COMP/IT-424 Classwork 1

TRUE OR FALSE

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

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 _the 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 _Viginere__ 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.

Questions

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

Unconditionally cannot be broken as the information is not there.

Computationally

The cost of breaking the cipher exceeds the value of the encrypted information

• The time required to break the cipher exceeds the useful lifetime of the information

2. What are the two main problems with the one-time pad.
Key distribution problem
practical problem of making large quantities of
random keys
.

Problems

Rectangular Transposition:

It’s a 3 x 5 Matrix as shown:

HEOTC
STSAI
LERCA

The key is 41253

Plaintext is The coast is clear

The Playfair Cipher:

Plaintext is

```
PT BOAT ONE OWE NINE LOST IN ACTION IN BLACKETT

STRAIT TWO MILES SW MERESU COVE X CREW OF TWELVE

X REQUEST ANY INFORMATION.
```