Unit 4 Data and Privacy

Short Introduction

Data transfer is discussed in previous unit but this unit discusses "secure data transfer". Data is converted to unreadable format before sending and again it is converted back to readable format when it reaches its destination. This unit discusses such type of conversions to secure the transferring of data. A computer is accessible to others if it is connected to a network. In this unit, security measures are discussed for sending sensitive data over a network.

Students' Learning Outcomes

1. Ethical issues related to security

- Understand ethical issues related to data security
- Understand that it is their responsibility to safeguard the privacy of others.

2. Importance of data privacy

- Explain privacy concerns that arise through the mass collection of data
- Analyze the personal privacy and security concerns that arise with any use of computational systems.

3. Simple Encryption

- Explain why encryption is an important need for everyday life on the Internet.
- Crack a message encrypted with a Caesar cipher using a Caesar Cipher Widget
- Crack a message encrypted with random substitution using Frequency Analysis
- Explain the weaknesses and security flaws of substitution ciphers

4. Encryption with Keys and passwords

- Explain the relationship between cryptographic keys and passwords.
- Explain in broad terms what makes a key difficult to "crack."
- Reason about strong vs. weak passwords using a tool that shows password strength.
- Characteristics of good password

5. Cyber crime

- Explain the characteristics of a phishing attack
- Explain how a DoS (denial of service) attack

Introduction

Computers are ubiquitous and are widely used by people of almost all ages. Often we need to give our personal information to a computer e.g. while creating an email account, shopping online, visiting a hospital or taking admission in a school. We expect that provided information will not be shared with others. Protecting data from malicious users is called data privacy or information privacy.

4.1 Ethical Issues Related to Security

4.1.1 Understanding Ethical Issues Related to Data Security

The foundation of all security systems is formed on ethical principles. If, we have data of others, it is our own ethical responsibility to keep it secure. Some of the data security issues are:

- Confidentiality & Privacy
- Fraud & Misuse
- Patent
- Copyright
- Trade secrets
- Sabotage

- **Confidentiality & Privacy**

  To keep the data of others as confidential is indeed taking care of others. For example, if a bank shares the information about my banking transactions with my business competitors then it can harm my business. Similarly, phone companies are supposed to keep the invoices and bills as confidential. Keeping privacy and confidentiality has become difficult in this era of computers and Internet.

  Due to more usage of computers, a wide range of data is collected and stored. This data may be related to credit cards, organisational fund raising campaigns, opinion polls, shop at home services, driving licenses, arrest records and medical records. The potential threats to privacy include the improper use of computerized data. If a company sells email IDs and phone numbers to another company for marketing purpose, it breaches the confidentiality of data.

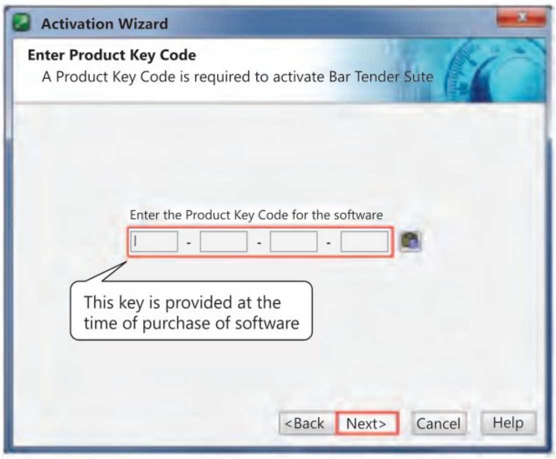
- **Piracy**

  Piracy means making illegal copies. It can be a book, software, movie, poetry, painting, house architecture or any other work protected by copyright law.

Do you know?

Open source software have no copyrights reservation. So, we can copy source code, modify it and can even sell it.

Software piracy is the illegal copying, distribution, or usage of software. Some software companies sell software with a confidential text, called the key of that software. This key is provided to only those people who buy that software. In this way illegal copies are stopped to be installed as shown in Figure 4.1. Some people start searching for that key by using illegal means. This is called cracking the key.



Activation Wizard

Enter Product Key Code

A Product Key Code is required to activate Bar Tender Sute

Enter the Product Key Code for the software

This key is provided at the time of purchase of software

Figure 4-1 Activating the software

Types of software piracy include:

- **Softlifting:** Borrowing and installing a copy of a software application from a colleague.

- **Client-server overuse**: Installing more copies of the software than you have licenses for.
- **Hard-disk loading:** Installing and selling unauthorized copies of software on refurbished or new computers.
- **Counterfeiting:** Duplicating and selling software having copyright.
- **Online piracy:** Typically involves downloading illegal software.

The software industry is prepared to battle against software piracy. The courts are dealing with an increasing number of lawsuits concerning the protection of software.

- **Fraud & Misuse**

Using computers over the Internet, some unauthorized activities can take place. Some of these include theft of money by electronic means, theft of services, and theft of valuable data. Sometimes, we receive an email asking us to click on a link to change our password. When we click on the link, a webpage opens asking us to give our username and password. If we give our username and password, actually our password is stolen by some malicious user.

Figure 4-2

Likewise, some emails try to fool us by stating that we have won a grand prize e.g. a car or a house. They ask us to pay a small amount as transfer fee to get that prize. Actually, it is just a way to fool people and get money from them.

