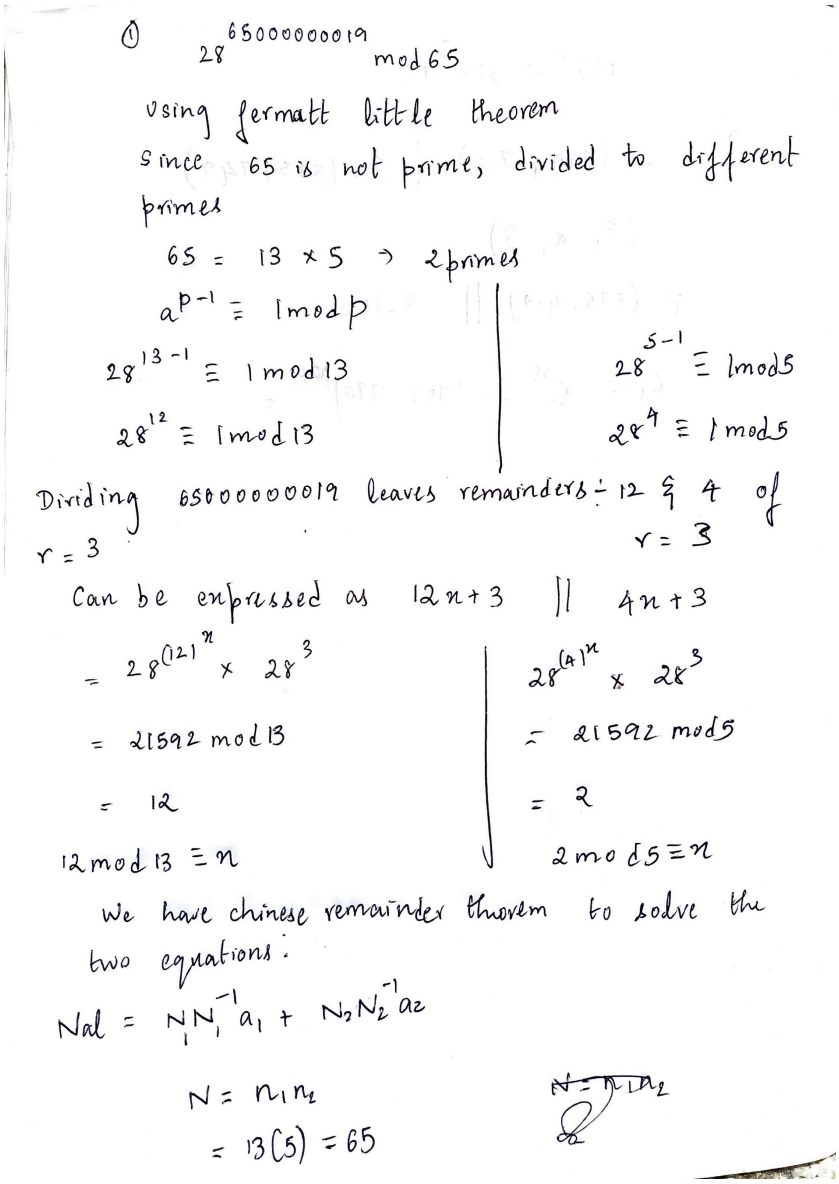
CSCI55500 Assignment # 3

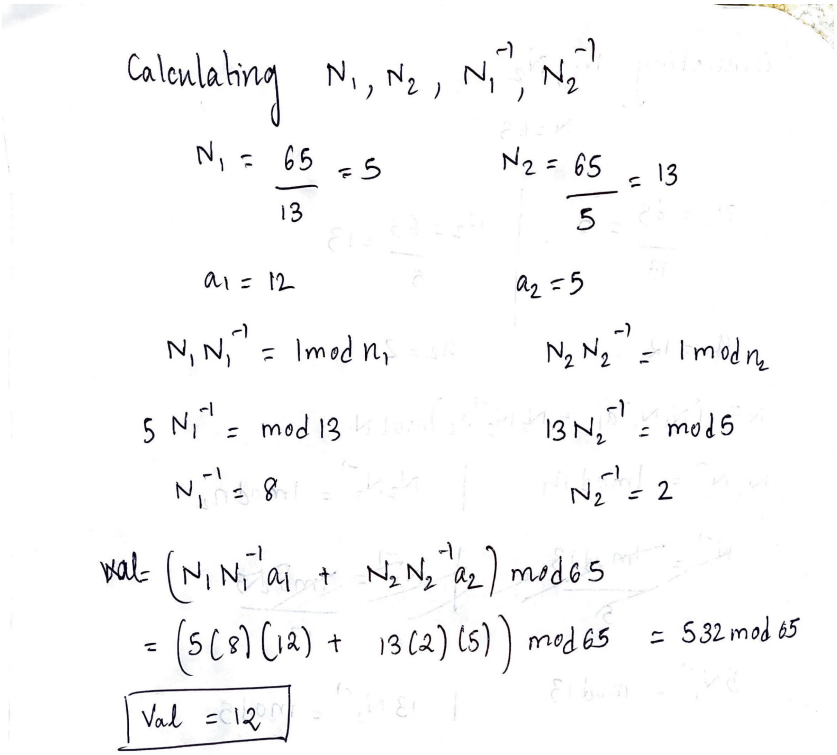
Eashwar Madhavan Perumal

March 6, 2023

1 Question 1

I have used the Fermat's Little Theorem and Chinese remainder theorem to solve this problem. Please find the photos below. The answer for 2865,000,000,019 (mod 65) which I got was 12.





