Lecture 4 – Computer Security & Cryptography

Computer Security

- Threats to computer security include criminals, computer crimes, and other hazards.

- Computer criminals:
    - Employees
    - Outside users
    - Hackers and crackers
    - Organized crime
    - Terrorists

Computer Crimes have tripled in the past two years!

- Malicious Programs such as Viruses
- Internet scams, such as phishing
- Social networking risks
- Rogue Wi-Fi hotspots
- Data manipulation such as Computer Fraud

Other Hazards

- Natural hazards such as fires, floods, and tornadoes
- Civil strife and terrorism such as Wars, riots, and terrorist activities
- Technological failures such as Voltage surge or spike

Measures to Protect Computer Security

- Restricting access
- Encrypting data
- Anticipating disasters
- Preventing data loss

Measure	Description
Restricting	Limit access to authorized persons using such measures as passwords and firewalls
Encrypting	Code all messages sent over a network
Anticipating	Prepare for disasters by ensuring physical security and data security through a disaster recovery plan
Preventing	Routinely copy data and store it at a remote location

Restricting Access

- Passwords
- Biometric scanning such as Fingerprint scanners
- Iris (eye) scanners
- Firewalls

Guidelines for passwords :

- Easy to remember, hard to guess
- Don’t use family or pet names
- Don’t make it accessible
- Use combination uppercase/lowercase letters, digits and special characters
- Don’t leave computer when logged in
- Don’t ever tell anyone
- Don’t include in an email
- Don’t use the same password in lots of places

Typical Password Criteria

- Contain six or more characters
- Contain at least one uppercase and one lowercase letter
- Contain at least one digit
- Contain at least one special character

Good or Bad?

- nelldale
- JohnLewis
- GingerCat
- Longhorns
- aatnv.AATNV
- One2Three
- 7December1939
- red&whIte%blUe7
- g&OoD#3PaSs

Encrypting Data

- Encryption is the process of coding information to make it unreadable, except to those who have the key
- E-mail encryption
- File encryption
- Web site encryption
- Virtual private networks (VPNs)
- Wireless network encryption (WEP, WPA, and WPA2)

Substitution cipher

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

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

Substitute the letters in the second row for the letters in the top row to encrypt a message

Encrypt(COMPUTER) gives FRPSXWHU

Substitute the letters in the first row for the letters in the second row to decrypt a message

Decrypt(Encrypt(COMPUTER)) gives COMPUTER

Open ended Questions :

- What is a copyright?

- What is plagiarism? Discuss how computers make plagiarism easy and tempting to busy people and how a plagiarist can be easily identified.

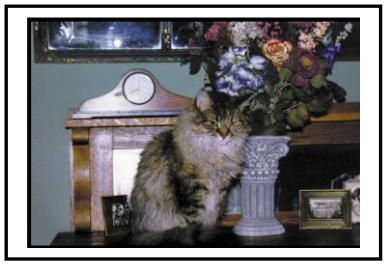
Artificial Intelligence (AI) and Social Issues /

Artificial Intelligence (AI)

Thinking Machines

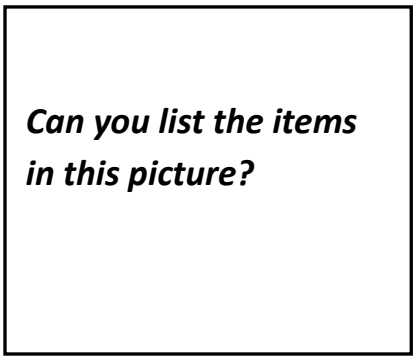
- A computer can do some things better - and certainly faster - than a human can.
- Adding a thousand four-digit numbers
- Counting the distribution of letters in a book
- Searching a list of 1,000,000 numbers for duplicates
- Matching fingerprints

BUT a computer would have
difficulty pointing out the cat in
this picture, which is easy for a human.



Humans do best

Can you list the items in this picture?



Computers do best

Can you :

count the distribution of letters in* a *book?

Add a thousand 4-digit* numbers*?

Match finger prints?

Search a list of a* million *values

for duplicates?

- **Artificial intelligence (AI)** The study of computer systems that attempt to model and apply the intelligence of the human mind.

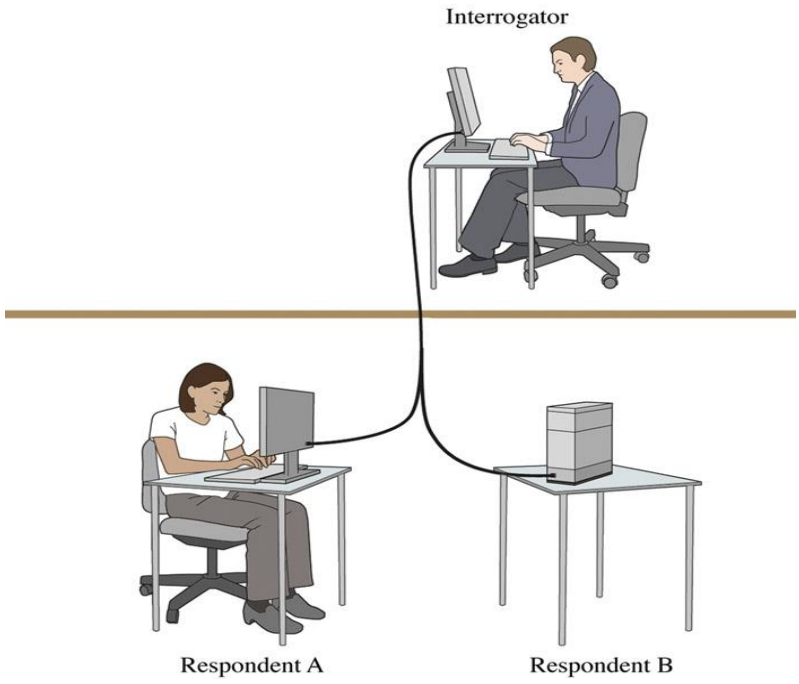
The Turing Test

In 1950 English **mathematician Alan Turing** wrote a landmark paper that asked the question:

Can machines think?

