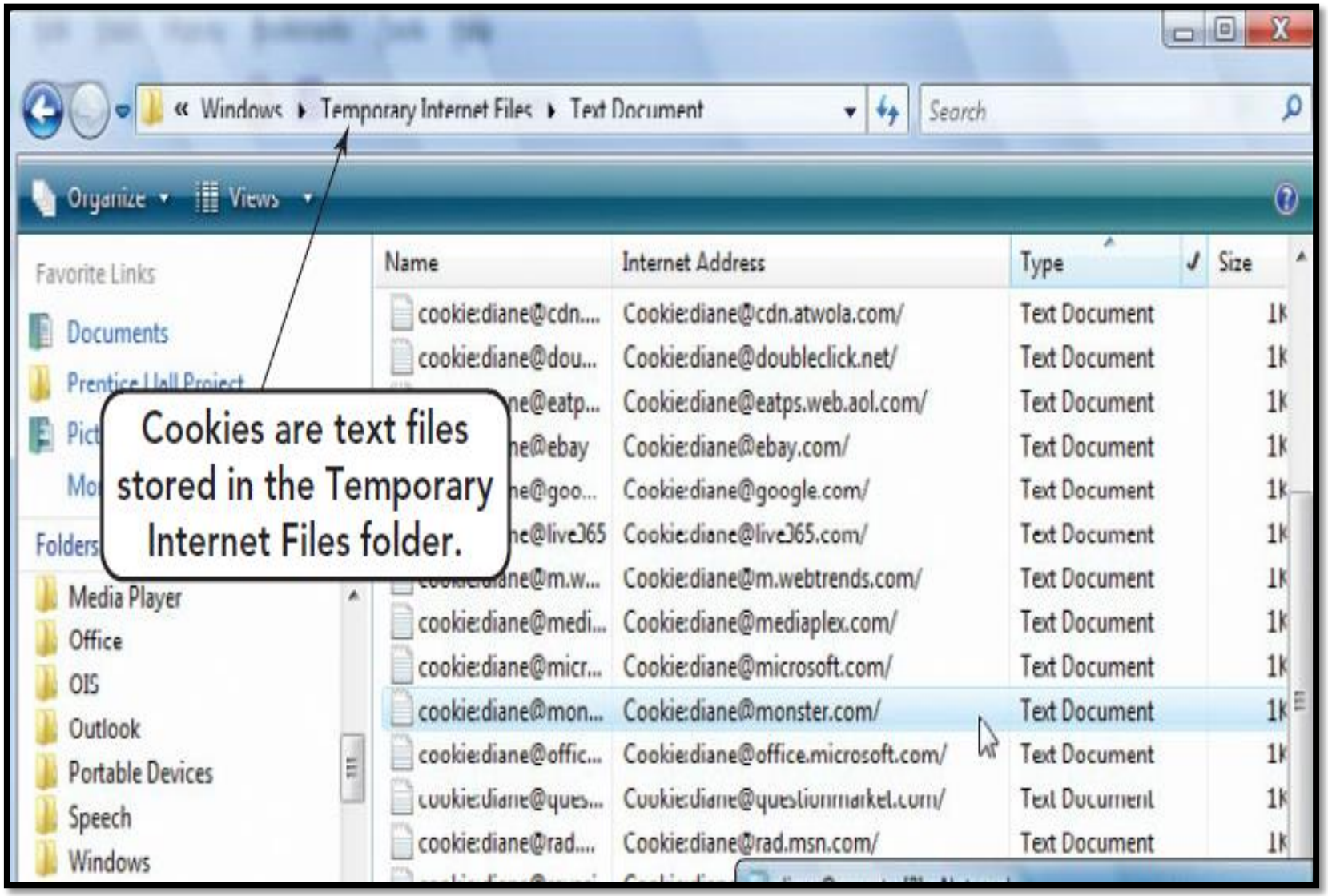
Dr./ Ahmed Mohamed Rabie Sayed

Chapter 9

Privacy, Crime and Security

Privacy refers to an individual's ability to restrict or eliminate the collection, use, and sale of confidential personal information.

Cookies Generally downloaded into folders that hold temporary Internet files are small text files that are written to your computer's hard disk by many of the Web sites you visit.


