Mục lục

❖ Chương 1,2: Computer- Part of computer

1. How many types of computers do you know? What are they?

There are 4 types of computers: Micro-computer, Mini-computer, Mainframe-computer, Portable-computer

2. What is the difference between a mainframe and a PC?

Mainframe	PC
- Large, powerful, expensive - Multi-user system used by many people at the same time - Used for processing very large amounts of data - The most powerful mainframes are called supercomputers	- The most common type of computer - Smaller, cheaper and less powerful than mainframes and minicomputer

3. How many main parts of a computer? What are they?

- There are 8 parts of a computer :
  - Hard disk drive
  - Motherboard
  - Memory chip
  - Powerful supply
  - Processor
  - Speaker
  - Expansion card
  - Floppy drive

4. What is computer hardware?

- The electronic and mechanical parts that make up a computer system are called hardware
// Computer hardware is the physical parts or components of a computer

5. What is computer software

- Information in the form of data and programs is known as software
// Computer software is instructions that can be stored and ran by hardware

6. What is a motherboard?

- The motherboard is a large circuit board which all other PC components connect to tin some way
// The motherboard (mainboard, system board, or mobo) is the main printed circuit board (PCB) found in computers and other expandable systems. It holds many of the crucial electronic components of the system, such as the central processing unit(CPU) and memory, and provides connectors for other peripherals

7. What does SIMMS stand for?

- Single in-line memory module

// SIMMS (single In-line memory module) is a module containing one or several random access memory (RAM) chips on a small circuit board with pins that connect to the computer motherboard

8. What is an expansion slot?

- An Expansion slot is a socket on the motherboard that used to insert expansion card which provides s additional feature to a computer such as sounds, graphics memories

// An expansion slot is a socket on the motherboard that is used to insert an expansion card (or circuit board), which provides additional features to a computer such as videos, sounds, advanced graphics, memory

9. What is cache memory?

- It's part of the memory store. It has extremely fast access. It's faster than normal Ram. It can speed up the computer

// Cache memory is a small block of high- speed memory (RAM) that enhances PC performance by pre-loading information from the main memory and passing it to the processor on-demand.

10. What is ROM?

- Read-only memory – this kind of memory contains all the constructions your computer needs to activate itself when you switch on. Unlink Ram, its contents are retained when you switch off

// ROM is a type of storage medium that permanently stores data on personal computers (PCs) and other electronic devices. It contains the programming needed to start a PC. It cannot be changed, it is permanent, meaning it also holds it's memory even when power is removed. By contrast, RAM lost its contents when you switch off.

11. What is different between Rom and Ram

- ROM is meant for permanent storage, and RAM is for temporary storage.

12. How many types of portable computers? What are they?

- There are 4 types of portable computers:
  - Notebook
  - Laptop
  - Subnotebook
  - Handheld or palmtop

13. Make a list of computer port

- Keyboard
- Mouse
- Serial port
- Video port
- COM I
- Parallel

14. Write the instruction for the virus checking a disk?

- Put the disk into the drive
- Start the virus checking program
- Select the drive to be checked
- Click the " Find" button
- Don't exit the program until the check is complete
- Select "Yes" or "No" for checking another disk

Bonus:

Instruction for replacing the motherboard in a PC

- Remove the old motherboard
- Add the processor
- Add the memory. Don't touch the contacts
- Fit the new motherboard
- Put it back together

What is CPU? What are its functions? What are its components?

CPU (Central Processing Unit) is the 'brain' of the computer.
It is an electronic circuitry within a computer that executes program instructions and coordinate the activities of all the other units
CPU includes 3 principal components:

- Arithmetic Logic Unit (ALU)
- Registers
- Control Unit (CU)

Multiple choices:

- the brain of the computer = central processing unit
- physical parts that make up a computer system = hardware
- program which can be used on a particular computer system = software
- the information which is presented to the computer = input
- results produced by a computer = output
- Hardware equipment attached to the CPU = peripheral devices
- visual display unit = monitor
- small device used to store information. Same as "diskettes". = floppy disk
- Any socket or channel in a computer system into which an input/output device may be connected = port

What is computer virus? What is a computer crime? what is a hacker?

- **Computer virus** is a type of malicious code or program that have been written to make a computer behave in an unexpected and undesired way.
- **Computer crime** is a crime that involves a computer and a network. Computers may have been used in the commission of a crime, or it may be the target.
- **Hacker** is the person who, with their technical knowledge, uses bugs or exploits to break into computer systems without authorization.

❖ Chương 3 + 4 : Input & Output devices

15. How many input devices do you know? What are they and their functions ? Give Vnese meaning for each? What is an input device?

An input device is a peripheral device used to provide data and control signals to an information processing system.

