COMP/IT-424 Assignment 1

Ferid Ruano
Tuesday / Thursday 12:00 PM
February 11, 2020

TRUE OR FALSE

1. The OSI security architecture provides a systematic framework for defining security attacks, mechanisms, and services. **True**
2. Authentication protocols and encryption algorithms are example of security mechanisms. **True**
3. Security services include access control, data confidentiality and data integrity, but do not include authentication. **True**
4. Patient allergy information is an example of an asset with a high requirement for integrity **True**
5. Data origin authentication does not provide protection against the modification of data unit. **True**
6. The connection- oriented integrity service addresses both message stream modification and denial of service. **True**
7. Information access threats intercept or modify data on behalf of users who should not have access to that data. **True**
8. Symmetric encryption is used to conceal the contents of blocks or streams of data of any size, including messages, files, encryption keys, and passwords. **True**
9. Symmetric encryption remains by far the most widely used of the two types of encryption. **True**
10. Symmetric encryption is a form of cryptosystem in which encryption and decryption are performed using different keys. It is also known as non- conventional encryption. **False**
11. The process of converting from plaintext to ciphertext is known as deciphering or decryption. **False**
12. When using symmetric encryption it is very important to keep the algorithm secret. **False**
13. Ciphertext generated using a computationally secure encryption scheme is impossible for an opponent to decrypt simply because the required information is not there. **False**
14. A scheme known as a one-time pad is unbreakable because it produces random output that bears no statistical relationship to the plaintext. **True**
15. The most widely used cipher is the Data Encryption Standard. **True**

COMP/IT-424 Assignment 1

MULTIPLE CHOICE

1. __________ is the most common method used to conceal small blocks of data, such as encryption keys and hash function values, which are used in digital signatures.

   A) Symmetric encryption
   B) Data integrity algorithms

   C) Asymmetric encryption
   D) Authentication protocols

2. __________ involves the passive capture of a data unit and its subsequent retransmission to produce an unauthorized effect.

   A) Disruption
   B) Replay

   C) Service denial
   D) Masquerade

3. A loss of __________ is the unauthorized disclosure of information.

   A) authenticity
   B) confidentiality

   C) reliability
   D) integrity

4. A _________ level breach of security could cause a significant degradation in mission capability to an extent and duration that the organization is able to perform its primary functions, but the effectiveness of the functions is significantly reduced.

   A) catastrophic
   B) moderate

   C) low
   D) high

5. A __________ takes place when one entity pretends to be a different entity.

   A) replay
   B) masquerade

   C) service denial
   D) passive attack

6. A(n) _________ service is one that protects a system to ensure its availability and addresses the security concerns raised by denial- of- service attacks.

A) replay **B) availability**

C) masquerade D) integrity

7. A(n) _________ 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.

A) threat B) attack
C) risk D) attack vector

8. Data appended to, or a cryptographic transformation of, a data unit that allows a recipient of the data unit to prove the source and integrity of the data unit and protect against forgery is a(n) __________ .

A) security audit trail **B) digital signature**

C) encipherment D) authentication exchange

9. _________ techniques map plaintext elements (characters, bits) into ciphertext elements.

A) Transposition **B) Substitution**

C) Traditional D) Symmetric

10. An original intelligible message fed into the algorithm as input is known as ________ , while the coded message produced as output is called the _________ .

A) decryption, encryption **B) plaintext, ciphertext**

C) deciphering, enciphering D) cipher, plaintext

11. A _________ attack involves trying every possible key until an intelligible translation of the ciphertext is obtained.

A) brute-force B) Caesar attack

C) ciphertext only D) chosen plaintext

12. The __________ takes the ciphertext and the secret key and produces the original plaintext. It is essentially the encryption algorithm run in reverse.

    A) Voronoi algorithm

    B) decryption algorithm

    C) cryptanalysis

    D) diagram algorithm

13. _________ attacks exploit the characteristics of the algorithm to attempt to deduce a specific plaintext or to deduce the key being used.

    A) Brute-force

    B) Cryptanalytic

    C) Block cipher

    D) Transposition

14. The _________ attack is the easiest to defend against because the opponent has the least amount of information to work with.

    A) ciphertext-only

    B) chosen ciphertext

    C) known plaintext

    D) chosen plaintext

15. A way to improve on the simple monoalphabetic technique is to use different monoalphabetic substitutions as one proceeds through the plaintext message. The general name for this approach is __________ .

    A) rail fence cipher

    B) cryptanalysis

    C) polyalphabetic substitution cipher

    D) polyanalysis cipher

16. The methods of _________ conceal the existence of the message in a graphic image.

    A) steganography

    B) decryptology

    C) cryptology

    D) cryptography

SHORT ANSWER

1. A **Security Mechanism** is any process, or a device incorporating such a process, that is designed to detect, prevent, or recover from a security attack. Examples are encryption algorithms, digital signatures and authentication protocols.

