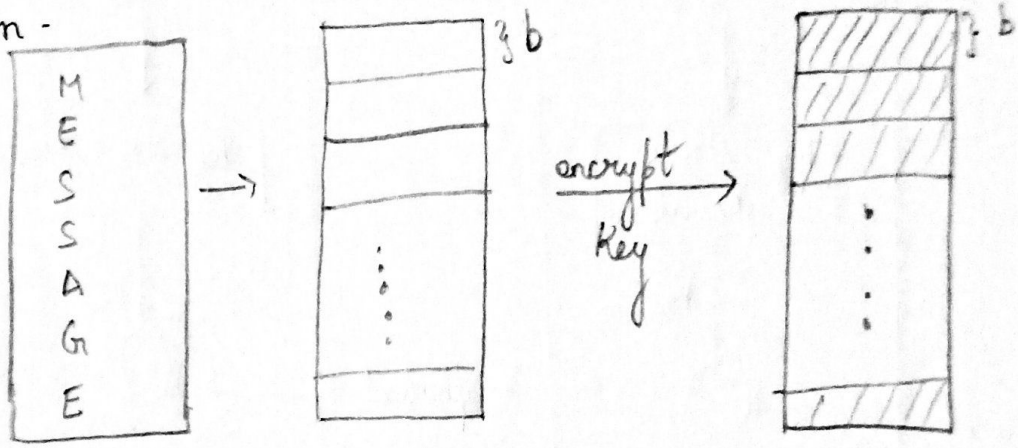
C Bhavesh Kumar
S20190010034

29/11/21 Cloud Computing End Semester 

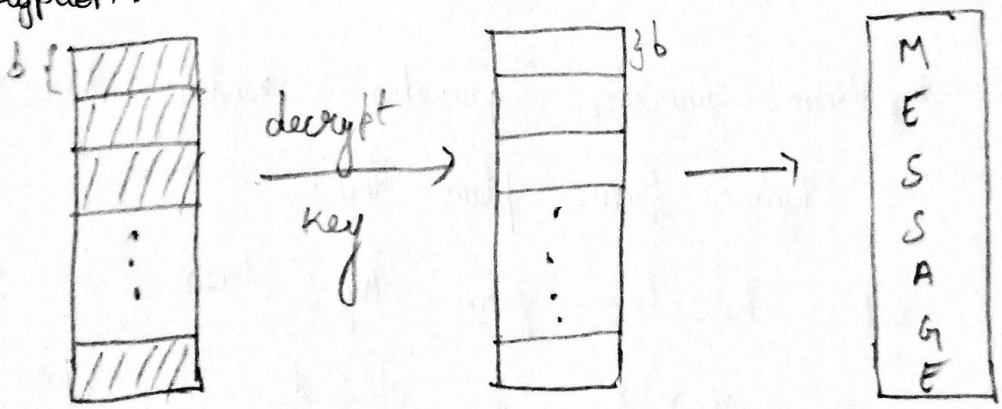
Question 1

Block cipher encryption: In block cipher encryption, we divide our plain text or message into blocks with b bits and apply the encryption algorithm on each of the block with the key specified.

encryption -




decryption.