- There are 8 input devices :
  - Joystick – Cần điều khiển (able to move in 8 directions. they are mostly used in computer games to control the way a picture on the screen moves)
  - Lightpen – Bút quang (used to draw pictures on a computer screen)
  - Scanner – Máy quét (allow users to take a printed picture or document and convert it into a digital file)
  - Digital Camera – Máy ảnh số (produce photos without film)
  - Mouse – Chuột máy tính (move the cursor rapidly)
  - Keyboard – Bàn phím máy tính (input text to the computer)
  - Microphone – Ống thu thanh hay thường đc gọi là Mic (input sound to the computer)
  - Touch screen – Màn hình cảm ứng

16. What does a scanner do ? Give a definition in your word?

- A scanner is an input device that allows a user to take printed pictures or documents and convert it into digital files

17. How many types of scanner do you know?

- There are 4 types of scanner :
  - Flatbed Scanners
  - Handheld Scanners
  - Film Scanner
  - Portable Scanners

18. What are the advantages and disadvantages of film cameras?

Advantages	Disadvantages
● Film cameras are cheap ● The quality of film cameras are much better than digital cameras ● Limited (or expensive) film make us think more about each exposure, which can result in better photographs	● Each picture cost a lot because there are processing costs ● Pictures can't be seen until printed out which can sometimes be inconvenient ● The picture has to be scanned to transfer images to PC ● Heavier than similar-sized digital cameras. ● Depend on a lab to develop images.

19. How many steps to input voice? What are they?

- There are 5 steps in voice input
  1) The user says a word into a microphone
  2) The microphone converts the word form audio signals to electrical signals
  3) The speech recognition board converts the signals into binary numbers
  4) The computer compares the binary code with its stored vocabulary
  5) The screen displays the correct word

20. What are the advantages and disadvantages of digital cameras?

Advantages:	Disadvantages
• Digital cameras don't use film • The cost for each picture is low • It is easy to download the pictures • lighter in weight than a film camera. • memory cards are tiny so they don't require much storage space • images from digital camera can be viewed immediately • images can be edited without being developed and you can choose to print only the image you want	• Digital cameras are expensive • The quality of digital cameras are lower than film cameras • Maybe lost the data • require computer skill to manage and edit images • difficult to focus • become obsolete much faster than film cameras • consume more batteries so photographer need to keep extra batteries

21. What is input devices

- An input device is a peripheral device used to provide data and control signals to an information processing system

22. What is an output device? What are they?

- An output device is a peripheral used to show the result of the data after processing
- There are 6 output devices: headphone, a projector, a printer, a speaker, an earphone and a monitor

23. How many types of printers? What are they?

- There are 3 types of printer
- They are: dot – matrix printer, ink-jet printer, and laser printer

24. What are the advantages and disadvantages of dot-matrix printers

Advantages	Disadvantages
- The dot matrix printers are cheap - They are cheapest to run - They use paper continuously unlike other printers that require frequent change of paper - The maintenance cost is low as compare other printers	- They have low print quality - They can't print color - The printer creates a great deal of noise.

25. What is a printer

- A printer is an output device used to print texts or pictures onto the paper

26. What are the advantages and disadvantages of ink-jet printers

Advantages	Disadvantages
- Create for photos and image-heavy document - Ink-jet printers have low start-up costs - Inkjet can print onto many types of paper - Almost no warm-up time is needed before printing - Inkjet printers tend to smaller. Lighter and easier to maintain than laser printers	- Inkjet is more expensive - Inkjet is water-based, so prints are susceptible to water damage and fading - Ink cartridge need frequent cleaning - Inkjet printers are getting faster, but still very slow compared to laser printers

27. Advantages and disadvantages of laser printers

Advantages	Disadvantages
- Print faster than inkjet printers - Laser printer produce perfect sharp black and text better than inkjet	- Need time to warm-up - Laser printer can't handle a variety of paper or printing material like ink-jet - Bigger and heavier than inkjet printers

28. How many main sections of keyboards? What are they?

- There are 4 main sections of keyboards
- They are: main keyboard key, function key, Editing key, and Numeric keyboard

29. What is computer crimes:

❖ is a crime that involve a computer and a network. Computers may have been used in the commission of a crime, or it may be the target.

❖ Computer crimes include :

- Hacking – unauthorized access to computer systems and tampering with other users data
- Pirating illegally copying and selling programs
- Intentionally attempting to spread viruses

Bonus:

1. **screen/monitor properties**:

- **price**: The price mainly depends on the screen size. common monitor sizes are 14-inch, 15-inch, 17-inch, 21-inch. The price also depends on aperture grill pitch, resolution and the number of controls
- **screen size**: is the diagonal distance from one corner to another. The actual area images are smaller than this
- **Aperture grill pitch**: This controls the space between the dots that make up the image. The less space between the dots, the better the display. most monitor offer 0.28mm dot pitch but some go as high as 0.31mm or as low as 0.25mm

- **maximum resolution**: the quality of the display depends on the number of dots which make up the image. The more dots, the better the display.
- **refresh rate**: The monitor refreshes the images on the screen all the time. The faster this happens, the fewer screen flickers. You should have a refresh rate of at least 72Hz.
- **Safety standards**: are international standards to control harmful signals
- **Power-saving feature**: the power the monitor uses automatically reduces when it is not in use.
- **On-screen menu**: digital controls on the screen allow you to adjust the images

❖ Chương 5 storage device

30. What are storage devices?

- Storage devices are hardware.
- Storage devices are used on computers to store the data.

