AMRAPALI INSTITUTE, HALDWANI
MID TERM EXAMINATION, MARCH 2008
CRYPTOGRAPHY AND NETWORK SECURITY (MCA 4.4(2))

TIME: 2 HRS **MM: 100**

NOTE: Attemt any five questions

1. a. What is the OSI security architecture?

Answer

The OSI Security Architecture is a framework that provides a systematic way of defining the requirements for security and characterizing the approaches to satisfying those requirements. The document defines security attacks, mechanisms, and services, and the relationships among these categories.

b. What is the difference between passive and active security threats?

Answer

***Passive attacks** have to do with eavesdropping on, or monitoring, transmissions. Electronic mail, file transfers, and client/server exchanges are examples of transmissions that can be monitored. **Active attacks** include the modification of transmitted data and attempts to gain unauthorized access to computer systems.*

c. List and briefly define categories of passive and active security attacks.

Answer

***Passive attacks:** release of message contents and traffic analysis. **Active attacks:** masquerade, replay, modification of messages, and denial of service*.

d. List and briefly define categories of security services.

Answer

***Authentication:** The assurance that the communicating entity is the one that it claims to be.*
***Access control:** The prevention of unauthorized use of a resource (i.e., this service controls who can have access to a resource, under what conditions access can occur, and what those accessing the resource are allowed to do).*
***Data confidentiality:** The protection of data from unauthorized disclosure.*
***Data integrity:** The assurance that data received are exactly as sent by an authorized entity (i.e., contain no modification, insertion, deletion, or replay).*
***Nonrepudiation:** Provides protection against denial by one of the entities involved in a communication of having participated in all or part of the communication.*
***Availability service:** The property of a system or a system resource being accessible and usable upon demand by an authorized system entity, according to performance specifications for the system (i.e., a system is available if it provides services according to the system design whenever users request them).*

2. a. List and briefly define categories of security mechanisms.

Answer

See table 1.3 of chapter 1, William Stallings book

b. What are the essential ingredients of a symmetric cipher?

Answer

Plaintext, encryption algorithm, secret key, ciphertext, decryption algorithm.

c. What are the two basic functions used in encryption algorithms?

Answer

Permutation and substitution.

d. How many keys are required for two people to communicate via a cipher?

Answer

One key for symmetric ciphers, two keys for asymmetric ciphers.

3. a. What is the difference between a block cipher and a stream cipher?

Answer

*A **stream cipher** is one that encrypts a digital data stream one bit or one byte at a time. A **block cipher** is one in which a block of plaintext is treated as a whole and used to produce a ciphertext block of equal length.*

b. What are the two general approaches to attacking a cipher?

Answer

Cryptanalysis and brute force.

c. List and briefly define types of cryptanalytic attacks based on what is known to the attacker.

Answer

__Ciphertext only__. One possible attack under these circumstances is the brute-force approach of trying all possible keys. If the key space is very large, this becomes impractical. Thus, the opponent must rely on an analysis of the ciphertext itself, generally applying various statistical tests to it. __Known plaintext.__ The analyst may be able to capture one or more plaintext messages as well as their encryptions. With this knowledge, the analyst may be able to deduce the key on the basis of the way in which the known plaintext is transformed. __Chosen plaintext.__ If the analyst is able to choose the messages to encrypt, the analyst may deliberately pick patterns that can be expected to reveal the structure of the key.

d. What is the difference between an unconditionally secure cipher and a computationally secure cipher?

Answer

An encryption scheme is __unconditionally secure__ if the ciphertext generated by the scheme does not contain enough information to determine uniquely the corresponding plaintext, no matter how much ciphertext is available. An encryption scheme is said to be __computationally secure__ if: (1) the *cost of breaking the cipher exceeds the value of the encrypted information, and (2) the time required to break the cipher exceeds the useful lifetime of the information.*

4. a. Briefly define the Caesar cipher.

Answer

*The **Caesar cipher** involves replacing each letter of the alphabet with the letter standing k places further down the alphabet, for k in the range 1 through 25.*

b. Briefly define the monoalphabetic cipher.

Answer

*A **monoalphabetic substitution cipher** maps a plaintext alphabet to a ciphertext alphabet, so that each letter of the plaintext alphabet maps to a single unique letter of the ciphertext alphabet.*

c. Briefly define the Playfair cipher.

Answer

*The **Playfair algorithm** is based on the use of a 5 × 5 matrix of letters constructed using a keyword. Plaintext is encrypted two letters at a time using this matrix.*

d. What is the difference between a monoalphabetic cipher and a polyalphabetic cipher?

Answer

*A **polyalphabetic substitution cipher** uses a separate monoalphabetic substitution cipher for each successive letter of plaintext, depending on a key.*

5. a. What are two problems with the one-time pad?

Answer

1. *There is the practical problem of making large quantities of random keys. Any heavily used system might require millions of random characters on a regular basis. Supplying truly random characters in this volume is a significant task.*

2. *Even more daunting is the problem of key distribution and protection. For every message to be sent, a key of equal length is needed by both sender and receiver. Thus, a mammoth key distribution problem exists.*

b. What is a transposition cipher?

Answer

*A **transposition cipher** involves a permutation of the plaintext letters.*

c. What is steganography?

Answer

Steganography involves concealing the existence of a message.

d. A generalization of the Caesar cipher, knows as the affine Caesar cipher, has the following form: For each plaintext letter p, substitute the ciphertext letter C:

C = E ([a, b], p) = (ap + b) mod 26

A basic requirement of any encryption algorithm is that it be one-to-one. That is, if p # q. then E(k,p) # E (k,q). Otherwise, decryption is impossible, because more than one plaintext character maps into the same ciphertext character. The affine Caesar cipher is not one-to-one for all values of a. For example, for a = 2 and b = 3, then E ([a, b], 0) = E ([a, b], 13) = 3.

