3.1 INTRODUCTION

In this Unit, we start our study of cryptography by discussing some simple ciphers. We must warn you that these ciphers are no longer used in real life situations; we discuss these for historical reasons and to introduce you to basic concepts of cryptography. In Sec. 3.2, we discuss the need for cryptography and introduce you to the basic terminology of cryptography. In Sec. 3.3, we discuss transposition ciphers. In Sec. 3.4, we discuss substitution ciphers. In Sec. 3.5, we discuss the affine cipher. In Sec. 3.6, we discuss the Vigenère cipher.

Objectives

After studying this unit, you should be able to

• explain the goals of cryptography;
• explain the basic terms of cryptography;
• explain what is a transposition cipher and give examples;
• encrypt and decrypt text using some simple transposition ciphers;
• explain what is a substitution cipher and give examples;
• encrypt and decrypt text using some simple substitution ciphers;
• explain the Vigenère cipher and encrypt and decrypt text using the cipher; and
• apply simple statistical methods for cryptanalysing cipher.

3.2 BASIC TERMINOLOGY AND SIMPLE CIPHERS

From time immemorial, human beings have communicated with each other. With the advancement of civilisation came the creation of political formations like countries with conflicting interests. It also lead to increased commercial activity. In political and
commercial activities, information is of great value and it often became necessary to communicate information in such a way that no one but the intended recipient receives the information. One of the main tools that has evolved to serve this purpose is cryptography.

The main objective of cryptography is to enable two parties communicate confidentially through an insecure channel by concealing its meaning to the unauthorised parties. By a channel, we mean any method of communication including the traditional means like letter, telephone, telegraph, etc. and the more modern like computer networks and communication through satellite. Insecure channel means that adversaries to the communicating parties can access the channel.

Traditionally, in cryptography, two communicating parties are called Bob and Alice. There is a third party, usually called Eve, who is eavesdropping on the conversation, trying to find out what they are saying to each other. Of course, it is not that Bob and Alice are ‘good’ and Eve is ‘bad’. For example, Alice and Bob could be terrorists plotting some terrorist act and Eve could be the government agency that is trying to prevent it.

Cryptography is a discipline which embodies principles, means and methods for the transformation of data in order to

1. hide its information content from unauthorised persons.
2. establish the authenticity of the data.
3. prevent its undetected modification.
4. prevent its repudiation.
5. prevent its unauthorised use.

In other words, the main goals of the cryptography are privacy/confidentiality, authentication, data integrity and non-repudiation. Let us see what these goal are.

**Privacy/Confidentiality**
To achieve the primary goal of confidentiality, Bob usually transforms the text in such a way that it becomes unintelligible and sends it to Alice. Alice knows how to get the original text from the transformed text. The whole procedure involves some secret information without which it is not possible to recover the original text from the transformed text. Eve, eavesdropper will not be able to recover the original text if she doesn’t have the necessary secret information.

**Authentication**
After the message reaches its destination, the receiver should be able to verify its origin. Eve should not be able to send a message to Bob pretending to be Alice. This aspect is called authenticity.

**Data integrity**
Another objective of cryptography is to protect the message from being tampered with during transit. When Bob receives a message from Alice, he should be able to check whether the message was modified during transmission, either accidentally or deliberately. Eve should not be able to alter the message by insertion, deletion or substitution of text. This aspect is called data integrity.
When initiating a communication, Alice and Bob should be able to identify each other. Finally, Alice should not be able to later deny that she sent the message. This aspect is called non-repudiation.

As discussed earlier, adversaries may also be active and try to modify the message. Adversaries are assumed to have complete access to the communication channel.

The fundamental and classical task of cryptography is to provide secrecy by encryption methods. The actual message to be sent is called plain text. The process of transforming plain text to render it unintelligible to unauthorised persons is called encryption or enciphering and transformed text is called cipher text. The reverse process of recovering the plain text from the cipher text by undoing the transformation is called decryption or deciphering.

Let us look at a simple example of cryptography at work. We will discuss a cipher supposed to have been used by Julius Caesar, a roman general and statesman.

### 3.2.1 Caesar Cipher

You may studied about Julius Caesar, the roman general and statesman who conquered Gaul, a region of Western Europe which included present day France, Luxembourg and Belgium, most of Switzerland, the western part of Northern Italy, as well as the parts of the Netherlands and Germany on the left bank of the Rhine. He developed a method, which is now known as Caesar Cipher, for communicating with the generals of his army.

**Example 1:** (Caesar cipher) Suppose the message we want to send, that is, the plain text, comprises letters from the English alphabet. We convert it to a cipher text by simply replacing each letter in the message with the letter that is three places further down the alphabet. That is, “A” is replaced by “D,” “B” is replaced by “E,” ..., “W” is replaced by “Z,” “X” is replaced by “A,” “Y” is replaced by “B,” and “Z” is replaced by “C”. To get back the original message from the cipher text, we perform the reverse operation, that is, replace each letter of the cipher text with the letter that is three places ahead in the alphabet. Thus, with this system, the word “YES” is encrypted as “BHV”, while the cipher text “ZKB” yields the plain text “WHY”. See Table 1.

<table>
<thead>
<tr>
<th>Plain text</th>
<th>A</th>
<th>B</th>
<th>C</th>
<th>D</th>
<th>E</th>
<th>F</th>
<th>G</th>
<th>H</th>
<th>I</th>
<th>J</th>
<th>K</th>
<th>L</th>
<th>M</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cipher text</td>
<td>D</td>
<td>E</td>
<td>F</td>
<td>G</td>
<td>H</td>
<td>I</td>
<td>J</td>
<td>K</td>
<td>L</td>
<td>M</td>
<td>N</td>
<td>O</td>
<td>P</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Plain text</th>
<th>N</th>
<th>O</th>
<th>P</th>
<th>Q</th>
<th>R</th>
<th>S</th>
<th>T</th>
<th>U</th>
<th>V</th>
<th>W</th>
<th>X</th>
<th>Y</th>
<th>Z</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cipher text</td>
<td>Q</td>
<td>R</td>
<td>S</td>
<td>T</td>
<td>U</td>
<td>V</td>
<td>W</td>
<td>X</td>
<td>Y</td>
<td>Z</td>
<td>A</td>
<td>B</td>
<td>C</td>
</tr>
</tbody>
</table>

**Table 1:** Caesar’s Cipher.

To look at a longer example, his message ‘I CAME I SAW I CONQUERED’ will be transformed as follows:

| Plain text | I | C | A | M | E | I | S | A | W | I | C | O | N | Q | U | E | R | E | D |
| Cipher text| L | F | D | P | H | L | V | D | Z | L | F | R | Q | T | X | H | U | H | G |

Try the following exercise to test your understanding of Caesar cipher.

**E1)** Encrypt the following text using Caesar cipher: THE DIE IS CAST
Let us now define a cryptosystem formally.

Definition 1: An alphabet \( \Sigma \) is a finite set whose elements are called symbols. A string over an alphabet is a finite sequence of symbols. Let us denote the set of all strings over \( \Sigma \) by \( \mathcal{L}(\Sigma) \). Let \( \Sigma \) and \( \Delta \) be two sets of symbols. A cryptosystem consists of the following components:

- **Plaintext-space** \( \mathcal{P} \) - a finite subset of \( \mathcal{L}(\Sigma) \).
- **Ciphertext-space** \( \mathcal{C} \) - a finite subset of \( \mathcal{L}(\Delta) \).
- **Key space** \( \mathcal{K} \) - a finite set of keys.
- **Encryption function** \( E_k \) - for each \( k \in \mathcal{K} \), there is an encryption function \( E_k: \mathcal{P} \rightarrow \mathcal{C} \) which is a one-to-one function.
- **Decryption function** \( D_k \) - for each \( k \in \mathcal{K} \), there is a decryption function \( D_k: \mathcal{C} \rightarrow \mathcal{P} \) such that \( D_k(E_k(x)) = x \) for all \( x \in \mathcal{P} \).

Let us see how we encrypt a message.

