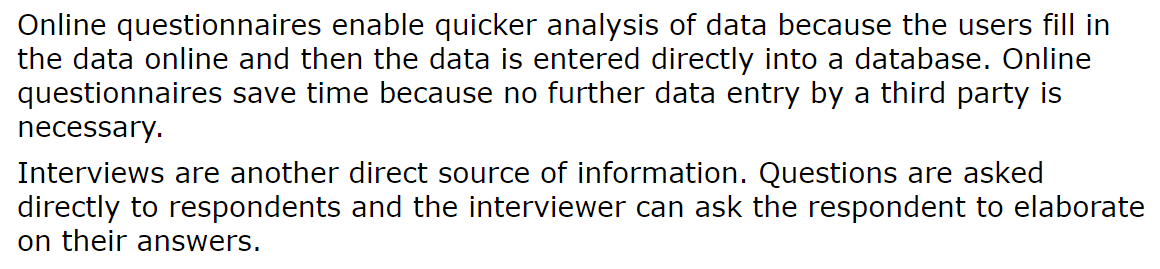
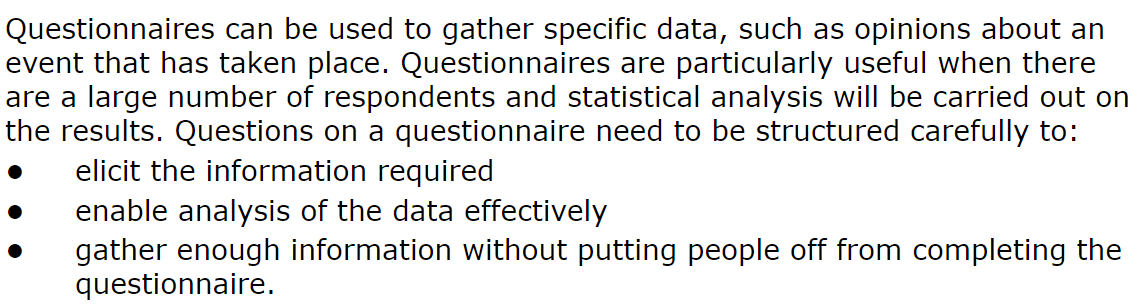




|  |  |
| --- | --- |
| Data | Context and meaning |
| evmaybe | Without context or meaning this is just a random word but its actually an Instagram username of a non binary person now its information |
| Vardaan | Without context or meaning this is just a random name but its actually the name of a short white individual now its information |
|  | Without context or meaning this is just a random picture but its actually my quite impressive COC (Clash Of Clans) base now its information |

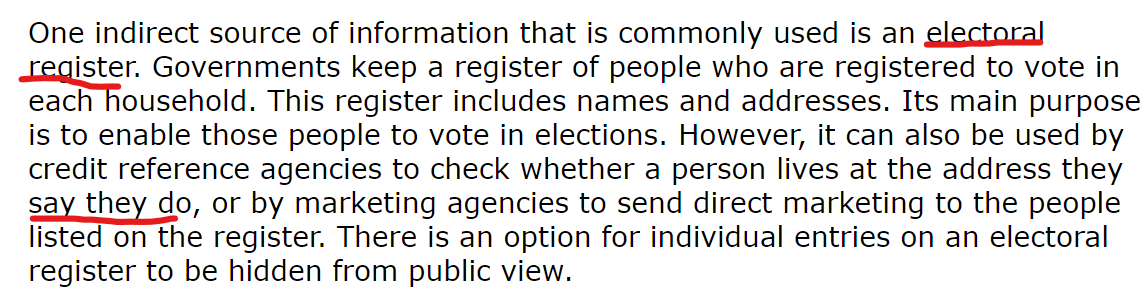
Direct data source also known as primary source means the data is used for the same purpose that it is collected for eg. The eng research thing we doing



