CH # 4 DATA AND PRIVACY

Topic No.	Title	Page No.
4.1	**Ethical Issues Related to Security** • Understanding Ethical Issues Related to Data security • Safeguarding Privacy of Others	110
4.2	**Importance of Data Privacy** • Privacy Concerns that Arise Through the Mass Collection of Data • Analysing the Personal Privacy and Security Concerns that Arise with any use of Computational System	118
4.3	**Simple Encryption** • Importance of Encryption for Everyday Life on the Internet • Substitution Cipher Methods • Using Vigenere Cipher Widget • Encrypted with Random Substitution using Frequency Analysis • Weaknesses and Security Flaws of Substitution Ciphers	122
4.4	**Encryption with Keys and Passwords** • Relationship between Cryptographic Keys and Passwords • Characteristics of a Good Password	129
4.5	**Cybercrime** • Characteristics of Phishing Attack • DoS (Denial of Service) Attack	130
*	**Exercise** • Choose the Correct Option (MCQs) • Fill in the Blanks • Short Questions	137

4.1 ETHICAL ISSUES RELATED TO SECURITY

LONG QUESTIONS

Q.1 Define data privacy. Explain some of the data security issues. (K.B+U.B)

Ans:

DATA PRIVACY

Definition:

"Protecting data from malicious users is called data privacy or information privacy."

Data Security issues:

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 and Privacy
- Piracy
- Fraud and Misuse
- Patent
- Copyright
- Trade secrets
- Sabotage

Confidentiality and Privacy:

Keeping privacy and confidentiality has become difficult in this era of computers and Internet.

Data Collection:

Due to more usage of computers, a wide range of data is collected and stored. This data may be related to credit cards, driving licenses etc. If a company sells personal data to others, it breaches the confidentiality of data.

Examples:

If a bank shares the information about someone's banking transactions with its business competitors, then it can harm the business.

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.

Software Piracy:

Software piracy is the illegal copying, distribution or usage of software.

Types of Piracy:

Types of software piracy include:

- Softlifting
- Client-server overuse
- Hard-disk loading
- Counterfeiting
- Online piracy

Fraud and Misuse:

Using computers over the Internet for the purpose of some unauthorized activities is called fraud and misuse. Some of these include theft of money by electronic means, theft of services, and theft of valuable data.

Example:

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.

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 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 and should also pay a certain amount.

Copyright Law:

Copyright law says that some idea or product cannot be copied. The rights are reserved for copying. Copyright can deal with misappropriation of data, computer programs, documentation or similar material. Usually, if a product is copyright protected then we see a symbol of copyright.

Fig: Copyright Symbol

Examples:

- The book you are reading is copyright protected. So, making its photocopy is illegal.
- Similarly, software products are mostly copyright protected. It means that we cannot copy them, like MS Windows, MS Office etc.

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.

Importance:

Keeping trade secrets in any field, like the computer science, is very important when more than one companies develop the same product but one of them takes lead.

Example:

There are many free email services but few of them have significant competitive advantage over others.

Sabotage:

Sabotage is the act of damaging something deliberately. 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.

Q.2 Write a detail note on: (K.B)

i) Confidentiality and Privacy ii) Fraud and Misuse

Ans:

CONFIDENTIALITY AND PRIVACY

Keeping privacy and confidentiality has become difficult in this era of computers and Internet.

Collection of Data:

Due to more usage of computers, a wide range of data is collected and stored. This data may be related to credit cards, organizational fund raising campaigns, opinion polls, shop at home services, driving licenses, arrest records and medical records.

Potential Threat:

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. To keep the data of others as confidential is indeed taking care of others

Examples:

- If a bank shares the information about my banking transactions with my business competitors then it can harm my business.
- Phone companies are supposed to keep the invoices and bills as confidential.

FRAUD AND MISUSE

Using computers over the Internet for the purpose of some unauthorized activities is called fraud and misuse. Some of these include theft of money by electronic means, theft of services, and theft of valuable data.

Examples:

- 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, 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.

Fig: Stealing Money and Valuable Data

Phishing:

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

Q.3 Define piracy. Write a detail note on piracy. **(K.B)**

Ans:

PIRACY

Definition:

‘Piracy means making illegal copies. It can be a copy of any work protected by copyright law.”

Example:

Piracy may include making copy of:

- Book
- Software
- Movie

- Poetry
- Painting
- House architecture etc.

Software Piracy:

Software piracy is the illegal copying, distribution or usage of software.

Types of Piracy:

Types of software piracy include:

- Softlifting
- Client-server overuse
- Hard-disk loading
- Counterfeiting
- Online piracy

Softlifting:

A type of piracy in which a legally licensed software is installed or copied in violation of its license agreement, called softlifting.

Example:

Borrowing and installing a copy of a software application from a colleague.

Client-server overuse:

Installing more copies of the software (in a network) than you have licenses for, is called client-server overuse.

Example:

This occurs when too many employees on a company network are using a copy of software than allowed.

Hard-disk loading:

Installing and selling unauthorized copies of software on refurbished or new computers.

Example:

You may have illegal copy of operating system on refurbished laptop.

Counterfeiting:

Counterfeiting is the duplicating and selling software having copyright. It looks like the original. It may have manual, logo and copyright symbol, resembling the genuine product.

Example:

Software that are available in the market at very low price, are mostly counterfeit software, such as MS Office.

Online Piracy:

Online piracy involves downloading illegal software. It is the fastest growing form of piracy.

Example:

Downloading the cracked copy of a copyright software from internet.

Q.4 Describe in detail safeguarding privacy of others personal information. (K.B)

Ans: **SAFEGUARDING PRIVACY**

Responsibility:

The organization, collecting the information of a person, is responsible for safeguarding the privacy.

Examples:

- 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.

- You may notice the boards on roads about cameras watching you. 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. This is just to safeguard your privacy.

