

Tutorial Sheet #01 (Network Security)

T1: What are the goals of Network Security? Explain the Taxonomy of attacks with relation to security goals.

T2: What are the various security mechanism to provide the security services in network security? Explain.

T3: What is steganography? Write procedure to hide “Hi” in the sentence “ A friend called a doctor”.

T4: Explain about the various types of active and passive attacks on the network in detail.

T5: Explain how attackers uses the following methods to attack in the network:

- (i) Packet sniffing
- (ii) Packet spoofing
- (iii) DNS spoofing

T6: List the various Symmetrical key cryptographic techniques.

T7: Use Brute-force attack to decipher the following message. Assume that you know it is an affine cipher and that the plain text “ab” is enciphered to “GL”.

XPALASXYFGFUKPXUSOGEUTKCDGFXANMGNVS

T8: Encrypt the message “this is an exercise” using one of the following ciphers. Ignore the space between words. Decrypt the message to get the original plaintext.

- a. Additive cipher with key = 20
- b. Multiplicative cipher with key = 15
- c. Affine cipher with key = (15, 20)

T9: Use a brute-force attack to decipher the following message enciphered by Alice using an additive cipher. Suppose that Alice always uses a key that is close to her birthday, which is on the 13th of the month:

NCJAEZRCLASJLYODEPRLYZRCLASJLCPEHZDTOPDZQLNZTY

T10: The plaintext “letusmeetnow” and the corresponding cipher text “HBCDFNOPIKLB” are given. You know that the algorithm is a Hill cipher, but you don’t know the size of the key. Find the key matrix.

T11: Eve has intercepted the following cipher text, using statistical attack find the plain text:

XLILSYWIMWRSAJSVWEPIJSVJSYVQMPPMSRHSPPEVWMXMWASVX-LQSVILY-
VVCFIJSVIXLIWIPPIV/VIGIMZIWQSVISJJVW

Soln1:

What are the goals of Network Security? Explain the Taxonomy of attacks with relation to security goals

The goals of network security are to protect the confidentiality, integrity, and availability of information and network resources. These three goals are commonly referred to as the CIA triad:

1. Confidentiality: This refers to the protection of information from unauthorized access, disclosure, or exposure.
2. Integrity: This refers to the protection of information from unauthorized modification or destruction, ensuring that it remains accurate and complete.
3. Availability: This refers to the protection of information and network resources from denial of service attacks, ensuring that they are accessible to authorized users when needed.

To achieve these goals, various security measures are implemented, such as firewalls, encryption, access controls, intrusion detection and prevention systems, and so on.

Attacks on network security can be classified into different categories based on the security goals they aim to compromise. Here is a taxonomy of attacks with relation to security goals:

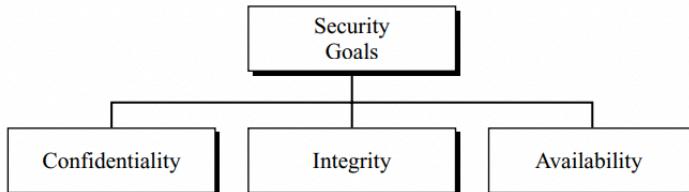
1. Confidentiality attacks: These attacks aim to breach the confidentiality of information, and examples include eavesdropping, data interception, and data theft.
2. Integrity attacks: These attacks aim to modify or destroy information, and examples include data tampering, injection attacks, and ransomware.
3. Availability attacks: These attacks aim to deny access to information and network resources, and examples include denial of service (DoS) attacks, distributed denial of service (DDoS) attacks, and network congestion attacks.
4. Authenticity attacks: These attacks aim to compromise the authenticity of information, such as impersonation attacks, phishing, and man-in-the-middle attacks.
5. Non-repudiation attacks: These attacks aim to undermine the non-repudiation of information, such as denial of service attacks on digital signatures or digital certificate authorities.

It's important to note that some attacks can target multiple security goals at once, such as a DoS attack that aims to compromise both availability and confidentiality. Network security professionals need to be vigilant and prepared to detect and respond to attacks in order to maintain the security and functionality of their networks.

1.1 SECURITY GOALS

Let us first discuss three **security goals: confidentiality, integrity, and availability** (Figure 1.1).