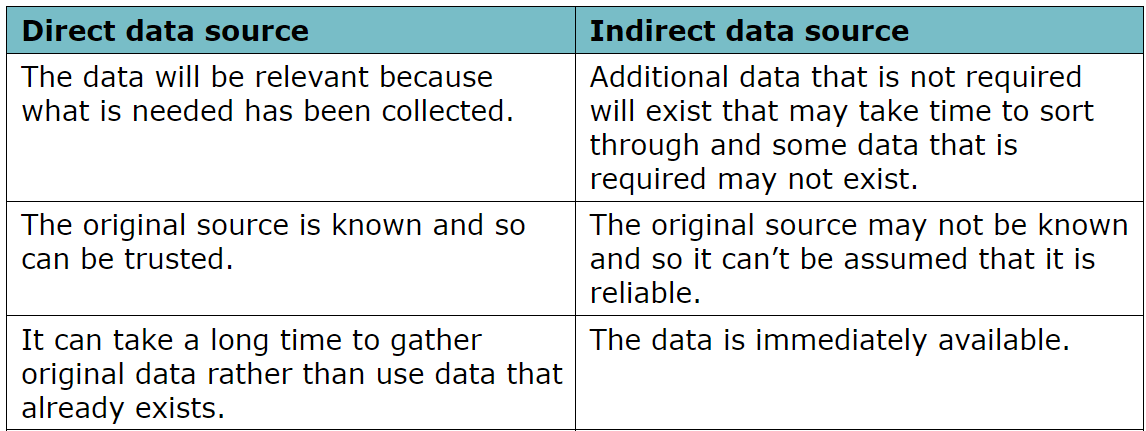
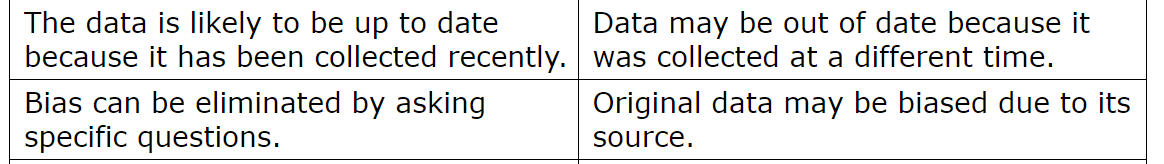
Observation people will observe to collect data they can be active (involved) or passive (just seeing)

* Pros - First hand information, unobtrusive (passive), detailed information, can be replicated, multiple interpretations.
* Cons - Time consuming, observer bias, limited generalizability, limited access, ethics, hawthorne effect.

Indirect data source or secondary source is when data is collected for some other purpose but ur taking the data for eg. Like a company sells u data or smthin and u use for ur purpose



Businesses can collect personal information from third parties to advertise more efficiently and make their products better



**Quality of information (1.2)**

* Accuracy - the data needs to be correct or then like whats the use yk for eg. The cost of a pack of beers is 495 rupees but you enter it as 3000 rupees (you added an extra zero by mistake) (also do not ask me why ik the price for a pack of beers!)
* Relevance – the information needs to be relevant like if we talking about the amount of profit a shop makes there is no use if there is an info about how 49.1% of all people dying are cause of smoking soo ye
* Age – the information needs to be up to date eg. U want to change sm setting in windows but the only tutorial u can find is win 10 ka but u have win 11 and the navigation to tht setting is a bit diff so then there is no use of tht info as it is not up to date.
* Level of detail – right amount of info needs to be there if info is too less then there is no use only but like if the lvel of detail is too high we will have to like sort through the needed info just like how im ranting here but u just want to know what level of detail is, but like too much info is better than lesss info cause then atleast u can sort it.
* Completeness – im just gonna give eg for this one so like ye if smone tells u there is IT exam tomm tht is still info but it aint complete cause they didn’t say what all chps are there so the information you got is not good quality (if you want some good quality stuff I have it msg me).

**Encryption (1.3)**

Encoding refers to the process of converting information from one form or format to another.

Which means if ur converting digital data to analogue data its encoding \*\*\*\*\*\*\*\*\*

Encryption is when data is scrambled so it cannot be understood

Encryption is important when sending personal sensitive data across a network or the internet

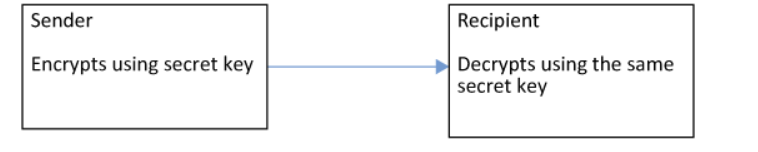
Caesar cipher is basiclally like the algorithm the data goes through to become encrypted like +3 or smthin

2 Types of encryption

* Symmetric – data is encrypted using secret key the secret key and the data is sent over like over the internet and after u receive u decrypt data by using the same secret key.

Adv – its fast

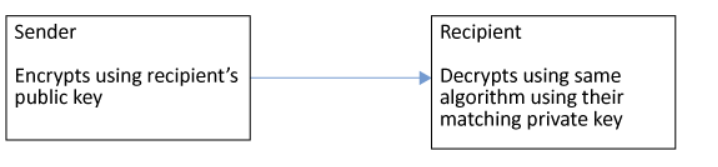
Dis adv – its not secure cause if smone like intercepts thw data they will get the scret key also then they can easily decrypt the data