Sometimes, some malicious user disguises himself as our friend and tries to get some confidential information. This is called **phishing**.

Figure 4-3

- **Patent**

  Patent is a way to protect an idea. If you are doing research in some field and you have an idea, then you must get patent for that idea. It gives you the right to exclude others from making or selling an invention using your idea.

  Example: If you are doing research in medical field and give a new idea to treat a particular disease, some pharmaceutical companies can make medicines on the basis of your idea. Ethically, they must seek your permission before making medicines using your idea. They should also pay a certain amount upon sale of the medicine. For this purpose, you must get a patent.

- **Copyright Law**

  Copyright is different from a patent as copyright law says that some idea or product cannot be copied. The rights are reserved for copying. Usually, if a product is copyright protected then we see a symbol of copyright as shown in Figure 4.4. For example, the book you are reading is copyright protected. So, making its photocopy is illegal.

  Figure 4-4 Copyright symbol

  Similarly, software products are mostly copyright protected. It means that we cannot copy them, like, MS Windows, MS Office etc. Copyright can deal with misappropriation of data, computer programs, documentation, or similar material.

- **Trade Secrets**

  Trade secrets are usually the secrets that are playing an important role for the success of a company. They have a lot of value and usefulness for the company. Keeping trade secrets in the computer science field is very important when more than one software companies develop the same product but one of them takes lead. For example, there are many free email services but few of them have significant competitive advantage over others.

- **Sabotage**

  Sabotage is a serious attack on a computer system. Some malicious user can attack the system while sitting remotely. One can send virus with some free software. A virus is a computer program written with negative intentions. It can change/destroy an information or sabotage a precious data.

4.1.2 Safeguarding Privacy of Others

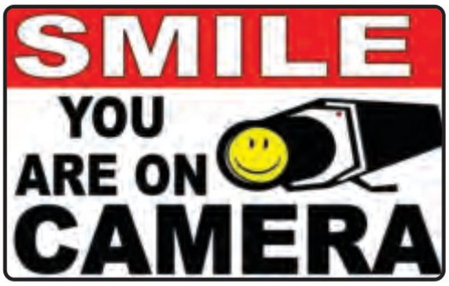


Figure 4-5

Did you notice the boards on roads about cameras watching you as shown in Figure 4-5? The purpose of such notices is to alarm you about your privacy and keep you within certain rules and regulations. Similarly, speed cameras are announced before taking your picture or recording your video. These steps are just to safeguard your privacy. In the same way, when you give information to an organisation, it is the duty of that organisation to safeguard your privacy. Your information is stored in NADRA (National Database and Registration Authority) along with information of your other family members. So, safeguarding this data is an ethical responsibility of NADRA.

Do you know?

CCTV stands for Closed-Circuit Television.

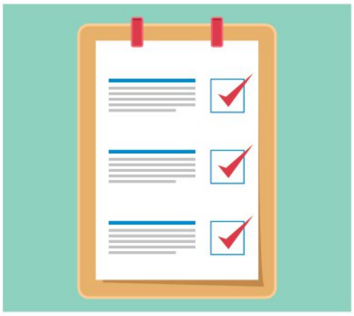


Figure 4-6

Most of the websites also declare their privacy policies (Figure 4-6), indicating what information they collect from you and your computer, and with whom they will share it. People usually do not read these policies. Most users mistakenly assume that their privacy is fully protected due to the privacy policy.

Actually, the website wants to inform you that how far they will go to safeguard your privacy.

4.2 Importance of Data Privacy

4.2.1 Privacy Concerns that Arise Through the Mass Collection of Data

Many organizations are keeping our data due to the computerized systems in-place. There can be more people/organizations having information about you than you think. For example:

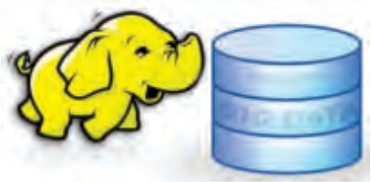


Figure 4-7

- A hospital may have your birth record,
- NADRA has your family information,
- Your school has your record,
- BISE (Board of Intermediate and Secondary Education),
- Passport office if you have a passport,
- Email service providers if you have email accounts,
- Online social networking websites etc.

There are companies interested in a lot more than just your name, address and other basic facts about your life. They want to know where you have travelled, what type of clothes you wear, how often you have been sick, if you buy a product then do you buy something else with that product or not and much more. Answers of these questions help them in decision making.

Example: If you buy a packet of potato crisps, then you usually buy a drink as well. This information is useful for a shopping mall to increase its sales if it introduces new offers on both potato crisps and drinks.

So, a piece of information can flow from one place to another without any intimation. It is due to mass collection of data.

Figure 4-8

Do you know?

There are certain companies, called data brokers, that solely exist to collect, aggregate, buy and sell consumer information.

4.2.2 Analysing the Personal Privacy and Security Concerns that Arise with any use of Computational Systems

With the advent of Internet, our computers are no longer stand-alone devices. In fact, now they are connected to millions of other computers in the world. Due to this connectivity, many security concerns also arise. Primarily, we want to secure our data according to the following three aspects.

1- **Confidentiality:** It means that we want to keep our data as confidential. We do not want to share it with unintended persons.