« Windows ▸ Temporary Internet Files ▸ Text Document
Search
Organize
Views
Favorite Links
Documents
Prentice Hall Project
Folders
Media Player
Office
OIS
Outlook
Portable Devices
Speech
Windows
Cookies are text files stored in the Temporary Internet Files folder.
Name
Internet Address
Type
Size
cookie:diane@cdn.... Cookie:diane@cdn.atwola.com/ Text Document 1k
cookie:diane@dou... Cookie:diane@doubleclick.net/ Text Document 1k
Cookie:diane@eatps.web.aol.com/ Text Document 1k
Cookie:diane@ebay.com/ Text Document 1k
Cookie:diane@google.com/ Text Document 1k
Cookie:diane@live365.com/ Text Document 1k
Cookie:diane@m.webtrends.com/ Text Document 1k
cookie:diane@medi... Cookie:diane@mediaplex.com/ Text Document 1k
cookie:diane@micr... Cookie:diane@microsoft.com/ Text Document 1k
cookie:diane@mon... Cookie:diane@monster.com/ Text Document 1k
cookie:diane@offic... Cookie:diane@office.microsoft.com/ Text Document 1k
Text Document 1k
cookie:diane@rad.... Cookie:diane@rad.msn.com/ Text Document 1k

Cookies are actually used for many useful and legitimate tasks:-

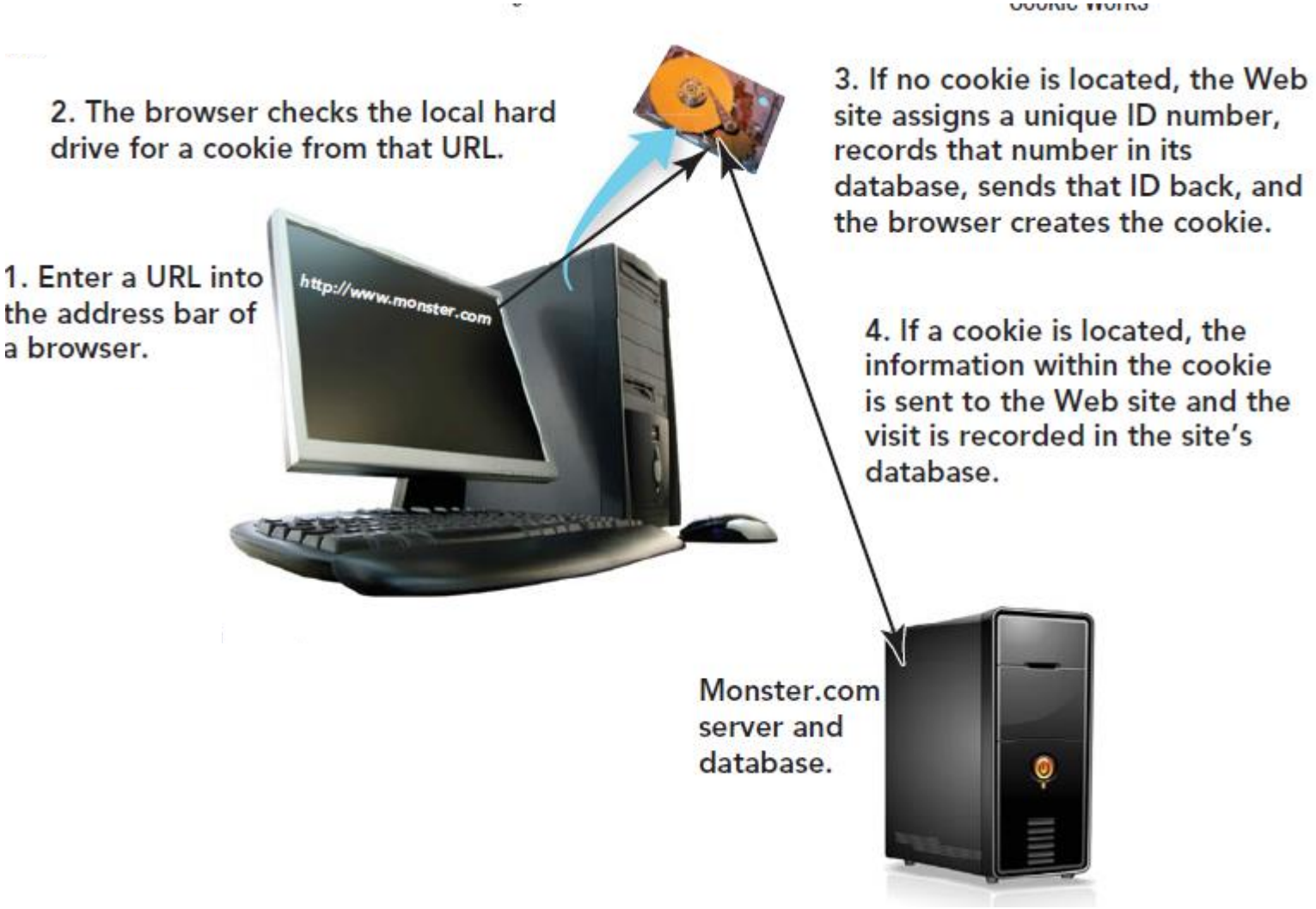
1- Cookies enable the Web site to obtain an actual count on the number of new and return visitors.

