Security

Data Integrity:
- Data Integrity is making sure that data is correct / valid
- Ensures that data received is same as the data sent

  e.g: Parity Check

Data Privacy:
- keeps Data confidential
- only seen by authorized personel

Security:
- It is to keep data safe
- Prevention of data loss
- e.g: Data backup

Security Measures To Protect Computers

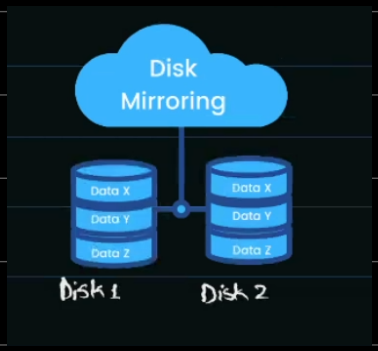
① Encryption

- Encryption scrambles the source code. / text (based on question)
- Using an encryption key
- If the file is accessed without authorization, it will be meaningless.
- It requires a decryption key to unscramble the algorithm.

② Data Backup

- A copy of data is made and stored elsewhere
- If the original data is lost, the backup can be used to restore data.

(3) Disk Mirroring



- Synchronisation

- The data is stored on two disks simultaneously
- If the first data disk drive fails, the data is accessed from the second disk.

(4) Firewall

- Prevents unauthorized access to the data
- Monitors incoming and outgoing traffic
- Blocks transmission from unauthorized sources/websites
- Maintains an allow list.
- Can be software or hardware both
- Can help to prevent hacking

⑤ User Account

- User has an username and password.
- Access to resources can be limited to specific account
- A person can not access system without valid username and password.

⑥ Anti-Malware

- Scans for malicious code (harmful code)
- Quarintines or deletes any malicious software found
- Scans can be scheduled at regular intervals

⑦ Access Rights

- Different access rights for individual / group
- To stop users from editing program

⑧ Physical Measure

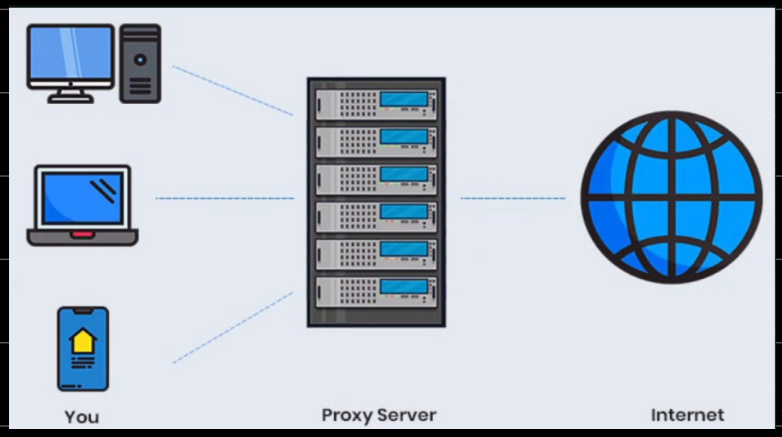
- Locked doors / keyboards
- Secure method of access.

Q- What are the other methods to protect data online?

- Running up to date anti virus
- Use of Proxy Server
- strong Biometrics / passwords

Proxy Server

- Acts as middle man and hides the public IP address of the user.



- Privacy ↑ increases + Security
- Cache memory in Proxy server reduces bandwidth usage
- Observes traffic

Q- What are the factors to consider when planning a data backup?

- How often should the data be backed up?

e.g: At the end of each day as students's progress may be edited each day

- What medium should the data be backed upto?

e.g: External Hard disk as it has larger capacity

- Where should the backup be stored?

e.g: off-site as if the building is damaged only the original data is lost.

- What is backed up?

e.g: only the updated file

- When should the backup take place?

e.g: over night

Malware

- Malware is a software that is intentionally designed to cause damage to a computer or server

Types of Malware

- Viruses
- Worms
- Logic bombs
- Trojan Horses
- Spyware

Q- Explain the term virus.

- Malicious code (Harmful code)
- that replicates itself
- can cause loss of data
- can cause computer to crash

- Expanding, so fills up HDD with data

- can fill up hard disk with data

Q- What are the ways to protect from virus?

- Use anti-virus
- Update anti-virus on regular basis.
- Avoid downloads from unknown sources
- Use a firewall
- Avoids suspicious websites

Virus

- Programs or program code that can replicate itself into another piece of software with the intention of deleting or corrupting files.

- Problem: Computer may stop working or files may get lost
- Solution: Run anti-virus software

- Requires host

Worms

- A standalone piece of software which can reproduce itself automatically and it does not require a host

Problem: Could corrupt user's computer // delete data // consumes bandwidth

Solution: Run anti-virus software in the background // keep OS uptodate // not connected on internet.