CCTV Camera

SHORT QUESTIONS

Q.1 In which format data is transfer between source and destination? (U.B)

Ans: **DATA TRANSFER**

Data is converted to unreadable format (encrypted) before sending and again it is converted back to readable format (decrypted) when it reaches its destination.

Q.2 Define data privacy or information privacy. (K.B)

Ans: **DATA PRIVACY**

Definition:

"Protecting data from malicious users is called data privacy or information privacy."

Q.3 Point out some of the data security issues. (K.B+U.B)

Ans: **DATA SECURITY ISSUES**

Some of the data security issues are:

- Confidentiality and Privacy
- Piracy
- Fraud and Misuse
- Patent
- Copyright
- Trade secrets
- Sabotage

Q.4 Write about confidentiality and privacy issue related to data security. (K.B)

Ans: **CONFIDENTIALITY AND PRIVACY**

Keeping privacy and confidentiality of data is the responsibility of the persons or organization that collects and stores data. If a company sells personal data to others, it breaches the confidentiality of data.

Examples:

Phone companies are supposed to keep the invoices and bills as confidential.

Q.5 What are the potential threats to privacy? (K.B)

Ans: **POTENTIAL THREATS**

The potential threats to privacy include the improper use of computerized data.

Example:

If a company sells email IDs and phone numbers to another company for marketing purpose, it breaches the privacy of data.

Q.6 Define piracy. **(K.B)**

Ans:

PIRACY

Definition:

"Piracy means making illegal copies. It can be a copy of any work protected by copyright law."

Example:

Piracy may include making copy of:

- Book
- Software etc.

Q.7 What is meant by cracking the key? **(K.B)**

Ans:

CRACKING KEY

Some people start searching for the key (product key) of a software by using illegal means. This is called cracking the key.

Q.8 Write down the types of software piracy. **(K.B)**

Ans:

TYPES OF SOFTWARE PIRACY

Types of software piracy include:

- Softlifting
- Client-server overuse
- Hard-disk loading
- Counterfeiting
- Online piracy

Q.9 Differentiate between softlifting and counterfeiting. **(K.B+U.B)**

Ans:

DIFFERENTIATION

The differences between softlifting and counterfeiting are as followed:

Softlifting	Counterfeiting
• A type of piracy in which a legally licensed software is installed or copied in violation of its license agreement, called softlifting.	• Counterfeiting is the duplicating and selling software having copyright.
• Borrowing and installing a copy of a software application from a colleague.	• Software that are available in the market at very low price, are mostly counterfeit software, such as MS Office.

Q.10 What do you know by online piracy? **(K.B)**

Ans:

ONLINE PIRACY

Online piracy involves downloading illegal software. It is the fastest growing form of piracy.

Example:

Downloading the cracked copy of a copyright software from internet.

Q.11 What action is taken by software industry against software piracy? **(K.B)**

Ans:

ACTION AGAINST PIRACY

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.

Q.12 What is open source software? **(Do you know?) (K.B)**

Ans:

OPEN SOURCE SOFTWARE

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

Q.13 What is meant by fraud and misuse? (K.B)

Ans:

FRAUD AND MISUSE

Using computers over the Internet for the purpose of some unauthorized activities is called fraud and misuse.

Example:

Some emails try to fool us by stating that we have won a grand prize e.g. a car or a house. Actually, it is just a way to fool people and get money from them.

Q.14 What is patent and why do we need to register it? (Ex. Q-4.3 [5]) (K.B)

Ans:

PATENT

Patent is a way to protect an idea. This ensures that the idea won't be misused and the owner will attain its full rights.

Need of Registration:

Registering patent, gives you the right to exclude others from making or selling an invention using your idea.

Q.15 What should a company do, if it uses someone's idea? (U.B)

Ans:

USING SOMEONE'S IDEA

If someone gives a new idea, such as to treat a particular disease, some pharmaceutical companies can make medicines on the basis of this idea. Ethically, they must seek permission and should also pay a certain amount.

Q.16 Differentiate between patent and copyright. (U.B)

Ans:

DIFFERENTIATION

The differences between patent and copyright are as followed:

Patent	Copyright
• Patent is a way to protect an idea.	• Copyright law says that some idea or product cannot be copied.
• It gives you the right to exclude others from making or selling an invention using your idea.	• It can deal with misappropriation of data, computer programs, documentation or similar material.
• If someone gives a new idea, such as to treat a particular disease, no one can make medicines on the basis of this idea without your permission.	• Software like MS Window, MS Office etc are copyright protected, so one cannot make copy of them.

Q.17 Define a virus. (K.B)

Ans:

VIRUS

Definition:

"A virus is a computer program written with negative intentions. It can change / destroy an information or sabotage a precious data."

Example:

Klez is an example of a virus.

Q.18 Who is responsible for safeguarding the privacy? (K.B)

Ans:

SAFEGUARDING PRIVACY

The organization, collecting the information of a person, is responsible for safeguarding the privacy.

Examples:

Your information is stored in NADRA along with information of your other family members. So, safeguarding this data is an ethical responsibility of NADRA.

Q.19 NADRA stands for what? **(K.B)**

Ans: **NADRA**

NADRA stands for National Database and Registration Authority.

Q.20 Why privacy policies are declared by different websites? **(U.B)**

Ans: **WEBSITES POLICIES**

Most of the websites declare their privacy policies. Actually, the website wants to inform you that how far they will go to safeguard your privacy.

Q.21 What is meant by warranty or liability? **(Summary) (K.B)**

Ans: **WARRANTY OR LIABILITY**

Promises made by an organization, like software developer, to repair or replace the product with in specific period of time, is known as warranty or liability.