Types of storage device (6 types)	Advantages	Disadvantages
Floppy disk	- cheap easy to transport - can be used many times	- don't have much storage capacity - can be affected by heat -slow
Fixed hard disk	- faster and more storage capacity than a floppy disk	- fixed inside
Removable hard disk	- fast and have high capacities	- not very common , expensive - not all conform to one standard
CD - ROM disk	- very common , comfort to a standard, removable - can hold a large amount of data	- read-only - slow
Magneto-optical disk	- removable, have large capacities, last for a long time - can write data on to them - provide faster data access and data transfer	- more expensive than magnetic hard drive not all common conform to one standard - not very common

❖ Chương 7: Networks

31. What is a network?

A network is simply two or more computers linked together. It allows us to share not only data files and software applications but also hardware like printers and other computer resources.

32. How many types of networks do you know?

Three

33. What are they?

They are LAN (Local Area Network), MAN (Metropolitan Area Network) and WAN (Wide Area Network)

34. What are the network's hardware components?

Server, hub, router, switch, modem, cable, bridge, PC, printer, access points

35. Which type of network is common and why?

LAN, because it is used by many people in small places. We can operate a LAN network easily to serve the purpose of connecting computers for sharing information. Everyone can own a LAN network at an affordable price. It doesn't require an ISP to manage a LAN network.

36. What is the difference between LAN and WAN?

LAN stands for Local Area Network: operates in small/ limited area/ location / place; Using Ethernet cable or wifi;

WAN stands for Wide Area Network: operates in wide/ large area/ location/ place

37. What are the advantages of LAN?

In LAN computers can exchange data and messages in an easy and fast way. It also saves time and makes our work fast. Every user can share messages and data with any other user on LAN. It provides high transmission speed, which can be hundreds of times faster than WAN

38. What are the advantages of WAN?

The principal advantage of a WAN is its size. By linking multiple sites together, WANs allow communication between entities on different sides of the country or even the other side of the world.

39. What are servers/ clients

The main computers that provide a service on the network are called servers, and the other computers that use the services are called clients.

40. How many types of network topology are there? what are they?

There are 5 types of network topology

There are Bus topology, Ring topology, Star topology, Extended Star topology, and Mesh topology.

41. What is a ring topology?

In a ring topology, each computer is connected to its neighbor in a circle. The data flows in one direction around the ring

42. What is a bus topology?

The bus topology has all the computers connected to a common cable, the data travels in both directions along the cable.

43. What is a star topology?

Star topology has a server computer at the center and a separate cable connecting the server to each of the other computers in the network. The central server controls the flow of data in the network.

44. What is the most common topology? why?

That is Star topology.

In a Star Network, the best advantage is when there is a failure in cables then only one computer might get affected and not the entire network.

45. What are the advantages of passwords?

It helps to prevent unauthorized users, or hackers, from breaking into the system

46. What are the rules of good passwords?

Be at least 6 characters long
Have a mixture of numbers and letters
Have a mixture of capital and small letters
Be easy to remember
Should not be a word from a dictionary
Should not be a common name
Should not include spaces, hyphens, dots, or symbols with a special meaning in computing, eg: $, *,...

47. Why shouldn't we use words in the dictionary and common names as passwords?

Because hackers can use special computer programs which automatically try all the works and combination words in a computerized dictionary to try to discover or crack other users' passwords

❖ Chương 8: Internet

48. What is the Internet?

- *Cách 1*:a global computer network providing a variety of information and communication facilities, consisting of interconnected networks using standardized communication protocols.
- *Cách 2:* The Internet is a **global network** of billions of computers and other electronic devices

49. What is Newgroup? What is Email? Structure of an email address?

- **Electronic mail (email or e-mail)** is a method of exchanging messages ("mail") between people using electronic devices
- **Structure of an email address:** <username>@<domain>.<type of organization>.<country>
  Example: AT149999@actvn.edu.vn
- **Newgroup:** A place on the internet where people who are interested in a particular subject can exchange messages about it, or the people who use this place
  Example:
  comp.* — Discussion of computer-related topics

50. What do TCP and IP stand for?

TCP: Transmission control protocol
IP: Internet protocol

51. What do TCP and IP mean in VNmese?

Bộ giao thức TCP/IP, (*Internet protocol suite* hoặc *IP suite* hoặc *TCP/IP protocol suite* - bộ giao thức liên mạng), là một bộ các giao thức truyền thông cài đặt chồng giao thức mà Internet và hầu hết các mạng máy tính thương mại đang chạy trên đó. Bộ giao thức này được đặt tên theo hai giao thức chính của nó là TCP (*Giao thức Điều khiển Giao vận*) và IP (*Giao thức Liên mạng*).

IP (Internet Protocol): giao thức liên mạng

TCP (Transmission control protocols): giao thức Điều khiển giao vận

52. What is the Internet protocol suite?

The ***Internet protocol suite*** is the conceptual model and set of communications ***protocols*** used in the ***Internet*** and similar computer networks. It is commonly known as TCP/***IP*** because the foundational ***protocols*** in the ***suite*** are the Transmission Control ***Protocol*** (TCP) and the ***Internet Protocol*** (***IP***).

53. How can we make use of the security of the Internet?

Security on the Web	Network security
Email privacy	Virus protection

When you use the Internet, ensure 4 following factors are guaranteed:
- Security on the Web
- Network security
- Email privacy
- Virus protection

54. How do you protect a message in email privacy?

The only way to protect a message is to put it in a sort of "envelope", that is, to encode it with some form of encryption

55. What do you do to avoid risks in security on the Web?

To avoid risks, you should set all security alerts to high on your Web browser.

