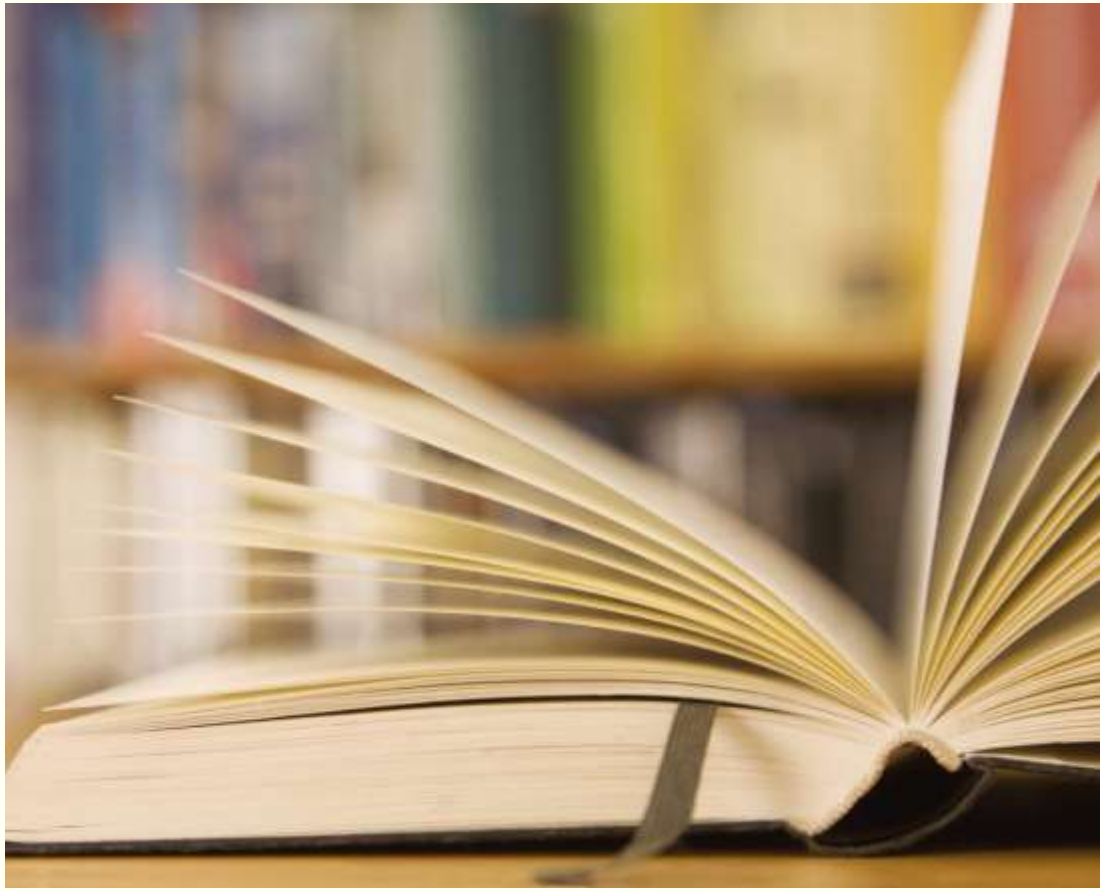
12. SECURITY AND ETHICAL ISSUES



FPT Education

FPT UNIVERSITY

Content

- 12.1 Introduction
- 12.2 Confidentiality
- 12.3 Ethical Principles
- 12.4 Privacy
- 12.5 Hackers

Objectives

After studying this chapter, the student should be able to:

- Define a database and a database management system (DBMS) and describe the components of a DBMS.
- Describe the architecture of a DBMS based on the ANSI/SPARC definition.
- Define the three traditional database models: hierarchical, networking, and relational.
- Describe the relational model and relations.
- Understand operations on a relational database based on commands available in SQL.
- Describe the steps in database design.
- Define ERM and E-R diagrams and explain the entities and relationships in this model.
- Define the hierarchical levels of normalization and understand the rationale for normalizing the relations.
- List database types other than the relational model.

Objectives (cont)

- Define three ethical principles related to the use of computers.
- Distinguish between physical and intellectual property and list some types of intellectual property.
- Define privacy as related to the use of computers.
- Give the definition of a computer crime and discuss types of attacks, motivation for attacks, and how to protect against attacks.
- Define hackers and the damage done by them

1 - INTRODUCTION

1. Introduction

- We are living in the information age. We need to keep information about every aspect of our lives. In other words, information is an asset that has a value like any other asset. As an asset, information needs to be secured from attacks.

