Classwork Week 2

True or False

1. Security attacks are classified as either passive or aggressive.

2. The more critical a component or service, the higher the level of required availability.

3. The field of network and Internet security consists of measures to deter, prevent, detect and correct security violations that involve the transmission of information.

4. The OSI security architecture was not developed as an international standard, therefore causing an obstacle for computer and communication vendors when developing security features.

5. The emphasis in dealing with active attacks is on prevention rather than detection.

6. All the techniques for providing security have two components: a security- related transformation on the information to be sent and some secret information shared by the two principals.

7. The data integrity service inserts bits into gaps in a data stream to frustrate traffic analysis attempts.

8. Rotor machines are sophisticated pre-computer hardware devices that use substitution techniques.

9. With the use of symmetric encryption, the principal security problem is maintaining the secrecy of the key.

10. An algorithm will produce a different output depending on the specific secret key being used at the time. The exact substitutions and transformations performed by the algorithm depend on the key.

11. On average, half of all possible keys must be tried to achieve success with a brute-force attack.

12. Mono-alphabetic ciphers are easy to break because they reflect the frequency data of the original alphabet.

13. A scheme known as a one-time pad is unbreakable because it produces random output that bears no statistical relationship to the plaintext.

14. The one-time pad has unlimited utility and is useful primarily for high-bandwidth

channels requiring low security.

15. Steganography renders the message unintelligible to outsiders by various transformations of the text.

Multiple Choice

1. A common technique for masking contents of messages or other information traffic so that opponents can not extract the information from the message is _____ .

   A) integrity B) encryption

   C) analysis D) masquerade

2. The three concepts that form what is often referred to as the CIA triad are _____ . These three concepts embody the fundamental security objectives for both data and for information and computing services.

   A) confidentiality, integrity and availability

   B) communication, integrity and authentication

   C) confidentiality, integrity, access control

   D) communication, information and authenticity

3. Verifying that users are who they say they are and that each input arriving at the system came from a trusted source is _____ .

   A) authenticity B) credibility

   C) accountability D) integrity

4. A _____ is any action that compromises the security of information owned by an organization.

   A) security attack B) security service

   C) security alert D) security mechanism

5. _____ is the protection of transmitted data from passive attacks.

   A) Access control B) Data control

   C) Nonrepudiation D) Confidentiality

6. _____ threats exploit service flaws in computers to inhibit use by legitimate users.

   A) Information access B) Reliability

   C) Passive D) Service

7. The protection of the information that might be derived from observation of traffic flows is _____ .

   A) connectionless confidentiality B) connection confidentiality

   C) traffic- flow confidentiality D) selective- field confidentiality

8. Joseph Mauborgne proposed an improvement to the Vernam cipher that uses a random key that is as long as the message so that the key does not need to be repeated. The key is used to encrypt and decrypt a single message and then is discarded. Each new message requires a new key of the same length as the new message. This scheme is known as a(n) _____ .

   A) pascaline B) one-time pad

   C) polycipher D) enigma

9. Restoring the plaintext from the ciphertext is _____ .

   A) deciphering B) transposition

   C) steganography D) encryption

10. Techniques used for deciphering a message without any knowledge of the enciphering details is _____ .

    A) blind deciphering B) steganography

C) cryptanalysis D) transposition

11. If both sender and receiver use the same key, the system is referred to as:

A) public-key encryption B) two-key

C) asymmetric D) conventional encryption

12. The _____ was used as the standard field system by the British Army in World War I and was used by the U.S. Army and other Allied forces during World War II.

A) Caesar cipher B) Playfair cipher

C) Hill cipher D) Rail Fence cipher

13. _____ refer to common two-letter combinations in the English language.

A) Streaming B) Transposition

C) Digrams D) Polyalphabetic cipher

14. A technique referred to as a _____ is a mapping achieved by performing some sort of permutation on the plaintext letters.