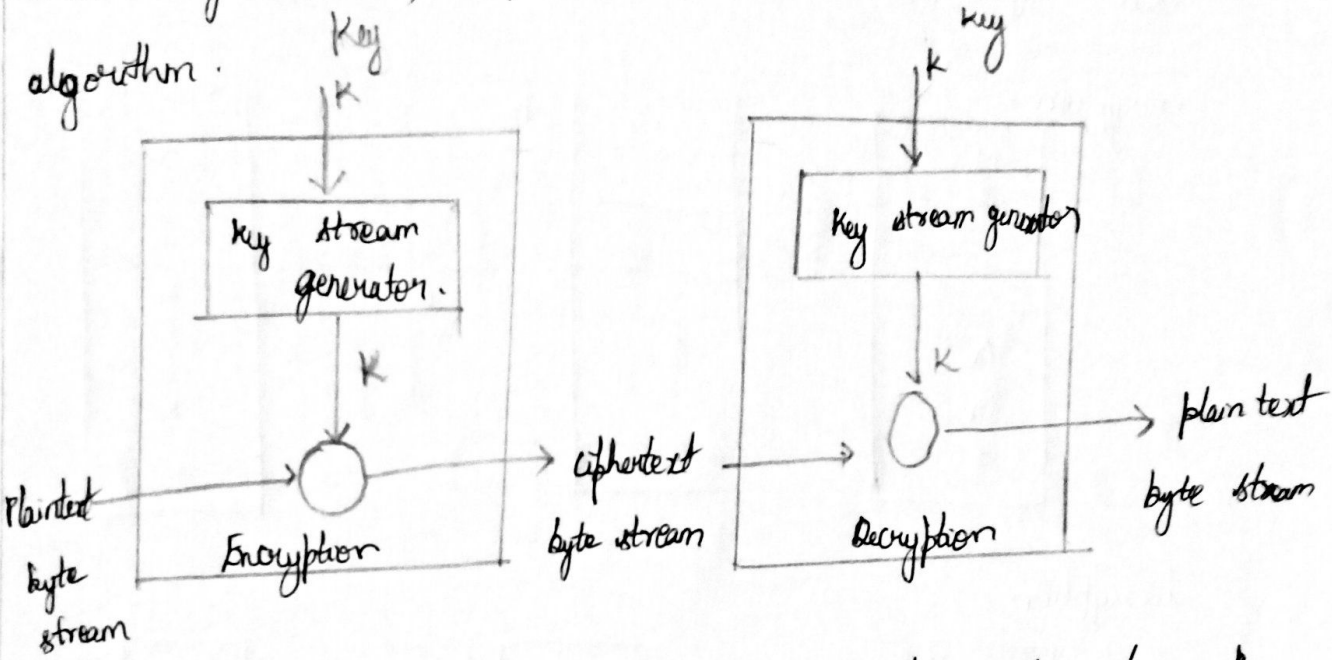

The size of the block remains same after encryption, so if there are b bits in a block then after encryption there are b bits in the block.

This is relatively slow compared to stream cipher.

For lengthy messages block cipher might not be secure a cryptanalyst can exploit regularities in plain text for

the task of decryption.

Stream encryption: In stream cipher encryption we encrypt the message by each byte. We create random bytes (key stream) and use it as the key to encrypt each byte (8 bits) of the message based on the encryption algorithm.




Here key stream generator generates random characters to encode a byte from plain text.

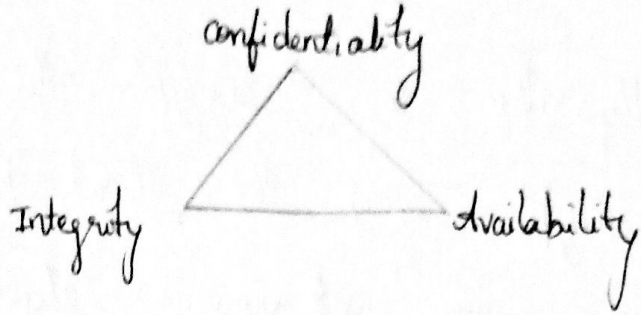
Usually each character from key stream is either added subtracted or xor'd to obtained the cipher text.

Stream encryption is relatively easy and fast compared to block encryption.

Also stream encryption proves to be useful if the message is long as we are eliminating regularities using randomness.

Question - 2

Confidentiality, Integrity and Availability make up the popular CIA triad in cloud security.




* Confidentiality :- This is to ensure that if a message is exchanged between two persons then only they can read their message. If a attacker tries to listen he shouldn't be able to figure out what is being communicated. Since we remain confidential hence the name confidentiality.

