http://www.giac.org/resources/whitepaper/cryptography/57.php and
http://en.wikipedia.org/wiki/Chosen-plaintext_attack

QUESTION 676
Which of the following statements pertaining to Secure Sockets Layer (SSL) is false?

A. The SSL protocol was developed by Netscape to secure Internet client-server transactions.
B. The SSL protocol's primary use is to authenticate the client to the server using public key cryptography and digital certificates.
C. Web pages using the SSL protocol start with HTTPS
D. SSL can be used with applications such as Telnet, FTP and email protocols.

Correct Answer: B
Explanation:
All of these statements pertaining to SSL are true except that it is primary use is to authenticate the client to the server using public key cryptography and digital certificates. It is the opposite, Its primary use is to authenticate the server to the client.
The following reference(s) were used for this question:
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).

QUESTION 677
Which of the following protects Kerberos against replay attacks?

A. Tokens
B. Passwords
C. Cryptography
D. Time stamps

Correct Answer: D
Explanation:
A replay attack refers to the recording and retransmission of packets on the network. Kerberos uses time stamps, which protect against this type of attack.
Source: HARRIS, Shon, All-In-One CISSP Certification Exam Guide, McGraw-Hill/Osborne, 2002, chapter 8: Cryptography (page 581).

QUESTION 678
Which of the following encryption methods is known to be unbreakable?

A. Symmetric ciphers.
B. DES codebooks.
C. One-time pads.
D. Elliptic Curve Cryptography.

Correct Answer: C
Explanation:
A One-Time Pad uses a keystream string of bits that is generated completely at random that is used only once. Because it is used only once it is considered unbreakable.

The following answers are incorrect:

Symmetric ciphers. This is incorrect because a Symmetric Cipher is created by substitution and transposition. They can and have been broken

DES codebooks. This is incorrect because Data Encryption Standard (DES) has been broken, it was replaced by Advanced Encryption Standard (AES).

Elliptic Curve Cryptography. This is incorrect because Elliptic Curve Cryptography or ECC is typically used on wireless devices such as cellular phones that have small processors. Because of the lack of processing power the keys used at often small. The smaller the key, the easier it is considered to be breakable. Also, the technology has not been around long enough or tested thourough enough to be considered truly unbreakable.

QUESTION 679
What level of assurance for a digital certificate verifies a user's name, address, social security number, and other information against a credit bureau database?

A. Level 1/Class 1
B. Level 2/Class 2
C. Level 3/Class 3
D. Level 4/Class 4

Correct Answer: B
Explanation:
Users can obtain certificates with various levels of assurance. Here is a list that describe each of them:

Class 1/Level 1 for individuals, intended for email, no proof of identity For example, level 1 certificates verify electronic mail addresses. This is done through the use of a personal information number that a user would supply when asked to register. This level of certificate may also provide a name as well as an electronic mail address; however, it may or may not be a genuine name (i.e., it could be an alias). This proves that a human being will reply back if you send an email to that name or email address.

Class 2/Level 2 is for organizations and companies for which proof of identity is required Level 2 certificates verify a user's name, address, social security number, and other information against a credit bureau database.

Class 3/Level 3 is for servers and software signing, for which independent verification and checking of identity and authority is done by the issuing certificate authority Level 3 certificates are available to companies. This level of certificate provides photo identification to accompany the other items of information provided by a level 2 certificate.

Class 4 for online business transactions between companies

Class 5 for private organizations or governmental security

References:
http://en.wikipedia.org/wiki/Digital_certificate veriSign introduced the concept of classes of digital certificates:
Also see:
Source: TIPTON, Harold F.& KRAUSE, Micki, Information Security Management Handbook, 4th edition (volume 1), 2000, CRC Press, Chapter 3, Secured Connections to External Networks

(page 54).

QUESTION 680
Which of the following would best describe a Concealment cipher?

A. Permutation is used, meaning that letters are scrambled.
B. Every X number of words within a text, is a part of the real message.
C. Replaces bits, characters, or blocks of characters with different bits, characters or blocks.
D. Hiding data in another message so that the very existence of the data is concealed.

Correct Answer: B
Explanation:
When a concealment cipher is used, every X number of words within a text, is a part of the real message. The message is within another message.

A concealment cipher is a message within a message. If my other super-secret spy buddy and I decide our key value is every third word, then when I get a message from him, I will pick out every third word and write it down. Suppose he sends me a message that reads, "The saying, `The time is right' is not cow language, so is now a dead subject." Because my key is every third word, I come up with "The right cow is dead." This again means nothing to me, and I am now turning in my decoder ring.

Concealment ciphers include the plaintext within the ciphertext. It is up to the recipient to know which letters or symbols to exclude from the ciphertext in order to yield the plaintext.
Here is an example of a concealment cipher:
i2l32i5321k34e1245ch456oc12ol234at567e

Remove all the numbers, and you'll have i like chocolate. How about this one?

Larry even appears very excited. No one worries.

The first letter from each word reveals the message leave now. Both are easy, indeed, but many people have crafted more ingenious ways of concealing the messages. By the way, this type of cipher doesn't even need ciphertext, such as that in the above examples.

Consider the invisible drying ink that kids use to send secret messages. In a more extreme example, a man named Histiaeus, during 5th century B.C., shaved the head of a trusted slave, then tattooed the message onto his bald head. When the slave's hair grew back, Histiaeus sent the slave to the message's intended recipient, Aristagoros, who shaved the slave's head and read the message instructing him to revolt.

The following answers are incorrect:

A transposition cipher uses permutations.
A substitution cipher replaces bits, characters, or blocks of characters with different bits, characters or blocks.
Steganography refers to hiding the very existence of the message.

Source: WALLHOFF, John, CBK#5 Cryptography (CISSP Study Guide), April 2002 (page 1).
and also see:
http://www.go4expert.com/forums/showthread.php?t=415

QUESTION 681