2- They can store site preferences set by the user. When the user returns to the site, the preferences are automatically applied.

3- Online retail sites use cookies to implement “shopping carts,” which enable you to make selections that will stay in your cart so that you can return to the online store for more browsing and shopping.

Some users point to several problems with cookies:-

Cookies can be deleted. If the cookie was holding your login ID and password, you might not remember them to log in again.


2. The browser checks the local hard drive for a cookie from that URL.
3. If no cookie is located, the Web site assigns a unique ID number, records that number in its database, sends that ID back, and the browser creates the cookie.
1. Enter a URL into the address bar of a browser.
http://www.monster.com
4. If a cookie is located, the information within the cookie is sent to the Web site and the visit is recorded in the site's database.
Monster.com server and database.

Computer crimes, computer-based activities that violate state, federal, or international laws.

Cybercrime describes crimes carried out by means of the Internet.

In a phishing attack, a "phisher" poses as a legitimate company in an e-mail or on a Web site in an attempt to obtain personal information such as your Social Security number, user name, password, and account numbers.

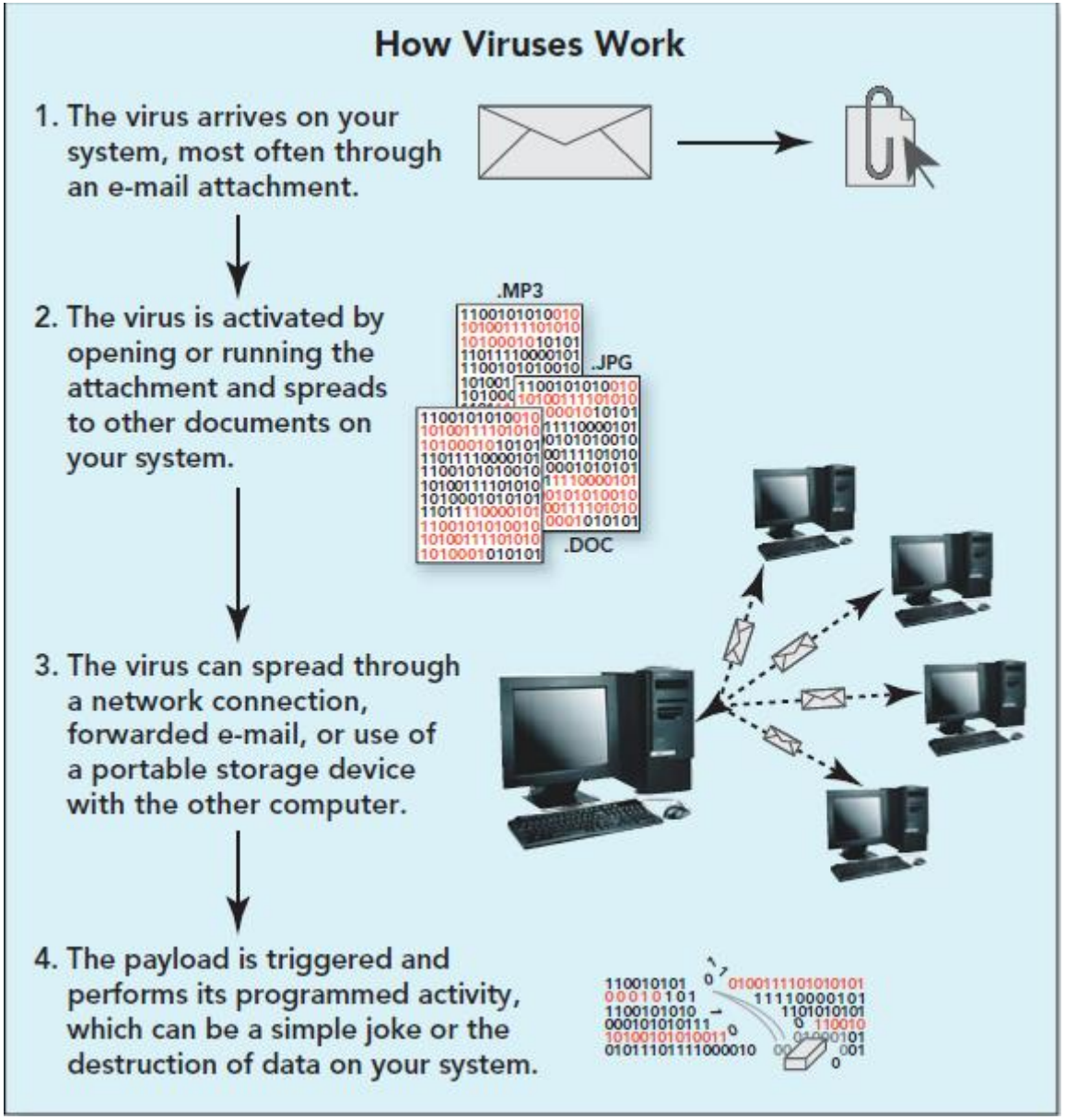
The term malware is short for *malicious software* and describes software designed to damage or infiltrate a computer system without the owner's consent or knowledge

