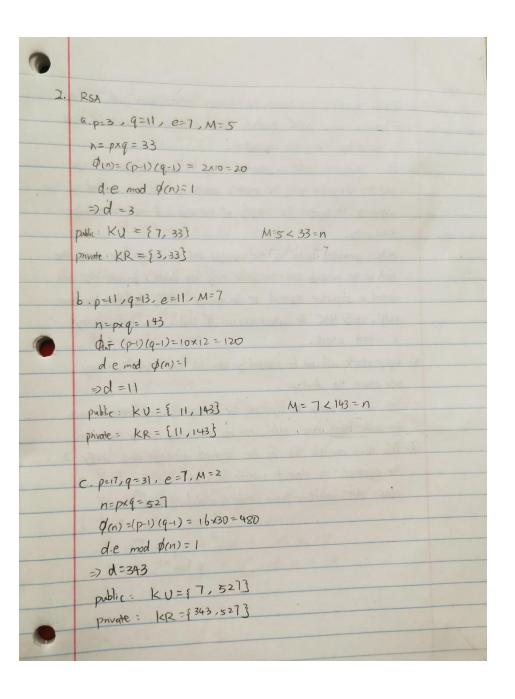
- 1. (i) Digital signature can ensure the message authentication and integrity of message while MAC produces MAC based on the message and the secret key using the algorithm.
  - ca) DS = the digital code is generated using the hash of the message and then encrypted using the sender's private key and it is added as signature. It protect the integrity of message and not affered by third party.

MAC: generated based on the message and the secret key using the hash of the message and encrypted using the sender's private key and added as signature append to the message. Using algorithm produce MAC, verify MAC for authentication. If true, then the integrity is without attack.

- (b) Replay attack will not be detected by both DS and MAC as they only assure the identities.
- (c) Yes, DS can verify the signature by decrypting and determine with the authorized user. MAC can usy secret key verify the user.
- (d) DS: Alice can ask Bob for the received message and verify
  the signature to prove it wasn't from her.

  MAC: MAC unable prove that Alice clicket send



C=10 e=5, n=35, what is M find d: die mod p(n) = 1 -:n=35 =5 x7 d(n)= 4x6=24 -: 0=5 =) d=5 =100000 M= Cd mod n = 105 mod 35 = 5 35x2857=99995 4. 125A, e=31, n=3599, find private key de mod p(n)=1 n= 3599 = 59 x61 Ø(n)=58 x 60 = 3480 de mod \$(n) = 1 => d=-449 private key: KR = 2-449, 3599} 5. q=11, X=2 a. Y=9, what is XA 55+9=64 YA = XXA mod q = 2 xA mod 11 => XA = 6 b. YB=3, what is key k 11x23+3=258 YB = 2 mod q = 2 mod 11 => XB = 8  $K = (Y_B)^{\times n} \mod q = 3^6 \mod 11 = 3$