56. What does SET stand for?

Secure electronic transactions

57. What are the most popular methods of protection in network security?

The most common methods of protections are passwords for access control, encryption and decryption systems, and firewalls.

58. How can you protect your PC from viruses?

If u want to protect your PC from virus, don't open email attachments from strangers and take care when downloading files from web(Plain text email alone can't pass a virus)
Remember to update your antivirus software as often as possible, since new viruses are being created all the time

BẢN DỊCH

1/ Cryptography was used to secure secret communications from military leaders

Cryptography was used to secure secret communications from military leaders, diplomats, spies and religious groups. The unprocessed readable information is called plaintext or plain data. The process of making the information unreadable is called encryption or ciphering. The result of encryption_is ciphertext cryptography. Reversing this process and retrieving the original readable information is called decryption or deciphering. To encrypt or decrypt information, an algorithm or so-called cipher is used.	Mật mã được sử dụng để bảo đảm thông tin liên lạc bí mật từ các nhà lãnh đạo quân sự, nhà ngoại giao, gián điệp và các nhóm tôn giáo. Thông tin có thể đọc được chưa qua xử lý được gọi là bản rõ hoặc dữ liệu thuần túy. Quá trình làm cho thông tin không thể đọc được được gọi là mã hóa hoặc mật mã. Kết quả của quá trình mật mã hóa bản mã mã hóa. Việc đảo ngược quá trình này và lấy lại thông tin có thể đọc được ban đầu được gọi là giải mã hoặc phiên mã. Để mã hóa hoặc giải mã thông tin, thuật toán hay còn gọi là mật mã được sử dụng.
How a cryptographic algorithm works, is controlled by a secret key, sometimes called password or passphrase. The key is known only to those who are authorized to read the information. Without knowing the key, it should be impossible to reverse the encryption process, or the time to attempt to reverse the process should required take so much time that the information would become useless.	Cách thức hoạt động của một thuật toán mật mã, được điều khiển bởi một khóa bí mật, đôi khi được gọi là mật khẩu hoặc cụm mật khẩu. Khóa chỉ được biết đối với những người được phép đọc thông tin. Nếu không biết khóa, sẽ không thể đảo ngược quá trình mã hóa, hoặc thời gian để cố gắng đảo ngược quá trình sẽ yêu cầu nhiều đến mức thông tin sẽ trở nên vô dụng.
Cryptanalysis or crypto-analysis is the *study* and analysis of existing ciphers or encryption algorithms, in order to *assess* their quality, to find weaknesses or to find a way to reverse the encryption process without having the key. Decryption without a key (often also without authorization) is a cryptanalytic attack, referred to as breaking or cracking a cipher.	Phân tích mật mã hay phân tích tiền điện tử là *nghiên cứu* và phân tích các mật mã hoặc thuật toán mã hóa hiện có, nhằm *đánh giá* chất lượng của chúng, tìm ra lỗ hổng hoặc tìm cách đảo ngược quá trình mã hóa mà không cần có khóa. Giải mã mà không có khóa (đôi khi không có ủy quyền) là một cuộc tấn công phân tích mật mã, được gọi là phá vỡ hoặc bẻ khóa mật mã.

A cryptanalytic attack can exploit weakness in the algorithm or crypto device itself, exploit its implementation procedures, or try out all possible keys. In general, there are two types of attack: The ciphertext-only attack, where the *cryptanalyst* has access to both ciphertext and its corresponding plaintext or assumed plaintext, to retríeve the corresponding key.	Một cuộc tấn công phân tích mật mã có thể khai thác lỗ hổng trong thuật toán hoặc bản thân thiết bị điện tử, khai thác các quy trình triển khai của nó hoặc thử tất cả các khóa có thể có. Nói chung, có hai kiểu tấn công: Tấn công chỉ sử dụng bản mã, trong đó *người phá mã* có quyền truy cập vào cả bản mã và bản rõ tương ứng hoặc bản rõ giả định, để lấy khóa tương ứng.
Cryptology comprises both cryptology (making) and cryptanalysis (breaking). The expression 'code', 'encoding' and 'decoding' are frequently used in cryptography. Code, however, is a simple replacement of information with other information, and doesn't use an algorithm. Generally, these are code books or tables that convert one value (letters, words or phrases) into another value (letter sequence, numerical value or special symbols).	Mật mã học bao gồm cả mật mã học (tạo) và phân tích mật mã (phá vỡ). Cụm từ 'mã', 'mã hóa' và 'giải mã' thường được sử dụng trong mật mã. Tuy nhiên, mã là sự thay thế thông tin đơn giản bằng thông tin khác và không sử dụng thuật toán. Nói chung, đây là những cuốn sách hoặc bảng mã chuyển đổi một giá trị (chữ cái, từ hoặc cụm từ) thành một giá trị khác (chuỗi chữ cái, giá trị số hoặc ký hiệu đặc biệt). đâu?
Cryptography, on the other hand, uses an algorithm (often a combination of fractioning, transposition and substitution) to manipulate the information. Although technically wrong, the expression 'encoding' is often used to indicate encryption or enciphering and one should therefore look at the context in which such expressions are used.	Mặt khác, mật mã học sử dụng một thuật toán (thường là sự kết hợp của phân số, chuyển vị và thay thế) để thao tác thông tin. Mặc dù sai về mặt kỹ thuật, cụm từ 'mã hóa' thường được sử dụng để biểu thị tái cấu trúc hoặc tái sắp xếp, do đó ta nên xem xét ngữ cảnh mà các cụm từ đó được sử dụng.