1. We choose a key \( k \in \mathcal{K} \).
2. We break up the plaintext into smaller units, each of which consists of a single letter, or a pair of letters, or a block of some fixed number of letters. These are known as message units.
3. Let \( E_k \) be the encryption function from \( \mathcal{P} \) to \( \mathcal{C} \) corresponding to the key \( k \in \mathcal{K} \) which takes any plaintext message unit to a ciphertext message unit, where we shall always assume that \( E_k \) is a 1-to-1 correspondence. Under this map, for any ciphertext message unit, there is a unique plaintext message unit for which it is the encryption.
4. We apply the inverse map, the decryption function \( D_k \) from \( \mathcal{C} \) to \( \mathcal{P} \) to recover the plaintext from the ciphertext.

Let us look at Caesar’s cipher to understand the terms.

**Example 2:** Let us see what \( \mathcal{P}, \mathcal{C}, E_k \) and \( D_k \) are in the Caesar cipher. Since we want to construct functions between two sets, the first step is to label all possible plain text message units and all possible cipher text units by means of mathematical objects. In this case, our plain text and cipher text message units are single letters from the 26-letter alphabet \( A - Z \), so we can label the letters using the integers \( 0, 1, 2, \ldots, 25 \), which we call their “numerical equivalents”, as in Table 2.

<table>
<thead>
<tr>
<th>A</th>
<th>B</th>
<th>C</th>
<th>D</th>
<th>E</th>
<th>F</th>
<th>G</th>
<th>H</th>
<th>I</th>
<th>J</th>
<th>K</th>
<th>L</th>
<th>M</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>1</td>
<td>2</td>
<td>3</td>
<td>4</td>
<td>5</td>
<td>6</td>
<td>7</td>
<td>8</td>
<td>9</td>
<td>10</td>
<td>11</td>
<td>12</td>
</tr>
<tr>
<td>N</td>
<td>O</td>
<td>P</td>
<td>Q</td>
<td>R</td>
<td>S</td>
<td>T</td>
<td>U</td>
<td>V</td>
<td>W</td>
<td>X</td>
<td>Y</td>
<td>Z</td>
</tr>
<tr>
<td>13</td>
<td>14</td>
<td>15</td>
<td>16</td>
<td>17</td>
<td>18</td>
<td>19</td>
<td>20</td>
<td>21</td>
<td>22</td>
<td>23</td>
<td>24</td>
<td>25</td>
</tr>
</tbody>
</table>

Table 2: Numerical equivalents of the characters in the English alphabet.

Recall from Unit 6 of MMT-003 that \( \mathbb{Z}_{26} \) is a quotient ring \( \mathbb{Z}/26\mathbb{Z} \). However, to make notation less cumbersome, we will regard the set \( \mathcal{A} = \{0, 1, 2, \ldots, 25\} \) as \( \mathbb{Z}_{26} \). To add
two numbers \( m, n \in \mathcal{A} \), we simply find the usual sum \( m + n \) and if it is greater than 26, take its remainder on division by 26 as the answer. If \( m + n \) is less than 26, the answer is just the usual sum \( m + n \). For example, the sum of 2 and 4 in \( \mathcal{A} \) is 6, while the sum of 24 and 12 is 10 in \( \mathcal{A} \). We can define multiplication similarly.

Under the correspondence in Table 2, let \( x \in \mathcal{A} = \{0, 1, \ldots, 25\} \) stand for a plain text message unit. Define a function \( f \) from the set \( \mathcal{A} \) to itself by the rule

\[
f(x) = x + 3
\]  

(1)

Note that, the addition in Eqn. (1) is the addition we defined in \( \mathcal{A} \). Thus, \( f(2) = 2 + 3 = 5 \), but \( f(24) = 1 \).

Therefore, what we have done in encrypting the word “YES” was to write down the numerical equivalent in \( \mathcal{A} \) to each letter under Table 2: “24 4 18”. Then, we find \( f(24) = 1 \), \( f(4) = 7 \) and \( f(18) = 21 \). The letter equivalents to 1, 7 and 21 are B, H and V.

To decipher a message, we subtract 3 or equivalently add 23 since 23 is the additive inverse of 3 under the addition we defined on \( \mathcal{A} \). In other words,

\[
f^{-1}(x) = g(x) = P + 23
\]  

(2)

will convert a cipher text message unit to a plain text unit. It is easy to see how the cipher text “ZKB”, mentioned above, gives the plain text “WHY” using this function. We leave this verification as an exercise.

For the Caesar cipher, any plain text message is a string \( p_1 p_2 \ldots p_k \) with \( p_i \in \mathcal{A} \). For example WHY corresponds to the string 22 7 24. Usually, strings are written without gaps. We have put small gaps so that there is no ambiguity. Similarly, ZKB corresponds to the string 25 10 24. So, both the plain text and cipher text are strings on the same set \( \mathcal{A} \) and we can take \( \mathcal{P} \) and \( \mathcal{K} \) to be subsets of \( \mathcal{L}(\mathcal{A}) \) consisting of strings of length \( \leq t \) for some \( t \). So, in this case, \( \Delta = \Sigma \). Further, the key space contains only one element, 3. The function \( E_3 \) is the function \( f \) in Eqn. (1) and the function \( D_3 \) is the function \( g \) defined in Eqn. (2).

* * *

In the next section, we will discuss a generalisation of Caesar cipher.

3.2.2 Shift Cipher

You may recall that electronic documents do not have just the characters from the alphabet. They also contain punctuation marks, numbers, symbol like \&, $ and so on. In fact, 265 different characters are possible in computers that use the ASCII encoding. So, we need a larger set of symbols than just \( \mathcal{A} \). Instead of \( \mathcal{A} \), we can take the set \( \mathcal{A}_N = \{0, 1, 2, 3, \ldots, N\} \) as the set of symbols. We can define addition and multiplication on \( \mathcal{A}_N \) as addition and multiplication modulo \( N \) as we did in the case of \( \mathcal{A} \). We can define the analogue of Caesar cipher on \( \mathcal{A}_N \) by

\[
f(x) = x + 3.
\]  

(3)

The inverse transformation is

\[
g(x) = f^{-1}(x) = x + N - 3
\]  

(4)

Another obvious direction in which we can generalise is to shift characters in the plaintext by \( b \) places for \( 0 < b < N \) instead of just by three places. In this case the encryption function is

\[
E_b(x) = x + b
\]  

(5)
and the decryption function is
\[ D_b(x) = f^{-1}(x) = x - b \]  

(6)

Here, of course, \(-b = N - b\), the additive inverse of \(b\) in \(\mathbb{Z}_N\).

In the case of shift cipher, \(\Sigma = \Delta = \mathcal{A}\) and \(\mathcal{P}\) and \(\mathcal{C}\) are subsets of \(\mathcal{L}(\mathcal{A})\) of length \(\leq t\) for some \(t\). Note that, this choice for \(\mathcal{P}\) and \(\mathcal{C}\) makes sense because, although it is possible to have plaintext or ciphertext of arbitrary length, all the media used for storage of plaintext or ciphertext have only finite capacity and so they cannot store strings of arbitrary length. We have \(\mathcal{K} = \{b|0 < b < N\}\). Further, \(E_b(x) = x + k\) and \(D_k(x) = x - k\) for \(k \in \mathcal{K}\). Let us now look at an example of shift cipher.

**Example 3:** Consider the plaintext ‘I CAME I SAW I CONQUERED’. Let us apply the shift transformation with shift parameter 7. The seventh letter after I is P. So, we replace I by P. Similarly the seventh letter after C is J; so we replace C by J. Proceeding this way, the text becomes ‘P JHTL P ZHD P JVUXBLYLK’. To decrypt this text we apply the inverse shift transformation which is a shift transformation with shift parameter \(26 - 7 = 19\).

***

Try the following exercises to test your understanding.

---

E3) Encrypt the text ‘ATTACK POSTPONED’ using a shift transformation with shift parameter 15.

E4) The ciphertext ‘T SLGP DTYO’ was obtained by applying the shift transformation with parameter 11. Find the plaintext.

---

In the next subsection, we will look at another generalisation of the shift cipher, the affine cipher.