MULTIPLE CHOICE QUESTIONS

1. **Protecting data from malicious users is called:** **(K.B)**

   (A) Data privacy (B) Information privacy

   (C) Authenticating (D) Both A & B

2. **On which principles, the foundation of all security systems is formed?** **(U.B)**

   (A) Computer (B) Ethical (C) Mathematical (D) Non-ethical

3. **Which is related to security issue?** **(U.B)**

   (A) Piracy (B) Copyright (C) Trade secrets (D) All of these

4. **Keeping privacy and confidentiality has become _________ in this era of computers and Internet.** **(K.B)**

   (A) Easy (B) Simple (C) Difficult (D) None of these

5. **The potential threats to privacy include the ___________use of computerized data.** **(K.B)**

   (A) Improper (B) Proper (C) Correct (D) Exact

6. **Some software companies sell software with a confidential text, called:** **(K.B)**

   (A) Installation key (B) Product key (C) Password (D) Both A & B

7. **Types of piracy are:** **(K.B)**

   (A) 2 (B) 4 (C) 5 (D) 7

8. **Installing more copies of the software than you have licenses for, is called:** **(K.B)**

   (A) Client-server overuse (B) Counterfeiting

   (C) Online piracy (D) Softlifting

9. **Installing and selling unauthorized copies of software on refurbished or new computers is called:** **(K.B)**

   (A) Counterfeiting (B) Softlifting (C) Online piracy (D) Hard disk loading

10. **Fastest growing form of piracy is:** **(K.B)**

    A) Online piracy (B) Softlifting (C) Counterfeiting (D) Hard disk loading

11. **Using computers for the purpose of some unauthorized activities is called:** **(K.B)**

    (A) Piracy (B) Fraud & misuse (C) Patent (D) Sabotage

12. **Which law says that some idea or product cannot be copied?** **(U.B)**

    (A) Privacy (B) Patent (C) Copyright (D) Piracy

13. To protect value and usefulness, we may apply: (U.B)

(A) Sabotage (B) Piracy (C) Trade secrets (D) Copyright

14. It is a serious attack on a computer system. (K.B)

(A) Patent (B) Sabotage (C) Trade secrets (D) Piracy

15. For what CCTV stands? (K.B)

(A) Closed Circuit Television (B) Closed Circuit Telecom

(C) Closed Circuit Telethon (D) Closed Cut Television

16. Which policies indicate what information is collected from you and your computer, and with whom this information will be shared? (U.B)

(A) Copyright (B) Privacy (C) Ethical (D) Legal

4.2 IMPORTANCE OF DATA PRIVACY

LONG QUESTIONS

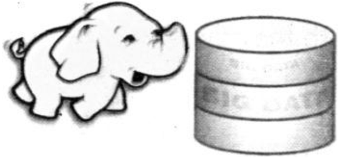
Q.1 What are the privacy concerns that arise through the mass collection of data? (K.B)

Ans:

PRIVACY CONCERNS

Many organizations are keeping our data due to the computerized systems in-place. Following concerns may arise due to mass collection of data:

- There can be more people/organizations having information about you than you think.
- A piece of information can flow from one place to another without any intimation.



Database

Organization Collecting Data:

Following are some organizations that keep personal data:

- 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

Reason for Keeping Data:

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.

Q.2 What are the security concerns that arise with any use of computational system? (K.B)

OR

Explain analyzing the personal privacy and security concerns that arise with any use of computational system.

Ans:

SECURITY CONCERNS

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.

Aspects to Secure Data:

Primarily, we want to secure our data according to the following three aspects:

- Confidentiality
- Integrity
- Availability

Confidentiality:

It means that we want to keep our data as confidential (private). We do not want to share it with unintended persons.

Examples:

If a bank shares the information about someone's banking transactions with its business competitors then it can harm the business.

Integrity:

Integrity refers to the accuracy and consistency of data. It means that we want to keep the data correct.

Example:

We do not want that the website of our bank shows less account balance than it actually is.

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.

Example:

If the ATM machine is out of order when we need money, then it becomes useless.

Importance:

All the security aspects are important in a computerized system during:

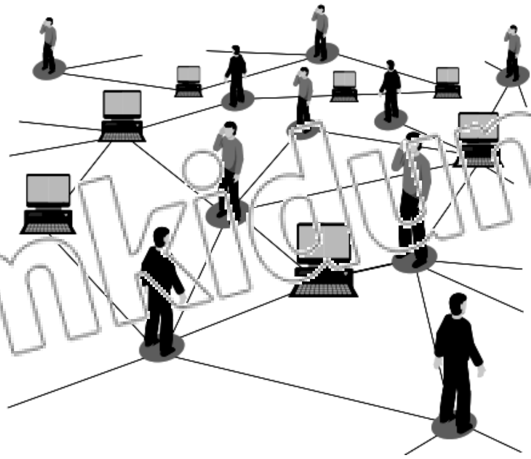
- Processing
- Storage
- Transmission of data

Computation:

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

Example:

Your grade in 9th class will be computed according to your marks in every subject.



Data Gathering

Fact Behind Privacy Concerns:

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

Companies Interest:

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.

Use of 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.

SHORT QUESTIONS

Q.1 What privacy concerns arise through the mass collection of data? (K.B)

Ans: **PRIVACEY CONCERNS**

Following concerns may arise due to mass collection of data:

- There can be more people/organizations having information about you than you think.
- A piece of information can flow from one place to another without any intimation.

Q.2 Write names of any four organization that keep our personal data. (K.B)

Ans: **NAMES OF ORGANIZATIONS**

Following are some organizations that keep personal data:

- NADRA
- Your school
- BISE (Board of Intermediate and Secondary Education)
- Online social networking websites

Q.3 How does data gathering help companies? Also write an example. (K.B)

OR

How data gathering is useful for companies? (U.B)

Ans: **DATA GATHERING**

Helpfulness:

Data gathering helps companies 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.

Q.4 What are brokers? (Do you know?) **(K.B)**

Ans:

BROKERS

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

Q.5 Why do security concerns arise due to the use of computational system? **(U.B)**

Ans:

SECURITY CONCERNS

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 arise.