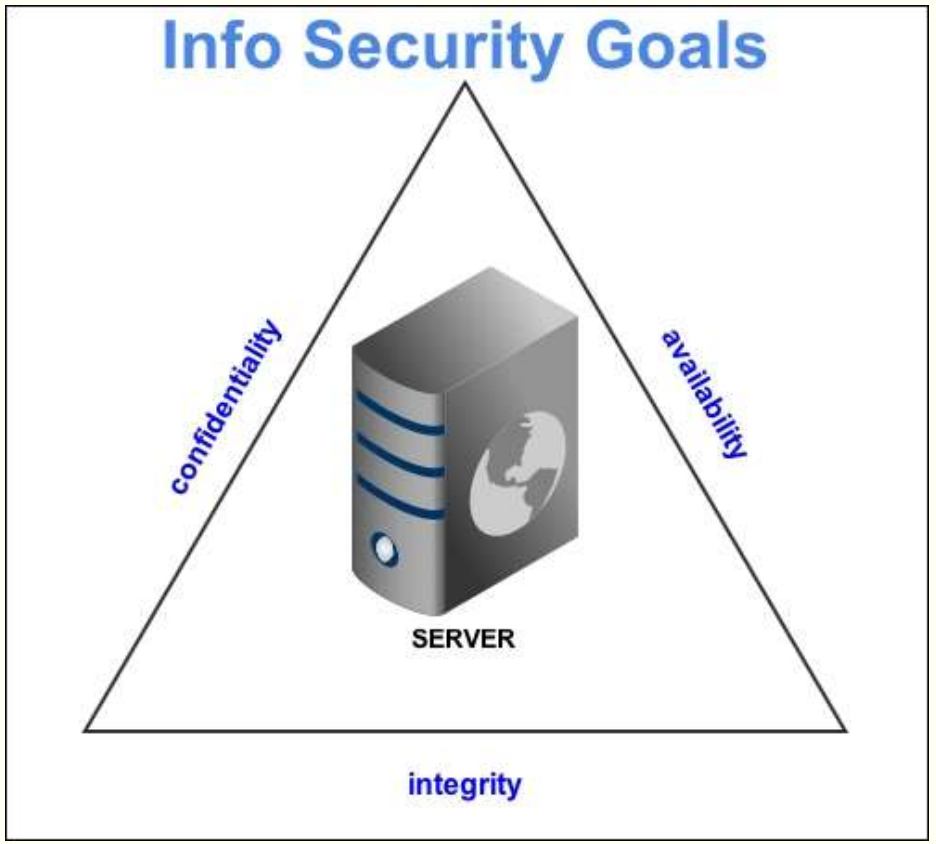
- To be secure, information needs
  - ❑to be hidden from unauthorized access (confidentiality),
  - ❑protected from unauthorized change (integrity),
  - ❑and available to an authorized entity when it is needed (availability).

2. Security goals

- **Confidentiality** is probably the most common aspect of information security. We need to protect our confidential information. An organization needs to guard against those malicious actions that endanger the confidentiality of its information.

- **Integrity** Information needs to be changed constantly. In a bank, when a customer deposits or withdraws money, the balance of their account needs to be changed. **Integrity** means that changes need to be done only by authorized entities and through authorized mechanisms.

- **Availability** The third component of information security is **availability**. The information created and stored by an organization needs to be available to authorized entities. Information is useless if it is not available. Information needs to be constantly changed, which means it must be accessible to authorized entities.



3. Attacks

- Our three goals of security—confidentiality, integrity, and availability—can be threatened by **security attacks**. Although the literature uses different approaches to categorizing the attacks, we divide them into three groups related to the security goals. Figure 16.1 shows the taxonomy