### 3.2.3 Affine Cipher

The Caesar cipher discussed earlier is a special case of the substitution cipher which includes only 26 of the 26! possible permutations of the 26 elements. Another special case of the substitution cipher is the **affine cipher**, which we describe now. In the affine cipher, we restrict the encryption functions to functions of the form

\[ E(x) = ax + b, \]

\(a \in \mathbb{Z}_{26}^*, b \in \mathbb{Z}_{26}\). These functions are called **affine functions**, hence the name **affine cipher**. Observe that when \(a = 1, b = 3\), we have the Caesar cipher.

In order that decryption is possible, it is necessary to ask when an affine function is injective. In other words, for any \(y \in \mathbb{Z}_{26}\), we want the equation

\[ ax + b \equiv y \]

to have a unique solution for \(x\). This equation is equivalent to

\[ ax = y - b \]

Now, as \(y\) varies over \(\mathbb{Z}_{26}\), so too, does \(y - b\) vary over \(\mathbb{Z}_{26}\). Hence, it suffices to study the congruence \(ax = y\), where \(y \in \mathbb{Z}_{26}\).

**Proposition 1:** The equation \(ax = y\) has a unique solution \(x \in \mathbb{Z}_{26}\) for every \(y \in \mathbb{Z}_{26}\) if and only if \(\gcd(a, 26) = 1\).
Classical Ciphers

Proof: This follows from proposition 2 in Unit 6 of MMT-003 with \( n = 26 \).

At this point we have shown that, if \( \gcd(a, 26) = 1 \), then an equation of the form \( ax \equiv y \) has, at most, one solution in \( \mathbb{Z}_{26} \). Hence, if we let \( x \) vary over \( \mathbb{Z}_{26} \), then \( ax \) takes on 26 distinct values in \( \mathbb{Z}_{26} \). That is, it takes on every value exactly once. It follows that, for any \( y \in \mathbb{Z}_{26} \), the congruence \( ax \equiv y \) has a unique solution for \( y \).

There is nothing special about the number 26 in this argument. The following result follows from proposition 2 in Unit 6 of MMT-003.

**Theorem 1:** The congruence \( ax \equiv y \) has a unique solution \( x \in \mathbb{Z}_m \) for every \( y \in \mathbb{Z}_m \) if and only if \( \gcd(a, m) = 1 \).

We would like to once again remind you that, in this unit, we represent \( \mathbb{Z}_m \) by the set \( A_m \) together with addition and multiplication modulo \( m \) as the binary operations.

Since \( 26 = 2 \times 13 \), the values of \( a \in \mathbb{Z}_{26} \) such that \( \gcd(a, 26) = 1 \) are \( a = 1, 3, 5, 7, 9, 11, 15, 17, 19, 21, 23 \) and \( 25 \). The parameter \( b \) can be any element in \( \mathbb{Z}_{26} \). Hence the affine cipher has \( 12 \times 26 = 312 \) possible keys. It is clear that this is much too small to be secure. In some cases it will be possible to break it by an exhaustive key search.

Let us now consider the general setting where the modulus is \( m \). Recall that

\[
\phi(m) = |\{a \in \mathbb{Z}_m | (a, m) = 1\}|
\]

**Definition 2:** Suppose \( a \geq 1 \) and \( m \geq 2 \) are integers. If \( \gcd(a, m) = 1 \), then we say that \( a \) and \( m \) are relatively prime. The number of integers less than \( m \) that are relatively prime to \( m \) is often denoted by \( \phi(m) \) (this function is called the Euler phi-function).

Corollary 3 in Unit 6 of MMT-003 gives the value of \( \phi(m) \) in terms of the prime power factorisation of \( m \).

**Theorem 2:** Suppose

\[
m = \prod_{i=1}^{n} p_i^{e_i},
\]

is the prime factorisation of \( m \), where the \( p_i \)'s are distinct primes and \( e_i > 0 \), \( 1 \leq i \leq n \). Then

\[
\phi(m) = \prod_{i=1}^{n} (p_i^{e_i} - p_i^{e_i-1}). \tag{7}
\]

If the encryption function is given by

\[
E(x) = ax + b, \text{ where } \gcd(a, m) = 1,
\]

then the number of choices for \( b \) is \( m \), and the number of choices for \( a \) is \( \phi(m) \). It follows that the number of keys in the affine cipher over \( \mathbb{Z}_m \) is \( m \phi(m) \), where \( \phi(m) \) is given by the formula above. For example, when \( m = 60 \), \( \phi(60) = 2 \times 2 \times 4 = 16 \) and the number of keys in the affine cipher is, therefore, 960.

We have seen earlier, in the case \( m = 26 \), that to decrypt, we need to solve the equation \( y = ax + b \) for \( x \) in \( \mathbb{Z}_{26} \), and that the equation will have a unique solution in \( \mathbb{Z}_{26} \) (since we have taken \( a \) to be relatively prime to 26). However, the discussion above does not give us an efficient method of finding the solution. What we require is an efficient algorithm to do this. Some results on modular arithmetic will provide us with the efficient decryption algorithm we seek.
By proposition 2 in Unit 6 of MMT-003 it follows that a has a multiplicative inverse modulo m if and only if \( \gcd(a, m) = 1 \); and if a multiplicative inverse exists, it is unique. Also, observe that if \( b = a^{-1} \), then \( a = b^{-1} \). In \( \mathbb{Z}_{26} \), there are 12 elements relatively prime to 26, so trial and error suffices to find the multiplicative inverse of these elements. \( 1^{-1} = 1, 3^{-1} = 9, 5^{-1} = 21, 7^{-1} = 15, 11^{-1} = 19, 17^{-1} = 23, \) and \( 25^{-1} = 25 \). All of these can be easily verified. This is left as an exercise.

Consider the equation \( y \equiv ax + b \). This is equivalent to

\[
ax = y - b \tag{8}
\]

Since \( \gcd(a, m) = 1 \), a has a multiplicative inverse modulo m, say c, so that \( ac = 1 = ca \). Multiplying both sides of the Eqn. (8) by \( a^{-1} \), we obtain

\[
c(ax) = c(y - b)
\]

We have

\[
c(ax) = (ca)x = 1x = x
\]

Consequently,

\[
x \equiv c(y - b),
\]

and the decryption function is, therefore,

\[
D(y) = a^{-1}(y - b) \pmod{m}
\]

We can completely describe the affine cipher as follows:

Let m be a positive integer. We have \( \Sigma = \Delta = \mathbb{Z}_m \), \( \mathcal{P} \) and \( \mathcal{C} \) are subsets of \( \mathcal{L}(\mathbb{Z}_m) \) consisting of strings of length \( \leq t \). The key space \( \mathcal{K} \) consists of all pairs \( (a, b) \in \mathbb{Z}_m \times \mathbb{Z}_m \) for which \( \gcd(a, m) = 1 \). The encryption function \( E_k \) for key \( k = (a, b) \) is

\[
E_k : \mathbb{Z}_m \rightarrow \mathbb{Z}_m, \ x \mapsto ax + b \pmod{m}
\]

The decryption function for key \( k = (a, b) \) is

\[
D_k : \mathbb{Z}_m \rightarrow \mathbb{Z}_m, \ x \mapsto a^{-1}(x - b) \pmod{m}
\]

**Example 4:** Let us take \( m = 26 \). Suppose that the key \( k = (7, 3) \). As noted before, \( 7^{-1} \pmod{26} = 15 \). The encryption function is

\[
E_k(x) = 7x + 3 \pmod{26},
\]

and the corresponding decryption function is

\[
D_k(y) = 15(y - 3) \pmod{26},
\]

that is,

\[
D_k(y) = 15y - 19 \pmod{26}.
\]

---

**E5)**

a) How many different shift transformations are there with an N-letter alphabet?

b) How many affine transformations are there when \( N = 26, 27, 28, 29, 30 \)?
Classical ciphers, also known as symmetric encryption, were the only type of encryption in use before the development of public-key encryption. This unit will comprise topics related to classical ciphers.