Q.6 What is integrity? **(K.B)**

Ans:

INTEGRITY

Definition:

Integrity refers to the accuracy and consistency of data. It means that we want to keep the data correct.

Example:

We do not want that the website of our bank shows less account balance than it actually is.

Q.7 Where the security aspects are important? **(K.B)**

Ans:

IMPORTANCE OF SECURITY ASPECTS

All the security aspects are important in a computerized system during:

- Processing
- Storage
- Transmission of data

Q.8 Define computation. **(K.B)**

Ans:

COMPUTATION

Definition:

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

Example:

Your grade in 9th class will be computed according to your marks in every subject.

Q.9 What are cookies? **(K.B)**

Ans:

COOKIES

Definition:

"Cookies are small pieces of data sent from website and stored on the user's computer by web browser."

Usage:

They are used to record browsing activities such as webpage visited or remember information like items added in shopping cart, password etc.

Q.10 Why companies use cookies? **(U.B)**

Ans:

USE OF 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.

MULTIPLE CHOICE QUESTIONS

1. **Security concerns arise due to _________ collection of data.** **(K.B)**
   (A) Less (B) Mass (C) Valid (D) Improper

2. **With the advent of __________ our computers are no longer stand-alone devices.** **(U.B)**
   (A) Internet (B) Virtual reality (C) GPA (D) AI

3. **Primarily, we want to secure our data according __________ aspect(s).** **(K.B)**
   (A) 1 (B) 2 (C) 3 (D) 5

4. **Which of the following is not the aspect to secure our data?** **(U.B)**
   (A) Confidentiality (B) Integrity (C) Encryption (D) Both A & B

5. **It means that we want to have access to the data when we want.** **(K.B+U.B)**
   (A) Confidentiality (B) Availability (C) Integrity (D) Interdependency

6. **All aspects of data security are important during ________ of data.** **(K.B+U.B)**
   (A) Processing (B) Storage (C) Transmission (D) All of these

7. **Using ____________ companies are able to gather personal data.** **(K.B+U.B)**
   (A) Cookies (B) PCs (C) Viruses (D) None of these

4.3 SIMPLE ENCRYPTION

LONG QUESTIONS

Q.1 Explain encryption. Also write its importance for everyday life on the internet. **(K.B+U.B)**

Ans:

ENCRYPTION

Definition:

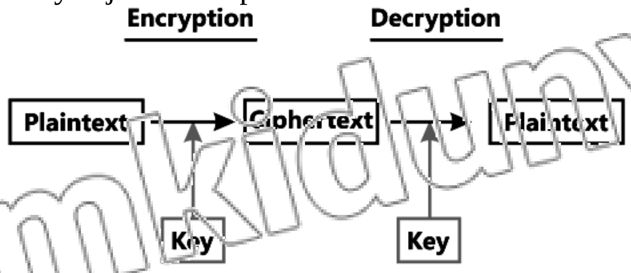
"Encryption is the process of encoding data in such a way that only authorized person can read it."

Encoding:

Encoding means conversion of the data to an unreadable format which is called ciphertext.

Secret Code / Key:

A secret code (called Key) is a set of characters, required to encrypt or to read the encrypted data. A key is just like a password.



Encryption – Decryption Process

Encryption in Ancient Time:

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.

Importance of Encryption on the Internet:

Encryption is one of the most important methods for providing data security from illegal access. In everyday life on the Internet, vast amounts of personal information are stored on multiple places. Importance of encryption can be described in the following three points:

Entering Personal Information

- Protection from Hackers
- Privacy Protection
- Data Protection across Devices

Protection from Hackers:

Encryption helps us to save data from hackers. Hackers don’t just steal information; they can also alter the data to commit fraud.

Example:

In a bank transaction of online money transfer, they can fraud by changing the target account number.

Privacy Protection:

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

Data Protection Across Devices:

Multiple devices (laptops and mobiles) are a big part of our lives, and transferring data from device to device is a risky proposition. Encryption can help to protect stored data across all devices, even during transfer.

Transferring Data

Q.2 Explain Caesar Cipher method with different examples. (K.B+U.B)

Ans:

CAESAR CIPHER

Definition:

“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.”

Reason For The Name:

Caesar was a Roman politician and military general. He 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.

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**.

Q.3 Write a detail note on Vigenere Cipher. (K.B+U.B)

Ans:

VIGENERE CIPHER

Definition:

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

Vigenere Cipher Table:

The table consists of 26 rows and 26 columns, where the first 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

Vigenere Cipher Table

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 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'. So, the letter 'P' is converted to 'O'. Similarly, we can encrypt the other letters.

In this way the word "**PAKISTAN**" is converted to cyphertext "**OIXLSUAQ**" as shown in table.

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

Interim Ciphertext:

If the key has less number of letters than plaintext, we repeat the letters of that key from beginning until it has same number of letters. This key is called **interim ciphertext.**

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.

SHORT QUESTIONS

Q.1 Define encryption. **(K.B)**

Ans: **ENCRYPTION**

Definition:

"Encryption is the process of encoding data in such a way that only authorized person can read it."

Q.2 Define ciphertext. **(Ex. Q-4.3 [1]) (K.B)**

Ans: **CIPHERTEXT**

Ciphertext (Cyphertext) is the result of encryption performed on plaintext using a method, called a Cipher. It is in unreadable form.

Q.3 Differentiate between plaintext and ciphertext. **(K.B+U.B)**

Ans: **DIFFERENTIATION**

Following are the differences between plaintext and ciphertext methods:

Plaintext	Ciphertext
• Unencrypted text is called plaintext.	• Encrypted text is called ciphertext.
• It is in readable form.	• It is in unreadable form.
• "PAKISTAN" is an example of plaintext.	• "SDNLVWDQ" is an example of ciphertext.

Q.4 Define Secret Code/Key in encryption. **(K.B)**

Ans: **SECRET CODE / KEY**

Definition:

"A secret code (called Key) is a set of characters, required to encrypt or to read the encrypted data."