2- **Integrity:** It means that we want to keep the data correct. For example, we do not want that the website of our bank shows less account balance than it actually is.

3- **Availability:** It means that we want to have access to the data when we want. If data is not available when needed, then in some cases it becomes useless.

All these aspects are important during the processing, storage and transmission of data in a computerized system.

Computation is a general term for any type of information processing that can be represented mathematically. For example, your grade in 9th class will be computed according to your marks in every subject.

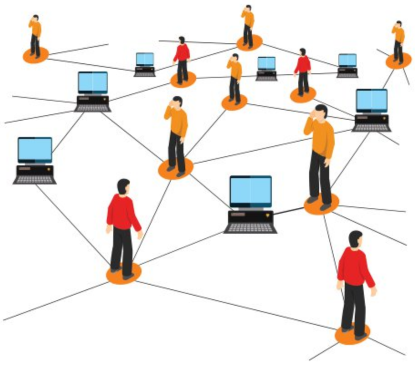


Figure 4-9

In everyone’s life there is stunning growth of usage of computational systems. This fact is behind raising concerns about privacy.

When we surf the Internet, personal information is generated that may be of interest to businesses or people with malevolent aims. Companies want to read minds of Web surfers and sometimes they store some piece of information with the Web surfer, called cookies.

Using "cookies," companies are able to track purchases and gather personal data. They can use this information to target their marketing. It can be considered an invasion of their privacy.

4.3 Simple Encryption

Encryption is the process of encoding data in such a way that only authorised person can read it. Encoding means conversion of the data to an unreadable format which is called ciphertext. A secret code (called Key) is required to read the data as shown in Figure 4-10. A key is just like a password.

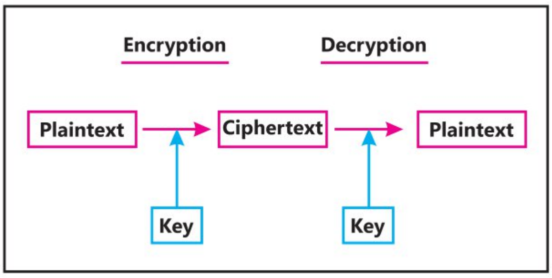


Figure 4-10 **Encryption - Decryption Process**

In ancient times when messages were carried by foot for miles, kings and rulers used to encrypt the letters they would send to allies. This helped to protect the secrecy of the message in case they were stolen.

A computer expert who can steal data when it moves from one location to other, is called hacker. Encryption helps us to save data from hackers.

Activity 4.1

You can devise a technique to encrypt a text. Like you can write letters of each word in reverse order. For example, the text "I like my school" becomes "I ekil ym loohcs". Another way is to put next letter in place of each letter, i.e., 'a' become 'b', 'b' becomes 'c' and 'z' becomes 'a'. So, in this way, "I like my school" becomes "J mjlf nz tdippm". Using your own technique encrypt the names of cities in Pakistan and give the key to your friends to identify those names.

Activity 4.2

If you hold up a script to a mirror, the writing looks reversed. You can easily write notes and other things to look like mirror writing. Get a sheet of thin white or light coloured paper. With a dark marker, write something on one side. Make sure you write it thick and dark enough so that it will show through the other side. Flip over the paper and trace what you wrote. You'll be tracing it backwards. It should come out like how you would see your regular writing if you were to hold it up to a mirror. For fun, write down different words, or write a note to someone, then reverse it and send it to them.

4.3.1 Importance of Encryption for Everyday Life on the Internet

Encryption is one of the most important methods for providing data security. In everyday life on the Internet, vast amounts of personal information are stored on multiple places. So, it is important to know how to keep data private. Encryption is important because it allows you to secure data from illegal access. Importance of encryption can be described in the following three points.

Figure 4-11

1. **Protection from Hackers**

   Hackers don’t just steal information; they can also alter the data to commit fraud. For example, in a bank transaction of online money transfer, they can fraud by changing the target account number.

2. **Encryption Protects Privacy**

   Encryption is used to protect sensitive data, including personal information for individuals. This helps to ensure privacy and minimising the opportunities for surveillance by criminals.

Figure 4-12

3. **Encryption Protects Data across Devices**
   Multiple (and mobile) devices are a big part of our lives, and transferring data from device to device is a risky proposition. Encryption technology can help protect stored data across all devices, even during transfer. Additional security measures like advanced authentication help deter unauthorized users.

4.3.2 Substitution Cipher Methods

Substitution Cipher methods are the methods of encryption in which the characters of original text are replaced by some other characters. This substitution is done by a fixed predefined system. In the following we discuss two commonly used substitution ciphers.

4.3.2.1 Caesar Cipher

Caesar was a Roman politician and military general who played a critical role in the rise of the Roman Empire. Caesar used this method of encryption for sending messages to his soldiers and generals. This is the reason for calling this method as Caesar Cipher. In this method, we replace each alphabet in the plaintext by another alphabet. The replacing alphabet is some fixed number of steps to the left or right of original alphabet in the sequence of alphabets.

Example 1: A three-character substitution to the right results in the following transformation of the standard English alphabet:

Initial alphabets:	ABCDEFGHIJKLMNOPQRSTUVWXYZ
Encryption alphabets:	DEFGHIJKLMNOPQRSTUVWXYZABC

Within this substitution scheme, the plaintext PAKISTAN would be encrypted into the ciphertext SDNLVWDQ.