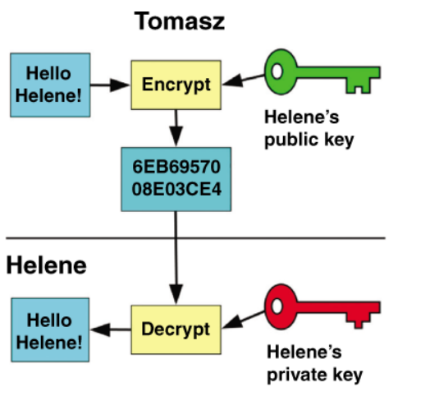


* Asymmetric - the sender encrypts the data with ur public key then you get the data then like u use ur private key to decrypt the data

Adv – its very secure as only u have ur private key

Dis adv – its slow cause many steps



recreate this thing

Applications of encryption is in hard rives and all

Then https websites again its simple

When a browser requests a secure page, it will check the digital certificate to ensure that it is

trusted, valid and that the certificate is related to the site from which it is coming. The

browser then uses the public key to encrypt a new symmetric key that is sent to the web

server. The browser and web server can then communicate using a symmetric encryption

key, which is much faster than asymmetric encryption.

1. **Handshake Phase**:
   * **Client Hello**: The client (e.g., web browser) initiates a connection to the server by sending a "ClientHello" message. This message includes information like the highest TLS version supported, a list of supported cryptographic algorithms (cipher suites), and a random number.
   * **Server Hello**: Upon receiving the ClientHello message, the server responds with a "ServerHello" message. This message includes the selected TLS version, the chosen cipher suite from the client's list, and another random number.
   * **Server Certificate**: The server sends its digital certificate to the client. The certificate contains the server's public key and is used to establish the server's identity.
   * **Server Hello Done**: The server indicates that it has completed its part of the handshake.
2. **Session Establishment**:
   * **Finished**: Both the client and server exchange "Finished" messages to confirm that the handshake was successful and that they are ready to begin secure communication using the negotiated session keys.
3. **Secure Data Transfer**:
   * **Application Data Exchange**: Once the secure session is established, the client and server can securely exchange application data (e.g., HTTP requests and responses, email content) using the agreed-upon encryption algorithms and session keys.

Throughout these steps, SSL/TLS ensures data confidentiality, integrity, and authentication by encrypting data transmitted between the client and server, preventing eavesdropping, tampering, and impersonation. Each SSL/TLS connection involves negotiating cryptographic parameters and keys to establish a secure channel for data transmission.

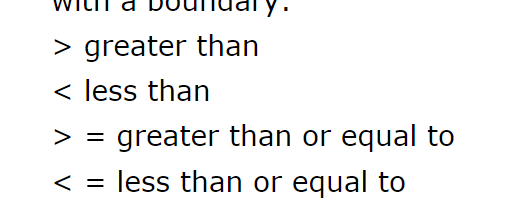
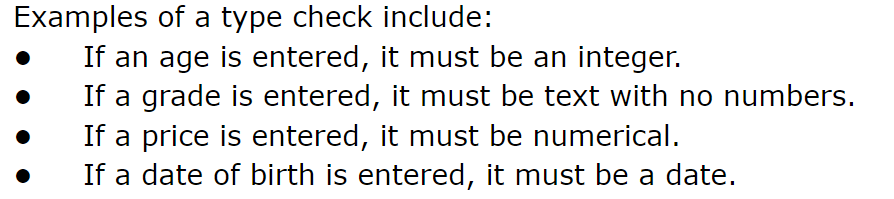
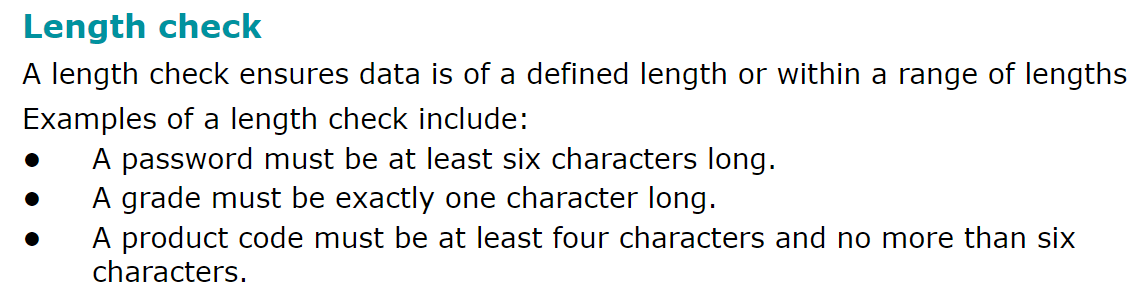
Email uses asymmetric