Example:

Let's assume that we want to encrypt "PAKISTAN" with the help of substitution "ZINDABAD". Here "ZINDABAD" is the secret code or key.

Q.5 Define a hacker. **(K.B)**

Ans: **HACKER**

"A computer expert who can steal data when it moves from one location to other, is called a hacker."

Q.6 How the importance of encryption can be described? **(U.B)**

Ans: **IMPORTANCE OF ENCRYPTION**

Importance of encryption can be described in the following three points:

- Protection from Hackers
- Privacy Protection
- Data Protection across Devices

Q.7 How does encryption help to save data from hackers? **(U.B)**

Ans: **PROTECTION FROM HACKERS**

Hackers don't just steal information; they can also alter the data to commit fraud. Encryption converts data in unreadable format, in this way it helps us to save data from hackers.

Example:

In a bank transaction of online money transfer, they can fraud by changing the target account number.

Q.8 How can a system be protected from unauthorized user? **(U.B)**

Ans: **PROTECTION FROM UNAUTHORIZED USER**

Advanced authentications, like password, biometric means etc, help to prevent unauthorized users to access the system.

Q.9 Define Substitution Cipher methods. **(U.B)**

Ans: **SUBSTITUTION CIPHER METHODS**

Definition:

"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."

Q.10 Write commonly used Substitution Cipher methods. **(K.B)**

Ans: **TYPES OF SUBSTITUTION CIPHER**

Two commonly used Substitution Ciphers methods are:

- Caesar Cipher
- Vigenere Cipher

Q.11 Define Caesar Cipher. **(K.B)**

Ans: **CAESAR CIPHER**

Definition:

"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."

Q.12 Write the plaintext PAKISTAN into ciphertext using three-characters substitution to the left for encrypting in Caesar Cipher method. **(Activity 4.3) (A.B)**

Ans:

ENCRYPITNG WORD PAKISTAN

A three-character substitution in Caesar Cipher to the left results in the following transformation of the standard English alphabet:

Initial alphabets:	ABCDEFGHIJKLMNOPQRSTUVWXYZ
Encryption alphabets:	XYZABCDEFGHIJKLMNOPQRSTUVW

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

Q.13 Define Vigenere Cipher. **(K.B+U.B)**

Ans:

VIGENERE CIPHER

Definition:

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

Q.14 How text is encrypted in Vigenere Cipher method? **(U.B)**

OR

What is Vigenere Cipher method?

Ans:

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 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.

Q.15 What is interim ciphertext? **(K.B)**

Ans:

INTERIM CIPHERTEXT

If the key has less number of letters than plaintext, we repeat the letters of that key from beginning until it has same number of letters. This key is called **interim ciphertext**.

Q.16 What do you know about Gaius Julius Caesar? **(Do you know?) (K.B)**

Ans:

GAIUS JULIUS CAESAR

Gaius Julius Caesar was born in July 13, 100 BC, Rome, Italy. He was a military general and played a great role in the rise of Roman Empire. He was also a historian and author of Latin prose. He was assassinated on March 15, 44 BC.

Q.17 Write famous quotes of Gaius Julius Caesar? **(K.B)**

Ans:

FAMOUS QUOTES

The famous quotes of Gaius Julius Caesar are:

- Experience is the teacher of all things.
- Men freely believe that which they desire.

Q.18 Differentiate between Caesar Cipher and Random Substitution methods. **(K.B+U.B)**

Ans:

DIFFERENTIATION

Following are the differences between Caesar Cipher and Random Substitution methods:

Caesar Cipher	Random Substitution
• In Caesar Cipher each alphabet is replaced by another alphabet, shifting the whole alphabet to fixed number of step to left or right of original text.	• In Random Substitution every letter of the alphabet is mapped to a random different letter of the alphabet.
• It is easy to crack.	• It is difficult to crack.

Q.19 What is cryptanalysis? (K.B)

Ans:

CRYPTANALYSIS

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 break classical ciphers.

Example:

'E' is the most common letter used in English language, most of the time such properties of plaintext are preserved in the ciphertext.

Q.20 What are the weaknesses and security flaws of the Substitution Cipher? (K.B)

Ans:

WEAKNESSES OF SUBSTITUTION CIPHER

The weaknesses and security flaws of the Substitution Cipher are:

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

MULTIPLE CHOICE QUESTIONS

1. Encoding means conversion of the data to ___________ format. (K.B)
(A) Readable (B) Unreadable (C) Corrupted (D) All of these

2. Data in unreadable form is called: (K.B)
(A) Plaintext (B) Decoded text (C) Secret Code (D) Ciphertext

3. Decryption is the process of ___________ data. (K.B)
(A) Decoding (B) Encoding (C) Transmitting (D) Computing

4. Decoding means conversion of the data to ___________ format. (K.B)
(A) Corrupted (B) Unreadable (C) Readable (D) All of these

5. Data in readable form: (K.B)
(A) Plaintext (B) Ciphertext (C) Secret Code (D) Binary coded

6. It is one of the most important methods for providing data security. (K.B)
(A) Decryption (B) Encryption (C) Decoding (D) Password

7. Encryption helps to protect data: (K.B)
(A) From Hackers (B) Privacy (C) Across devices (D) All of these

8. Commonly used substitution ciphers is: (K.B)
(A) Caesar (B) Vigenere (C) Random (D) Both A & B

9. Gaius Julius Caesar was a _________ politician and military general. (K.B)
(A) German (B) Roman (C) Scottish (D) Britain

10. In Caesar Cipher the replacing alphabet is some fixed number of steps to the ________ of original alphabet in the sequence of alphabets. (K.B+U.B)
(A) Left (B) Right (C) Left or Right (D) Mid