Figure 1.1 *Taxonomy of security goals*



Confidentiality

Confidentiality is probably the most common aspect of information security. We need to protect our confidential information. An organization needs to guard against those malicious actions that endanger the confidentiality of its information. In the military, concealment of sensitive information is the major concern. In industry, hiding some information from competitors is crucial to the operation of the organization. In banking, customers' accounts need to be kept secret.

As we will see later in this chapter, confidentiality not only applies to the storage of the information, it also applies to the transmission of information. When we send a piece of information to be stored in a remote computer or when we retrieve a piece of information from a remote computer, we need to conceal it during transmission.

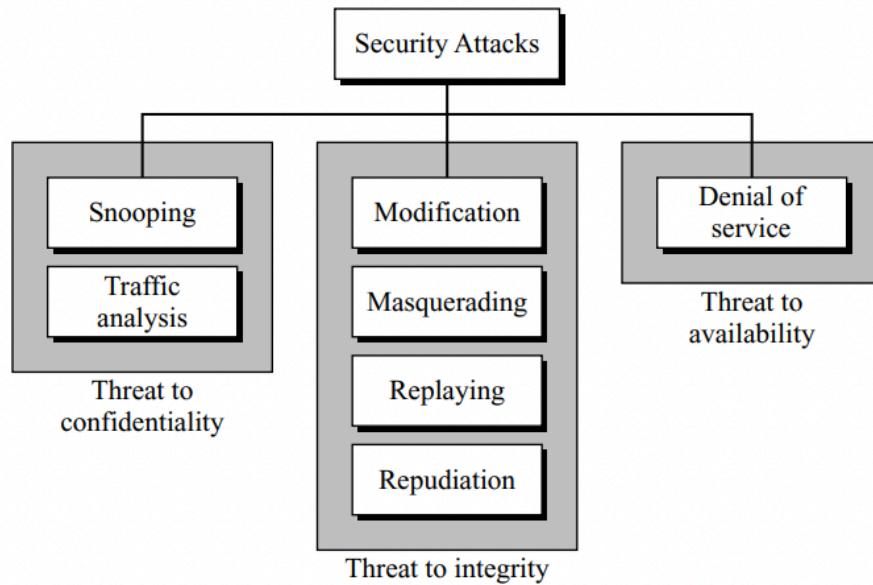
Integrity

Information needs to be changed constantly. In a bank, when a customer deposits or withdraws money, the balance of her account needs to be changed. **Integrity** means that changes need to be done only by authorized entities and through authorized mechanisms. Integrity violation is not necessarily the result of a malicious act; an interruption in the system, such as a power surge, may also create unwanted changes in some information.

Availability

The third component of information security is **availability**. The information created and stored by an organization needs to be available to authorized entities. Information is useless if it is not available. Information needs to be constantly changed, which means it must be accessible to authorized entities. The unavailability of information is just as harmful for an organization as the lack of confidentiality or integrity. Imagine what would happen to a bank if the customers could not access their accounts for transactions.

Figure 1.2 Taxonomy of attacks with relation to security goals



Attacks Threatening Confidentiality

In general, two types of attacks threaten the confidentiality of information: snooping and traffic analysis.

- **Snooping**

Snooping refers to unauthorized access to or interception of data. For example, a file transferred through the Internet may contain confidential information. An unauthorized entity may intercept the transmission and use the contents for her own benefit. To prevent snooping, the data can be made nonintelligible to the interceptor by using encipherment techniques discussed in this book.

- **Traffic Analysis**

Although encipherment of data may make it nonintelligible for the interceptor, she can obtain some other type information by monitoring online traffic. For example, she can find the electronic address (such as the e-mail address) of the sender or the receiver. She can collect pairs of requests and responses to help her guess the nature of transaction.

Attacks Threatening Integrity

The integrity of data can be threatened by several kinds of attacks: modification, masquerading, replaying, and repudiation.

- **Modification**

After intercepting or accessing information, the attacker modifies the information to make it beneficial to herself. For example, a customer sends a message to a bank to do some transaction. The attacker intercepts the message and changes the type of transaction to benefit herself. Note

that sometimes the attacker simply deletes or delays the message to harm the system or to benefit from it.