Let us look at the process of symmetric encryption in a general set-up. Encryption schemes are used to keep messages or stored data secret. Suppose Alice and Bob want to communicate over an insecure channel without Eve coming to know what they are saying to each other. Alice encrypts or enciphers the message $P$, which we call plaintext, using a predetermined key, and obtains a cipher text $C$. The plaintext could be anything, a word processor file, an image file or a database file or any other kind of file. Alice transmits the cipher text $C$ to Bob, who converts it back into plain text by decryption. To decrypt or decipher, Bob needs some secret information, a decryption key. Now, Eve may still be able to intercept the cipher text. However, the encryption should guarantee secrecy and prevent her from deriving any information about the plain text from the observed cipher text without the secret information that is needed to decrypt the message.

To use a specific cryptosystem, Alice and Bob will employ the following procedure. They choose a random key $k \in \mathcal{K}$ first. They can meet at some mutually agreed place, away from the prying eyes of Eve, and decide upon the key. They could also use a secure channel. A secure channel could be a trusted courier, for example. Another possibility is to use a key exchange protocol like the Diffie-Hellman protocol that we will discuss in the third Block of this course.

Suppose Alice wants to communicate a message to Bob over an insecure channel later. Suppose this message is a string $x = x_1, x_2, \ldots, x_n$ for some integer $n \geq 1$, where each plain text symbol $x_i \in \Sigma$, $1 \leq i \leq n$. Alice encrypts each $x_i$ using the encryption rule $E_k$ specified by the predetermined key $k$. Hence Alice computes $E_k(x_i), 1 \leq i \leq n$ and sends the resulting cipher text string $y = y_1, y_2, \ldots, y_n$ over the channel. When Bob receives $y = y_1, y_2, \ldots, y_n$, he decrypts it using the decryption function $D_k$, obtaining the original plain text string $x_1, x_2, \ldots, x_n$. Fig. 1 is an illustration of the communication channel.

![Fig. 1: The Communication Channel.](image)

Note that, each encryption function $E_k$ is an injective function (i.e., one-to-one), otherwise, decryption could not be accomplished in an unambiguous manner. For example, if

$$y = E_k(x_1) = E_k(x_2) \quad \text{where} \quad x_1 \neq x_2,$$

then Bob has no way of knowing whether $y$ should decrypt to $x_1$ or $x_2$.

Note that if $\mathcal{P} = \mathcal{C}$, it follows that each encryption function is a permutation. That is, if the set of plain texts and cipher texts are identical, then each encryption function just rearranges (or permutes) the elements of this set. In the example of the Caesar cipher above, we have seen that $\mathcal{P} = \mathcal{C}$ as they are both equal to the set of strings of length $\leq t$ in the set of symbols $\mathcal{A}$.

Let us recall the following definition of an algorithm:
Definition 3: An algorithm is a formula or set of steps for solving a particular problem. To be an algorithm, a set of rules must be unambiguous and have a clear stopping point.

From every encryption method, we get an encryption algorithm, which performs various modifications on the plain text, and a decryption algorithm, which essentially reverses the modifications done by the encryption algorithm. Algorithms for classical schemes use the same secret key for both encrypting and decrypting the text. So, these encryption methods are therefore called symmetric.

Classical ciphers are often divided into substitution ciphers and transposition ciphers.

In a substitution cipher, letters (or groups of letters) are systematically replaced throughout the message for other letters (or groups of letters). The earliest known use of a substitution cipher, and the simplest, was the Caesar cipher.

In a transposition cipher, the letters themselves are kept unchanged, but rather their order within the message is scrambled according to some well-defined scheme.

We can devise more complex algorithms by performing several simple transformations one after another.

Definition 4: A product cipher $F$ is a cipher obtained by composing different ciphers $f_1, f_2, \ldots, f_k$, i.e. $F = f_1 \circ f_2 \circ f_3 \circ \cdots \circ f_k$ where $\circ$ denotes composition of functions.

Modern ciphers, for example the data encryption standard (DES), iterate through several stages of substitution and transposition.

The rest of this unit deals only with transposition ciphers and substitution ciphers.

---

E7) What is the key space of the generalised Caesar cipher when

a) the plain text space is $\{0,1,\ldots,25\}$?

b) the plain text space is $\{0,1,\ldots,N-1\}$, for any positive integer $N$?

E8) The cipher text VHFUHW has been generated with the (generalised) Caesar cipher on the plain text space $\{0,1,\ldots,25\}$. Determine the key and the plain text.

E9) Which of the following schemes is a cryptosystem? We always let $S = \{0,1,\ldots,25\}$ to be the set of alphabets. The plaintext $P$ and $C$ consist of strings of length $\leq t$ on $S$ for some $t$.

a) Each letter $c \in S$ is replaced by $kc$, $k \in \{1,2,\ldots,26\}$.

b) Each letter $c \in S$ is replaced by $kc$, $k \in \{1,2,\ldots,26\}$, $\gcd(k,26) = 1$.

Cryptography is not used by law abiding people alone. Even criminals and terrorists use cryptography to keep their secrets. In this case, the law enforcement agencies will play the role of Eve. Suppose you are an law enforcement officer and you want to read a communication between two law breakers. You are not privy to the enciphering and deciphering information used by the two people, but you would nevertheless like to be able to read the enciphered messages. If you succeeded in doing so, you would have broken the cipher, and the science of breaking ciphers is called cryptanalysis.

To break a cryptosystem, you need two types of information. The first is the general nature (the structure) of the system. For example, suppose you know that the cryptosystem uses a shift transformation on single letters of the 26-letter alphabet $A \rightarrow Z$ with numerical equivalents $0 \rightarrow 25$, respectively.
The second type of information is the knowledge of a specific choice of certain parameters connected with the given type of cryptosystem. In our example, the second type of information you need to know is the choice of the shift parameter $b$. Once one has that information, one can encipher and decipher by the formulas $C = P + b$ and $P = C - b$. Of course, the shift cipher is too weak and if it is known that the text has been encrypted using a shift cipher, we can easily find the plain text by trying all possible keys.

In the earlier days, both the ciphering algorithm and the keys were kept secret. However, the modern designers of cryptosystems always make the assumption that the general structural information is known. This assumption is called Kerchoff's law.

In practice, users of cryptography often have a special computer chip or software for enciphering and deciphering text. The chip or software usually uses only one type of cryptosystem. Over a period of time the information about what type of system they are using might leak out. To increase their security, therefore, the users frequently change the choice of parameters used with the system. So, any cryptosystem has to have sufficiently many keys so that the cryptosystem cannot be solved by exhaustive key search, i.e. by trying out all the possible keys.

We conclude this section here. In the next section, we will start our discussion of simple ciphers with transposition ciphers.

### 3.3 SUBSTITUTION CIPHERS

A substitution cipher is one in which each character in the plain text is substituted for another character in the cipher text. The receiver inverts the substitution on the cipher text to recover the plain text. This cryptosystem has been used for hundreds of years.

In classical cryptography, there are four types of substitution ciphers:

- **A simple substitution cipher**, or **mono-alphabetic cipher**, is one in which each character of the plain text is replaced with a corresponding character of cipher text.

  **Definition 5:** Suppose $\Sigma = \Delta$, i.e. the set of alphabets for the plaintexts and ciphertexts are the same. Let $P$ be the set of all strings of length $t$ over $\Sigma$. So, $P$ consists of elements of the form $m = m_1m_2 \ldots m_t$, where each $m_i \in \Sigma$. Let $\mathcal{K}$ be the set of all permutations on the set $\Sigma$. Define for each $e \in \mathcal{K}$ an encryption transformation $E_e$ as:

  $$E_e(m) = e(m_1)e(m_2) \ldots e(m_t) = c_1c_2, \ldots, c_t = c,$$

  where $m = m_1m_2 \ldots m_t \in \mathcal{M}$. In other words, for each symbol in a t-tuple, replace it by another symbol from $\Sigma$ according to some fixed permutation $e$. To decrypt $c = c_1, c_2, \ldots, c_t$ compute the inverse permutation $d = e^{-1}$ and use it to decrypt as follows:

  $$D_d(c) = d(c_1)d(c_2) \ldots d(c_t) = m_1m_2 \ldots m_t = m$$

  $E_e$ is called a **simple substitution cipher** or a **mono-alphabetic substitution cipher**.

