(2) a) DES uses symmetric-key algorithm for encryption of data. It requires that the sender and receiver both know the same private key because it uses the same key for both encryption & decryption. As it uses 56-bit low key length, which makes it more vulnerable to brute force attacks as processing power increased, DES became insecure. A 56-bit key is not safe against brue force attacks, An attacker can try every possible key until the right one is discovered. Hence, This flaw it has been replaced by more secured encryption system like AES with greater lengths of keys as it key sizes are 128, 192 & 256 bits.

(2) c) Mostly due to a vulnerability known as the "meet in the middle" attack, 2DES does not considerably raise the security level over DES. Because 2DES employs two rounds of encription, This attack takes use of this feature and enables attackers to simultaneously

guess the encryption key used at the beginning of the encryption process and the decryption ~~process~~ key used at the end. Attackers can significantly restrict the effective key space by comparing the middle point of the guesses, making 2DES only ~~significantly~~ slightly secure than DES. As a result; even with 2 keys, 2DES is not seen to be secure against modern cryptographic attacks which prompted the creation & deployment of 3DES & other more secure algorithms such as AES.

3a) The probability of X, Y & Z stepping together in an A5/1 stream cipher, which uses majority rule for stepping can be calculated and by the probability the X, Y & Z stepping together would be 2/8 times which would be 25%.

3b) Given the A5/1 stream cipher's majority rule mechanism for deciding the stepping of register X, Y & Z, the probability that X & Z steps in, but not Y

necessarily X_1. is 2/8 times which would be 25%. This accounts for combinations of majority ~~votes~~ where X & Z align against Y or all three allign.

(2b) In 3DES we use 3 different key to encryption process. So, we begin with the encryption of ~~first key~~ plain text and then with the second key we encrypt the cipher text. Next with the last key we encrypt the cipher text which makes the attacking difficult as there are 168 keys. So, the 3DES is more secure compare to 2DES and it solves the 2DES problem.

(5a) As Alice encrypts plaintext blocks $P_0, P_1, \ldots P_n$ using CTR and obtains ciphertext blocks $C_0, C_1, \ldots C_n$. As the Furdy changes block C_k to X. So, because of ~~the~~ this kth block will be effected while the other blocks are not effected. The teomenology use is

$C_0 = P_0 \oplus E(IV, k)$ $\quad P_0 = C_0 \oplus E(IV, k)$

$C_1 = P_1 \oplus E(IV+1, k)$ $\quad P_1 = C_1 \oplus E(IV+1, k)$

$C_2 = P_2 \oplus E(IV+2, k)$. $\quad P_2 = C_2 \oplus E(IV+2, k)$

So, By using them we can say that by changing the block C_k to X only the k^{th} block is effected and not the other blocks as the other blocks except k^{th} block remain uneffected.

(5) b) If trudy changes ctr to ctr' then all the blocks will get effected because the ctr is a prime part for decryption. So, By changing ctr to ctr' every block gets effected and every block faces changes. As the counter is changed so, all blocks are effected.

(4) a) AES operates on block data So, the block length is 256 and the 9173 bits of data should fit it which gives use $\frac{\text{data size}}{\text{block size}} = \frac{9173}{256}$