- **Masquerading**

Masquerading, or spoofing, happens when the attacker impersonates somebody else. For example, an attacker might steal the bank card and PIN of a bank customer and pretend that she is that customer. Sometimes the attacker pretends instead to be the receiver entity. For example, a user tries to contact a bank, but another site pretends that it is the bank and obtains some information from the user.

- **Replaying**

Replaying is another attack. The attacker obtains a copy of a message sent by a user and later tries to replay it. For example, a person sends a request to her bank to ask for payment to the attacker, who has done a job for her. The attacker intercepts the message and sends it again to receive another payment from the bank.

- **Repudiation**

This type of attack is different from others because it is performed by one of the two parties in the communication: the sender or the receiver. The sender of the message might later deny that she has sent the message; the receiver of the message might later deny that he has received the message.

An example of denial by the sender would be a bank customer asking her bank to send some money to a third party but later denying that she has made such a request. An example of denial by the receiver could occur when a person buys a product from a manufacturer and pays for it electronically, but the manufacturer later denies having received the payment and asks to be paid.

Attacks Threatening Availability

We mention only one attack threatening availability: denial of service.

- **Denial of Service**

Denial of service (DoS) is a very common attack. It may slow down or totally interrupt the service of a system. The attacker can use several strategies to achieve this. She might send so many bogus requests to a server that the server crashes because of the heavy load. The attacker might intercept and delete a server's response to a client, making the client to believe that the server is not responding. The attacker may also intercept requests from the clients, causing the clients to send requests many times and overload the system

Soln2:

What are the various security mechanism to provide the security services in network security? Explain.

- **Encipherment**

Encipherment, hiding or covering data, can provide confidentiality. It can also be used to complement other mechanisms to provide other services. Today two techniques—cryptography and steganography—are used for enciphering. We will discuss these shortly

- **Data Integrity**

The data integrity mechanism appends to the data a short checkvalue that has been created by a specific process from the data itself. The receiver receives the data and the checkvalue. He creates a new checkvalue from the received data and compares the newly created checkvalue with the one received. If the two checkvalues are the same, the integrity of data has been preserved.

- **Digital Signature**

A digital signature is a means by which the sender can electronically sign the data and the receiver can electronically verify the signature. The sender uses a process that involves showing that she owns a private key related to the public key that she has announced publicly. The receiver uses the sender's public key to prove that the message is indeed signed by the sender who claims to have sent the message.

- **Authentication Exchange**

In authentication exchange, two entities exchange some messages to prove their identity to each other. For example, one entity can prove that she knows a secret that only she is supposed to know.

- **Traffic Padding**

Traffic padding means inserting some bogus data into the data traffic to thwart the adversary's attempt to use the traffic analysis.

- **Routing Control**

Routing control means selecting and continuously changing different available routes between the sender and the receiver to prevent the opponent from eavesdropping on a particular route.

- **Notarization**

Notarization means selecting a third trusted party to control the communication between two entities. This can be done, for example, to prevent repudiation. The receiver can involve a trusted party to store the sender request in order to prevent the sender from later denying that she has made such a request.

- **Access Control**

Access control uses methods to prove that a user has access right to the data or resources owned by a system. Examples of proofs are passwords and PINs.

Table 1.2 Relation between security services and security mechanisms

| Security Service | Security Mechanism |
|----------------------|---|
| Data confidentiality | Encipherment and routing control |
| Data integrity | Encipherment, digital signature, data integrity |
| Authentication | Encipherment, digital signature, authentication exchanges |
| Nonrepudiation | Digital signature, data integrity, and notarization |
| Access control | Access control mechanism |

3. We mentioned five security services: *data confidentiality*, *data integrity*, *authentication*, *nonrepudiation*, and *access control*.

- Data confidentiality* is to protect data from disclosure attack.
- Data integrity* is to protect data from modification, insertion, deletion, and replaying.
- Authentication* means to identify and authenticate the party at the other end of the line.
- Nonrepudiation* protects against repudiation by either the sender or the receiver of the data.
- Access control* provides protection against unauthorized access to data.

