Name : Sradha Kedia

Date of Examination : 18 December, 2021

Time of Examination : 9:30 am to 1:30 pm

Examination Roll no. : 20234757053

Semester : III

Unique Paper Code : 223401302

Title of Paper : Information Security

Email-Id : 200083@cs.du.ac.in

Mobile no. of student : ~~200083@cs.du.ac.in~~ 9899519848

Question no. : 1

No. of pages : 4

Name of the program : MCA

Name of the Department : DUCS

Ans-1 (i) Modular Arithmetic IS is a system of arithmetic for integers, where values reset to zero and begin to increase again, after reaching a certain pre-defined value, called modulo.

- Modular arithmetic is widely used in
  - Computer Science
  - Cryptography
- Modular arithmetic allows us to easily create groups, rings and fields which are fundamental building blocks of most modern public key crypto systems.

The size of key domain will be (A-Z) 26 and (0-9) 10 i.e. 26+10 = 36 So the size of the key domain is 36. the modulus is also 36.

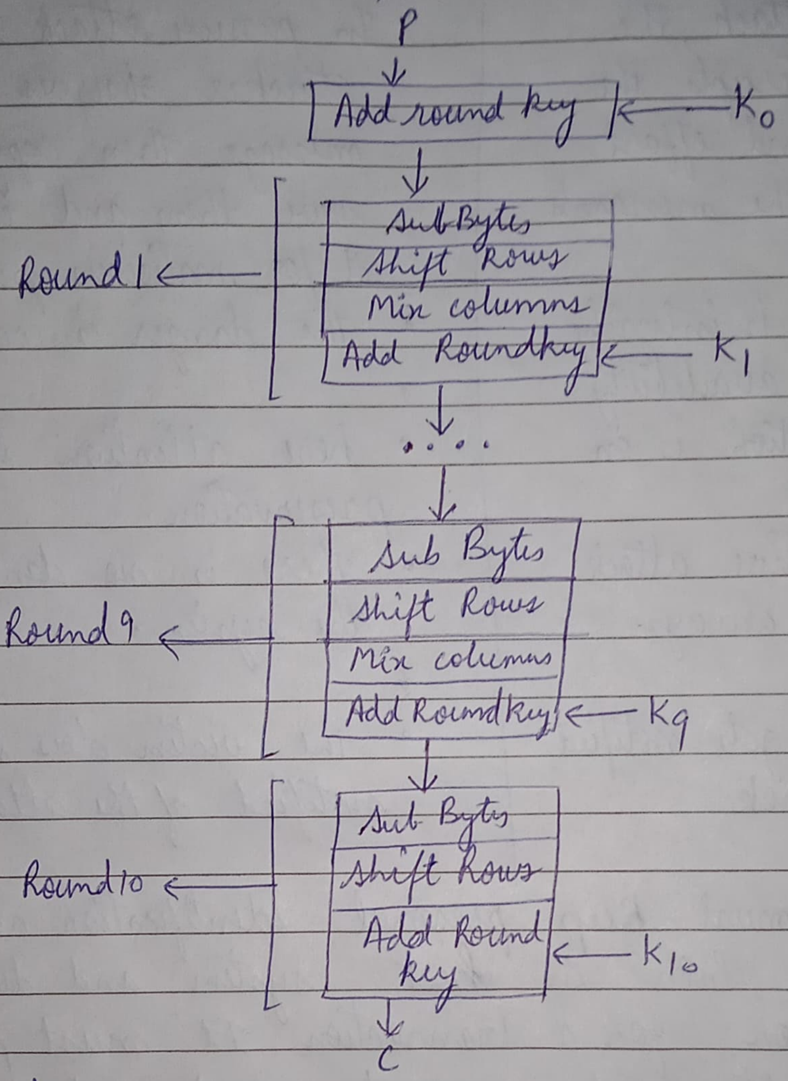
Alice needs to use the set Z_{36}.

ii)

Confusion	Diffusion
• It hides the relationship between cipher text & key.	• It hides the relation between ciphertext and plaintext.
• It obscures the relationship b/w plaintext and ciphertext.	• It spreads the plain text stastics through the ciphertext.
• If a single bit in the key is changed, most or all bits in ciphertext will also be changed.	• If a single symbol in plain text is changed, several symbol in ciphertext will also be changed.
• Vagueness is increased in resultant	• Redundancy is increased in resultant
• Both stream and block ciphers uses confusion	• only block ciphers uses diffusion.

AES is a symmetric cypher, which means a single key is used to encrypt and decrypt.
It is also a block cipher, which implies that it encrypts inputs of 128 bits in multiple rounds before outputing the final output each round gets different key called round key.

with ACS-128, we have 10 rounds :



→ steps –

- Add round key - adds some dependency on the key, and as such some confusion.

Shift Rows – A modification on one bit in one column of the state affects other columns of the state and with mix columns changing one byte of the state affects other bytes of state. These two steps adds diffusion.

- Sub Byles adds non-linearing and confusion.

(iii)

Active Attack	Passive Attack
• In active attack, the attacker interupts the connection and effort to modify the message's content.	• In passive attack, the attacker observes the message, then copy and save them and can use it for malicious purposes.
• The danger is integrity as well as availability.	• The danger is confidentally
• here, attention is on detection.	• here attention is on preservation.
• due to active attack system is always damaged.	• There is no damage to the system.
• the victim gets notified of the attack.	• the victim does not get notified of the attack.

The system must keep personal identification numbers confidential, both in host system and during transmission for a transaction. It must protect the integrity of account records and of individual transaction. Availability of the host system is important to the economic well being of the bank. But not to its fudiciary responsibility. the availability of the individual letter machine is of less concern. so, confidentiality, integrity and availability are highly required in an ATM system.