Spyware s software that collects your personal information, monitors your Web surfing habits, and distributes this information to a third party, often leading to identity theft. Some spyware, such as adware, generates pop-up ads and targeted banner ads, and is usually considered a nuisance rather than malic

A computer virus is hidden code that attaches itself to a program, file, or e-mail message referred to as a host.

A logic bomb is hidden computer code that sits dormant on a system until a certain event or set of circumstances triggers it into action.

A time bomb is a hidden piece of computer code set to go off on some date and time in the future usually causing a malicious act to occur to the system.


How Viruses Work
1. The virus arrives on your system, most often through an e-mail attachment.
2. The virus is activated by opening or running the attachment and spreads to other documents on your system.
.MP3
.JPG
.DOC
3. The virus can spread through a network connection, forwarded e-mail, or use of a portable storage device with the other computer.
4. The payload is triggered and performs its programmed activity, which can be a simple joke or the destruction of data on your system.

A worm is a program that resembles a computer virus in that it can spread from one computer to another.

Denial of service (DoS) attack, a form of network vandalism, an attacker attempts to make a service unavailable to other users, generally by bombarding the service with meaningless data. Because network administrators can easily block data from specific IP addresses, hackers must commandeer as many computers as possible to launch their attack.

Syn flooding is a form of denial of service attack in which a hostile client repeatedly sends SYN (synchronization) packets to every port on the server, using fake IP addresses, which uses up all the available network connections and locks them up until they time out.

Techniques Used to Obtain Passwords

Password Guessing	Computer users too often choose a password that is easily guessed, such as "password." Other popular passwords are "qwerty" (the first six letters of the keyboard), obscene words, personal names, birthdays, celebrity names, movie characters such as Frodo or Gandalf, and cartoon characters such as Garfield.
Shoulder Surfing	In a crowded computer lab, it's easy to peek over someone's shoulder, look at the keyboard, and obtain his or her password. Watch out for shoulder surfing when using an ATM machine too.
Packet Sniffing	A program called a packet sniffer examines all of the traffic on a section of a network and looks for passwords, credit card numbers, and other valuable information.
Dumpster Diving	Intruders go through an organization's trash hoping to find documents that contain lists of user IDs and even passwords. It's wise to use a shredder!
Social Engineering	This is a form of deception to get people to divulge sensitive information. You might get a call or an e-mail from a person who claims, "We have a problem and need your password right now to save your e-mail." If you comply, you might give an intruder entry to a secure system.
Superuser Status	This enables system administrators to access and modify virtually any file on a network. If intruders gain superuser status, perhaps by using a rootkit, they would then have access to the passwords of everyone using the system.

Hackers are computer hobbyists who enjoy pushing computer systems (and themselves) to their limits. They experiment with programs to try to discover capabilities that aren't mentioned in the software manuals.

Cybergangs are groups of hackers or crackers working together to coordinate attacks, post online graffiti, or engage in other malicious conduct

Crackers (also called black hats) are hackers who become obsessed (often uncontrollably) with gaining entry to highly secure computer systems. Their intent, however, is to destroy data, steal information, or perform other malicious acts.

More than a few hackers and crackers have turned pro, offering their services to companies hoping to use hacker expertise to shore up their computer systems' defenses. Those who undertake this type of hacking are called ethical hackers, or white hats.

Cyberstalking or using the Internet, social networking sites, e-mail, or other electronic communications to repeatedly harass or threaten a person.

Cyberbullying involves situations in which one or more individuals harass or threaten another individual less capable of defending himself or herself, using the Internet or other forms of digital technology

A computer security risk is any event, action, or situation—intentional or not—that could lead to the loss or destruction of computer systems or the data they contain.