A) transposition cipher B) polyalphabetic cipher

C) Caesar cipher D) monoalphabetic cipher

Short Answer

1. The _____ service is concerned with assuring the recipient that the message is from the source that it claims to be from. This service must also assure that the connection is not interfered with in such a way that a third party can masquerade as one of the two legitimate parties for the purposes of unauthorized transmission or reception.

2. Two specific authentication services defined in X.800 are peer entity authentication and _____ authentication.

Classwork Week 2

3. In the context of network security, _____ is the ability to limit and control the access to host systems and applications via communications links.

4. _____ prevents either sender or receiver from denying a transmitted message. Thus, when a message is sent, the receiver can prove that the alleged sender in fact sent the message and when a message is received, the sender can prove that the alleged receiver in fact received the message.

5. Viruses and worms are two examples of _____ attacks. Such attacks can be introduced into a system by means of a disk that contains the unwanted logic concealed in otherwise useful software. They can also be inserted into a system across a network.

6. An _____ is an assault on system security that derives from an intelligent act that is a deliberate attempt to evade security services and violate the security policy of a system.

7. _____ is the use of a trusted third party to assure certain properties of a data exchange.

8. A _____ cipher processes the input one block of elements at a time producing an output block for each input block whereas a _____ cipher processes the input elements continuously producing output one element at a time.

9. An encryption scheme is _____ 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.

10. The earliest known and simplest use of a substitution cipher was called the _____ cipher and involved replacing each letter of the alphabet with the letter standing three places further down the alphabet.

11. The best known multiple letter encryption cipher is the _____ which treats digrams in the plaintext as single units and translates these units into ciphertext digrams.

12. The task of making large quantities of random keys on a regular basis and distributing a key of equal length to both sender and receiver for every message sent are difficulties of the _____ scheme.

13. The simplest transposition cipher is the _____ technique in which the plaintext is written down as a sequence of diagonals and then read off as a sequence of rows.

14. The most widely used cipher ever is the _____ .

Classwork Week 2

15. The _____ consist of a set of independently rotating cylinders through which electrical pulses can flow. Each cylinder has 26 input pins and 26 output pins with internal wiring that connects each input pin to a unique output pin.

Questions

1. What is the difference between an unconditionally secure cipher and a computationally secure cipher?
2. What are the two main problems with the one-time pad.

Problems

Rectangular Transposition:

Eve has stumbled upon the encrypted message

HEOT CSTS AILE RCA

After a productive interrogation, she determines that the message was encrypted using (horizontal) rectangular transposition. Noting that there are $15 = 3 \times 5$ letters in the ciphertext, she establishes that the message has been written as either a 3×5 matrix, or a 5×3 matrix. (If it were 1×15, it would have been explained as a transposition cipher, rather than rectangular transposition). She writes them both down:

```
HEO
TCS
TSA
ILE
RCA
```

```
HEOTC
STSAI
LERCA
```

After some trial and error and rearrangement Eve managed to break the code and retrieve the plaintext. Can you? (Show your work)

Classwork Week 2

The Playfair Cipher:

Perhaps the most famous cipher of 1943 involved the future president of the U.S., J. F. Kennedy, Jr. On 2 August 1943, Australian Coastwatcher Lieutenant Arthur Reginald Evans of the Royal Australian Naval Volunteer Reserve saw a pinpoint of flame on the dark waters of Blackett Strait from his jungle ridge on Kolombangara Island, one of the Solomons. He did not know that the Japanese destroyer Amagiri had rammed and sliced in half an American patrol boat PT-109, under the command of Lieutenant John F. Kennedy, United States Naval Reserve. Evans received the following message at 0930 on the morning of the 2 of August 1943:

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

The coastwatchers regularly used the Playfair system. Evans deciphered it with the key

ROYAL NEW ZEALAND NAVY

About ten hours later, at 10:00 p.m. Kennedy and his crew were rescued.
Can you decrypt the cipher text? (Translate TT into tt) (Show your work)