2. An **Active** attack attempts to alter system resources or affect their operation.

3. "The protection afforded to an automated information system in order to attain the applicable objectives of preserving the integrity, availability and confidentiality of information system resources" is the definition of **Computer Security**.

4. A loss of **Availability** is the disruption of access to or use of information or an information system.

5. Irreversible **Encipherment** mechanisms include hash algorithms and message authentication codes, which are used in digital signature and message authentication applications.

6. In the United States, the release of student grade information is regulated by the **FERPA**.

7. A loss of **Integrity** is the unauthorized modification or destruction of information.

8. A **Passive** attack attempts to learn or make use of information from the system but does not affect system resources.

9. **Symmetric** encryption is a form of cryptosystem in which encryption and decryption are performed using the same key.

10. A technique for hiding a secret message within a larger document or picture in such a way that others cannot discern the presence or contents of the hidden message is **Steganography**.

11. An encryption scheme is said to be **Computationally Secure** if the cost of breaking the cipher exceeds the value of the encrypted information and the time required to break the cipher exceeds the useful lifetime of the information.

12. The two types of attack on an encryption algorithm are cryptanalysis based on properties of the encryption algorithm, and **Brute Force** which involves trying all possible keys.

13. Cryptographic systems are characterized along three independent dimensions: The type of operations used for transforming plaintext to ciphertext; The way in which the plaintext is processed; and **Number of Keys Used** .

14. All encryption algorithms are based on two general principles: substitution and **Transposition**.

15. One of the simplest and best known polyalphabetic ciphers is **Vigenere** cipher. In this scheme, the set of related monoalphabetic substitution rules consists of the 26 Caesar ciphers with shifts of 0 through 25. Each cipher is denoted by a key letter which is the ciphertext letter that substitutes for the plaintext letter a.

CIPHER PROBLEMS

COMP/IT-424 Assignment 1

1. Construct a Playfair matrix with the key *largest*.

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

2. Construct a Playfair matrix with the key *occurrence*. Make a reasonable assumption about how to treat redundant letters in the key.

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

3. a. Using the following Playfair matrix:

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

Encrypt the message

Must see you over Cadogan West Coming at Once

Encrypted Message: UZTB DLG ZPN NWLG TGTUERO VLDB DUHFPE RH WQSRZ

b. Repeat part a. above using the Playfair matrix from Problem 1

Encrypted Message: UZTB DLG ZPN NWLG TGTUERO VLDB DUHFPE RH WQSRZ

c. How do you account for these results? Can you generalize your conclusion?

COMP/IT-424 Assignment 1

Encrypt

- Same Row - Right Shift
- Same Column - Down Shift
- Any Rectangle - Slope of imaginary line between both elements in matrix
  - Negative Slope: Right shift top and left shift bottom until other element's column.
  - Positive Slope: Left shift top and right shift bottom until other element's column.
- Odd length messages appended with an X.

4. A certain symmetric encryption system E1 uses the following secret key (K1) for confidential communication between A and B **FEA01FAA3459012D (hex)**
A decides to deliver this secret key (K1) to B by transmitting it over the same insecure channel using a second encryption scheme E2

a- What method of encryption would you suggest for E2?

Public key cryptography that uses RSA encryption to send data over an insecure network.

b- Based on your suggestion, what would be the size in bits of the key (K2) used in encryption system E2?

The commonly used size in bits is 2048. So, 2048 bits.

c- If a system of computers has the ability to try 64 keys every 100 microseconds in an effort to decipher the message encrypted by E1 by brute force, how long (on average) would it take to break the code?

At 64 keys per 100 milliseconds, a brute force attack would take 2^{64} **/ (1 / 0.0001 * 64*60*60*24*345) = 966956.441733 Years**

d- Is E1 computationally secure?

Using brute force, E1 would be computationally secure.

5. The Vigenere Cipher:

This problem explores the use of a one-time pad version of the Vigenere cipher. In this scheme the key is a stream of random numbers between 0 and 26. For example if the key is 3 19 5… then the first letter of the plaintext is encrypted with a shift of 3 letters, the second with a shift of 19 letters, the third with a shift of 5 letters and so on.

a. Encrypt the plaintext **sendmoremoney** with the keystream

$C_i = (M_i + K_i) \% 26$

9 0 1 7 23 15 21 14 11 11 2 8 9

Encryption: BEOKJDMSXZPMH

b. Using the ciphertext obtained in part a above, find a key so that the cipher decrypts to the plaintext **cashnotneeded**

$K_i = (C_i - M_i)\ OR\ K_i = 26 - (C_i - M_i)$

COMP/IT-424 Assignment 1

Key: 25 4 22 3 22 15 19 5 19 21 12 8 4