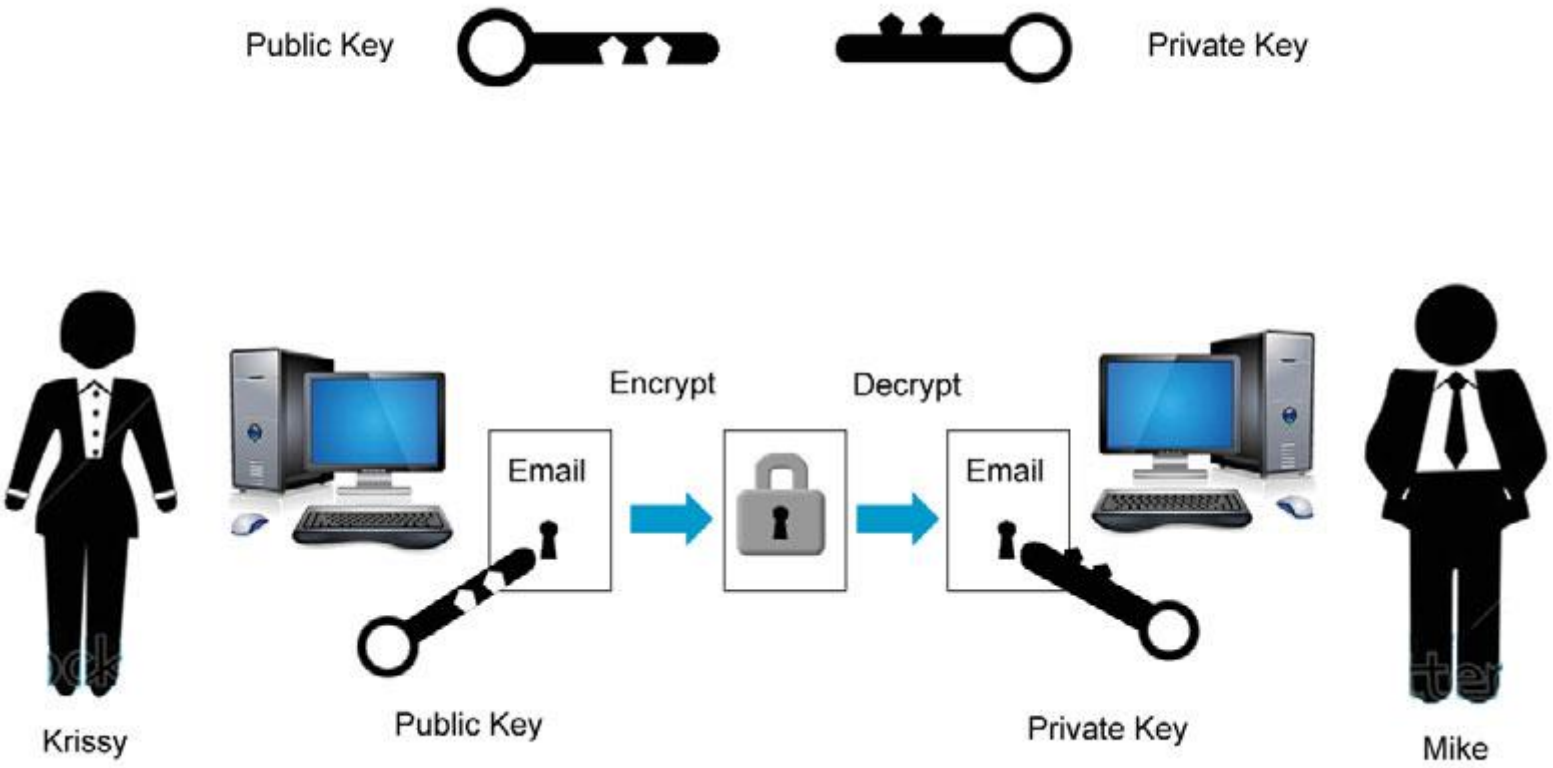
Biometric authentication devices such as retinal scanners, hand geometry readers, and fingerprint scanners are often used to provide access to restricted locations.

A firewall is a computer program or device that permits an organization's internal computer users to access the external Internet but severely limits the ability of outsiders to access internal data.

Encryption refers to a coding or scrambling process that renders a message unreadable by anyone except the intended recipient.

Public key encryption (asymmetric key encryption) is a computer security process in which two different keys—an encryption key (the public key) and a decryption key (the private key)—are used.

Public key infrastructure (PKI) is a uniform set of encryption standards that specify how public key encryption, digital signatures, and digital certificates should be implemented in computer systems and on the Internet.


Public Key
Private Key
Encrypt
Decrypt
Email
Email
Krissy
Public Key
Private Key
Mike