Example 2: A five-character substitution to the right results in the following transformation of the standard English alphabet:

Initial alphabets:	ABCDEFGHIJKLMNOPQRSTUVWXYZ
Encryption alphabets:	FGHIJKLMNOPQRSTUVWXYZABCDE

Within this substitution scheme, the plaintext PAKISTAN would be encrypted into the ciphertext UFPNXYFS.

Activity 4.3

Use a three-character substitution to the left for encrypting the plaintext PAKISTAN into ciphertext.

4.3.2.2 Vigenere Cipher

Vigenere cipher is another substitution cipher, which uses a table known as Vigenere Cipher table for substituting the letters of plaintext.

Vigenere Cipher Table: The table is shown in Table 4-1. The table consists of 26 rows and 26 columns, where the 1^{st} row contains the original alphabets from A – Z. In each subsequent row the alphabet is shifted by one letter to the right. All the columns are labeled by alphabets from A – Z, and all the rows are also labeled by alphabets from A – 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	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

Table 4-1

Vigenere Cipher Method: In this method, we have a substitution key that is combined with the plaintext to generate the ciphertext. We encrypt each letter of the plaintext by finding that letter in column labels of the Vigenere table (Table 4-1) and in that column, we find a letter that is in front of the row label for the respective letter of the key. We continue this process until all the text is finished.

Example: Let's assume that we want to encrypt "PAKISTAN" with the help of substitution key "ZINDABAD". We find 'P' (first letter of plaintext) in column labels and 'Z' (first letter of substitution key) in row labels. We can observe that the row and the column meet at letter 'O' as marked with yellow colour in Table 4-1. So, the letter 'P' is converted to 'O'. Similarly, we find the letter 'A' in column labels which is the first column (marked with green colour) in Table 4-1. and we find the letter 'I' in the row labels. Row and the column meet at the letter 'I'. So, 'A' is replaced with 'I'.

In this way the word "PAKISTAN" is converted to cypher text "OIXLSUAQ" as shown in Table 4-2.

Column Label	P	A	K	I	S	T	A	N
Row Label	Z	I	N	D	A	B	A	D
Common Letter	O	I	X	L	S	U	A	Q

Table 4-2

Important Note: If the key has less number of letters, then we repeat the letters of that key from beginning. For example, to encrypt the text "PAKISTAN" having 8 letters with the key "BEAUTY" having 6 letters, we repeat the letters of the key to make them equal in length to the given plaintext. So, the key becomes "BEAUTYBE" having same number of letters and this key is called ***interim ciphertext***.

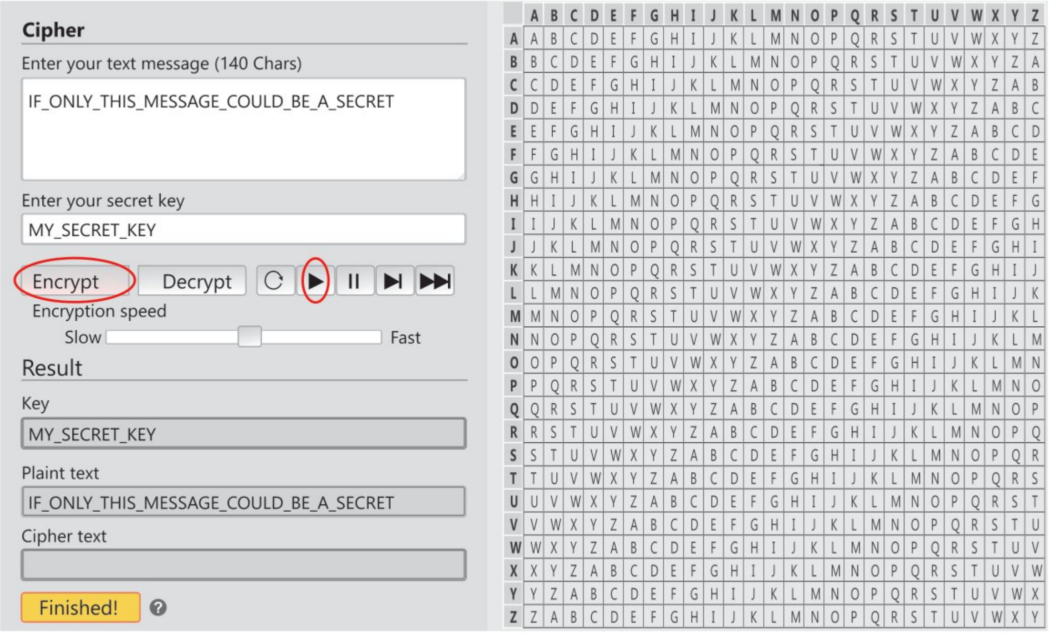
Activity 4.4

Prepare a chart for the sports you likes the most. In the chart, write names of your favourite players in plaintext as well as in ciphertext. You can use some key of your own choice.