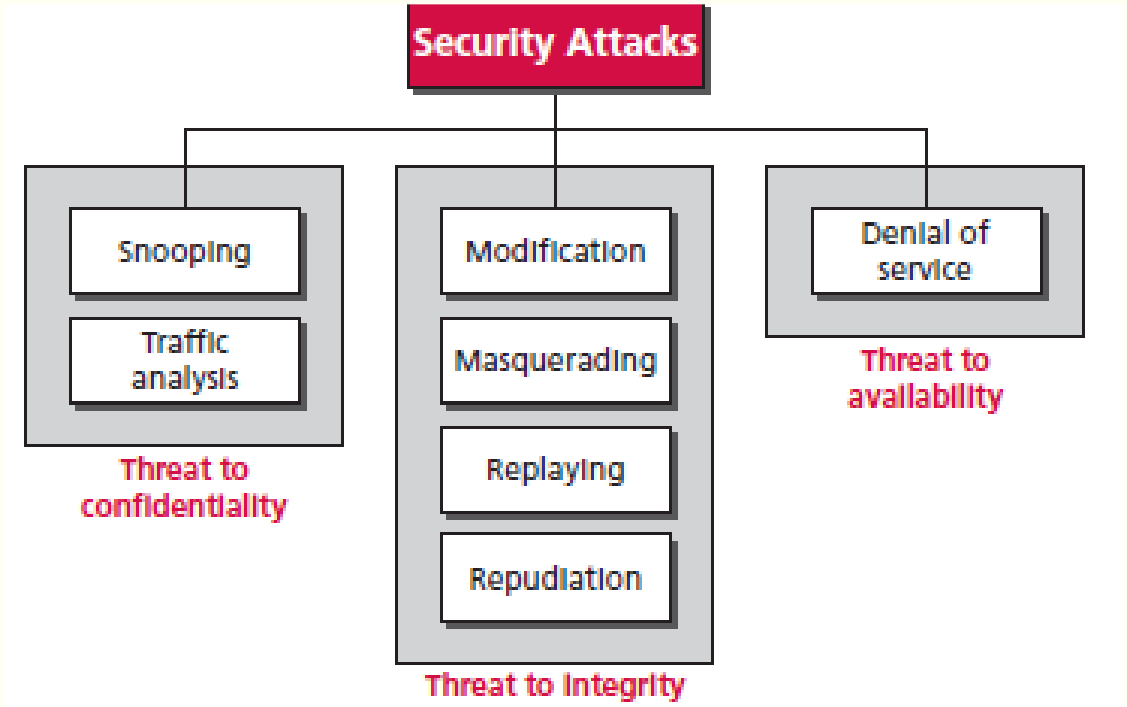
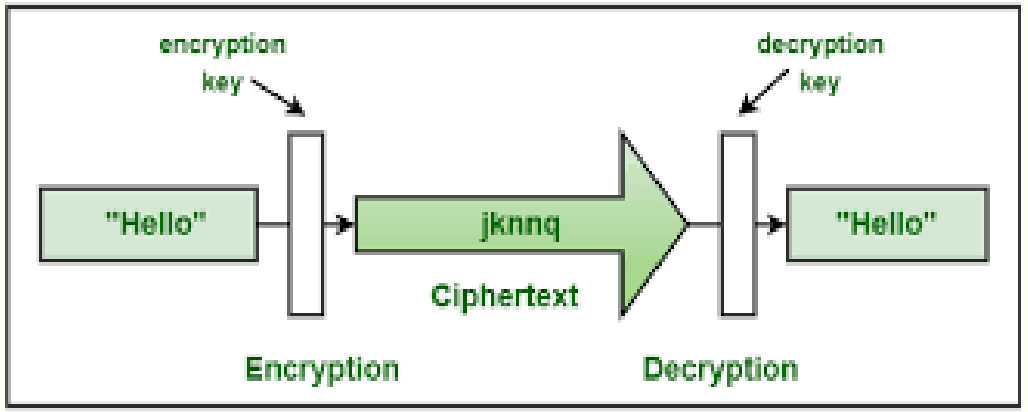


Figure 12.1 Taxonomy of attacks with relation to security goals

4. Services and techniques

- ITU-T defines some security services to achieve security goals and prevent attacks. Each of these services is designed to prevent one or more attacks while maintaining security goals. Two techniques are below

Cryptography (general)
Although in the past cryptography referred only to the encryption and decryption of messages using secret keys.



Cryptography

Steganography (specific)
The word steganography, with origins in Greek, means 'covered writing', in contrast to cryptography, which means 'secret writing'..

This book is mostly about cryptography, not steganography.
□ □□□ □ □ □ □ □□
0 1 0 0 0 0 1

Single space between words = binary digit 0
Double space between words = binary digit 1
0100001

2- CONFIDENTIALITY

1. Symmetric-key ciphers

- A symmetric-key cipher uses the same key for both encryption and decryption, and the key can be used for bidirectional communication, which is why it is called symmetric. Figure 16.2 shows the general idea behind a symmetric-key cipher.