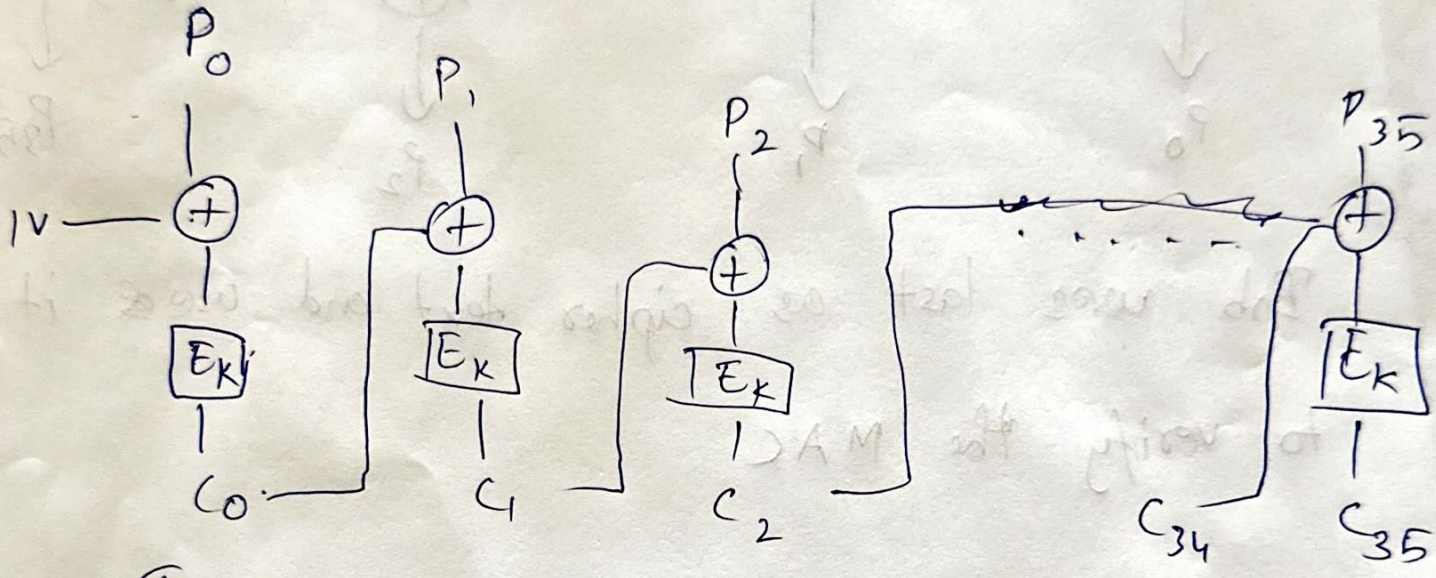
$= 36$ blocks

(4) b) $C_0 = E(IV \oplus P_0, k)$

$C_1 = E(C_0 \oplus P_1, k)$

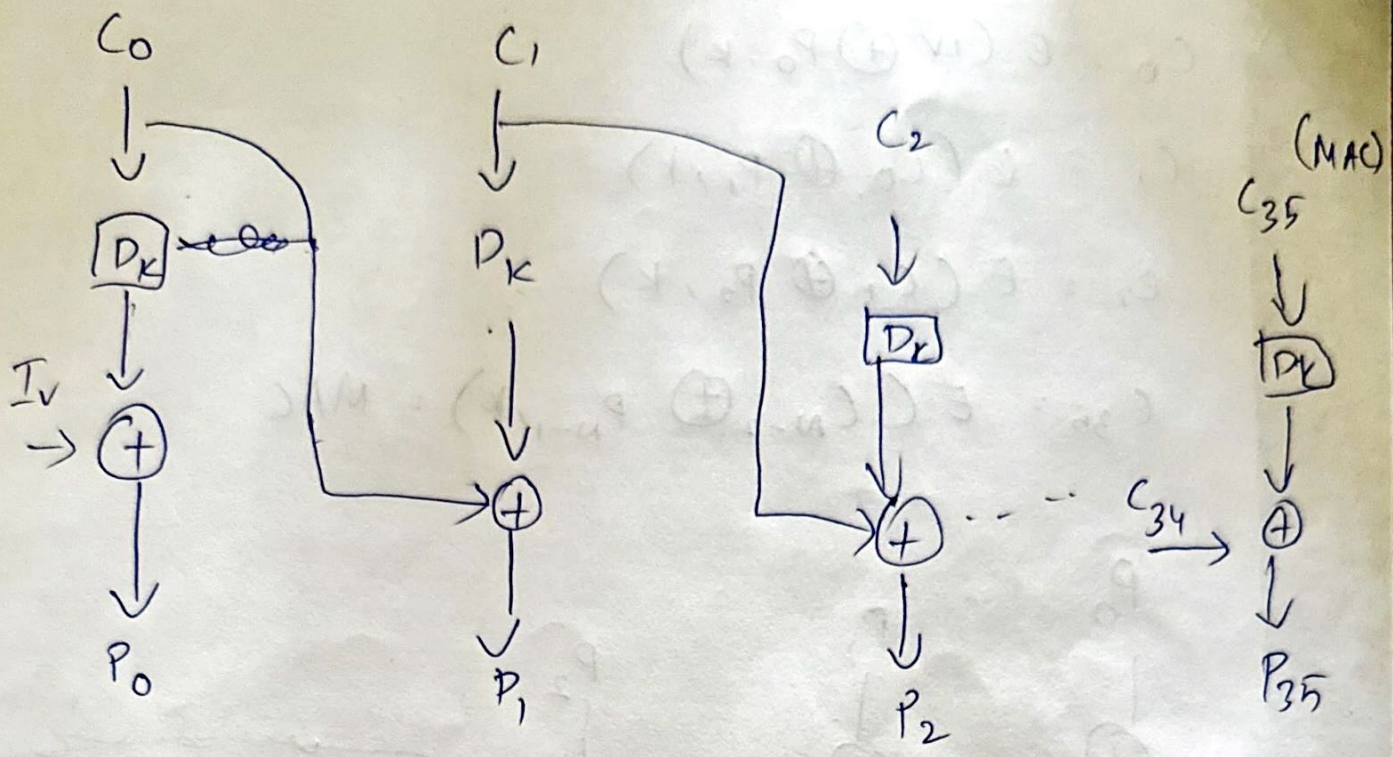
$C_2 = E(C_1 \oplus P_2, k) \ldots$

$C_{35} = E(C_{N-2} \oplus P_{N-1}, k) = MAC$



That is the encryption she gets

(4) c)



Bob uses last as cipher text and uses it to verify the MAC

S. Vivek Reddy

1. True
2. True
3. True
4. False
5. True
6. False
7. True
8. True
9. False
10. True
11. True
12. True
13. False
14. False
15. False