2/• So far we have assumed that our cryptographic algorithms are being used to provide

• So far we have assumed that our cryptographic algorithms are being used to provide confidentiality. However, there are many other applications. Whenever we use cryptography it is important that we check that it is helping us achieve our desired objectives. We illustrate a potential misuse of cryptography with an example.	• Cho đến nay, ta giả định rằng các thuật toán mật mã đang được sử dụng đều cung cấp tính bảo mật. Tuy nhiên, có rất nhiều ứng dụng khác. Bất cứ khi nào chúng ta sử dụng mật mã, điều quan trọng là chúng ta phải kiểm tra xem nó có đang giúp chúng ta đạt được các mục tiêu mong muốn hay không. Chúng tôi minh họa việc sử dụng sai mật mã bằng một ví dụ.
• In 1983 MGM produced a film called War Games. It became a cult film that highlighted the dangers of hacking: One synopsis describes the film by saying The fate of mankind rests in the hands of a teenager who accidentally taps into the Defence Department's tactical computer'. Its opening scene showed the teenager hacking into his university's computer system and changing his girlfriend's grades. At that time, many universities were storing examination results on databases that could be accessed remotely. Not surprisingly, they were concerned that their results might be vulnerable to the type of unauthorized manipulation depicted in the film and wanted to introduce appropriate protection.	• Năm 1983 MGM sản xuất một bộ phim mang tên War Games. Nó đã trở thành một bộ phim đình đám nêu bật sự nguy hiểm của việc hack: Nội dung của phim nói về số phận của nhân loại nằm trong tay của một thiếu niên, kẻ đã vô tình xâm nhập vào máy tính chiến thuật của Bộ Quốc Phòng. Cảnh mở đầu cho chúng ta thấy cậu thiếu niên đã tấn công vào hệ thống máy tính của trường đại học nơi mà cậu theo học để sửa điểm cho bạn gái. Tại thời điểm mà bộ phim công chiếu, rất nhiều trường đại học lưu trữ kết quả chấm thi trên cơ sở dữ liệu với cơ chế truy cập từ xa. Không ngạc nhiên khi họ lo ngại rằng kết quả của họ có thể bị thay đổi bởi kiểu truy cập trái phép được mô tả trong phim và muốn có biện pháp bảo vệ thích hợp.
• One proposal was to encrypt each student's grades. However, this did not really achieve the objective and it is both important and interesting to understand why. It is easy to see what encrypting the grades achieves. The result is that anyone who hacks into the database does not see the grade of any individual student. Instead they see meaningless data attached to each name.Unfortunately, this does not necessarily prevent constructive alteration of grades by hackers. If a hacker has failed, but happens to know that a specific student has good grades, then they merely change the meaningless data by	Một đề xuất được đưa ra là mã hóa điểm của mỗi học sinh. Tuy nhiên, điều này không thực sự đạt được kết quả mong muốn và nó vừa quan trọng lẫn thú vị để hiểu được lý do. Thật dễ dàng để có thể xem được điểm số đã được mã hóa. Kết quả đạt được là bất kỳ ai tấn công trái phép vào hệ thống cơ sở dữ liệu sẽ không thể tìm thấy được điểm của bất cứ học sinh nào. Thay vào đó, họ thấy những dữ liệu vô nghĩa được đính kèm với những cái tên. Nhưng thật không may, điều này lại không thiết yếu để ngăn chặn sự thay đổi mang tính suy diễn của hacker. Giả sử nếu một hacker bị trượt bài kiểm tra, nhưng trong trường hợp biết được một học sinh cụ thể

their name so that it is identical to that associated with the other student. Of course, if they do not know the precise grades of the other student, then they do not know their newgrades. Nevertheless, they know that they now have a pass grade. This is just one of many instances where the use encryption fails to meet the user's objectives. It is not the answer to all problems. Note also that, in this particular example, the algorithm has not been broken. In fact it has not even been attacked. All that has happened is that the failed to analyse the problem correctly.	đạt được điểm cao, thì họ chỉ việc thay đổi dữ liệu vô nghĩa bằng tên của họ để nó giống với dữ liệu liên quan của học sinh kia. Tất nhiên, nếu họ không biết điểm chính xác của học sinh kia thì họ cũng không biết được điểm mới của mình. Nhưng, họ biết rằng bây giờ họ đã đạt được điểm cao. Đây là một trong nhiều trường hợp mã hóa không đáp ứng được mục tiêu cho người dùng. Nó không phải là câu trả lời cho mọi vấn đề. Lưu ý rằng trong ví dụ cụ thể này, thuật toán mã hóa không hề bị phá vỡ. Trong thực tế nó còn chưa hề bị tấn công. Tất cả những gì xảy ra là do không phân tích được vấn đề một cách chính xác

3/ Data Encryption Standard (DES) , Advanced Encryption Standard (AES)