I. Are there any limitations on the value of b? Explain why or why not.
II. Determine which values of a are not allowed.
III. Provide a general statement of which values of a are and are not allowed. Justify your statement.

Answer

a. *No. A change in the value of b shifts the relationship between plaintext letters and ciphertext letters to the left or right uniformly, so that if the mapping is one-to-one it remains one-to-one.*

b. *2, 4, 6, 8, 10, 12, 13, 14, 16, 18, 20, 22, 24. Any value of a larger than 25 is equivalent to a mod 26.*

c. *The values of a and 26 must have no common positive integer factor other than 1. This is equivalent to saying that a and 26 are relatively prime, or that the greatest common divisor of a and 26 is 1. To see this, first note that $E(a, p) = E(a, q)$ $(0 \le p \le q < 26)$ if and only if $a(p - q)$ is divisible by 26.* ***1.*** *Suppose that a and 26 are relatively prime. Then, $a(p - q)$ is not divisible by 26, because there is no way to reduce the fraction a/26 and $(p - q)$ is less than 26.* ***2.*** *Suppose that a and 26 have a common factor $k > 1$. Then $E(a, p) = E(a, q)$, if $q = p + m/k \neq p$.*

6. a. A ciphertext has been generated with an affine cipher. The most frequent letter of the ciphertext is 'B', and the second most frequent letter of the ciphertext is 'U', Break this code.

Answer

Assume that the most frequent plaintext letter is e and the second most frequent letter is t. Note that the numerical values are e = 4; B = 1; t = 19; U = 20. Then we have the following equations:

$1 = (4a + b) \bmod 26$
$20 = (19a + b) \bmod 26$

Thus, $19 = 15a \bmod 26$. By trial and error, we solve: $a = 3$.
Then $1 = (12 + b) \bmod 26$. By observation, $b = 15$.

b. A disadvantage of the general monoalphabetic cipher is that both sender and receiver must commit the permuted cipher sequence to memory. A common technique for avoiding this is to use a keyword from which the cipher sequence can be generated. For example, using the keyword CIPHER, write out the keyword followed by unused letters in normal order and match this against the plaintext letters:

Plain: a b c d e f g I j k l m n o p q r s t u v w x y z
Cipher: C I P H E R A B D F G J K L M N O P Q S T U V W X Y Z

If it is felt that this process does not produce sufficient mixing, write the remaining letters on successive lines and then generate the sequence by reading down the columns:

C	I	P	H	E	R
A	B	D	F	G	J
K	L	M	N	O	Q
S	T	U	V	W	X
Y	Z				

This yields the sequence

C A K S Y I B L T Z P D M U H F N V E G O W R J Q X

Such a system is used in the example in Section 2.2 (the one that begins " it was disclosed yesterday"). Determine the keyword.

Answer

SPUTNIK

c. When the PT-109 American patrol boat, under the command of Lieutenant John F. Kennedy, was sunk by a Japanese destroyer, a message was received at an Australian wireless station in playfair code:

```
 KXJEY   UREBE   ZWEHE   WRYTU   HEYFS
 KREHE  GOYFI    WTTTU    OLKSY   CAJPO
BOTEI    ZONTX   BOBNT   GONEY   CUZWR
GDSON   SXBOU   YWRHE   BAAHY  USEDQ
```

The key used was royal new Zealand navy. Decrypt the message, Translate TT into tt.

Answer

PT BOAT ONE OWE NINE LOST IN ACTION IN BLACKETT STRAIT TWO MILES SW MERESU COVE X CREW OF TWELVE X REQUEST ANY INFORMATION

d. I. Construct a Playfair matrix with the key largest.
II. Construct a Playfair matrix with the key occruuence. Make a reasonable assumption about how to treat redundant letters in the key.

Answer

a.

L	A	R	G	E
S	T	B	C	D
F	H	I/J	K	M
N	O	P	Q	U
V	W	X	Y	Z

b.

O	C	U	R	E
N	A	B	D	F
G	H	I/J	K	L
M	P	Q	S	T
V	W	X	Y	Z

7. a. (I) Using this playfair matrix.

M	F	H	I/G	K
U	N	O	P	Q
Z	V	W	X	Y
E	L	A	R	G
D	S	T	B	C

Encrypt this message:

Must see your over cadogan west. Coming at once.

Note: The message is from the Sherlock Holmes story, The Adventure of the Bruce-Partington Plans.

II. How do you account for the results of this problem? Can your generalize your conclusion?

Answer

a. UZTBDLGZPNNWLGTGTUEROVLDBDUHFPERHWQSRZ

b. UZTBDLGZPNNWLGTGTUEROVLDBDUHFPERHWQSRZ

c. A cyclic rotation of rows and/or columns leads to equivalent substitutions. In this case, the matrix for part a of this problem is obtained from the matrix of Problem 2.10a, by rotating the columns by one step and the rows by three steps.

b. I. How many possible keys does the Playfair cipher have? Ignore the fact that some keys might produce identical encryption results. Express your answer as an approximate power of 2.

II. Now take into account the fact that some Playfair keys produce the same encryption results. How many effectively unique keys does the Playfair cipher have?

Answer

a. *$25! \approx 2^{84}$*

b. *Given any 5x5 configuration, any of the four row rotations is equivalent, for a total of five equivalent configurations. For each of these five configurations, any of the four column rotations is equivalent. So each configuration in fact represents 25 equivalent configurations. Thus, the total number of unique keys is 25!/25 = 24!*