Logic Bombs

- Code embedded in a program on a computer. When certain conditions are met (such as specific date) they are activated to carry out tasks such as deleting files or sending data to a hacker. (May be part of worms/viruses)

Trojan Horse

- Malicious Program often disguised as legitimate software with the intent of harming the computer

Same as that greek horse story, where the soldiers hid inside a horse and when they entered the city, they attacked.

Spyware

- Software that gathers info by monitoring e.g: key presses on user's keyboard
- The info is then sent back to the person who sent the software.

Solution: Anti-spyware software // limited use of keyboard, use on screen keyboard

Phishing

- Someone sends emails to users, when clicked, takes the user to fake website, so they could obtain somebody's confidential data or to install malware.

Problem: Identity Fraud // misuse of financial data

Solution: Ignore suspicious emails and undergo frequent security awareness training.

Pharming

- Malicious code installed on user's computer or web server. The code redirects the user to fake website

Data Integrity

Validation: Checks that data entered is reasonable

Verification: Checks that data entered is same as the original

Validation

- **Range Check:** Checks that whether the data entered is b/w a lower and upper limit. e.g: using 13 as months or -120 as age

- **Format Check:** Checks whether the data has been entered in the agreed format e.g: format of date : dd/mm/yyyy

- **length Check:** Checks whether data has required number of characters. e.g: Phone number should contain 7 numbers

- **Presence Check:** Checks to make sure a field is not left empty when it should contain data. e.g: verification code should be present.

- **Existence Check:** Checks if data in a file or filename actually exists. e.g: registered name is found

- **Limit Check:** Checks only one of the limits (such as upper limit or lower limit)
  e.g: 1.5 litre only

Verification

- Is a way of preventing errors when data is entered manually using a keyboard or when data is transferred from one computer to another

Verification During Data Entry

① Double Entry ② Visual Check ③ Check digit

Double Entry: Data is entered twice, using two different people and then compared

Visual Check: Entered data is compared with the original document

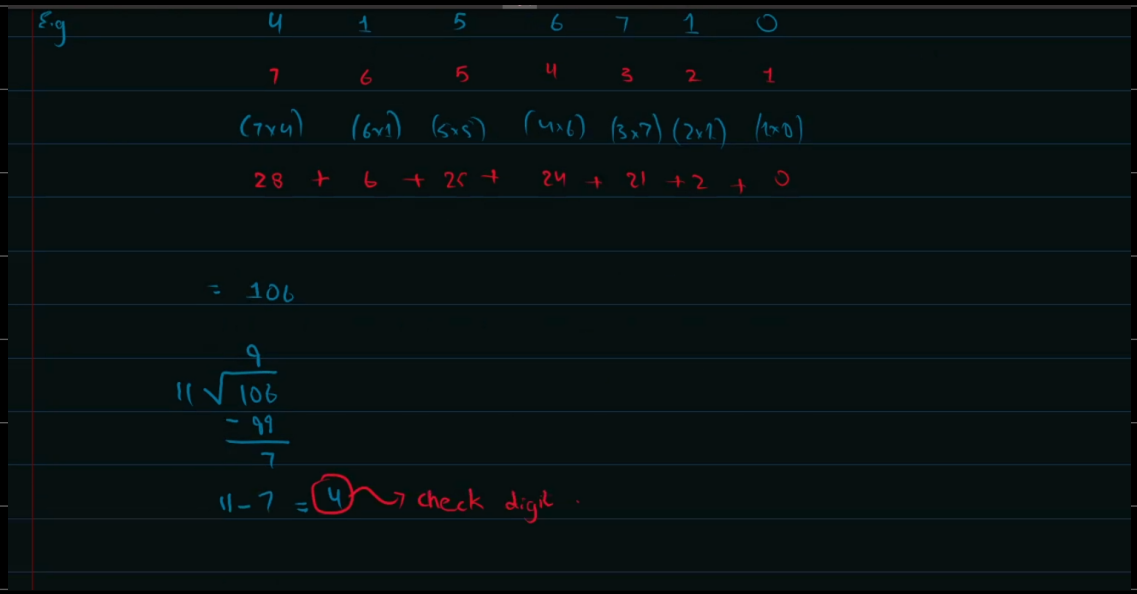
Check Digit: Is an additional digit added to a number