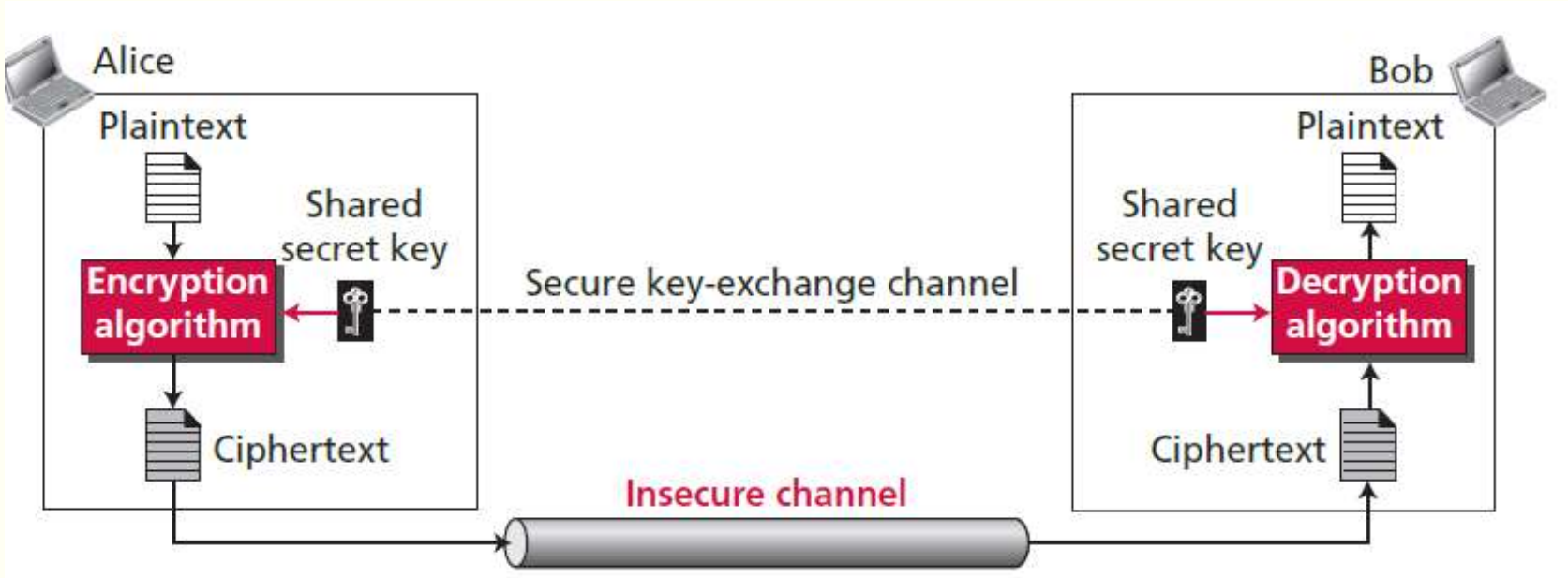


Figure 12.2 General idea of a symmetric-key cipher

2. Asymmetric-key ciphers

- Symmetric- and asymmetric-key ciphers will exist in parallel and continue to serve the community.
- In symmetric-key cryptography, the secret must be shared between two persons. In asymmetric-key cryptography, the secret is personal (unshared); each person creates and keeps his or her own secret.
- Compare between two system :

Symmetric-key cryptography is based on sharing secrecy; asymmetric-key cryptography is based on personal secrecy.

- And

In symmetric-key cryptography, symbols are permuted or substituted; in asymmetric-key cryptography, numbers are manipulated.

3. General idea

- Figure 12.3 shows the general idea of asymmetric-key cryptography as used for encipherment.