Other part

Soln3:

What is steganography? Write procedure to hide "Hi" in the sentence "A friend called a doctor".
Chatgpt

Steganography is the practice of hiding a secret message within a seemingly innocuous carrier, such as an image, audio, or text. The goal of steganography is to conceal the existence of the hidden message, making it difficult for anyone to detect or intercept it.

Here is a procedure to hide the message "Hi" in the sentence "A friend called a doctor" using steganography:

1. Choose a secret message to hide, in this case, "Hi".
2. Choose a cover text, which is the text that will carry the hidden message. In this case, "A friend called a doctor" will be the cover text.
3. Select a steganography technique to hide the secret message within the cover text. For this example, we will use a simple technique that involves replacing certain letters in the cover text with the letters of the secret message.
4. To hide "Hi" in "A friend called a doctor", we can replace the letters "h" and "i" in "called" with "H" and "i", respectively. The resulting sentence would be "A friend caHled a doctiOr".
5. Send the modified sentence to the intended recipient, who knows the steganography technique and can extract the hidden message.

To extract the hidden message, the recipient would need to know the steganography technique used to hide the message. In this case, they would simply look for the letters "H" and "i" in the word "called" and reconstruct the hidden message as "Hi".

It's important to note that this is a very simple example of steganography, and more advanced techniques can be used to hide messages in different ways, such as changing the color values of pixels in an image or altering the audio frequencies of a sound file.

BOOK

Steganography Although this book is based on cryptography as a technique for implementing security mechanisms, another technique that was used for secret communication in the past is being revived at the present time: steganography. The word steganography, with origin in Greek, means “covered writing,” in contrast with cryptography, which means “secret writing.”

Cryptography means concealing the contents of a message by enciphering; steganography means concealing the message itself by covering it with something else.

Text Cover :

The cover of secret data can be text. There are several ways to insert binary data into an innocuous text. For example, we can use single space between words to represent the binary digit 0 and double space to represent binary digit 1. The following short message hides the 8-bit binary representation of the letter A in ASCII code (01000001).

This book is mostly about cryptography, not steganography.

| | | |
|---|---|--|
| <input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/> | <input type="checkbox"/> <input type="checkbox"/> | <input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/> |
| 0 1 0 | 0 0 | 0 1 |

In the above message there are two spaces between the “book” and “is” and between the “not” and “steganography”. Of course, sophisticated software can insert spaces that differ only slightly to hide the code from immediate recognition.

Another, more efficient method, is to use a dictionary of words organized according to their grammatical usages. We can have a dictionary containing 2 articles, 8 verbs, 32 nouns, and 4 prepositions. Then we agree to use cover text that always use sentences with the pattern article-noun-verb-article-noun. The secret binary data can be divided into 16-bit chunks. The first bit of binary data can be represented by an article (for example, 0 for a and 1 for the). The next five bits can be represented by a noun (subject of the sentence), the next four bits can be represented by a verb, the next bit by the second article, and the last five bits by another noun (object). For example, the secret data “Hi”, which is 01001000 01001001 in ASCII, could be a sentence like the following:

A friend called a doctor.
0 10010 0001 0 01001

This is a very trivial example. The actual approach uses more sophisticated design and a variety of patterns.

Soln4:

Explain about the various types of active and passive attacks on the network in detail
CHATGPT

In network security, attacks can be classified as either active or passive. Active attacks involve modifying, disrupting, or destroying data or network resources, while passive attacks involve monitoring or eavesdropping on data without modifying it. Here are some of the most common types of active and passive attacks in network security:

1. Passive attacks:
 - a. Eavesdropping: This type of attack involves an attacker listening in on network traffic to obtain sensitive information such as usernames, passwords, and financial data. Attackers can use various tools and techniques, such as packet sniffers, to intercept data in transit.
 - b. Traffic Analysis: In this attack, an attacker analyzes network traffic to gather information about network topology, communication patterns, and sensitive information. Attackers can use this information to launch more targeted attacks, such as social engineering attacks.
 - c. Port Scanning: Port scanning involves an attacker scanning a network to identify open ports and vulnerable services. Once a vulnerable service is identified, the attacker can launch an attack against it.
 - d. Password Attacks: Password attacks are a type of attack that involves trying to guess or crack a user's password. Attackers can use various techniques such as dictionary attacks and brute-force attacks to guess passwords.
2. Active attacks:
 - a. Denial-of-Service (DoS) and Distributed Denial-of-Service (DDoS): DoS and DDoS attacks involve overwhelming a network or server with traffic or requests, making it inaccessible to legitimate users. In a DDoS attack, multiple compromised systems are used to launch the attack, making it more difficult to defend against.
 - b. Man-in-the-Middle (MitM) Attacks: MitM attacks involve an attacker intercepting and modifying communication between two parties. Attackers can use this technique to steal sensitive information, such as login credentials or financial data.
 - c. Spoofing Attacks: Spoofing attacks involve an attacker impersonating a legitimate user or system to gain unauthorized access or deceive users. Examples of spoofing attacks include IP spoofing, email spoofing, and DNS spoofing.
 - d. Injection Attacks: Injection attacks involve an attacker injecting malicious code or data into a system, such as a SQL injection attack, which allows an attacker to execute malicious SQL queries on a database.
 - e. Malware: Malware is a type of software designed to harm or exploit a system. Examples of malware include viruses, Trojans, and ransomware. Malware can be used to steal data, destroy systems, or launch further attacks.

It's important to note that attacks can often be combined, and attackers can use a variety of techniques to achieve their goals. To defend against these attacks, it's

essential to implement multiple layers of defense, such as firewalls, intrusion detection and prevention systems, access controls, and regular software updates.

BOOK

Table 1.1 *Categorization of passive and active attacks*

| <i>Attacks</i> | <i>Passive/Active</i> | <i>Threatening</i> |
|--|-----------------------|--------------------|
| Snooping Traffic analysis | Passive | Confidentiality |
| Modification Masquerading Replaying Repudiation | Active | Integrity |
| Denial of service | Active | Availability |

Passive Attacks

In a passive attack, the attacker's goal is just to obtain information. This means that the attack does not modify data or harm the system. The system continues with its normal operation. However, the attack may harm the sender or the receiver of the message. Attacks that threaten confidentiality—snooping and traffic analysis—are passive attacks. The revealing of the information may harm the sender or receiver of the message, but the system is not affected. For this reason, it is difficult to detect this type of attack until the sender or receiver finds out about the leaking of confidential information. Passive attacks, however, can be prevented by encipherment of the data.

Active Attacks

An active attack may change the data or harm the system. Attacks that threaten the integrity and availability are active attacks. Active attacks are normally easier to detect than to prevent, because an attacker can launch them in a variety of ways.

Soln5

Explain how attackers uses the following methods to attack in the network:

- (i) Packet sniffing
- (ii) Packet spoofing
- (iii) DNS spoofing

Attackers use different methods to attack networks, and here are some common methods used by attackers to conduct network attacks:

(i) Packet Sniffing:

Packet sniffing involves the interception and analysis of network traffic. Attackers use this method to capture data packets in transit and extract sensitive information such as usernames, passwords, and financial data. Attackers can use packet sniffer or network analyzers to eavesdrop on traffic passing through a network segment. Once the attacker captures the data packets, they can use tools to reconstruct the data and extract the desired information. To protect against packet sniffing attacks, network administrators can use encryption protocols such as SSL or TLS to secure data in transit.

(ii) Packet Spoofing:

Packet spoofing involves an attacker sending packets with a forged or false source IP address. This technique allows the attacker to impersonate a trusted device and gain unauthorized access to a network or server. Attackers can use packet spoofing to launch various types of attacks, such as a Denial of Service (DoS) attack or a man-in-the-middle (MitM) attack. To prevent packet spoofing attacks, network administrators can use ingress and egress filtering to block packets with forged IP addresses.

(iii) DNS Spoofing:

DNS spoofing is a type of attack that involves an attacker intercepting and modifying DNS (Domain Name System) queries and responses. Attackers use DNS spoofing to redirect users to malicious websites, steal sensitive information, or launch phishing attacks. In a DNS spoofing attack, the attacker spoofs a DNS response and sends it to the victim's computer, redirecting the user to a fake website. To prevent DNS spoofing attacks, network administrators can use DNSSEC (DNS Security Extensions), which adds a digital signature to DNS responses to ensure their authenticity.