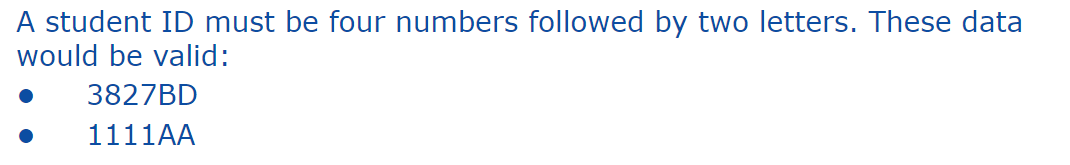
Hard disk

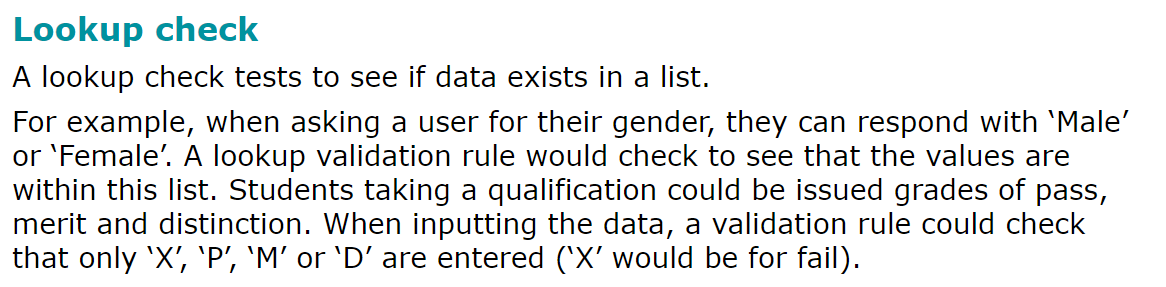
Disk encryption involves securing all data stored on a disk by encrypting every bit of information, ensuring comprehensive protection. Unlike encrypting individual files, disk encryption requires an encryption key to access any file on the disk. This encryption method extends beyond disks to other storage media like USB flash drives and backup tapes, which are susceptible to loss or theft due to their portability. Encrypting these devices prevents unauthorized access, as the encrypted data is indecipherable without the encryption key. Access to encrypted data is typically granted through password entry or biometric authentication like fingerprint scanning. Overall, disk encryption safeguards data on storage media, mitigating risks associated with data loss or theft.

**Checking accuracy of data (1.4)**

Validation (when ur entering data only)

* Presence check – it is used to see if data is entered eg. Mandatory fields
* Range check – it is used to ensure that data is entered within a range for eg. Like ur birthday u cant put 01-13-23
* Type check - 
* Length check - 

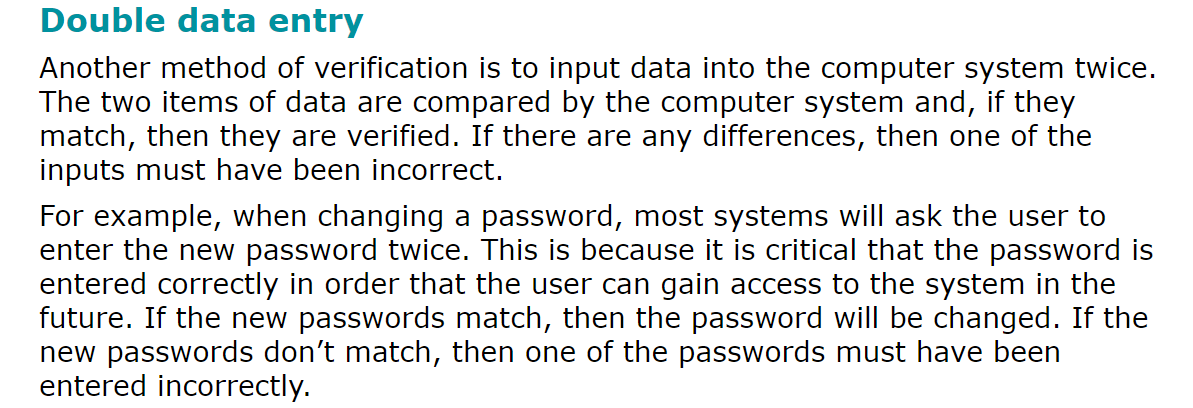
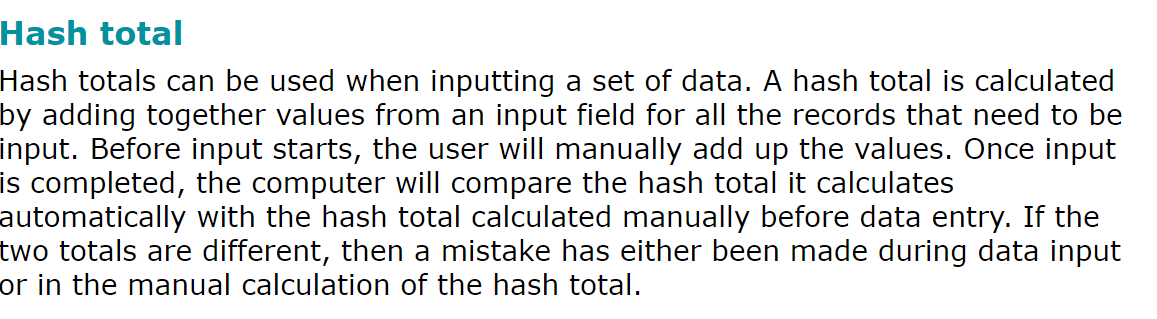
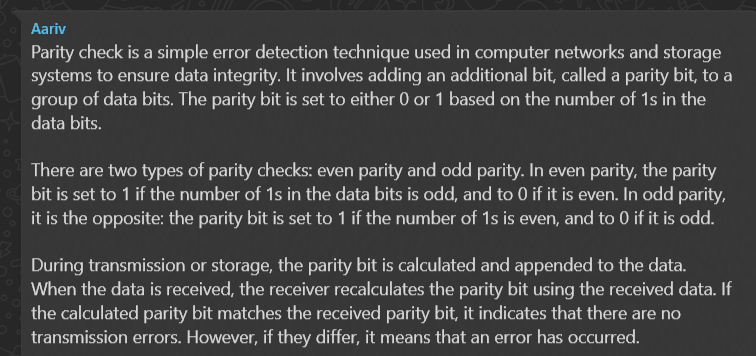
Format check – if u log into ur company website maybe its mandatory tht u have xxx.com like [aastik@xxx.com](mailto:aastik@xxx.com) not gmail.com