4.3.3 Using Vigenere Cipher Widget

There is a widget available at the website:
https://studio.code.org/s/vigenere/stage/1/puzzle/1

It is called Vigenere Cipher Encryption Widget. It shows animation of the encryption and decryption of plaintext by using Vigenere Cipher method according to a given key. Screenshot of this widget is shown in Figure 4-13. You can type text on upper left corner and provide a key for encryption. Press the "Encrypt" button and then click on ▶ to see the animation of encryption. Both the buttons are marked with red circles in Figure 4-13. Similarly, we can decrypt a ciphertext to see the original message.



Cipher

Enter your text message (140 Chars)

IF_ONLY_THIS_MESSAGE_COULD_BE_A_SECRET

Enter your secret key

MY_SECRET_KEY

Encryption speed

Slow Fast

Result

Key

MY_SECRET_KEY

Plaint text

IF_ONLY_THIS_MESSAGE_COULD_BE_A_SECRET

Cipher text

	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

Figure 4-13 vigenere cipher widget

- **Practical to Decrypt a message**

  To decrypt a message, we find the letters of key in the rows of Vigenere table and then in that row we locate the letter of encrypted text. When the letter is found we take the column heading for that letter as decrypted letter. For example, to decrypt "OIXLSUAQ" with key "ZINDABAD" we find the row for the letter 'Z' and in that rows we find the letter 'O' where we can identify the column heading, i.e., 'P' in this case. Similarly, we continue with each letter of the cypher text and decrypt the cypher text.

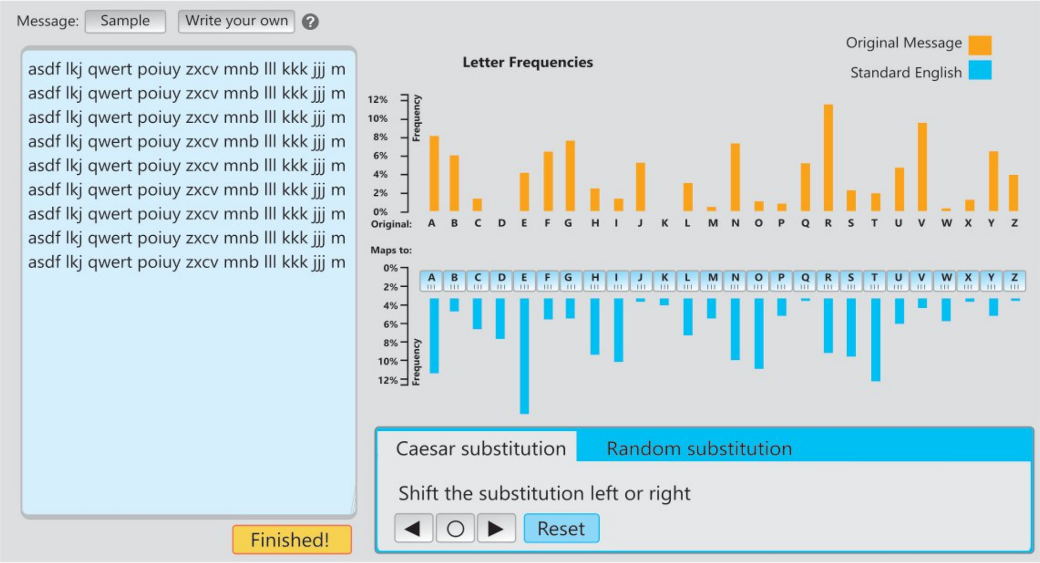
Do you know?

Gaius Julius Caesar was born in July 13, 100 BC, Rome, Italy and was assassinated on March 15, 44 BC. His famous quotes are:

1) Experience is the teacher of all things.
2) Men freely believe that which they desire

4.3.4 Encrypted with Random Substitution using Frequency Analysis

Messages encrypted with the Caesar cipher are very easy to crack. What if instead of shifting the whole alphabet, we map every letter of the alphabet to a random different letter of the alphabet? This is called a random substitution cipher.



asdf lkj qwert poiuy zxcv mnb lll kkk jjj m
asdf lkj qwert poiuy zxcv mnb lll kkk jjj m
asdf lkj qwert poiuy zxcv mnb lll kkk jjj m
asdf lkj qwert poiuy zxcv mnb lll kkk jjj m
asdf lkj qwert poiuy zxcv mnb lll kkk jjj m
asdf lkj qwert poiuy zxcv mnb lll kkk jjj m
asdf lkj qwert poiuy zxcv mnb lll kkk jjj m
asdf lkj qwert poiuy zxcv mnb lll kkk jjj m
asdf lkj qwert poiuy zxcv mnb lll kkk jjj m

Shift the substitution left or right

Figure 4-14 Random Substitution using Frequency Analysis Widget

We can visit the website:

https://studio.code.org/s/frequency_analysis/stage/1/puzzle/1 to view the widget for this purpose. It's screenshot is shown in Figure 4-14.

In this version of the tool, you'll be interacting more with the graphs that show letter frequency.

Activity 4.5

Load the Sample message (hard) from the message dropdown. This will load a message that has been encrypted with a random substitution cipher.

You will crack the message by guessing what each letter of the alphabet contained in the original ciphertext should be changed to. You can do so by dragging the blue letters of the alphabet directly underneath the orange letter you want to change in the original ciphertext. Letters that have been changed using your guesses will no longer be highlighted orange in the message window on the left.

Play with some of the sorting options available in the Random substitution cipher tab to get different views on the letter frequencies in the input text as well as standard English text.