Data Encryption Standard (DES) Some modern block substitution ciphers are the Data Encryption Standard (DES), the Advanced Eneryption Standard (AES), and the newer GK-Crypt algorithm. The Data Encryption Standard treats each block of 8 bytes, or 64 bits, as 16 units of 4-bits each. (4-bit units are sometimes called nibbles or nybbles.) The left half of the block is used to generate eight 4-bit quantities. These 32 bits are permuted (shuffled) in a fixed manner and then exclusive-ored (combined) with the right half. Then the left and right halves are swapped, and this operation is repeated for 16 rounds. (There are also some bit permutations at the beginning and end, but they add no strength. They are there to make the encryption hard to simulate in software.) The DES was state-of-the-art for the mid-1970's, but its small 56-bit key size made it obsolete by about 1990. The trend has been away from bitwise hardware-oriented encryption. Advanced Encryption Standard (AES) The Advanced Encryption Standard (AES) is also a block cipher, using a block size of 16 bytes, or 128 bits, and a key size of 128 bits in current implementations. The key may be increased to 192 bits or 256 bits in the future, when 128 becomes inadequate. The first step in AES is to expand the key to 128 bytes, to make 10 round keys of 16 bytes each. This is done by performing repeated substitution and exclusive-or operations on the key bytes. The 10 round keys are then used to perform 10 rounds of encryption. Each round consists of 3 steps, First the message is combined with the key using an exclusive-or operation. In the second step the 16-byte message is considered as 4 words of 4	Tiêu chuẩn mã hóa dữ liệu(DES) Một số mật mã thay thế khối hiện đại gồm có Tiêu chuẩn mã hóa dữ liệu (DES), Tiêu chuẩn mã hóa nâng cao (AES) và thuật toán GK-Crypt mới. Tiêu chuẩn Mã hóa Dữ liệu coi mỗi khối 8 byte, hoặc 64 bit, là 16 đơn vị 4 bit. (Đơn vị 4 bit đôi khi được gọi là nibbles hoặc nybbles.) Nửa trái của khối được sử dụng để tạo ra tám đại lượng 4 bit. 32 bit này được hoán vị (xáo trộn) một cách cố định và sau đó được tính toán độc quyền (kết hợp) với nửa bên phải. Sau đó, hai nửa bên trái và bên phải được đổi chỗ cho nhau, và thao tác này được lặp lại trong 16 vòng(lần). (Cũng có một số hoán vị bit ở đầu và cuối, nhưng chúng không làm cho mã hóa mạng hơn. Chúng ở đó để làm cho mã hóa khó được mô phỏng trong phần mềm.) DES là phương pháp hiện đại nhất vào giữa những năm 1970, nhưng kích thước khóa nhỏ với 56-bit của nó đã khiến nó trở nên lỗi thời vào khoảng năm 1990. Xu hướng không còn là mã hóa theo hướng phần cứng cấp bit nữa. Tiêu chuẩn mã hóa nâng cao (AES) Tiêu chuẩn mã hóa nâng cao (AES) cũng là một mật mã khối, sử dụng kích thước khối là 16 byte hoặc 128 bit và kích thước khóa là 128 bit trong các triển khai hiện tại. Khóa có thể được tăng lên 192 bit hoặc 256 bit trong tương lai, khi 128 bit trở nên không đủ dài. Bước đầu tiên trong AES là mở rộng khóa lên 128 byte, tạo thành 10 vòng khóa, mỗi khóa 16 byte. Điều này được thực hiện bằng cách thực hiện các phép toán thay thế và loại trừ lặp đi lặp lại trên các byte khóa. 10 vòng khóa sau đó được sử dụng để thực hiện 10 vòng mã hóa. Mỗi vòng bao gồm 3 bước, Đầu tiên thông điệp được kết hợp với khóa bằng cách sử dụng một phép toán độc quyền. Trong bước thứ hai, thông điệp 16 byte được coi là 4 từ, mỗi từ 4 byte.

bytes each. These 4 words are shifted left by 1, 2, 3 and 4 byte positions, respectively. In the third step each column of the 4x4 block of bytes is mixed using a linear transformation, that is, each column vector is multiplied by certain matrix of values.	4 từ này được dịch chuyển sang trái lần lượt các vị trí 1, 2, 3 và 4 byte. Trong bước thứ ba, mỗi cột của khối 4x4 byte được trộn bằng cách sử dụng một phép biến đổi tuyến tính, tức là mỗi vectơ cột được nhân với một ma trận giá trị nhất định.
This last step is called a Hill cipher for Lester Hill who invented it around 1920. It was used by both the US and Russian military in the period between the two World Wars. Methods for breaking the Hill cipher were developed by Jack Levine at UNC Raleigh. Some features of the AES are it has a fixed block size, it uses the same key for every block, it uses the same permutation in every round, and the permutations are simple shifts applied within a single 4-byte word.	Bước cuối cùng này được gọi là mật mã Hill cho Lester Hill, người đã phát minh ra nó vào khoảng năm 1920. Nó được cả quân đội Mỹ và Nga sử dụng trong thời kỳ giữa hai cuộc Thế chiến. Các phương pháp phá mật mã Hill được phát triển bởi Jack Levine tại UNC Raleigh. Một số tính năng của AES là nó có kích thước khối cố định, nó sử dụng cùng một khóa cho mọi khối, nó sử dụng cùng một hoán vị trong mỗi vòng và các hoán vị là những sự thay đổi đơn giản được áp dụng trong một từ 4 byte.