In conclusion, attackers use different methods to conduct network attacks, and to protect against these attacks, network administrators must implement various security measures such as encryption protocols, ingress and egress filtering, and DNSSEC. It's also important to keep network devices and software up-to-date and to implement security best practices such as strong password policies, access controls, and regular security audits.

Soln6:

List the various Symmetrical key cryptographic techniques.

Symmetric key cryptography, also known as secret key cryptography, is a type of cryptography where both the sender and receiver use the same secret key to encrypt and decrypt messages. Here are some of the most commonly used symmetric key cryptographic techniques:

1. Data Encryption Standard (DES):

DES is a symmetric key block cipher that uses a 56-bit key and encrypts data in 64-bit blocks. While DES is no longer considered secure for modern use, it was widely used for many years and served as the basis for many subsequent encryption algorithms.

2. Advanced Encryption Standard (AES):

AES is a symmetric key block cipher that uses a variable-length key and can encrypt data in 128-bit, 192-bit, or 256-bit blocks. AES is widely used in modern cryptography due to its high level of security and efficiency.

3. Blowfish:

Blowfish is a symmetric key block cipher that can use keys up to 448 bits long and can encrypt data in 64-bit blocks. While Blowfish is no longer considered secure for modern use, it was widely used in the past and served as the basis for the Twofish cipher.

4. Twofish:

Twofish is a symmetric key block cipher that can use keys up to 256 bits long and can encrypt data in 128-bit blocks. Twofish was designed as a successor to Blowfish and is still considered secure for modern use.

5. Triple DES (3DES):

Triple DES is a symmetric key block cipher that uses three different 56-bit keys to encrypt data in 64-bit blocks. While 3DES is slower and less efficient than other encryption algorithms, it is still widely used in certain applications that require a high level of security.

In conclusion, symmetric key cryptography provides a fast and efficient way to encrypt data using the same secret key for both encryption and decryption. While there are several symmetric key cryptographic techniques available, AES is widely used due to its high level of security and efficiency.

Soln7:

Use Brute-force attack to decipher the following message. Assume that you know it is an affine cipher and that the plain text “ab” is enciphered to “GL”.

XPALASXYFGFUKPXUSOGEUTKCDGFXANMGNVS

4. [15] Use a brute-force attack to decipher the following message. Assume that you know it is an affine cipher and that the plaintext “ab” is enciphered to “GL”.

XPALASXYFGFUKPXUSOGEUTKCDGFXANMGNVS

We know that “ab” -> “GL”. This means that

$$00 \rightarrow 06 \quad \text{and} \quad 01 \rightarrow 11$$

We can construct two equations from these two pieces of information:

$$00 \times k_1 + k_2 \equiv 06 \pmod{26} \quad 01 \times k_1 + k_2 \equiv 11 \pmod{26}$$

Solving these two equations give us $k_1 = 5$ and $k_2 = 6$. This means,

$$P = ((C - k_2) \times k_1^{-1}) \pmod{26} = ((C + 20) \times 21) \pmod{26}$$

Ciphertext: XPALASXYFGFUKPXUSOGEUTKCDGFXANMGNVS

Plaintext: the best of a fight is making up afterwards

Soln8:

Encrypt the message “this is an exercise” using one of the following ciphers. Ignore the space between words. Decrypt the message to get the original plaintext.

- a. Additive cipher with key = 20
- b. Multiplicative cipher with key = 15
- c. Affine cipher with key = (15, 20)

2. [15] Encrypt the message “**this is an exercise**” using one of the following ciphers.
Ignore the space between words. Decrypt the message to get the original plaintext

- a. Additive cipher with key = 20

For additive cipher, $C = (P + k) \bmod 26$ where C = Cipher text, P = Plain text and $k = 20$

- b. Multiplicative cipher with key = 15

For multiplicative cipher, $C = (P \times k) \bmod 26$ where C = Cipher text, P = Plain text and $k = 15$

- c. Affine cipher with key = (15, 20)