11. Using One-character substitution to the left, the plaintext BINARY would be encrypted into: (A.B)
(A) CJOBSZ (B) AHMZQX (C) DKPCTA (D) ZGLYPW

12. In which method we have a substitution key to generate ciphertext? (K.B+U.B)
(A) Caesar Cipher (B) Random (C) Vigenere Cipher (D) All of these

13. In Vigenere cipher a substitution key is combined with the plaintext to generate: (K.B)
(A) Original text (B) Decoded text (C) ASCII text (D) Ciphertext

14. If the key has less number of letters than original text, then we repeat the letters of that key from: (U.B)

(A) Beginning (B) Mid (C) End (D) All of these

15. It shows animation of the encryption and decryption of plaintext by using Vigenere Cipher method. (U.B)

(A) Vigenere Cipher Key (B) Vigenere Cipher Table
(C) Vigenere Cipher Widget (D) None of these

16. Gaius Julius Caesar was born in: (K.B)

(A) July 13, 1000 BC (B) June 13, 100 BC (C) July 23, 100 BC (D) July 13, 100 BC

17. Caesar was assassinated on(K.B)

(A) July 15, 44 BC (B) March 15, 44 BC (C) August 14, 44 BC (D) March 15, 54 BC

18. Messages encrypted with the Caesar cipher are very _______ to crack. (K.B)

(A) Easy (B) Difficult (C) Hard (D) Challenging

19. The most common letter used in the English language is: (K.B)

(A) ‘E’ (B) ‘O’ (C) ‘M’ (D) ‘A’

20. In simple substitution cipher the frequency distributions of symbols in the plaintext and in the ciphertext are: (K.B)

(A) Different (B) Changed (C) Identical (D) All of these

4.4 ENCRYPTION WITH KEYS AND PASSWORDS

SHORT QUESTIONS

Q.1 What is the relationship between passwords and cryptographic keys?

OR

Differentiate between passwords and cryptographic keys. (U.B)

Ans: **RELATIONSHIP**

Following is the relationship between passwords and cryptographic keys:

Passwords	Cryptographic Keys
• Passwords are set of secret characters used for authentication to enter a system.	• Cryptographic keys are used to encrypt or to read an encrypted message.
• Password is generated, read, remembered, and reproduced for a human use.	• A key is used by the software or human to process a message by using that key and the cryptographic algorithm.

Q.2 What is Captcha? (K.B)

Ans: **CAPTCHA**

Captcha stands for Completely Automated Public Turing Test to Tell Computer and Humans Apart. It is used to check whether the user is a human or a machine.

Q.3 How does a password help? (U.B)

Ans: **PASSWORD**

A password helps to prevent unauthorized people from accessing:

- Files
- Programs
- Other resources

Q.4 What are the characteristics of a good password? (K.B)

Ans: **CHARACTERISTICS OF A PASSWORD**

A good password must contain the following characteristics:

- It should be difficult to guess or crack.

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

MULTIPLE CHOICE QUESTIONS

1. It is used for authentication to enter a system. (K.B)
(A) Password (B) Key (C) Captcha (D) Cryptographic key

2. It is possible that a password can be used as a: (K.B)
(A) Passcode (B) Captcha (C) Key (D) None of these

3 It is used on websites to check whether the user is a human or a machine. (U.B)
(A) Code (B) Captcha (C) Key (D) Password

4. A password helps to prevent unauthorized people from accessing: (K.B+U.B)
(A) Files (B) Programs (C) Other resources (D) All of these

4.5 CYBERCRIME

LONG QUESTIONS

Q.1 What is cybercrime? Explain different examples of cybercrime. (K.B+U.B)

Ans:

CYBERCRIME

Definition

"A crime in which computer network or devices are used is called a cybercrime."

Examples:

Some examples of cybercrime are:

- Identity Theft
- Transaction Fraud
- Advance Fee Fraud
- Hacking
- Piracy
- Phishing
- DoS Attack

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 a common crime in the online arena. Some examples of transaction fraud are:

- A scammer may offer an item for sale through an auction site with no intention of delivering, once he/she receives payment.
- A criminal might purchase an item for sale using a stolen credit card.

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.

Prize Offer Advertisement

Hacking:

An activity of accessing someone else's computer illegally, is called hacking. It is a practice of cybercrime. This happens mostly when you download some file from internet and execute it without knowing details.

Hacker Using Spyware

Piracy:

Piracy means making illegal and unauthorized copies of the software without owner's permission. Piracy is a type of a cybercrime.

Phishing:

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

DoS Attack:

DoS stands for Denial of Service. In computing, DoS attack is a cyber-attack to make a machine or network resource unavailable.

Q.2 Define phishing. Write down the characteristics of phishing emails and websites. (K.B)

Ans:

PHISHING

Definition

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

Characteristics of Phishing Emails:

Following are some characteristics of Phishing Emails:

- Appealing subject
- Attractive message
- Forged sender's address
- Contents of actual website
- Form for the recipient

Appealing Subject:

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:

- Change of Password Required Immediately
- Email Account Updates

Attractive Message:

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

Forged Sender's Address:

It normally uses forged sender's address.

Example:

Forged emails may look like:

- admin@facebook.com
- info@gmail.com etc.
- principal@yourschool.edu.pk

In such email there can be some link that has no relation with your school. So, while filling online forms, take care of the URL appearing in the address bar of the web browser.

Contents of Actual Website:

It usually takes contents such as logos, images from the actual website to make the fraudulent email look like a genuine email.

Form for the Recipient:

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:

Following are some characteristics of Phishing Website:

- Original look
- Links to legitimate website
- Similar name
- Use of forms

Original Look:

It looks like original due to same contents such as images, texts, logos, colour scheme etc.

Links to Legitimate Website:

It may contain actual links to web contents of the legitimate website such as contact us, privacy or disclaimer to trick the visitors.

Similar Name:

It may use similar name as that of the actual website.

Use of Forms:

It may use forms to collect visitors' information where these forms are similar to those in the legitimate website.