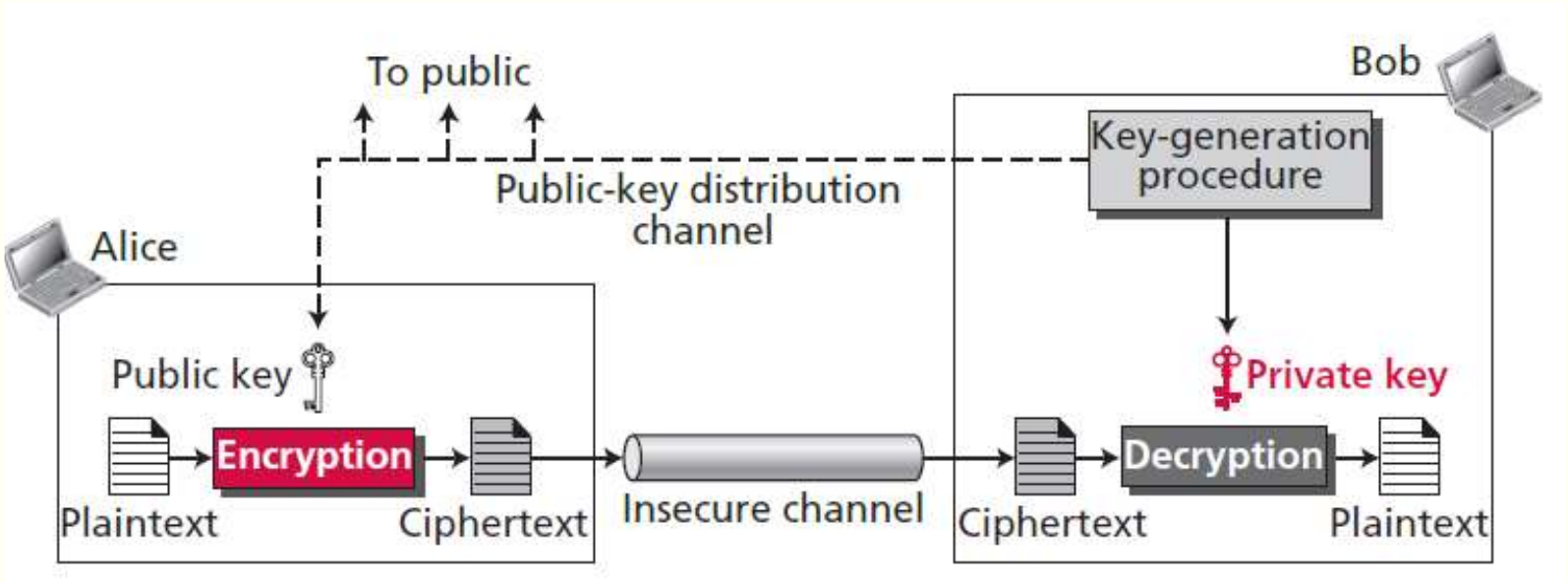


Figure 12.3 General idea of asymmetric-key cryptosystem

R4. SA cryptosystem

- Although there are several asymmetric-key cryptosystems, one of the common public-key algorithms is the RSA cryptosystem, named for its inventors (Rivest, Shamir, and Adleman).
- RSA uses two exponents, e and d, where e is public and d is private

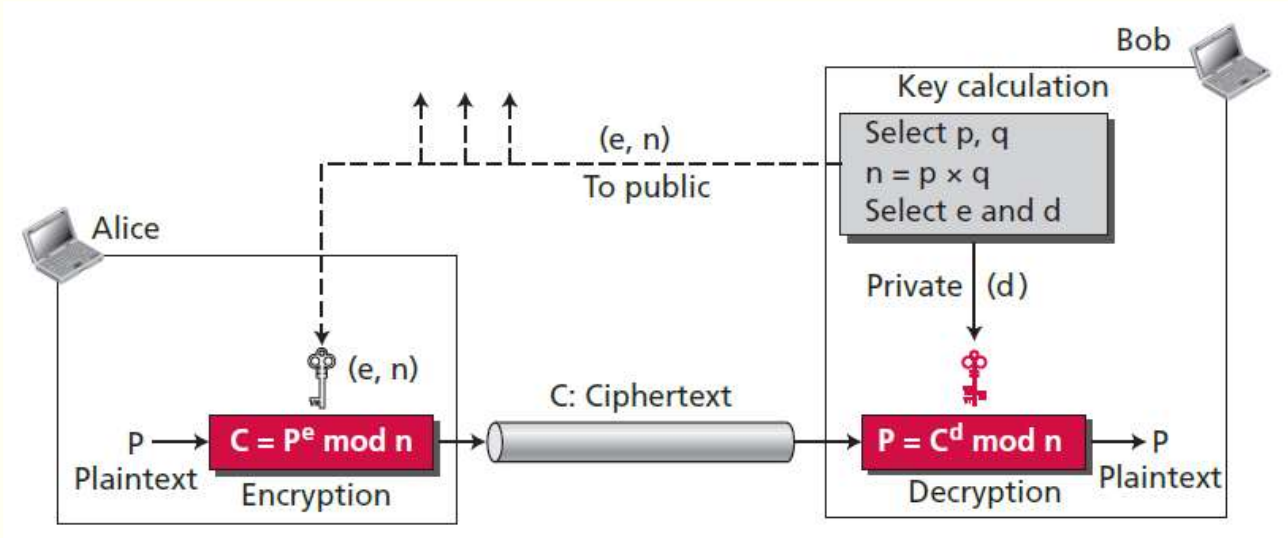


Figure 12.4 Encryption, decryption, and key generation in RSA

3 - ETHICAL PRINCIPLES

1. ETHICAL PRINCIPLES

- One of the ways to evaluate our responsibility towards the rest of the world when using a computer is to base our decisions on ethics.
- Ethics is a very complex subject that would take several books to describe in detail. In this chapter, we discuss only three principles that can be related to our goal, shown in Figure 12.5.

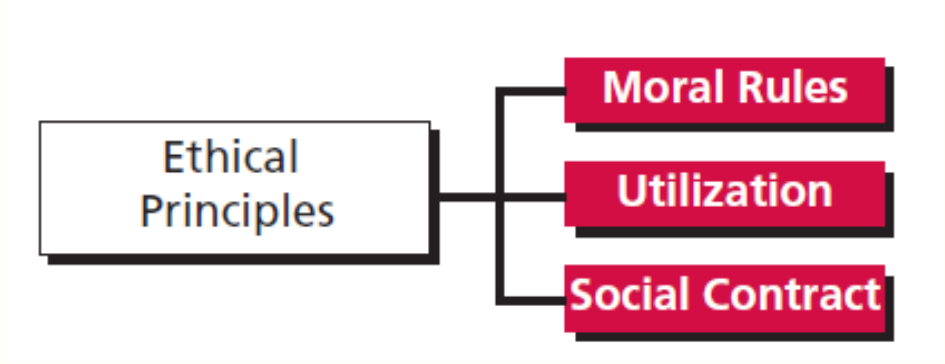


Figure 12.5 Three main principles of ethics

2. Moral rules

- The first ethical principle states that when we make an ethical decision, we need to consider if the decision is made in accordance with a universally accepted principle of morality.
- For example, if we want to illegally access a computer to get some information, we need to ask ourselves if this act is moral.