Do you know?

'E' is the most common letter used in the English language?

May be the most common letter in your encrypted text maps to the letter 'E', but may be not! You'll have to do a bit of guess and check to see if that substitution makes sense.

In cryptanalysis, frequency analysis is the study of the frequency of letters or groups of letters in a ciphertext. The method is used as an aid to breaking classical ciphers.

4.3.5 Weaknesses and Security Flaws of Substitution Ciphers

- The simplest of all substitution ciphers are those in which the cipher alphabet is merely a cyclical shift of the plaintext alphabet. The explanation for this weakness is that the frequency distributions of symbols in the plaintext and in the ciphertext are identical, only the symbols having been relabelled
- Another major problem with simple substitution ciphers is that the frequencies of letters are not masked at all.

4.4 Encryption with Keys and Passwords

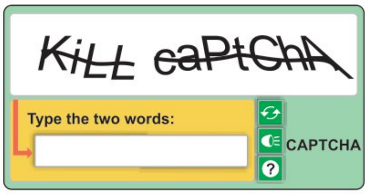
4.4.1 Relationship between Cryptographic Keys and Passwords

Passwords are used for authentication to enter a system whereas cryptographic keys are used to read an encrypted message. So, with respect to computer security a "key" is not synonymous with "password". It is also possible that a password can be used as a key. The basic difference between these two is that a password is generated, read, remembered, and reproduced for a human use while a key is used by the software or human to process a message by using that key and the cryptographic algorithm.

Figure 4-15

Do you know Captcha?

We can write a program that can access a website and give it a password. It can be used to hack a password if the program keeps trying different password for long time. Moreover, a program can also add unnecessary data by filling a form again and again. To avoid this situation only humans are allowed to use a system instead of a computer program. So, a picture is shown on a website whenever there is a form and you are asked to read that image and fill a field. The image contains text in irregular form which is readable for human but not easily for a machine.



Some server computers store key on our computers when we access them first time. For later use, the same key is used on our behalf but without any action from our side.

4.4.2 Characteristics of a Good Password

A good password should be difficult to guess or crack. It helps to prevent unauthorized people from accessing files, programs, and other resources. A good password:

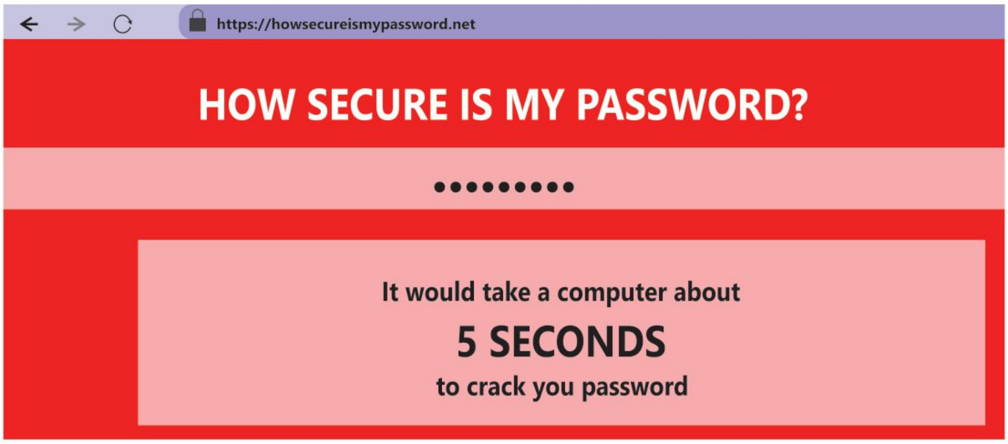
- is at least eight characters long
- doesn't contain your user name, real name, kid’s name or company name
- doesn't contain a complete word
- is significantly different from previous passwords
- contains uppercase letters, lowercase letters, numbers, and symbols

Activity 4.6

All students go to computer laboratory and access the following website:

https://howsecureismypassword.net/

Notice the time a computer can find your password. Screenshot of this utility is shown in Figure. Class teacher can point out some other same type of utilities.



https://howsecureismypassword.net

HOW SECURE IS MY PASSWORD?

●●●●●●●●●

It would take a computer about

5 SECONDS

to crack you password

4.5 Cybercrime

The Internet is an amazing tool for communication, allowing users to connect instantly over great distances. Unfortunately, the same communication is also a great tool for criminals. A crime in which computer network or devices are used is called a cybercrime. For example:

- **Identity Theft**

  One common form of cybercrime is identity theft. Hackers may use fake emails to trap someone to give passwords and account information.

- **Transaction Fraud**

  Simple financial fraud is another common crime in the online arena. A scammer may offer an item for sale through an auction site with no intention of delivering once he/she receives payment. Alternatively, a criminal might purchase an item for sale using a stolen credit card. It is also possible

Figure 4-16

to buy something from own credit card but then reporting the card stolen. This is a transactional fraud if the cardholder claims chargeback.

- **Advance Fee Fraud**

  Sometimes the hackers congratulate you upon winning a big prize and ask you pay a small amount in advance, so that the prize can be dispatched. This is a common type of cybercrime. The lure of easy wealth has found many victims of these frauds.