Q.3 Explain DoS attack with a diagram. **(K.B+U.B)**

Ans:

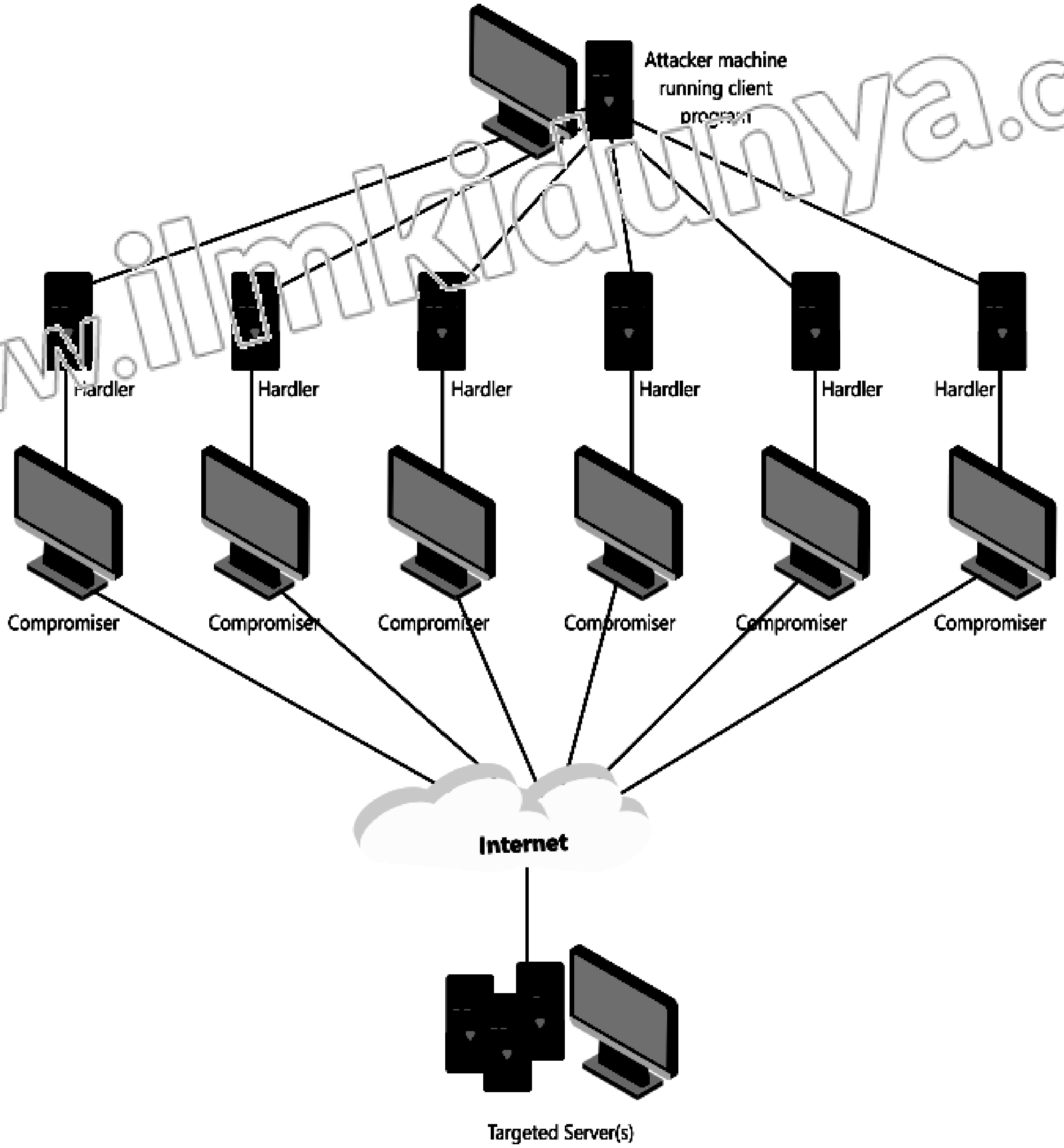
DoS ATTACK

Definition

"DoS stands for Denial of Service. In computing, DoS attack is a cyber-attack to make a machine or network resource unavailable."

Explanation:

It means a service is denied. 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.



Dos Attack

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.

DoS Attackers Target:

DoS attackers often target web servers of high-profile organizations such as:

- Banks
- Commerce companies
- Media companies
- Government organization
- Trade organizations

Loss by DoS Attacks:

DoS attacks do not typically result in the theft or loss of significant information or other assets, but they can cost the victim a great deal of time and money.

SHORT QUESTIONS

Q.1 What type of tool an Internet is? (K.B)

Ans: **INTERNET**

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.

Q.2 Define cybercrime (K.B)

Ans: **CYBERCRIME**

Definition

"A crime in which computer network or devices are used is called a cybercrime."

Examples:

- Identity Theft
- Transaction Fraud

Q.3 Write two examples of transaction fraud. (K.B+U.B)

Ans: **TRANSACTION FRAUD**

Simple financial fraud is a common crime in the online arena. Some examples of transaction fraud are:

- A criminal might purchase an item for sale using a stolen credit card.
- It is also possible to buy something from own credit card but then reporting the card stolen. This is a transactional fraud if the cardholder claims chargeback

Q.4 What is hacking? (K.B)

Ans: **HACKING**

An activity of accessing someone else's computer illegally, is called hacking. It is a practice of cybercrime. This happens mostly when you download some file from internet and execute it without knowing details.

Q.5 Define spyware. (K.B)

Ans: **SPYWARE**

Definition:

"A type of malware (malicious software) that aims to gather information, about a person or organization sometimes without their knowledge. This type of software is called spyware."

Example:

A software installed in your computer connects someone else to your computer without your permission.