* Lookup check - 

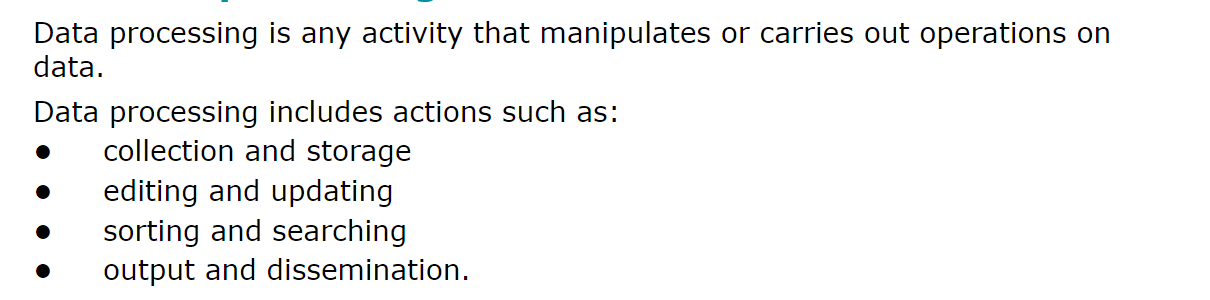
If in the first eg. Other is not there then it will give error

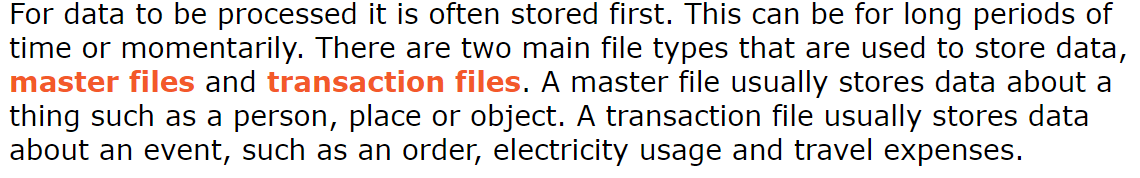
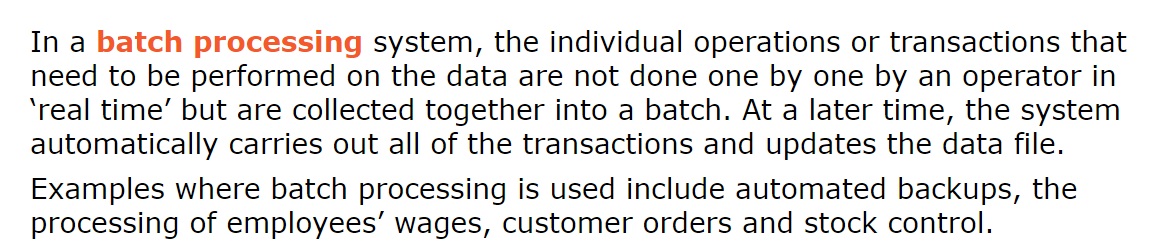
* Consistency check – compares data in one field with data from another field that already exists within a record for eg u enter ur address in one field and in another its diff.
* Check digit – mostly used in barcodes algorithm performed which generated a number like 4 or smthin then once u enter it will use same algorithm to generate number if it’s a diff num tht means data is inputed incorrectly.

