Module-1

Short Question

1. What is the OSI security architecture?
2. What is the difference between passive and active security threats?
3. List and briefly define categories of passive and active security attacks.
4. List and briefly define categories of security services.
5. List and briefly define categories of security mechanisms.
6. What are the essential ingredients of a symmetric cipher?
7. What are the two basic functions used in encryption algorithms?
8. How many keys are required for two people to communicate via a symmetric cipher?
9. What is the difference between a block cipher and a stream cipher?
10. What are the two general approaches to attacking a cipher?
11. Why do some block cipher modes of operation only use encryption while others use both encryption and decryption?
12. What is triple encryption?
13. Why is the middle portion of 3DES a decryption rather than an encryption?

Long Question

1. Consider an automated teller machine (ATM) in which users provide a personal identification number (PIN) and a card for account access. Give examples of confidentiality, integrity, and availability requirements associated with the system. In each case, indicate the degree of importance of the requirement.
2. Repeat Problem 1.1 for a telephone switching system that routes calls through a switching network based on the telephone number requested by the caller.
3. Consider a desktop publishing system used to produce documents for various organizations.
   a. Give an example of a type of publication for which confidentiality of the stored data is the most important requirement.
   b. Give an example of a type of publication in which data integrity is the most important requirement.
   c. Give an example in which system availability is the most important requirement.
4. For each of the following assets, assign a low, moderate, or high impact level for the loss of confidentiality, availability, and integrity, respectively. Justify your answers.
   a. An organization managing public information on its Web server.
   b. A law-enforcement organization managing extremely sensitive investigative information.
   c. A financial organization managing routine administrative information (not privacy-related information).
   d. An information system used for large acquisitions in a contracting organization that contains both sensitive, pre-solicitation phase contract information and routine...
administrative information. Assess the impact for the two data sets separately and the information system as a whole.
e. A power plant contains a SCADA (supervisory control and data acquisition) system controlling the distribution of electric power for a large military installation. The SCADA system contains both real-time sensor data and routine administrative information. Assess the impact for the two data sets separately and the information system as a whole.

5. Draw a matrix that shows the relationship between security services and attacks.
6. Draw a matrix that shows the relationship between security mechanisms and attacks.
7. This problem uses a real-world example of a symmetric cipher, from an old U.S. Special Forces manual (public domain). The document, filename SpecialForces.pdf, is available at this book’s Web site.
a. Using the two keys (memory words) cryptographic and network security, encrypt the following message:
   Be at the third pillar from the left outside the lyceum theatre tonight at seven. If you are distrustful bring two friends.
Make reasonable assumptions about how to treat redundant letters and excess letters in the memory words and how to treat spaces and punctuation. Indicate what your assumptions are. Note: The message is from the Sherlock Holmes novel, The Sign of Four.
b. Decrypt the ciphertext. Show your work.
c. Comment on when it would be appropriate to use this technique and what its advantages are.

8. Show that Feistel decryption is the inverse of Feistel encryption.
9. Consider a Feistel cipher composed of 16 rounds with block length 128 bits and key length 128 bits. Suppose that, for a given k, the key scheduling algorithm determines values for the first eight round keys, k1, k2, . . . , k8, and then sets k9 = k8, k10 = k7, k11 = k6, . . . , k16 = k1
   Suppose you have a ciphertext c. Explain how, with access to an encryption oracle, you can decrypt c and determine m using just a single oracle query. This shows that such a cipher is vulnerable to a chosen plaintext attack. (An encryption oracle can be thought of as a device that, when given a plaintext, returns the corresponding ciphertext. The internal details of the device are not known to you, and you cannot break open the device. You can only gain information from the oracle by making queries to it and observing its responses.)

10. What RC4 key value will leave S unchanged during initialization? That is, after the initial permutation of S, the entries of S will be equal to the values from 0 through 255 in ascending order.
11. Is it possible to perform encryption operations in parallel on multiple blocks of plaintext in CBC mode? How about decryption?
12. Suppose an error occurs in a block of ciphertext on transmission using CBC. What effect is produced on the recovered plaintext blocks?
Multiple Choice Questions

1. Security is not as simple as it might first appear to the novice.
2. In developing a particular security mechanism or algorithm, one must NOT consider potential attacks on those security features.
3. Having designed various security mechanisms, it is necessary to decide where to use them.
4. Security mechanisms typically involve more than a particular algorithm or protocol.
5. Computer and network security is essentially a battle of wits between a perpetrator who tries to find holes and the designer or administrator who tries to close them.
6. There is a natural tendency on the part of users and system managers to perceive little benefit from security investment before a security failure occurs.
7. Security does not require regular monitoring.
8. Security is still too often an afterthought to be incorporated into a system after the design is complete rather than being an integral part of the design process.
9. Attack is a potential for violation of security, which exists when there is a circumstance, capability, action, or event that could breach security and cause harm. That is, a threat is a possible danger that might exploit vulnerability.
10. Threat is an assault on system security that derives from an intelligent threat. That is, an intelligent act that is a deliberate attempt (especially in the sense of a method or technique) to evade security services and violate the security policy of a system.

Fill in the blanks:

1. The generic name for the collection of tools designed to protect data and to thwart hackers is ______________.
2. ______________ assures that private or confidential information is not made available or disclosed to unauthorized individuals.
3. ______________ assures that individuals control or influence what information related to them may be collected and stored and by whom and to whom that information may be disclosed.
4. ______________ assures that information and programs are changed only in a specified and authorized manner.
5. ______________ assures that a system performs its intended function in an unimpaired manner, free from deliberate or inadvertent unauthorized manipulation of the system.
6. ______________ assures that systems work promptly and service is not denied to authorized users.
7. Preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information is known as ______________.
8. Guarding against improper information modification or destruction, including ensuring information non-repudiation and authenticity is known as ______________.
9. Ensuring timely and reliable access to and use of information is known as ____________.
10. ____________ is verifying the users who they say they are
11. __________________