Q.6 What is NR3C? (Do you know?) (K.B)

Ans: **NR3C**

NR3C stands for National Response Centre for Cyber Crime. It is a law enforcement agency of Pakistan dedicated to fight cybercrime. It is working under FIA (Federal Investigation Agency).

Website:

Its website is: http://www.nr3c.gov.pk.

Q.7 Define phishing. (K.B)

Ans: **PHISHING**

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

Q.8 Write down the some examples of appealing subjects in phishing emails. (K.B+U.B)

Ans: **APPEALING SUBJECTS**

Following are some examples of appealing subjects in phishing emails:

- Official Data Breach Notification
- Packet Delivery at your Home Address
- IT Reminder: Your Password Expires in Less Than 24 Hours
- Revised Vacation & Sick Time Policy
- Someone tried to open your account. Change your password immediately.

Q.9 Write down the characteristics of phishing website. (K.B+U.B)

Ans: **CHARACTERISTICS OF PHISHING WEBSITE**

Following are some of the characteristics of phishing website:

- Original look
- Links to legitimate website
- Similar name
- Use of forms

Q.10 Define Denial of Service. (Ex. Q-4.3 [3]) (K.B)

Ans: **DENIAL OF SERVICE**

Definition

"In computing, Denial of Service (DoS) is a cyber-attack to make a machine or network resource unavailable."

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.

Q.11 What type of loss is done by DoS attacks? (K.B+U.B)

Ans: **LOSS BY DoS ATTACKS**

DoS attacks do not typically result in the theft or loss of significant information or other assets, but they can cost the victim a great deal of time and money.

Activity 4.7 (K.B+U.B+A.B)

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 down each category.

CYBERCRIME CATEGORIES ON NR3C

- Hacking
- Identity theft
- Financial fraud
- Digital piracy
- Malicious software
- Money laundering
- Computer viruses and worms
- Data theft
- Denial of service attack
- Intellectual property rights
- Website defacement
- Cyber stalking
- Social engineering
- Electronic terrorism, vandalism and extortion

MULTIPLE CHOICE QUESTIONS

1. It is a great tools for criminals. (K.B)

(A) Virtual reality (B) Internet (C) Mobile (D) Google

2. The lure of easy wealth has found many victims of these frauds. (K.B)

(A) Transaction (B) Identity theft (C) Hacking (D) Advance fee

3. An activity of accessing someone else's computer illegally is called: (K.B+U.B)

(A) Phishing (B) Programming (C) Hacking (D) Surfing

4. A law enforcement agency of Pakistan dedicated to fight cybercrime is: (K.B)

(A) FIA (B) NR3C (C) FBR (D) NAB

5. A cyber attack to make machine or network resource unavailable, is called: (K.B+U.B)

(A) DoS (B) Hacking (C) Phishing (D) None of these

6. DoS attack results in loss of: (K.B+U.B)

(A) Information (B) Time (C) Money (D) Both B & C

EXERCISE

Q-4.1 Choose the correct option.

1. Which of the following doesn't includes the types of software piracy? (K.B+U.B)

(i) Softlifiting (ii) Liability
(iii) Client server overuse (iv) Online piracy

2. Which of the following is not a cybercrime? (K.B+U.B)

(i) Hacking (ii) Phishing crime (iii) Identity Theft (iv) Decryption

3. Which of the following is not the characteristics of phishing emails? (K.B+U.B)

(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? (K.B+U.B)

(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 characteristic of good password? (K.B+U.B)

(i) Is eight characters long (ii) Doesn’t contains username
(iii) Contains uppercase letters (iv) Password is your name only

Q-4.2 Fill in the blanks.

1. Making illegal copies of software is called ___________. **(K.B)**
2. ________________ is a general term for any type of information processing that can be represented mathematically. **(K.B+U.B)**
3. ________________ is the process of the encoding data.
4. When a key has less number of character than the text to encrypt, then repeating letters of the key is called ______________. **(K.B+U.B)**
5. ________________ is a cyber attack to make machine or network resource unavailable for a user. **(K.B+U.B)**

Q-4.3 Write short answers.

1. Define cyphertext. (K.B)

Ans: See SQ. 3 (Topic 4.3)

2. Why do we need an installation key whereas a software can be protected with a password? (U.B)

Ans:

NEED OF INSTALLATION KEY

Following are the reasons for using installation key instead of password to protect a software:

- Installation key is automatically expired after a certain number of use where a password never expires.
- Installation key is used to install software while password is set to use a software.
- Installation key is public where as password is private.
- Installation key cannot be reset by the user while a password can be.

3. Define Denial of Service. **(K.B)**

Ans: See SQ. 10 (Topic 4.5)

4. Give a reason to add captcha on websites. **(U.B)**

Ans: See SQ. 3 (Topic 4.4)

5. What is Patent, and why do we need to register it? **(K.B+U.B)**

Ans: See SQ. 14 (Topic 4.1)

ANSWER KEY

Q-4.1 Choose the correct option.

1	ii	2	iv	3	iv	4	iv	5	iv

Q-4.2 Fill in the blanks.

1	Piracy	2	Computation	3	Encryption	4	Interim cyphertext	5	Denial of Service

ANSWER KEY

4.1 ETHICAL ISSUES RELATED TO SECURITY

1	D	2	B	3	D	4	C	5	A	6	D	7	C	8	A
9	D	10	A	11	B	12	C	13	C	14	B	15	A	16	B

4.2 IMPORTANCE OF DATA PRIVACY

1	B	2	A	3	C	4	C	5	B	6	D	7	A

4.3 SIMPLE ENCRYPTION

1	B	2	D	3	A	4	C	5	A	6	B	7	D	8	D	9	B	10	C
11	B	12	C	13	D	14	A	15	C	16	D	17	B	18	A	19	A	20	C

4.4 ENCRYPTION WITH KEYS AND PASSWORDS

1	A	2	C	3	B	4	D

4.5 CYBERCRIME

1	B	2	D	3	C	4	B	5	A	6	D