How will we know when we've succeeded?

The Turing Test



In a Turing test, the interrogator must determine which respondent is the computer and which is the human

The **Turing test** is used to empirically determine whether a computer has achieved intelligence

- **Weak equivalence** Two systems (human and computer) are equivalent in results (output), but they do not arrive at those results in the same way
- **Strong equivalence** Two systems (human and computer) use the same internal processes to produce results

Expert Systems

- **Expert system** A software system based the knowledge of human experts in a specialized field
    - An expert system uses a set of rules to guide its processing
    - The inference engine is the part of the software that determines how the rules are followed

Example: What type of treatment should I put on my lawn?

- NONE—apply no treatment at this time
- TURF—apply a turf-building treatment
- WEED—apply a weed-killing treatment
- BUG—apply a bug-killing treatment
- FEED—apply a basic fertilizer treatment
- WEEDFEED—apply a weed-killing and fertilizer combination treatment

An execution of our inference engine

- **System**: Does the lawn have large, bare areas?
- **User**: No
- **System**: Does the lawn show evidence of bugs?
- **User**: No
- **System**: Is the lawn generally thin?
- **User**: Yes
- **System**: Does the lawn contain significant weeds?
- **User**: Yes
- **System**: You should apply a weed-killing and fertilizer combination treatment.

Language Processing

- There are three basic types of processing going on during human/computer voice interaction.
    - Voice recognition—recognizing human words.
    - Natural language comprehension—interpreting human communication.
    - Voice synthesis—recreating human speech
- Common to all of these problems is the fact that we are using a natural language, which can be any language that humans use to communicate.

Limitations of Computing & Ethical Issues

- The computer can outperform human beings in speed, memory , repetition and accuracy.
- A computer can process data faster than any other machine designed to perform a similar task.

- It has memory. It has the capacity to remember what it has done. It can store instructions in its memory and follow these through unaided.

- A computer can tirelessly perform the same operations millions of times in exactly the same way without getting bored and tired the way a human clerk would.

- A computer's high-speed processing is accompanied by high-accuracy results. No other system can have as much accuracy as a computer system.

Blame it on the Computer : The computer has done this and that. Actually this is not the computer which has done this **but** the user. Despite its various features, a computer does have the following limitations:

a. No Self Intelligence

Today, a computer is able to do a work which is impossible for man. Computers are used to do risky and dangerous work and where sharp actually is needed. But it does not have any intelligence of its own. It works according to the instruction only.

b. No Decision-Making power

The computer cannot take any decision of its own. It does only those tasks which are already instructed to it.

c. No learning power

The computer has no learning power. Once you give instructions to a computer how to perform a task, the very task is cannot perform if you do not give it any instructions for the next time. For example, when you are taught how to solve a problem and it same type of problem is given to you to solve, then you can do it because you have learned how to solve the problem.

However, they do not have common sense. We can't teach it to think morally or ethically. It just does what we tell it to do. They will never experience human emotions or concepts...it will only provide us the foundation and **software** to allow us to enter them into its system, but they will not process it like humans do.

Its limitations is how much data we put into it. How much memory it has. Its life expectancy is how long the hardware survives. They get replaced easily because as the years passes, the technology and components get better. Their limitations is how we built them.

d. Programmed by Humans:

Though the computer is programmed to work efficiently, fast and accurately but it is programmed by human beings to do so. Without a program, a computer is nothing. A program is a set of instructions. Computer only follows these instructions. If the instructions are not accurate the working of the computer will not accurate as well .

e. Thinking:

The computer **can not** think itself. The concept of artificial intelligence shows that the computer can think. But still this concept is dependent on a set of instructions provided by the human beings.

f. Self Care:

A Computer cannot care itself like a human. A computer is dependent still to human beings for this purpose.

g. Retrieval of Memory:

A computer can retrieve data very fast but this technique is linear. A human being's mind does not follow this rule. A human mind can think randomly which a computer machine cannot.

h. Feelings:

One of the main limits in the computer is of feeling. A computer cannot feel about some like a human. A computer cannot meet human in respect of relations.

Human can feel, think and caring but a computer machine itself cannot.

A computer cannot take place of human because computer is always dependent of human.

Ethical Issues

Digital Divide

- *What is it?*
- *How does it affect you?*
- *What is the One Laptop per Child initiative?*
    - *Why are developing countries at such a disadvantage?*
- *How do smartphones relate to the issue?*

- The term 'digital divide' describes the fact that the world can be divided into **people who do and people who don't have access to - and the capability to use - modern information technology**, such as the telephone, television, or the Internet.

  The digital divide exists between those in cities and those in rural areas. For example, a 1999 study showed that 86% of Internet delivery was to the 20 largest cities. The digital divide also exists between the educated and the uneducated, between economic classes, and, globally, between the more and less industrially developed nations.