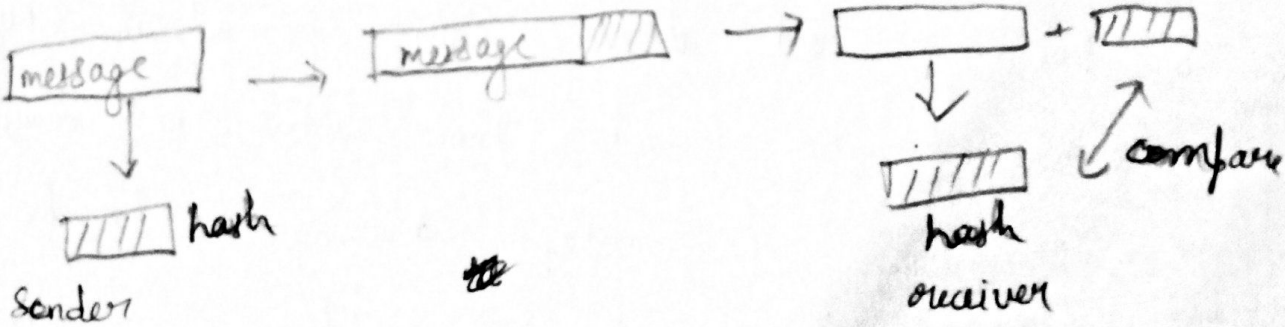
* Integrity :- This is to ensure correctness and trustworthiness of the message communicated. Suppose person A contacts person B and attacker listen in between (MITM Attack), even if he doesn't know what is communicated he can change the message causing it to be utter rubbish when recieved on the other side.

* Availability :- The cloud services must be always 24/7 available and shouldn't be prone to attacks such as DDOS etc

By ensuring the CIA in cloud security we can can provide secure services.

* Confidentiality can be achieved using encryption and decryption Algorithm. We encrypt the message using secret key and decrypt using the secret key hence remaining confidental. There are various algorithms symmetric, asymmetric etc to achieve confidentiality.

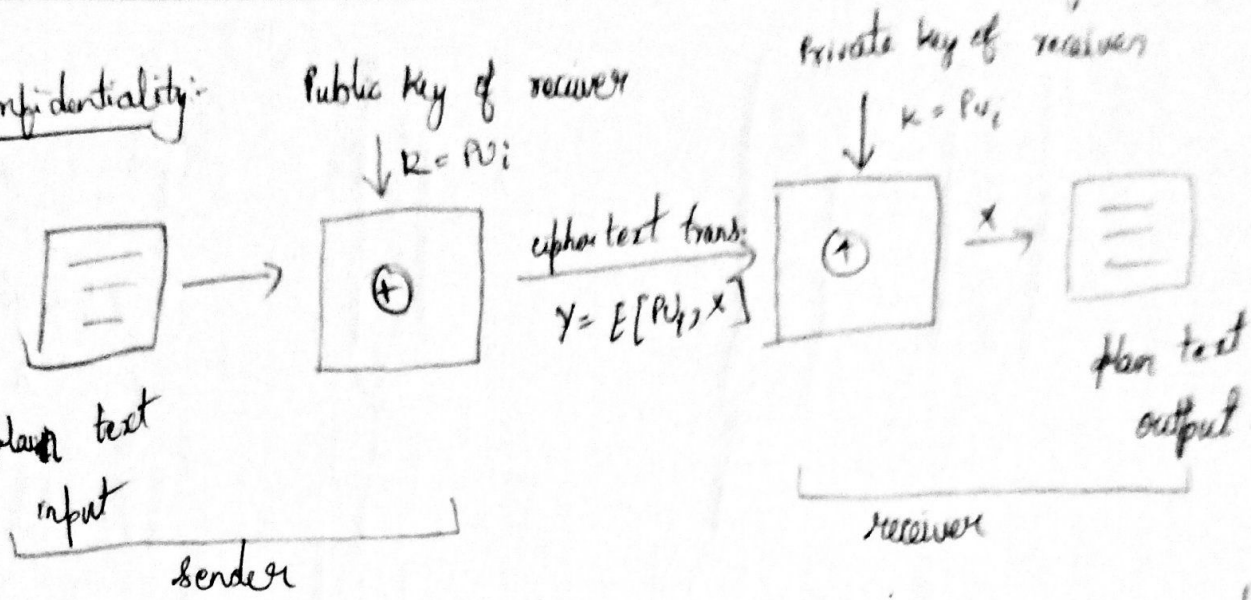
* Integrity can be achieved using hash functions. We take our message x and use hash function H to generate hash H(x) which is unique. We append it along the message and on reciever side again apply same fuction to generate hash and compare both. This hash can be read) modified by attacker so we can encrypt the hash as well.