- **Hacking**

  Another cybercrime is the practice of hacking, illegally accessing someone else's computer. This happens mostly when you download some file from internet and execute it without knowing details. A software installed in your computer connects someone else to your computer without your permission. The aim is to gather information about a person or organization sometimes without their knowledge. This type of software is called spyware as shown in Figure 4-17.

Figure 4-17

- **Piracy**

  Piracy is also a type of a cybercrime. Details about piracy already discussed in Section 4.1.1.

Do you know?

National Response Centre for Cyber Crime (NR3C) is a law enforcement agency of Pakistan dedicated to fight cybercrime. It is working under FIA (Federal Investigation Agency) and its website is available at http://www.nr3c.gov.pk. (Screenshot in Figure)

Not secure | www.nr3c.gov.pk
FEDERAL INVESTIGATION AGENCY
NATIONAL RESPONSE CENTRE FOR CYBER CRIME
HOME ABOUT US SERVICES CYBER CRIME REPORT CYBER CRIME FAQ CONTACT US
CYBER SCOUTS
DEVOTED VOLUNTEERS TO HELP PAKISTAN FIGHT TECHNOLOGY DRIVEN CRIME
CYBER SCOUT

Activity 4.7

Find the categories of cybercrime at http://www.nr3c.gov.pk and make notes about each. Teacher can make groups of students and ask each group to make chart on each category.

4.5.1 Characteristics of a Phishing Attack

Phishing is the fraudulent attempt by sending emails to obtain sensitive information such as usernames, password and credit card details.

Figure 4-18

- **Characteristics of Phishing Emails**

1. It normally appears as an important notice, urgent update or alert. The subject of such email is set in a way that the email recipient believes that the email has come from a trusted source.

   Examples:

   a. "Someone tried to open your account. Change your password Immediately"

   b. Official Data Breach Notification

   c. Packet Delivery at your Home Address

   d. IT Reminder: Your Password Expires in Less Than 24 Hours

   e. Change of Password Required Immediately

   f. Revised Vacation & Sick Time Policy

   g. Email Account Updates

2. It sometimes contains messages that sound attractive rather than threatening e.g. promising the recipients a prize or a reward.

3. It normally uses forged sender's address. For example, admin@facebook.com, info@gmail.com etc. You can also open an

email if it is from principal@yourschool.edu.pk. In email there can be some link that has no relation with your school. So, while filling online forms, take care of the URL (Uniform Resource Locator) appearing in the address bar of the web browser.

4. It usually takes contents such as logos, images from the actual website to make the fraudulent email look like a genuine email.
5. It may contain a form for the recipient to fill in personal/financial information and let recipient submit it. This information is submitted to a different database.

- **Characteristics of a Phishing Website**
  1. It looks like original due to same contents such as images, texts, logos, colour scheme etc.
  2. It may contain actual links to web contents of the legitimate website such as contact us, privacy or disclaimer to trick the visitors.
  3. It may use similar name as that of the actual website.
  4. It may use forms to collect visitors' information where these forms are similar to those in the legitimate website.

4.5.1 DoS (Denial of Service) Attack

In computing, a denial-of-service attack (DoS attack) is a cyber-attack to make a machine or network resource unavailable. It means a service is denied. For example, if you want to visit a website but someone else is already sending too many requests to the same website using computer programs, then you may not be able to access that website. This type of attack is shown in Figure 4-19. It is just like a robot is sending many requests in small amount of time, but for a user, either the service becomes very slow or it is denied. So, by flooding the targeted machine or resource with superfluous requests is an attempt to overload the system. It may also cause shutting down a machine or network.