- **A homophonic substitution cipher** is like a simple substitution cryptosystem, except a single character of plain text can map to one of several characters of cipher text. For example, “A” could correspond to either 5, 13, 25, or 56, “E” could correspond to either 7, 19, 31, or 42, and so on. Usually, only vowels are mapped to more than one character. Strictly speaking, this is not a cryptosystem according to our definition because we don’t get a function in this case.
• A **polygram substitution cipher** is one in which blocks of characters are encrypted in groups. For example, “ABA” could correspond to “RTQ,” “ABB” could correspond to “SLL,” and so on.

• A **polyalphabetic substitution cipher** is made up of multiple simple substitution ciphers. For example, there might be five different simple substitution ciphers used; the particular ones used changes with the position of each character of the plain text.

The earliest known use of a substitution cipher, and the simplest, was the Caesar cipher, which is an example of a simple substitution cipher. The cipher text alphabet is actually a rotation of the plain text alphabet and not an arbitrary permutation.

ROT13 is a simple encryption programme commonly found on UNIX systems; it is also a simple substitution cipher. In this cipher, “A” is replaced by “N,” “B” is replaced by “O,” and so on. Every letter is rotated 13 places.

Encrypting a file twice with ROT13 restores the original file.

\[ P = \text{ROT13} (\text{ROT13} (P)) \]

Polygram substitution ciphers are ciphers in which groups of letters are encrypted together.

Polyalphabetic substitution ciphers have multiple one-letter keys, each of which is used to encrypt one letter of the plain text. The first one encrypts the first letter of the plain text, the second one encrypts the second letter of the plain text, and so on. After all the keys are used, the keys are recycled. If there were 20 one-letter keys, then every twentieth letter would be encrypted with the same key. This is called the **period** of the cipher. In classical cryptography, ciphers with longer periods were significantly harder to break than ciphers with short periods. There are computer techniques that can easily break substitution ciphers with very long periods. The **Vigenère cipher**, which we will discuss later in this unit, is an example of a polyalphabetic substitution cipher.

**Remark 1:** In the case of the substitution cipher, we might as well take \( \Delta = \Sigma = \{A, B, C, \ldots, Z\} \). We used \( \Delta \) in the Caesar cipher because encryption and decryption were algebraic operations. In most substitution ciphers, it is more convenient to think of encryption and decryption as permutations of alphabetic characters.

### 3.3.1 The Vigenère Cipher

The best known, and one of the simplest examples of the **polyalphabetic substitution cipher** is the **Vigenère cipher**. This cipher is named after Blaise de Vigenère, who lived in the sixteenth century. As described earlier, polyalphabetic substitution ciphers have multiple one-letter keys, each of which is used to encrypt one letter of the plain text. The first one encrypts the first letter of the plain text, the second one encrypts the second letter of the plain text, and so on. After all the keys are used, the keys are recycled.

Using the correspondence \( A \leftrightarrow 0, B \leftrightarrow 1, \ldots, Z \leftrightarrow 25 \) described earlier, we can associate each key \( k \) with an alphabetic string of length \( m \), called a **keyword**. The Vigenère cipher encrypts \( m \) alphabetic characters at a time: each plain text element is equivalent to \( m \) alphabetic characters. Let us look at a small example.

**Example 5:** Suppose \( m = 6 \) and the keyword is `CEASAR`. This corresponds to the numerical equivalent \( k = (2, 4, 0, 18, 0, 17) \). Suppose the plain text is the string ‘ICAMEISAWICONQUERED’.
We convert the plain text elements to residues modulo 26, write them in groups of six, and then “add” the keyword modulo 26, as follows:

```
8  2  0 12 4  8 18 0 22 8  2 14 13 16 20 4 17 4 3
2  4 0 18 0 17 2 4 0 18 0 17 2 4 0 18 0 17 2
10 6 0 4 25 20 4 22 0 2 5 15 20 24 22 17 21 5
```

The alphabetic equivalent of the cipher text string would thus be ‘KGAEECUEWACFPUUWRVF’. To decrypt, we can use the same keyword, but we would subtract it modulo 26 instead of adding.

---

The alphabetic equivalent of the cipher text string would thus be ‘KGAEECUEWACFPUUWRVF’. To decrypt, we can use the same keyword, but we would subtract it modulo 26 instead of adding.

---

Try this exercise to test your understanding of Vigenère cipher.

---

E10) Encrypt the string ‘ICAMEISAWICONQUERED’ using the Vigenère cipher. Use the keyword ‘GAUL’.

E11) Decrypt the string ‘WTBTYKXXHOTXHJEL’ which was encrypted using Vigenère cipher with the keyword ‘WAIT’.

---

Another way of understanding and implementing the Vigenère cipher is by using the Vigenère tableau. See Table 3. Each of the 26 ciphers is laid out horizontally, with the key letter for each cipher to its left. A normal alphabet for the plain text runs across the top. The process of encryption is simple: Given a key letter x and a plain text letter y, the cipher text letter is at the intersection of the row labelled x and the column labelled y; in this case the cipher text is V. To encrypt a message, a key is needed that is as long as the message. Usually, the key is a repeating keyword. Let us look at the same Example 5 considered above. Using the Vigenère tableau (see Table 3), the message ‘ICAMEISAWICONQUERED’ is encrypted as follows:

```
key: CAESARCAESARCAESAR
plain text: ICAMEISAWICONQUERED
cipher text: KGAEECUEWACFPUUWRVF
```

Decryption is equally simple. The key letter again identifies the row. The position of the cipher text letter in that row determines the column, and the plain text letter is at the top of that column.

The strength of this cipher is that there are multiple cipher text letters for each plain text letter, one for each unique letter of the keyword. Thus, the letter frequency information is lost. However, not all knowledge of the plain text structure is lost. There is enough information available which will enable us to break this cipher.

In the next section, we discuss another important class of ciphers, the transposition ciphers.

---

### 3.4 TRANSPOSITION CIPHERS

As we mentioned in the previous section, in transposition cipher, the set of letters in the given plaintext remains the same but the position of the letters are altered. The transposition cipher, also called the permutation cipher, has been in use for hundreds of years. This is because, the encryption is thus achieved by performing some sort of permutation on the plain text characters.

A simple transposition cipher preserves the number of symbols, and thus is easily cryptanalysed. We shall defer the discussion on cryptanalysis of these ciphers, as well as that of other encryption schemes, to the last section.
### Table 3: The Vigenère Tableau

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

### Mathematical Preliminaries and Classical Ciphers
The following are some implementations of the transposition cipher:

### 3.4.1 The Row Transformation Cipher

This is the simplest transposition cipher. We fix the number of rows, say m. In the row transformation cipher, the plain text is written downwards on successive columns, starting a new column when the m\textsuperscript{th} row is reached. The message is then read off in rows. For example, if we have three rows and a message of ‘WE ARE DISCOVERED FLEE AT ONCE’, the sender writes out

```
W R I O R F E O E P
E E S V E L A N J D
A D C E D E T C X Q
```

The extra odd letters at the end are “nulls”, added to round off the pattern, or to confuse an eavesdropper. The cipher text is read off as ‘WRIOR FEOP EESVE LANJD ADCEDE TCXE’.

(Grouping letters into blocks of a standard size, typically five, was a practice developed for the ease of transmission.)

### 3.4.2 Simple Columnar Transposition Cipher

In the simple columnar transposition cipher, we fix the number of columns. The plain text is written horizontally onto a piece of graph paper of width m and the cipher text is read off vertically. Decryption is a matter of writing the cipher text vertically onto a piece of graph paper of identical width and then reading the plain text off horizontally.

The following diagram illustrates the simple columnar transposition cipher with column width six.

Plain text: ‘WE ARE DISCOVERED FLEE AT ONCE’

```
W E A R E D
I S C O V E
R E D F L E
E A T O N C
E U V W X Y
```

Cipher text: ‘WIRE ESEAU ACDTV ROFOW EVLNX DEECY’

The ancient Greeks, and the Spartans in particular, are said to have used this cipher to communicate during military campaigns in what is known as the scytale cipher. A scytale is a tool used to perform a transposition cipher, consisting of a cylinder with a strip of paper wound around it on which is written a message.