* Availability can be achieved by proper logging and firewall rules to regularly check if there is any abnormality

Question 3

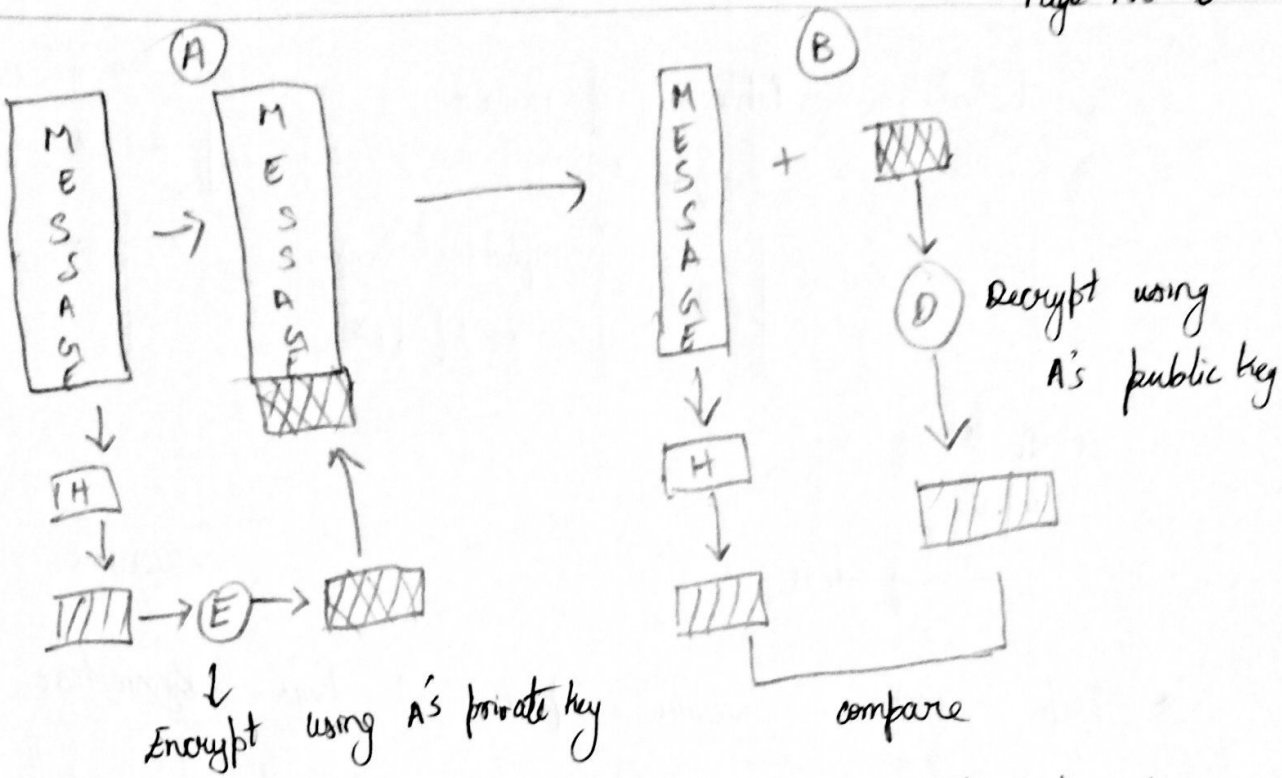
Confidentiality:




* Each user creates pair of keys, public and private key. the public key is shared with everyone while the private key is kept secret.
* Suppose a user A wants to send user B a message. He uses user B's public key to encrypt the message and send him. Since only B knows his private key only he can decrypt the message hence ensuring confidentiality.
* This is asymmetric encryption as we are using different keys for encrypting and decrypting.

Authentication:

* One way hash function is used to authenticate using the asymmetric encryption.