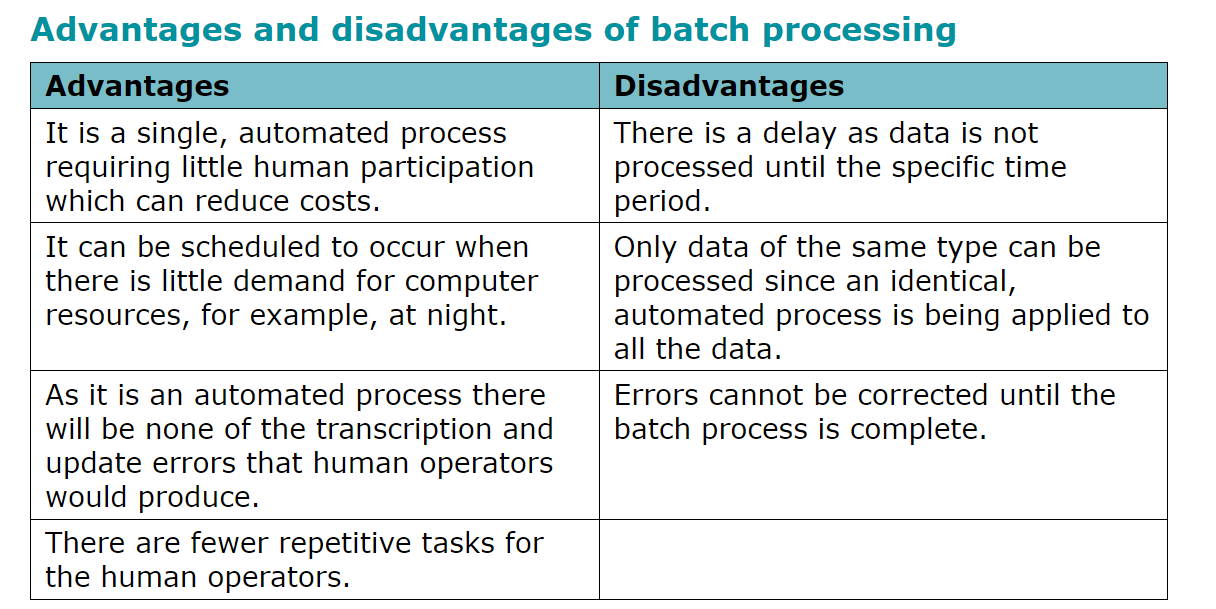
Verification

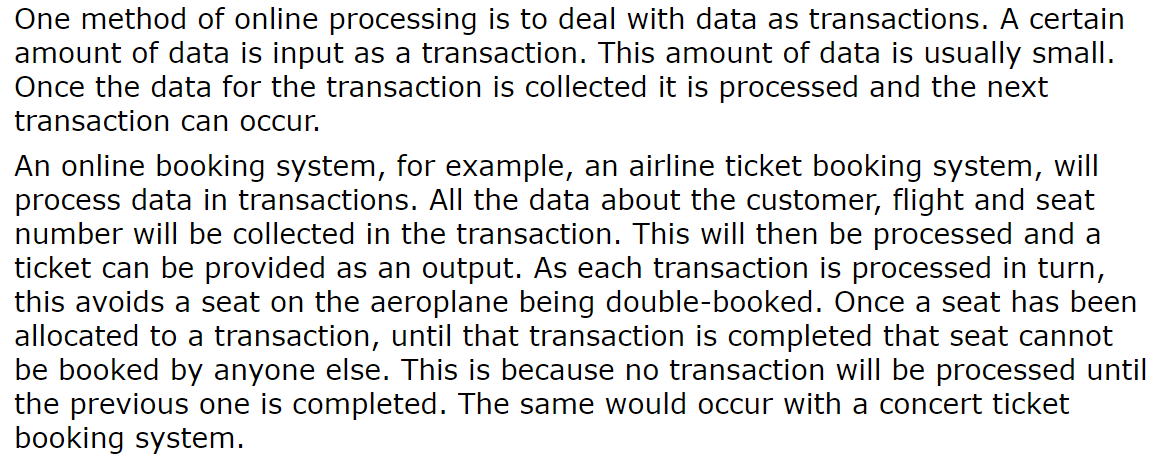
* Visual checking – pretty obv
* Double data entry - 
* Hash total - 
* Control total – another version of hash total but more useful maybe like the total no of items to be inputed
* Parity check - idk try to understand ask miss and aariv tomm
* Checksum - so like a checksum value is created by passing the data into like an algorithm and the value and the data is sent then when u recive the data the check sum value is calculated again and if this value is diff than the value which was there before u can tell that some sort of corruptions has occurred in transmission so data is sent again