The recipient uses a rod of the same diameter on which he wraps the paper to read the message. It has the advantage of being fast and not prone to mistakes. It can, however, be easily broken.

### 3.4.3 Other Transposition Techniques

The two ciphers described above are easy to break. To make it more complex, we could permute the order of the columns after writing the message in a rectangle in a similar
fashion as before. That is, to encrypt, we write the message row by row, shuffle the columns, and then read off the ciphertext column by column. The order of the columns then becomes the key to the algorithm. For example,

Plaintext: RETURN TO HEADQUARTERS AT ONCE

Key: 4 3 1 2 5 6 7
R E T U R N T
O H E A D Q U
A R T E R S A
T O N C E X Y

ciphertext: ‘TETN UAEC EHRO ROAT RDRE NQSX TUAY’

A pure transposition cipher has the drawback that the ciphertext has the same letter frequencies as the plaintext. Thus, to cryptanalyze this kind of cipher is fairly straightforward. In the case of the type of columnar transposition you have just seen, in order to break it, you need to arrange the ciphertext in a matrix and shuffle the columns around. Read off the resulting text you get at each trial until you hit upon a message which makes sense.

We can increase the degree of security of the transposition cipher by performing more than one stage of transposition. Shuffling the columns more than once greatly enhances the security of this cipher as it becomes more difficult to arrive at the original plaintext by rearranging the columns of the matrix, without knowing the key. Thus, let us encrypt the foregoing message again, using the same algorithm.

Key: 4 3 1 2 5 6 7
Input: T E T N U A E
C E H R O R O
A T R D R E N
Q S X T U A Y

Output: ‘THRX NRDT EETS TCAQ UORU AREA EONY’

What do we achieve by repeating the transposition? To answer this question, let us first assign a number to each letter in the original plaintext message, that number being its position in the message. Hence, the original message is represented by

01 02 03 04 05 06 07 08 09 10 11 12 13 14
15 16 17 18 19 20 21 22 23 24 25 26 27 28

After the first transposition we have

03 10 17 24 04 11 18 25 02 09 16 23 01 08
15 13 04 23 19 14 11 01 26 21 18 08 06 28

Notice that this sequence of numbers has some pattern to it.

But after the second transposition, we have

17 09 05 27 24 16 12 07 10 02 22 20 03 25
15 13 04 23 19 14 11 01 26 21 18 08 06 28
This is a more complex permutation and is much more difficult to cryptanalyze.

We shall end this section with a formal definition of the transposition cipher. Let us assume that the plain text consists of letters from the English alphabet, and to each letter of the alphabet, we assign a number designated by its order. For example, 0 corresponds to A, 1 corresponds to B, . . . , 25 corresponds to Z. Thus the English alphabet can be represented by \( \mathbb{Z}_{26} \), according to the following table:

<table>
<thead>
<tr>
<th></th>
<th>A</th>
<th>B</th>
<th>C</th>
<th>D</th>
<th>E</th>
<th>F</th>
<th>G</th>
<th>H</th>
<th>I</th>
<th>J</th>
<th>K</th>
<th>L</th>
<th>M</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>1</td>
<td>2</td>
<td>3</td>
<td>4</td>
<td>5</td>
<td>6</td>
<td>7</td>
<td>8</td>
<td>9</td>
<td>10</td>
<td>11</td>
<td>12</td>
<td></td>
</tr>
<tr>
<td>13</td>
<td>14</td>
<td>15</td>
<td>16</td>
<td>17</td>
<td>18</td>
<td>19</td>
<td>20</td>
<td>21</td>
<td>22</td>
<td>23</td>
<td>24</td>
<td>25</td>
<td></td>
</tr>
</tbody>
</table>

**Definition 6:** Let \( m \) be some fixed positive integer. Let \( \mathcal{P} \) and \( \mathcal{C} \) be set of strings of length at most \( t \) and let \( \mathcal{K} \) consist of all permutations of \( \{1, 2, \ldots, m\} \). We divide the plaintext into strings of length \( m \) encrypt and decrypt as follows: For a key (i.e., a permutation) \( \pi \), we define

\[
ed_{\pi}(x_1, x_2, \ldots, x_m) = (x_{\pi(1)}, x_{\pi(2)}, \ldots, x_{\pi(m)})
\]

and

\[
d_{\pi}(y_1, y_2, \ldots, y_m) = (y_{\pi^{-1}(1)}, y_{\pi^{-1}(2)}, \ldots, y_{\pi^{-1}(m)}),
\]

where \( \pi^{-1} \) is the inverse permutation to \( \pi \).

Let us consider the following example which gives a slightly different type of implementation of the transposition cipher from the ones discussed above:

**Example 6:** Suppose \( m = 5 \) and the key is the following permutation \( \pi \):

\[
\begin{array}{ccccc}
1 & 2 & 3 & 4 & 5 \\
3 & 5 & 2 & 1 & 4
\end{array}
\]

Then the inverse permutation \( \pi^{-1} \) is the following:

\[
\begin{array}{ccccc}
1 & 2 & 3 & 4 & 5 \\
4 & 3 & 1 & 5 & 2
\end{array}
\]

Now, suppose we are given the plain text ‘RETURN TO HEADQUARTERS’ We first group the plain text into groups of six letters:

**RETUR | NTOHE | ADQUA | RTERS**

Let us now apply the permutation to the block RETUR as shown in Fig. 2. Let us similarly permute the remaining blocks according to the permutation \( \pi \). We get the following

**UTRRE | HONET | UQAAD | RERST |**

So, the cipher text is ‘UTRREHONETUQAADRERST’. We can decrypt the ciphertext in a similar fashion, using the inverse permutation \( \pi^{-1} \).

***

Try the following exercise to test your understanding of the transposition ciphers.
E12) Use the simple columnar transposition cipher of width six to encrypt the plain text “CANCEL LAST ORDER HEADQUARTERS.”

E13) In order to make the cipher in Exercise 12 more secure, permute the order of the columns according to the key 453261. Write down the cipher text you obtain after this step. Re-encrypt the cipher text using the same algorithm, and write down the final output.

In the next section, we will adopt the point of view of Eve who would like to read the messages without the key. We will discuss cryptanalysis of ciphers.

### 3.5 CRYPTOANALYSIS

**Cryptanalysis** is the science of studying attacks against cryptographic schemes. Successful attacks may, for example, recover the plain text (or parts of the plain text) from the cipher text, substitute parts of the original message, or forge digital signatures. Cryptography and cryptanalysis are often subsumed by the more general term **cryptology**.

There is a fundamental assumption in cryptanalysis usually referred to as **Kerckhoff’s principle**. It states that the adversary knows all the details of the cryptosystem, including algorithms and their implementations. According to this principle, the security of a cryptosystem must be entirely based on the secret keys. It would be more difficult for an adversary if she does not know what type of cryptosystem is being used, but as we mentioned earlier, this type of information can be leaked out easily enough, once the system has been used over a period of time. Hence, the security of a cryptosystem will be compromised if we base it only on this factor. Depending on the actual resources of the adversary Eve, there are different levels of attacks on cryptosystems. The most common types, in increasing order of strength, are:

1. **Ciphertext-only attack.** Eve has the ability to obtain ciphertexts. This is likely to be the case in any encryption situation. If this kind of attack is successful, then the encryption method is completely insecure.

2. **Known-plaintext attack.** Eve is able to obtain plaintext-ciphertext pairs. With the information she has from these pairs, she attempts to decrypt a ciphertext for which she does not have the plaintext. This kind of information may be available to Eve if, for example, the messages are sent in some standard format which she knows.

3. **Chosen-plaintext attack.** Eve has the ability to obtain ciphertexts for some particular plaintexts. She then uses this knowledge to try and decrypt a ciphertext for which she does not have the plaintext. Such a situation may arise if, for
example, Eve sends some data to Alice which she knows will be encrypted and then transmitted. Eve then intercepts the encrypted message, and uses the information to decipher some other ciphertext, without any further interaction. In this kind of attack, it is sufficient if the adversary carries out this operation just once.