4/ An intrusion detection system (IDS) is a device or software application that monitors

An intrusion detection system (IDS) is a device or software application that monitors a network or systems for malicious activity or policy violations. Any malicious activity or violation is typically reported either to an administrator or collected centrally using a security information and event management (SIEM) system. A SIEM system combines outputs from multiple sources and uses alarm filtering techniques to distinguish malicious activity from false alarms. Information security intrusion detection systems (IDSS) became commercially available in the late 1990s. An IDS works like a burglar alarm in that it detects a violation (some system activity analogous to an opened or broken window) and activates an alarm. This alarm can be audible and/or visual (producing noise and lights, respectively), or it can be silent (an e-mail message or pager alert). With almost all IDSS, system administrators can choose the configuration of the various alerts and the alarm levels associated with each type of alert. Mary IDSS enables administrators to configure the systems to notify them directly of trouble via e-mail or pagers. The systems can also be configured-again like a burglar alarm-to notify an external security service organization of a "break-in." The configurations that enable IDSS to provide customized levels of detection and response are quite complex. A current extension of IDS technology is the intrusion prevention system (IPS), which can detect an intrusion and also prevent that intrusion from SUccessfully attacking the organization by means of an active response. Because the two systems often coexist, the combined term intrusion detection and prevention system (IDPS) is generally used to describe current anti-intrusion technologies.	Hệ thống phát hiện xâm nhập (IDS) là một thiết bị hoặc ứng dụng phần mềm mục đích giám sát mạng hoặc hệ thống để tìm hoạt động phá hoại hay vi phạm chính sách. Mọi hoạt động phá hoại hay vi phạm thường được báo cáo cho quản trị viên hoặc được thu thập tập trung bằng cách sử dụng hệ thống quản lý sự kiện và thông tin bảo mật (SIEM). Hệ thống SIEM kết hợp các đầu ra từ nhiều nguồn và sử dụng kỹ thuật lọc cảnh báo để phân biệt hoạt động độc hại với cảnh báo sai. Hệ thống phát hiện xâm nhập an toàn thông tin (IDSS) đã được thương mại hóa vào cuối những năm 1990. IDS hoạt động giống như một cảnh báo trộm ở chỗ nó phát hiện một hành vi vi phạm (một số thực thi của hệ thống tương tự như một cửa sổ mở hoặc bị hỏng) và kích hoạt một cảnh báo. Cảnh báo này có thể có tiếng và /hay hình ảnh (tạo ra tiếng ồn và ánh sáng tương ứng) hoặc có thể im lặng (một tin nhắn email hoặc cảnh báo máy nhắn tin). Với hầu hết tất cả các IDSS, quản trị viên hệ thống có thể chọn cấu hình của các cảnh báo khác nhau và các mức cảnh báo liên quan đến từng loại cảnh báo. Mary IDSS cho phép quản trị viên cấu hình hệ thống để thông báo trực tiếp cho họ về sự cố qua email hoặc máy nhắn tin. Các hệ thống cũng có thể được cấu hình lại giống như một hệ thống báo trộm - để thông báo cho một tổ chức dịch vụ an ninh bên ngoài về một "đột nhập". Các cấu hình cho phép IDSS cung cấp các mức phát hiện và phản hồi tùy chỉnh là khá phức tạp. Một phần mở rộng hiện tại của công nghệ IDS là hệ thống phòng chống xâm nhập (IPS), hệ thống này có thể phát hiện ra sự xâm nhập và cũng ngăn chặn sự xâm nhập đó tấn công tổ chức một cách thành công bằng một phản ứng tích cực. Bởi vì hai hệ thống thường cùng tồn tại, thuật ngữ kết hợp phát hiện và ngăn chặn xâm nhập (IDPS) thường được sử dụng để mô tả các công nghệ chống xâm nhập hiện tại.

One of the best reasons to install an IDPS is that they serve as deterrents by increasing the fear of detection among would-be attackers. If internal and external users know that an organization has an intrusion detection and prevention system, they are less likely to probe or attempt to compromise it, just as criminals are much less likely to break into a house that has an apparent burglar alarm, Another reason to install an IDPS is to cover the organization when its network cannot protect itself against known vulnerabilities or is unable to respond to a rapidly changing threat environment. There are many factors that can delay or undermine an organization's ability to secure its systems from attack and subsequent loss	Một trong những lý do tốt nhất để cài đặt IDPS là chúng đóng vai trò là biện pháp ngăn chặn bằng cách làm tăng nỗi sợ bị phát hiện giữa những kẻ tấn công. Nếu người dùng bên trong và bên ngoài biết rằng một tổ chức có hệ thống phát hiện và ngăn chặn xâm nhập, họ sẽ ít có khả năng thăm dò hoặc cố gắng xâm nhập nó, cũng như tội phạm ít có khả năng đột nhập vào một ngôi nhà có báo động trộm rõ ràng, một lý do khác cài đặt IDPS là để bảo vệ tổ chức khi mạng của tổ chức đó không thể tự bảo vệ khỏi các lỗ hổng đã biết hoặc không thể phản ứng với môi trường đe dọa thay đổi nhanh chóng. Có nhiều yếu tố có thể trì hoãn hoặc làm suy yếu khả năng của một tổ chức trong việc bảo vệ hệ thống của mình khỏi bị tấn công và những thất bại sau đó.