For affine cipher,

**$T = (P \times k_1) \bmod 26$ where T = Intermediate text,
 P = Plain text and
 $k_1 = 15$**

**$C = (T \times k_2) \bmod 26$ where C = Cipher text,
 T = Intermediate text and
 $k_2 = 20$**

The final result is given in Table below:

| Cipher | Plaintext | Ciphertext |
|--------------------------|----------------------------|-------------------------|
| Additive, key = 20 | This is an exercise | NBCMCMUHYRYLWCMY |
| Multiplicative, key = 15 | This is an exercise | ZBQKQKANIHIVEQKI |
| Affine, key = (15, 20) | This is an exercise | TVKEKEUHCBCPYKEC |

Soln9:

Use a brute-force attack to decipher the following message enciphered by Alice using an additive cipher. Suppose that Alice always uses a key that is close to her birthday, which is on the 13th of the month:

NCJAEZRCLASJLYODEPRLYZRCLASJLCPEHZDTOPDZQLNZTY

3. [10] Use a brute-force attack to decipher the following message enciphered by Alice using an additive cipher. Suppose that Alice always uses a key that is close to her birthday which is on the 13th of the month.

NCJAEZRCLASJLYODEPRLYZRCLASJLCPEHZDTOPDZQLNZTY

We can try the keys 13, 12, 14, 11, 15 which are close to Alice's birthday. When we use the key = 11, the plaintext makes sense.

Key = 11

Ciphertext: NCJAEZRCLASJLYODEPRLYZRCLASJLCPEHZDTOPDZQLNZTY

Plaintext: cryptography and steganography are two sides of a coin

Soln10:

The plaintext “letusmeetnow” and the corresponding cipher text “HBCDFNOPIKLB” are given. You know that the algorithm is a Hill cipher, but you don’t know the size of the key. Find the key matrix.

- 36.** The length of the message is 12. The size of the block needs to divide 12. This means that the size of the block can be 1, 2, 3, 4, 6, 12. Since the first and the last size is trivial, we can ignore them. We need to try the block sizes 2, 3, 4, and 6.

9

However, the size of message (12) does not allow us to test for the matrices of size 4 or 16. If the size of the key matrix is 4, we need at least the plaintext/ciphertext of size 16. If the size of the key matrix is 6, we need to have a plaintext/ciphertext of size 36. Our only choices are to test for the key matrices of size 2 and 3.

- a.** Let us first try the block size 2. Following Example 3.21 in the text, we can make a plaintext/ciphertext pair of the first four of the given plaintext and given ciphertext (letu → HBCD). In this case the plaintext matrix and ciphertext are

$$P = \begin{bmatrix} 11 & 04 \\ 19 & 08 \end{bmatrix} \quad C = \begin{bmatrix} 07 & 01 \\ 02 & 03 \end{bmatrix}$$

Since P is not invertible in modulo 26 arithmetic, we can not proceed.

- b.** Let us now try the block size 3. Following Example 3.21 in the text, we can make a plaintext/ciphertext pair of the first nine character of the given plaintext and given ciphertext (let usm eet → HBCDFNOPI). In this case the plaintext and ciphertext matrices are

$$P = \begin{bmatrix} 11 & 04 & 19 \\ 20 & 18 & 12 \\ 04 & 04 & 19 \end{bmatrix} \quad C = \begin{bmatrix} 07 & 01 & 02 \\ 03 & 05 & 13 \\ 14 & 15 & 08 \end{bmatrix}$$

Since P is not invertible in modulo 26 arithmetic, we can not proceed. This means that we cannot solve the problem with the information given.

Soln11:

Eve has intercepted the following cipher text, using statistical attack find the plain text:

XLILSYWIMWRSAJSVWEPIJSVJSYVQMPPMSRHSPPEVWMXMWASVX-LQSVILY
VVCFIJSVIXLIWIPPIVVGIMZIWQSVISJJIVW

Eve has intercepted the following ciphertext. Using a statistical attack, find the plaintext.

XLILSYWIMWRSAJSVWEPIJSVJSYVQMPPMSRHSPPEVWMXMWASVX-LQSVILY
VVCFIJSVIXLIWIPPIVVGIMZIWQSVISJJIVW

Solution

When Eve tabulates the frequency of letters in this ciphertext, she gets: I =14, V =13, S =12, and so on. The most common character is I with 14 occurrences. This means key = 4 because the distance b/w e and I is 4 (e.f.g.h.i).

the house is now for sale for four million dollars it is worth more hurry before the seller receives more offers