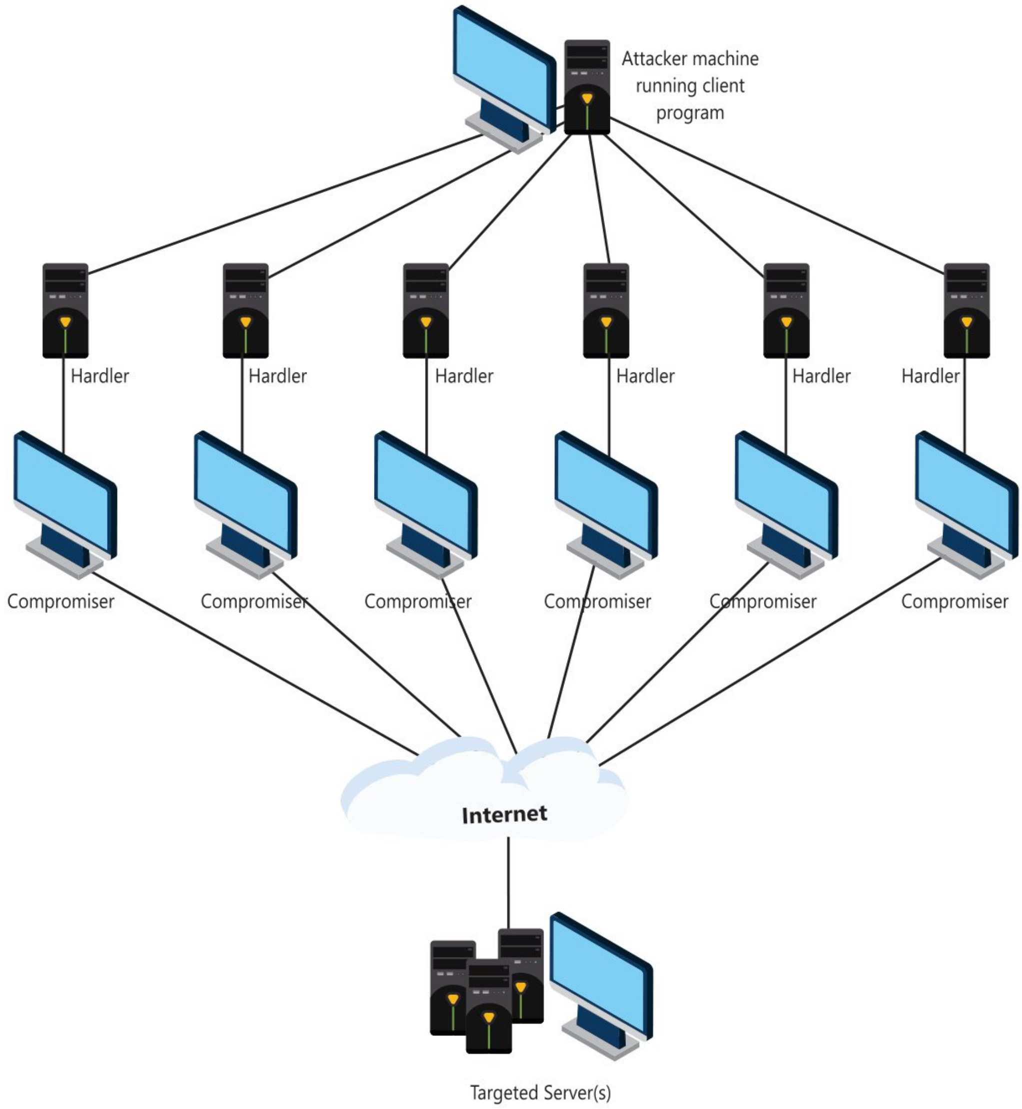


Figure 4-19 Dos Attack

DoS attackers often target web servers of high-profile organizations such as banking, commerce, and media companies, or government and trade organizations. Though DoS attacks do not typically result in the theft or loss of significant information or other assets, they can cost the victim a great deal of time and money.

SUMMARY

- We need to be careful by sending data over the internet.
- Every organization to whom the data is entrusted, it is their responsibility regarding confidentiality and privacy of the data.
- Piracy means making illegal and unauthorized copies of the software without owner's permission.
- Softlifting is called borrowing and installing a copy of a software application from a colleague.
- Client-server overuse is installing more copies of the software than you have licenses for.
- Hard-disk loading means installing and selling unauthorized copies of software on refurbished or new computers.
- Counterfeiting is called duplicating and selling copyrighted programs.
- Using computer for the purpose of some unauthorized activities is called fraud or misuse.
- Promises made by a software developer is known as warranty or liability.
- Patent can protect an idea so that it won't be misuse and the owner will attain its full rights.
- To protect value and usefulness we may imply trade secrets.
- The computer can be attacked while sitting remotely, in this way sensitive information will be sabotaged.
- Encoding means conversion of the data to an unreadable format which is called ciphertext. Key is needed to read it.
- Passwords are used for authentication to enter a system.
- A crime in which computer network or devices are used is called a cybercrime.
- Illegally accessing someone else's computer is called hacking.
- Denial-of-Service attack (DoS attack) is a cyber-attack to make a machine or network resource unavailable for a user.

EXERCISE

4-1 Choose the correct option.

1. Which of the following doesn't includes the types of software piracy?

(i) Softlifiting (ii) Liability

(iii) Client server overuse (iii) Online piracy

2. Which of the following is not a cybercrime?

(i) Hacking (ii) Phishing crime

(iii) Identity Theft (iv) Decryption

3. Which of the following is not the characteristics of phishing emails?

(i) Official data breach notification

(ii) Email account update

(iii) IT reminder

(iv) Similar domain of actual website

4. Which of the following is not characteristics of phishing website?

(i) Similar domain of actual website

(ii) Using of forms to collect visitors

(iii) Actual link to web content

(iv) Email account updates

5. Which of the following is not a characteristics of good password?

(i) Is eight characters long

(ii) Doesn't contains username

(iii) Contains uppercase letters

(iv) Password is your name only

4-2 Fill in the blanks:

1. Making illegal copies of software is called ____________.

2. ____________ is a general term for any type of information processing that can be represented mathematically.

3. ____________ is the process of encoding data.
4. When a key has less number of character than the text to encrypt, then repeating letters of the key is called ___________.
5. ____________ is a cyber attack to make machine or network resource unavailable for a user.

4-3 Answer the following questions.

1. Define cypher text.
2. Why do we need an installation key whereas a software can be protected with a password?
3. Define Denial of Service.
4. Give a reason to add captcha on websites.
5. What is Patent, and why do we need to register it?

Activity 4.8

Teacher will divide a class in groups and each group has maximum 4 students. Student will make a key having maximum 5 letters and write 4 words in cypher text with respect to that key. Each encrypted text has at most 10 letters. Teacher will collect these papers from students and divide them randomly to groups and they will be asked to decrypt. The winner will be the group which decrypts the text first.