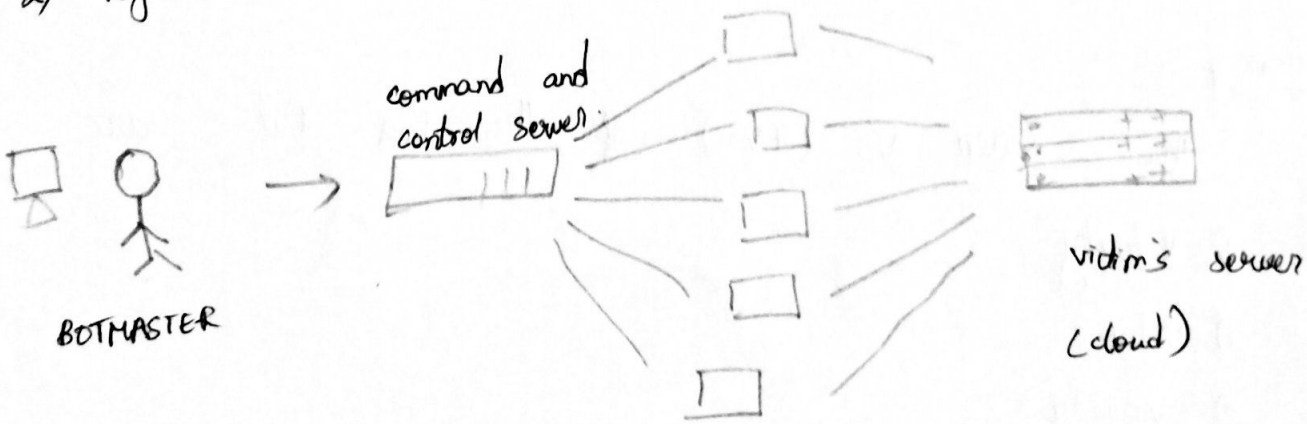



* If user A sends a message to user B then he can hash his message using hash function H and encrypt the hash value using his private key.
* He appends this to his message and sends to B. Since B knows it is from A, he uses public key of A to decrypt hash and compare with the hash that he calculated.
* Using the following method we authenticate the message.
* Since one way hash function is used there is no way to get the message even if hash is found out somehow.

Question-5

## DDOS Attack

* It is a denial of service attack where the attacker sends a huge amount of traffic to the victim's server to make the service unavailable.
* service unavailability means making server unable to respond to legitimate requests.
* There are two types of DDOS attacks
  1) low-rate DDOS attack ( cannot be detected easily)
  2) high-rate DDOS attack ( can be detected easily)




* Botnet is the set of compromised devices used to send traffic.
* Attacker hides his identity by using command and control server and BOTNET.
* First botmaster configures the commands that needs to be sent to Botnet where the traffic is sent.

* At a scheduled time the commands are lauched and BOTNET receives instruction to send traffic.

Prevention techniques :-

* High rate DDOS can be easily prevented using anti DDOS software / hardware by creating denial of service response plan.
* Using whitelist firewall approach can prevent such attacks
* Practicing good cyber hygiene and scaling up the bandwidth can be some of prevention techniques.

Question_4

The seven V's (7V's) of the Big Data are

1) Velocity
2) volume
3) variety
4) variability
5) veracity
6) value
7) visibility / visualisation

Let us consider the example of weather data to explore all of them.

1) velocity - velocity is the rate at which the data is being generated and processed. Today we have various weather stations, satellites collecting weather data. So the weather data is generated in high velocity.

2) Volume - volume is the amount of data generated. Since there are various source for weather data the amount of data we get each day is very high. They say most of the data generated until now is generated in last two years.

3) variety - variety of data that we find. for example in weather data we have various data like longitude, latitude, fog, humidity etc.

4) variability - The variability or the rate of change in data. If the weather changes suddenly the weather data obtained also varies.

5) veracity - veracity is the trustworthiness of data

6) value - Value is the value of data, how valuable is your data. Using weather data we can predict climate hence it is valuable.

7) visualisation - How visible is your data and to what amount you can visualise it. In case of weather data we can visualise the humidity at a given latitude / longitude and plot it to understand variation

. Structured data

* The data which is well structured, organised.
* We can use relational database for structured data.
* concurrency of data is present and hence mostly preferred in multitasking.
* It is schema dependent
* High performance compared to semi or unstructured data.
* Ex - weather data.

unstructured data.

* Data is fully non organised.
* Data is based on binary or character data.
* More flexible since there are no dependencies.
* Ex. videos, audios.

Semi structured data

* Data is organised to some extend, more flexible than structure
* concurrency is not present.