The first principle of ethics says that we should avoid doing anything if it is against universal morality.

For the study, Curry's group studied ethnographic accounts of ethics from 60 societies, across over 600 sources. The universal rules of morality are:

1. Help your family
2. Help your group
3. Return favors
4. Be brave
5. Defer to superiors
6. Divide resources fairly
7. Respect others' property

3. Utilization

- The second theory of ethics is related to the consequences of the act. An act is ethical if it results in consequences which are useful for society.
- Example: If a person accesses a bank's computer and erases customer records, is this act useful for society? Since this action may damage the financial status of the bank's customer, it is detrimental to society. It does not bring about a good result. It is not ethical.

The second principle of ethics says that an act is ethical if it brings about a good result.

4. Social contract

- The social contract theory says that an act is ethical when a majority of people in society agrees with it. If someone breaks into somebody else's house and commits a robbery, does this act receive the approval of a majority of society? Since the answer is negative, this act is not ethical.

The third principle of ethics says an act is ethical if a majority of people in society agree with it.

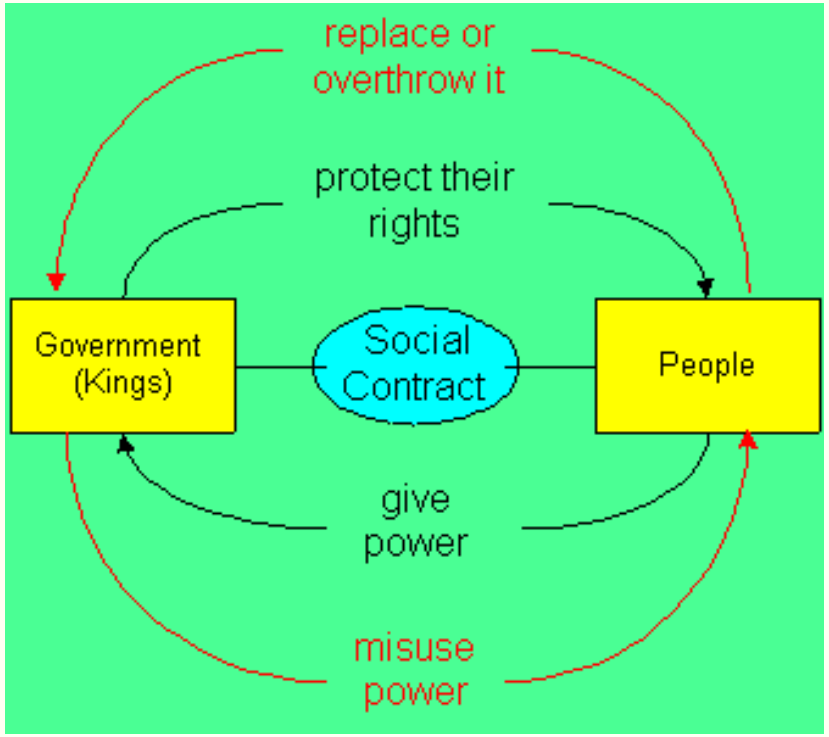


Figure 12.6 Majority of people in society

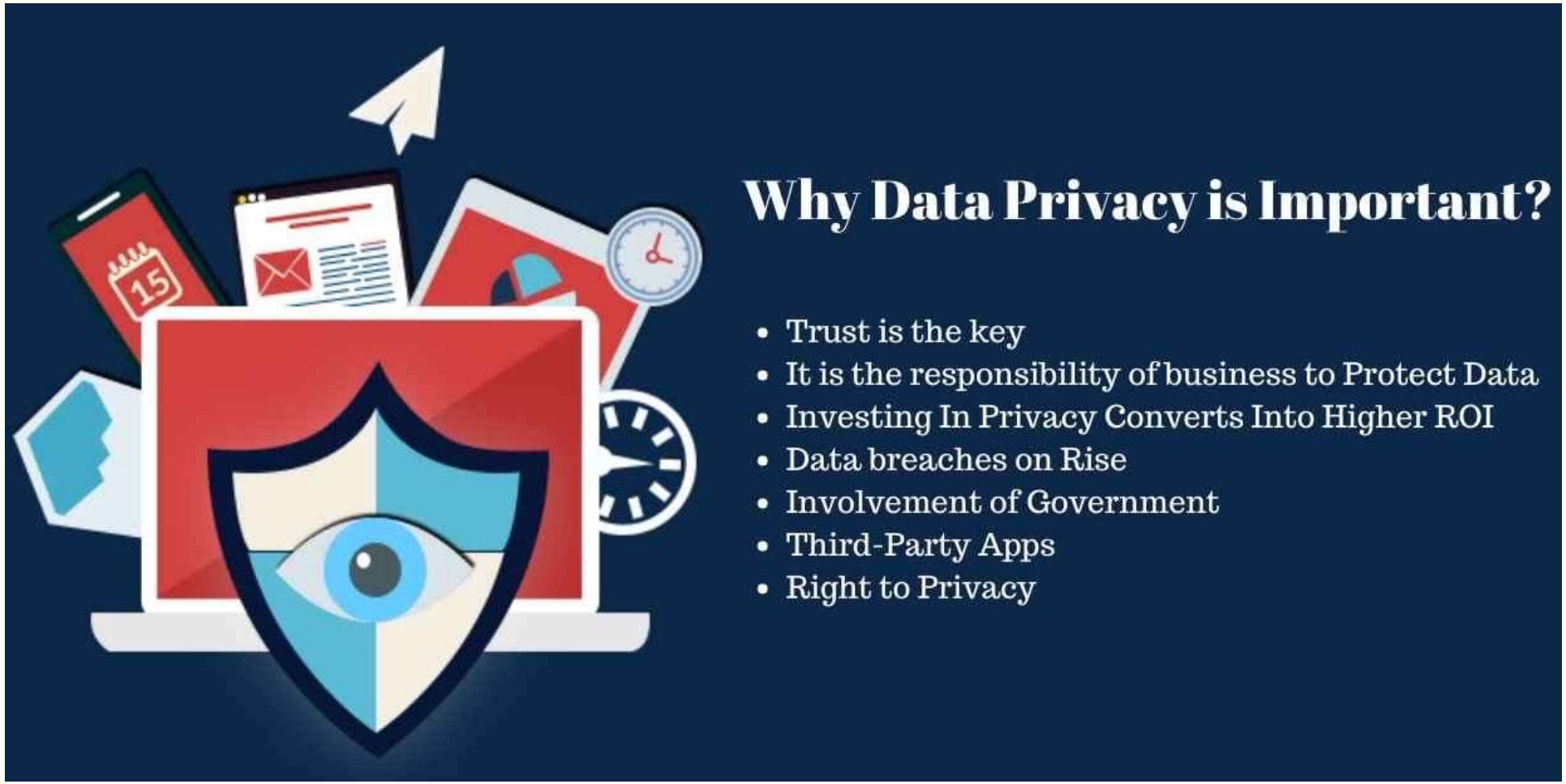
4- PRIVACY

1. Introduction

- Today, a large amount of personal information about a citizen is collected by private and public agencies. Although in many cases the collection of this information is necessary, it may also pose some risks.
- Some of the information collected by government or private companies can be used commercially. In many countries, a citizen's right to privacy is, directly or indirectly, mentioned in the nation's constitution.
- Codes of ethics related to the use of computers to collect data, as shown below:

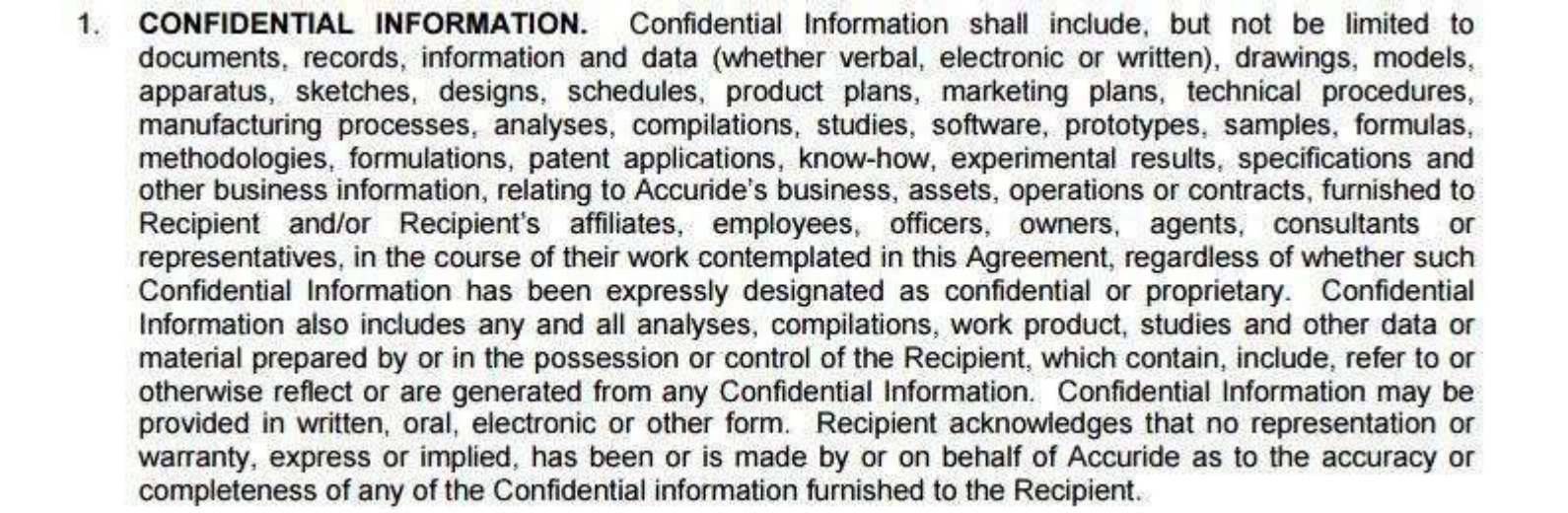
1. Collect only data that are needed.
2. Be sure that the collected data are accurate.
3. Allow individuals to know what data have been collected.
4. Allow individuals to correct the collected data if necessary.
5. Be sure that collected data are used only for the original purpose.
6. Use encryption techniques