5/ One of the main attractions for users to have mobile phones is

One of the main attractions for users to have mobile phones is that they offer the ability to toum and to make telephone calls from almost anywhere. However, since the mobile phones are wireless, the phone message is transmitted across the airwaves until it reaches the nearest base station, where it is transferred to the fixed landline. Since intercepting radio signals is likely to be carsier than intercepting landline calls, one of the initial security requirements for GSM was that their mobile phones should be no less secure than the conventional fixed telephones. This requirement was satisfied by providing encryption for transmissions from the handset to the nearest base station. Another serious security Issue was the problem of the operator being able to identify the phone so that they knew whom to charge. Thus, for GSM, there were the following two major security requirements: confidentiality, which was a customer requirement and user authentication, which was a system requirement. Each user is issued with a personalized smart card, called a SIM, which contains a 128-bit secret authentication value known only to the operator. This value is then used as the key to a challenge- response authentication protocol using an algorithm, which can be selected by the operator: When the user attempts to make a call, their identity is transmitted to the system operator via a base station. Since the base station does not know the SIM's secret key and may not even know the authentication algorithm, the central system generates a challenge and sends it, with the response appropriate for the card, to the base station. This enables the base station to check the	Một trong những điểm hấp dẫn chính để người dùng sử dụng điện thoại di động là chúng cung cấp khả năng kết nối và gọi điện từ hầu hết mọi nơi. Tuy nhiên, vì điện thoại di động sử dụng đường truyền không dây, tin nhắn của điện thoại được truyền qua sóng điện từ cho đến khi nó đến trạm cơ sở gần nhất, nơi nó được chuyển đến tuyến đường truyền cố định. Vì việc chặn các tín hiệu vô tuyến dường như phức tạp hơn so với việc chặn các cuộc gọi trên đường dây cố định, một trong những yêu cầu bảo mật ban đầu đối với GSM là điện thoại di động của họ không được ít bảo mật hơn so với điện thoại cố định thông thường. Yêu cầu này đã được thỏa mãn bằng cách cung cấp mã hóa cho các đường truyền từ thiết bị cầm tay đến trạm cơ sở. Một vấn đề bảo mật nghiêm trọng khác là vấn đề nhà điều hành có thể nhận dạng điện thoại để họ tính phí sử dụng đúng người. Do đó, đối với GSM, có hai yêu cầu bảo mật chính sau đây: tính bảo mật, một là yêu cầu của khách hàng và xác thực người dùng, một là yêu cầu hệ thống. Mỗi người dùng được đăng ký một thẻ thông minh cá nhân, gọi là SIM, chứa giá trị xác thực bí mật 128-bit mà chỉ nhà điều hành mới biết. Giá trị này sau đó được sử dụng làm chìa khóa cho một giao thức xác thực phản hồi phức tạp bằng cách sử dụng một thuật toán, có thể được lựa chọn bởi nhà điều hành: Khi người dùng cố gắng thực hiện cuộc gọi, danh tính của họ sẽ được truyền tới nhà điều hành hệ thống thông qua một trạm cơ sở. Vì trạm cơ sở không biết khóa bí mật của SIM và thậm chí có thể không biết thuật toán xác thực, hệ thống trung tâm tạo ra một thách thức và gửi nó, với phản hồi thích hợp với thẻ, đến trạm cơ sở. Điều này cho phép trạm cơ sở kiểm tra tính hợp lệ của phản hồi

validity of the response.	
In addition to the authentication algorithm the SIM also contains a stream cipher encryption algorithm, which is common throughout the network. This algorithm is used to encrypt the messages from the mobile phone to the base station. The key management for the encryption keys is ingenious and makes use of the authentication protocol. The authentication algorithm accepts a 128 bit challenge and computes a 128-bit respornse, which depends on the card's authentication key. However, only 32 bits are transmitted from the SIM to the base station as the response.	Ngoài thuật toán xác thực, SIM còn chứa một thuật toán mã hóa dòng/luồng, thuật toán này phổ biến trong toàn mạng. Thuật toán này được sử dụng để mã hóa các thông điệp từ điện thoại di động đến trạm cơ sở. Việc quản lý khóa cho các khóa mã hóa rất tinh xảo và tận dụng được giao thức xác thực. Thuật toán xác thực chấp nhận độ phức tạp 128 bit và tính toán một phản hồi 128 bit, thứ phụ thuộc vào khóa xác thực của thẻ. Dù vậy, chỉ có 32 bit được truyền từ SIM đến trạm cơ sở dưới dạng một phản hồi
This means that when the authentication process has been completed there are 96 bits of secret information known only to the SIM, the base station, and the host Computer. Of these bits, 64 are then allocated for the determination of the encryption key. Note that the encryption key changes every time that authentication takes place.	Điều này có nghĩa là khi quá trình xác thực đã hoàn tất, có 96 bit xác thực bí mật chỉ được biết đến bởi SIM, trạm cơ sở và máy chủ. Trong số các bit này, 64 bit sau đó được cấp phát để xác định khóa mã hóa. Lưu ý rằng khóa mã hóa thay đổi mỗi khi quá trình xác thực diễn ra