4. **Adaptively-chosen-plaintext attack.** This is the same as the previous attack, except now Eve may repeat the process more than once to obtain more plaintext-ciphertext pairs. This means she has more access to the encrypting device.

5. **Chosen and adaptively-chosen-ciphertext attack.** These two attacks are similar to the above plaintext attacks. Eve can choose ciphertexts and then access the corresponding plaintexts from Bob. That is, in this attack, Eve has access to the decryption device.

In order to break a cryptosystem, the goal is to determine the key that was used. Let us now see how the attacks listed above work.

A simple ciphertext-only attack is the following. The attacker Eve decrypts the ciphertext with all keys from the key space until she finds the correct plaintext among the few plaintexts that make sense. That attack is called *exhaustive key search*. This attack will work for cryptosystems with very small key spaces. For example, the Caesar cipher uses only 26 keys. It is, therefore, very easy to determine the plaintext from the ciphertext by the method of exhaustive key search, and checking which plaintext makes sense. This also yields the secret key being used. (Note that the notion of a “small” key space depends on how much computing power is available.)

So, for a secure cryptosystem, the minimum requirement is that it should resist an exhaustive key search, i.e., the key space should be very large. However, a large key space is not sufficient to guarantee security because there are other methods of cryptanalysis which will succeed in certain ciphers as we shall see below.

**Cryptanalysis of the Affine Cipher**

As a simple illustration of how cryptanalysis can be performed using statistical data, let us look at the **affine cipher**. The following example is from [15], page 27.

Suppose Eve has intercepted the following ciphertext:

FMXVEDKAPHFERBNDRXRSREFMORUDSDKDVSHVUFEDKAPRCKDLYEVLRHRH

The frequency analysis of this ciphertext is given in Table 4.
There are only 57 characters of ciphertext, but this is sufficient to cryptanalyze an affine cipher. The ciphertext characters that occur frequently are: R (8 occurrences), D (6 occurrences), E, H, K (5 occurrences each), and F, S, V (4 occurrences each). Since E and T are the two most common letters (see Table 5), our first guess is that R is the encryption of e and D is the encryption of t. This means that $E_k(4) = 17$ and $E_k(19) = 3$. Recall that $E_k(x) = ax + b \pmod{26}$, where $a$ and $b$ are unknowns. So, we have the equations

$$4a + b \equiv 17 \pmod{26}$$
$$19a + b \equiv 3 \pmod{26}.$$ 

You can check that $a = 6$, $b = 19$ in $Z_{26}$ satisfy these equations. But this is an illegal key, since $\gcd(a, 26) = 2 > 1$. So our first guess is wrong.

Let us now check if R is the encryption of e and E is the encryption of t. Proceeding as above, we obtain $a = 13$, which is again not a valid key.

The next possibility is that R is the encryption of E and H is the encryption of T. We get $a = 8$ in this case, which is also impossible. Let us now check if R is the encryption of E and K is the encryption of T. We now obtain $a = 3$, $b = 5$, which is at least a legal key. To confirm that this is the key, we have to find the decryption function corresponding to $k = (3, 5)$, and then decrypt the ciphertext to see whether or not we get a string which makes sense. The decryption function corresponding to $(3, 5)$ as the key is $D_k(y) = 9y - 19 \pmod{26}$. Under this transformation, the given ciphertext yields:

$$\text{Thus, we conclude that we have determined the correct key.}$$

E14) Using frequency analysis, cryptanalyse and decipher the following message, which you know was enciphered using a shift transformation of single-letter plain text message units in the 26-letter alphabet:

PXPXXENVDRUXVTNLXHYMGMAAAXYKXJN
XGVRFXXMAHWGXWXWLEHGZXXKVBJAXKMXQM.

E15) In a long string of cipher text which was encrypted by means of an affine map on single-letter message units in the 26-letter alphabet, you observe that the most frequently occurring letters are “Y” and “V”, in that order. Assuming that those cipher text message units are the encryption of “E” and “T” respectively, read the message “QAOOYYQQEVHEQV”.

---

### Table 4: Frequency of Occurrence of the 26 Ciphertext Letters

<table>
<thead>
<tr>
<th>letter</th>
<th>frequency</th>
<th>letter</th>
<th>frequency</th>
</tr>
</thead>
<tbody>
<tr>
<td>A</td>
<td>2</td>
<td>N</td>
<td>1</td>
</tr>
<tr>
<td>B</td>
<td>1</td>
<td>O</td>
<td>1</td>
</tr>
<tr>
<td>C</td>
<td>0</td>
<td>P</td>
<td>2</td>
</tr>
<tr>
<td>D</td>
<td>7</td>
<td>Q</td>
<td>0</td>
</tr>
<tr>
<td>E</td>
<td>5</td>
<td>R</td>
<td>8</td>
</tr>
<tr>
<td>F</td>
<td>4</td>
<td>S</td>
<td>3</td>
</tr>
<tr>
<td>G</td>
<td>0</td>
<td>T</td>
<td>0</td>
</tr>
<tr>
<td>H</td>
<td>5</td>
<td>U</td>
<td>2</td>
</tr>
<tr>
<td>I</td>
<td>0</td>
<td>V</td>
<td>4</td>
</tr>
<tr>
<td>J</td>
<td>0</td>
<td>W</td>
<td>0</td>
</tr>
<tr>
<td>K</td>
<td>5</td>
<td>X</td>
<td>2</td>
</tr>
<tr>
<td>L</td>
<td>2</td>
<td>Y</td>
<td>1</td>
</tr>
<tr>
<td>M</td>
<td>2</td>
<td>Z</td>
<td>0</td>
</tr>
</tbody>
</table>

---

algorithmsarequitegeneraldefinitionsofarithmeticprocesses
Cryptanalysis of Simple Substitution Ciphers

We can easily break substitution even when the key space is extremely large because the cipher does not hide the underlying frequencies of the different letters of the plain text. If the plain text consists of letters from the English alphabet, then the total number of all permutations on this set is 26!, i.e., the size of the key space is 26! ≈ 4 × 10^{26}, which is extremely large. However, the key being used can be determined quite easily by examining a modest amount of cipher text. This follows from the simple observation that the distribution of letter frequencies is preserved in the cipher text. For example, the letter E occurs more frequently than the other letters in ordinary English text. Hence the letter occurring most frequently in a sequence of cipher text blocks is most likely to correspond to the letter E in the plain text. By observing a modest amount of cipher text blocks, a cryptanalyst can determine the key. Such cipher text-only attacks use statistical properties of the plain text language.

Let us look at this method of frequency analysis in greater detail. We assume that the plain text string is ordinary English text, without punctuation or spaces. (This makes cryptanalysis more difficult than if punctuation and spaces were encrypted.)

Frequency table that give the estimated relative frequencies the 26 letters are available. The estimates in Table 5 were obtained by Beker and Piper.

<table>
<thead>
<tr>
<th>Letter</th>
<th>Probability</th>
</tr>
</thead>
<tbody>
<tr>
<td>A</td>
<td>.082</td>
</tr>
<tr>
<td>B</td>
<td>.015</td>
</tr>
<tr>
<td>C</td>
<td>.028</td>
</tr>
<tr>
<td>D</td>
<td>.043</td>
</tr>
<tr>
<td>E</td>
<td>.127</td>
</tr>
<tr>
<td>F</td>
<td>.022</td>
</tr>
<tr>
<td>G</td>
<td>.020</td>
</tr>
<tr>
<td>H</td>
<td>.061</td>
</tr>
<tr>
<td>I</td>
<td>.070</td>
</tr>
<tr>
<td>J</td>
<td>.002</td>
</tr>
<tr>
<td>K</td>
<td>.008</td>
</tr>
<tr>
<td>L</td>
<td>.040</td>
</tr>
<tr>
<td>M</td>
<td>.024</td>
</tr>
<tr>
<td>N</td>
<td>.067</td>
</tr>
<tr>
<td>O</td>
<td>.075</td>
</tr>
<tr>
<td>P</td>
<td>.019</td>
</tr>
<tr>
<td>Q</td>
<td>.001</td>
</tr>
<tr>
<td>R</td>
<td>.060</td>
</tr>
<tr>
<td>S</td>
<td>.063</td>
</tr>
<tr>
<td>T</td>
<td>.091</td>
</tr>
<tr>
<td>U</td>
<td>.028</td>
</tr>
<tr>
<td>V</td>
<td>.010</td>
</tr>
<tr>
<td>W</td>
<td>.023</td>
</tr>
<tr>
<td>X</td>
<td>.001</td>
</tr>
<tr>
<td>Y</td>
<td>.020</td>
</tr>
<tr>
<td>Z</td>
<td>.001</td>
</tr>
</tbody>
</table>

Table 5: Probabilities of Occurrence of the 26 Letters

On the basis of the above probabilities, Beker and Piper divide the 26 letters into five groups as follows:

1. E, having probability about 0.120
2. T, A, O, I, N, S, H, R, each having probabilities between 0.06 and 0.09
3. D, L, each having probabilities around 0.04
4. C, U, M, W, F, G, Y, P, B, each having probabilities between 0.015 and 0.023
5. V, K, J, X, Q, Z, each having probabilities less than 0.01.