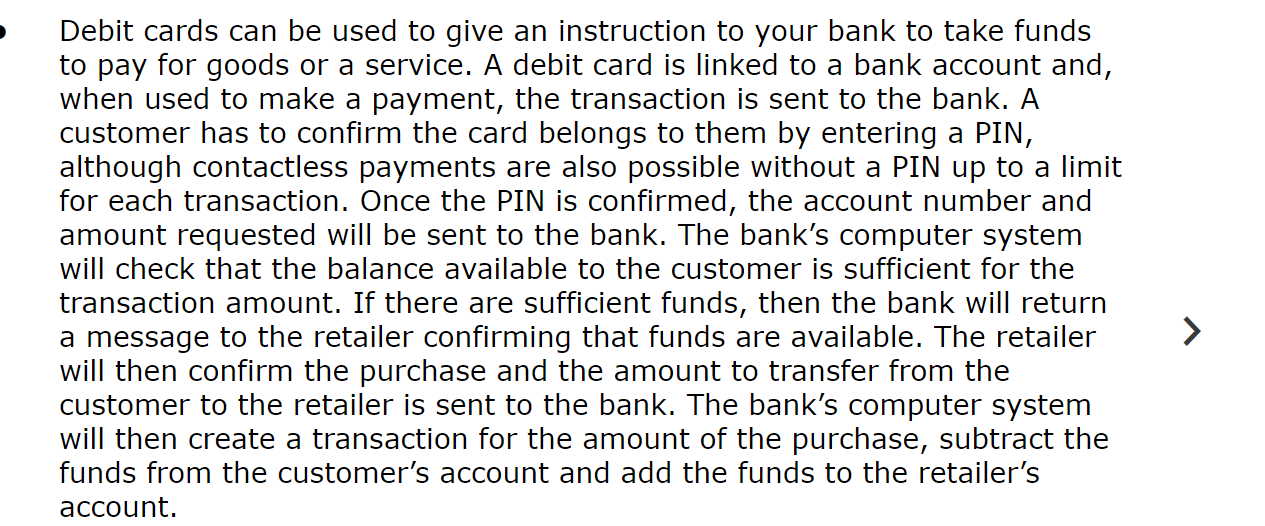
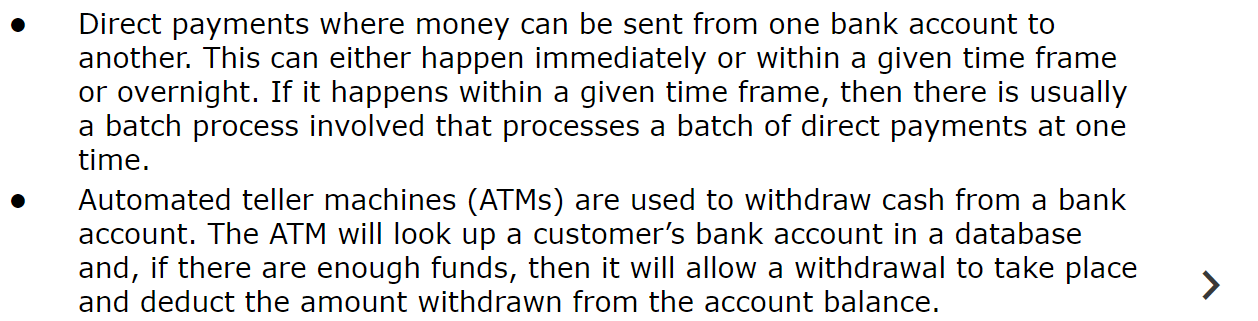
**Data processing (1.5)**