2. Why Data Privacy is important?



4. Non-Disclosure Agreement

- A NDA can also be known by other names such as a confidentiality, non-use or trade secret agreement.
- Essentially, a non-disclosure (NDA) agreement is a legally binding contract between parties that requires them to keep certain information confidential.



1. **CONFIDENTIAL INFORMATION.** Confidential Information shall include, but not be limited to documents, records, information and data (whether verbal, electronic or written), drawings, models, apparatus, sketches, designs, schedules, product plans, marketing plans, technical procedures, manufacturing processes, analyses, compilations, studies, software, prototypes, samples, formulas, methodologies, formulations, patent applications, know-how, experimental results, specifications and other business information, relating to Accuride's business, assets, operations or contracts, furnished to Recipient and/or Recipient's affiliates, employees, officers, owners, agents, consultants or representatives, in the course of their work contemplated in this Agreement, regardless of whether such Confidential Information has been expressly designated as confidential or proprietary. Confidential Information also includes any and all analyses, compilations, work product, studies and other data or material prepared by or in the possession or control of the Recipient, which contain, include, refer to or otherwise reflect or are generated from any Confidential Information. Confidential Information may be provided in written, oral, electronic or other form. Recipient acknowledges that no representation or warranty, express or implied, has been or is made by or on behalf of Accuride as to the accuracy or completeness of any of the Confidential information furnished to the Recipient.

Figure 12.7 An example of NDA

5 - HACKERS

1. Introduction

- The word hacker today has a different meaning than when it was used in the past. Previously, a hacker was a person with a lot of knowledge who could improve a system and increase its capability.
- Today, a hacker is someone who gains unauthorized access to a computer belonging to someone else in order to copy secret information.

Figure 12.8 Types of Hackers

2. Types of Hackers

- **Black Hat Hacker** Basically, these are the "bad guys". They are the types of hackers who break into computer networks with purely negative motives such as monetary gain or reputation.
- **White Hat Hacker** As opposed to the black hat, these are the "good guys". They are ethical hackers who create algorithms to break existing internet networks so as to solve the loopholes in them.
- **Grey Hat Hacker** Basically, these are hackers who exploit the internet systems only to make public, certain vast datasets of information that would be of benefit to everyone.
- **Blue Hat Hacker** In one word, this is the amateur. Usually, their techniques are deployed out of ill motives such as revenge attacks.
- **Red Hat Hacker** The objective of a red hat hacker is to find black hat hackers, intercept and destroy their schemes.
- **Green Hat Hacker** This is the set of individuals who simply want to observe and learn about the world of hacking. It comprises those who join learning communities to watch videos and tutorials about hacking.

3. Common types of hacking

- Hacking for financial gain Lone black hat hackers as well as hacking collectives are typically thieves. Their cybercrimes are targeted at either directly stealing money, enabling later theft via data hijacking, or selling the acquired data to other cybercriminals.
- Corporate espionage With so many industries as cutthroat as they are, it's unsurprising that companies are often willing to get dirty to triumph over the competition. Corporate (or industrial) espionage is the commercial application of hacking, malware, phishing, and other unsavory spying techniques to obtain privileged insider information from a business competitor — aka information hacking.
- State-sponsored hacking The potential rewards from security hacking can be so great, even governments want to get in on the party. Countries all across the world are constantly playing games of cat-and-mouse cyber warfare with one another. Everyone knows that everyone else is doing it, and everyone acts surprised and offended when they get caught.