Method For calculating Check Digit

1. Each digit in the number is given a weighting e.g: 7, 6, 5, 4, 3, 2, 1

2. The digit is multiplied by its weighting and then each value is added to make a total.

3. The total is divided by 11 and the remainder subtracted from 11.

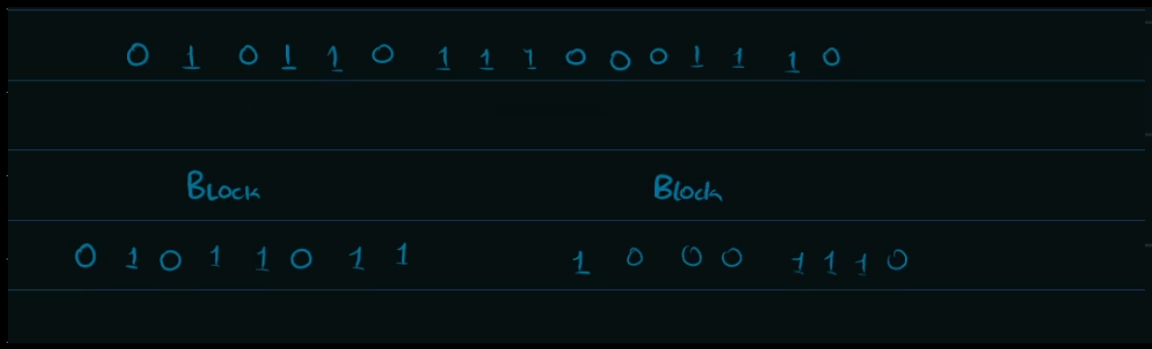


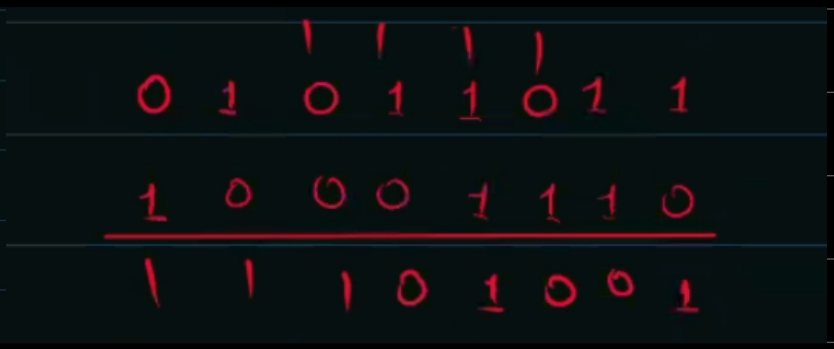
Verification During Data Transfer

① Checksum ② Parity Check ③ Automatic Repeat Request

Checksum

- bytes sent as a block
- bytes added up before transmission
- Results of addition is sent with the data block.
- same calculation is carried out at receiver's end.
- The two values are compared





- Original method is in Sir's notes. (not included)

Parity Check

- Even Parity (Even number of 1's)
- Odd Parity (odd number of 1's)

5 Parity checks are often used to check for errors that may occur during data transmission.

(a) A system uses **even parity**.

Tick (✓) to show whether the following three bytes have been transmitted correctly or incorrectly.

Received byte	Byte transmitted correctly	Byte transmitted incorrectly
11001000		✓
01111100		✓
01101001	✓	

[3]

The word "F L O W C H A R T" was transmitted using nine bytes of data (one byte per character). A tenth byte, the parity byte, was also transmitted.

The following block of data shows all ten bytes received after transmission. The system uses **even parity** and column 1 is the parity bit.

	letter	column 1	column 2	column 3	column 4	column 5	column 6	column 7	column 8
byte 1	F	1	0	1	0	0	1	1	0
byte 2	L	1	0	1	0	1	1	0	0
byte 3	O	1	0	1	0	1	1	1	1
byte 4	W	1	0	1	1	0	1	1	1
byte 5	C	1	0	1	0	0	0	1	1
byte 6	H	0	0	1	0	1	0	0	0
byte 7	A	0	0	1	0	0	1	0	1
byte 8	R	1	0	1	1	0	0	1	0
byte 9	T	1	0	1	1	0	1	0	0
parity byte		1	0	1	1	1	1	1	0

(i) **One** of the bits has been transmitted incorrectly.

Write the byte number and column number of this bit:

Byte number 7

Column number 6

[2]

Q- How a parity block check can identify a bit that has been corrupted?

- Each byte has a parity bit
- An additional parity byte is sent with vertical and horizontal parity
- Each row and column must have an even or odd number of 1's.
- Identify the incorrect row and column
- The intersection is the error.

Automatic Repeat Request (ARQ)

- ARQ uses **acknowledgement** (a message sent to the sender indicating that data has been received correctly) and **timeout** (time interval allowed to elapse before an acknowledgement is received)

- When receiving device detects an error, it asks for the data packet to be resent The sending device will resend the data if negative acknowledgement or timeout has occurred. If no error is detected, then positive acknowledgement is sent.