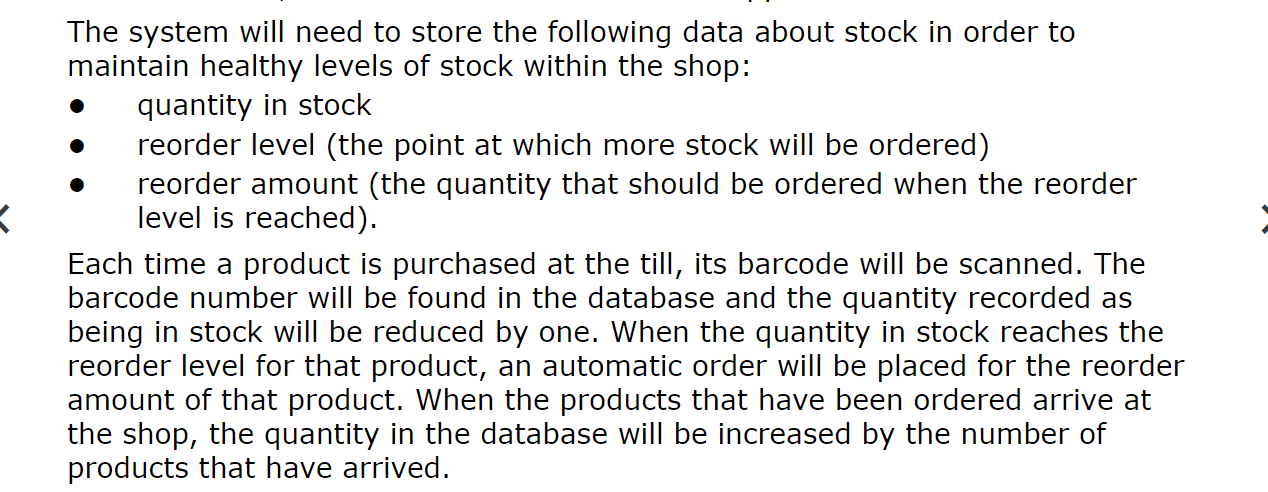
Batch Processing - 



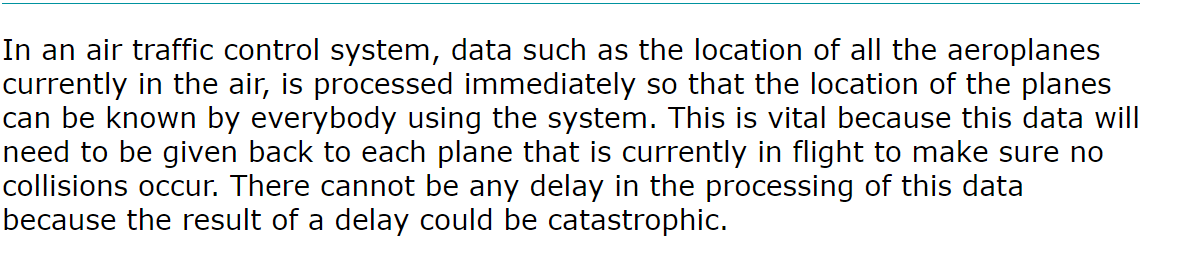
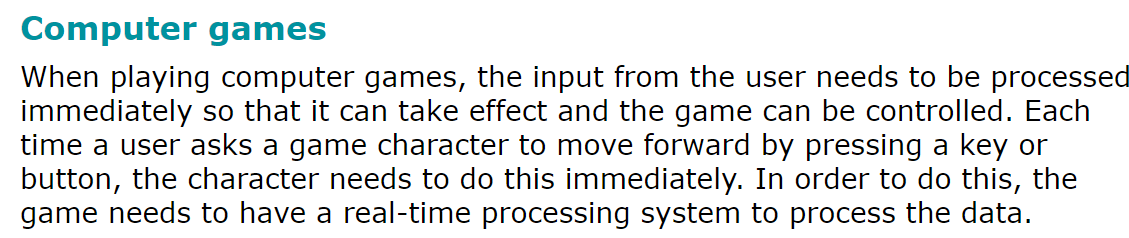
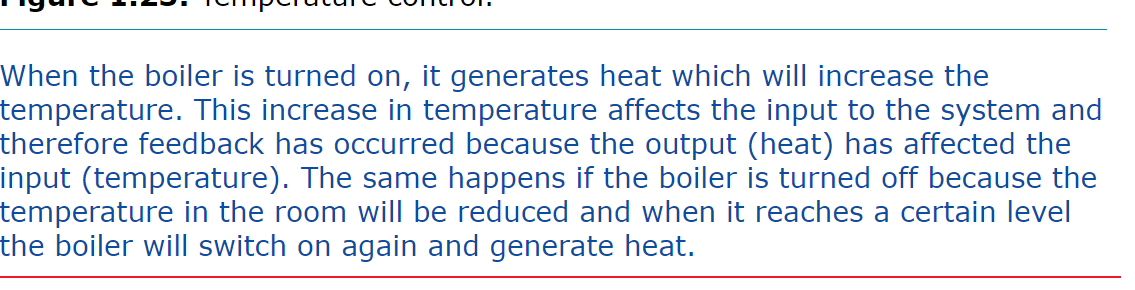
Online processing - 

* Electronics funds transfer – (EFT) 

Direct debits are also there its like if u have a subsription or smthing it auto debits money to keep it going like tht

* Online stores – u can buy a productr from anywhere and then pay using EFT eg. Amazon
* Automatic stock control - 
* Electronic data exchange – weird thing idk
* Business to nusiness buying and selling – when busniness buys 8in bulk the supplier will prob have an interface to make easier its like recipets billa all of tht physical stuff but its made online soo ye

Real Time Processing – data is processed as soon as it is inputted

* Air trafgfic ontrol - 
* Computer games - 
* Centrol heating system - 
* Air conditioning system is same as heating but opposite
* Rocket guidance systems - 