It may also be useful to consider sequences of two or three consecutive letters called digrams and trigrams, respectively. The 30 most common digrams are (in decreasing order) TH, HE, IN, ER, AN, RE, ED, ON, ES, ST, EN, AT, TO, NT, HA, ND, OU, EA, NG, AS, OR, TI, IS, ET, IT, AR, TE, SE, HI, and OF. The twelve most common
trigrams are (in decreasing order) THE, ING, AND, HER, ENT, THA, NTH, WAS, ETH, FOR, and DTH.

**Homophonic substitution ciphers** are much more complicated to break than simple substitution ciphers, but still do not obscure all of the statistical properties of the plain text language. With a known-plain text attack, the ciphers are trivial to break. A cipher text-only attack is harder, but only takes a few seconds on a computer.

The best known, and one of the simplest examples of the **polyalphabetic substitution cipher** is the *Vigenère cipher*. Observe that the number of possible keywords of length $m$ in a Vigenère cipher is $26^m$, so even for relatively small values of $m$, an exhaustive key search would require a long time. For example, if we take $m = 5$, then the key space has size exceeding $1.1 \times 10^7$. This is already large enough to preclude exhaustive key search by hand.

We can break the Vigenère cipher by Kasiski method. Kasiski described this method in 1863, but apparently it was discovered earlier by Charles Babbage. We will give an outline of the method. If you are interested in more details, you can refer to books given as references at the end of the block. The method is based on the observation that two identical segments of plaintext will be encrypted to the same cipher text if they occur $d$ positions apart where $m \mid d$, $m$ being the length of the key word. In Kasiski method, we do the following: We search identical segments of ciphertexts of length at least 3 and note down the distances between such occurrences, say $d_1$, $d_2$, ..., If we obtain several such distances, then $m$ will probably divide all of them and hence it will divide their greatest common divisor. By looking at the various divisors of the greatest common divisor, we try to find the length of the key word.

Suppose we guess that the length of the key word is 5. We write the cipher text in grid of length 5. For example, if the cipher text is PXPXKXENVDRUXVTNLXHYMXGMAAXYKXJN and our guess is the text has been encrypted using Vigenère cipher with a key word of length 5. Then, we arrange the ciphertext in 5 columns as follows:

<table>
<thead>
<tr>
<th>1</th>
<th>2</th>
<th>3</th>
<th>4</th>
<th>5</th>
</tr>
</thead>
<tbody>
<tr>
<td>P</td>
<td>X</td>
<td>P</td>
<td>X</td>
<td>K</td>
</tr>
<tr>
<td>X</td>
<td>E</td>
<td>N</td>
<td>V</td>
<td>D</td>
</tr>
<tr>
<td>R</td>
<td>U</td>
<td>X</td>
<td>V</td>
<td>T</td>
</tr>
</tbody>
</table>

We analyse the frequencies of each of the columns separately, treating them as ciphertexts obtained using five different shift ciphers. If our guess about the length is correct, we can obtain the key using this method.

In a **transposition cipher** the plain text remains the same, but the order of characters is shuffled around. Since the letters of the cipher text are the same as those of the plain text, a frequency analysis on the cipher text would reveal that each letter has approximately the same likelihood as in English. This gives a very good clue to a cryptanalyst, who can then use a variety of techniques to determine the right ordering of the letters to obtain the plain text. Putting the cipher text through a second transposition cipher greatly enhances security. There are even more complicated transposition ciphers, but computers can break almost all of them.

Although many modern algorithms use transposition, it is troublesome because it requires a lot of memory and sometimes requires messages to be only of certain lengths. Substitution is far more common.

**3.6 SUMMARY**
In this unit we have covered the following points.

1. The definition of cryptography, and its goals.
2. The basic terms related to cryptography like encryption, decryption, plain text, cipher text and keys of a cipher.
4. Some substitution ciphers.
5. Various tools and methods for cryptanalysis of ciphers.

3.7 SOLUTIONS/ANSWERS

E1) WKH GLH LV FDVW
E2) BEWARE OF THE IDES OF MARCH
E3) ‘PIIPRZ EDHIEDCTS’.
E4) We apply a shift transformation with shift parameter 15 to recover the plaintext ‘I HAVE SIND’.
E5) a) N.
   c) The number of shift transformations on an m letter alphabet is mφ(m). Using Eqn. (7) we get the values as 312, 486, 812, 240.
E6) THRPXDH.
E7) a) \{1, \ldots, 25\}.
   b) \{1, \ldots, N-1\}.
E8) The key is 8 and the plain text is “SECRET”. Since the number of keys is just 26, we can decrypt the given cipher text easily, by trying out all the keys, one by one, until we get a word that makes sense.
E9) a) Not a cryptosystem because the encryption function is not injective. An example: Let k = 2. The letter A corresponds to 0, which is mapped to 0 (i.e., A). The letter N corresponds to 13, which is mapped to 213 = 0 (i.e., to A). By definition, the encryption function has to be injective. So, the system cannot be a cryptosystem.
   b) A cryptosystem. The key space is \{1, 2, \ldots, 26\}. If k is a key and \sigma a plain text unit, then k\sigma \mod 26 is the cipher text. This describes the encryption function for key k. The decryption function is the same, except that k is replaced by k^{-1} \mod 26.
E10) The answer is ‘OCUXKIMLCIWZTQOPXEX’.
E11) The answer is ‘ATTACKPOSTPONED’.
E12) Plain text: CANCEL LAST ORDER
The encryption is carried out as follows:

<table>
<thead>
<tr>
<th>C</th>
<th>A</th>
<th>N</th>
<th>C</th>
<th>E</th>
<th>L</th>
</tr>
</thead>
<tbody>
<tr>
<td>L</td>
<td>A</td>
<td>S</td>
<td>T</td>
<td>O</td>
<td>R</td>
</tr>
<tr>
<td>D</td>
<td>E</td>
<td>R</td>
<td>H</td>
<td>E</td>
<td>A</td>
</tr>
<tr>
<td>D</td>
<td>Q</td>
<td>U</td>
<td>A</td>
<td>R</td>
<td>T</td>
</tr>
<tr>
<td>E</td>
<td>R</td>
<td>S</td>
<td>X</td>
<td>Y</td>
<td>Z</td>
</tr>
</tbody>
</table>

Cipher text: CLDDE AAEQR NSRUS CTHAX EOERY LRATZ
E13) The cipher text obtained after the first encryption, applying the key 453261 is: LRATZ CTHAX NSRUS CLDDE AAEQR EOERY. Take this cipher text as the input and apply the same algorithm. That is, we write the input horizontally in a rectangle of width six and permute the columns according to same key 453261. The final output is: CSDQY TXCAE AASAO LTRDR RHUEE ZNLER.

E14) Use the fact that “X” occurs most frequently in the cipher text to find that the key \( b = 19 \). The message is:

\[
\text{WEWERELUCKYBECAUSEOFTENTHEFREQUENCY METHODNEEDSLONGERCIPHERTEXT.}
\]

E15) SUCCESSATLAST
Bibliography