2 Question 2

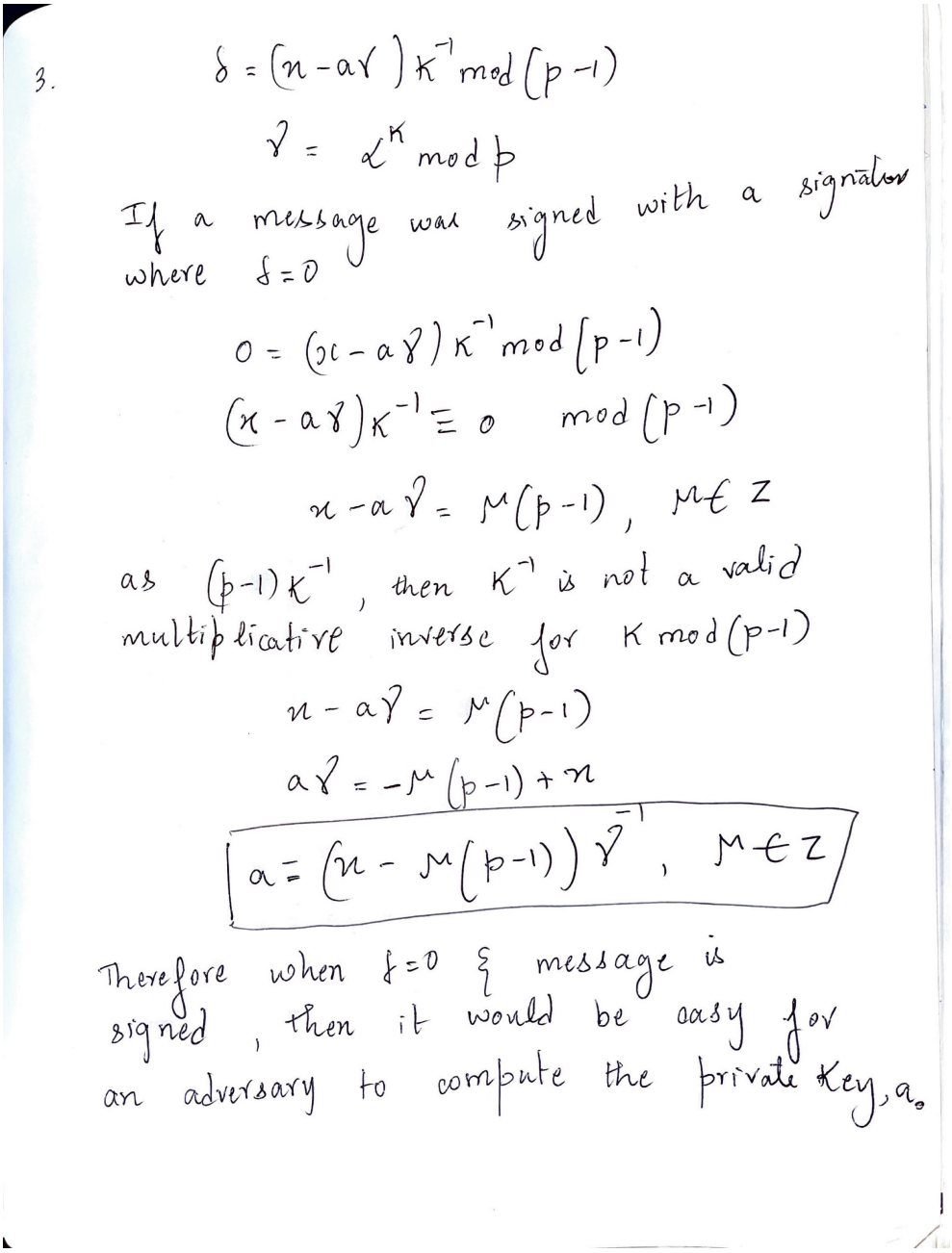
The elgamal cipher text can be decrypted by doing the following steps:

1. First read the (x,y) cipher point on a row and allot it to c1,c2
2. Calculate the value of shared secret, s with the formula, s = pow(c1,a) * mod p.
3. Calculate the multiplicative inverse of s and p
4. Caculate the value of m through m = c2 * sInv * modp
5. There is a loop where the letters are iterated through and we obtain the individual m values by ASCII character conversion

We obtain the decrypted plain text which is as below:
she stands up in the garden where she has been working and looks into the distance she has sensed a change in the weather there is another gust of wind a buckle of noise in the air and the tall cypressess way she turns and moves uphill towards the house climbing over a low wall feeling the first drops of rain on her bare arms she crosses the loggia and quickly enters the house.

3 Question 3

I have attached the proof in the picture below.



4 Question 4

I have attached the code with the zip file which also includes the readme file.

1. To find the number of points over E. I found the solution through brute force. The number of points were 1009
2. The lexically largest points are the largest points of x,y which are satisfying the equation and in this case (1038, 1037)
3. The points (1014,291) do not belong to E. I validated it by substituting the points in the equation.

4. With the given values of alpha1, alpha2, beta1, beta2,Z, K and the Plain text values (575,419). I was able to substitute it in the formula c1 = mod(k * alpha,Z) c2 = mod(x * k*beta,Z I obtained the cipher text values as (936,36),(632,511)

5. With the values of the generator (818,121). We would be able to find the value Ka, Kb through the formula: ka = a(Alpha); kb = b(Alpha) Shared Key secret, kc = a * kb The secret key which I got was [757, 711]

5 Question 5

To make the authentication process a bit more simpler efficient, Bob does not have to send r2 He can compute it as z = Hash(r1 + K) where k is the shared secret key, r1 the random value generated by alice and sent to Bob and send the values of (z,r1) to alice who can then check if Hash(r1 + K) is equal to z and easily authenticate Bob.

Since we are still using the shared secret key, the message can only be opened by bob who has the key.

6 Question 6

This question is about evaluating the four security services: Confidentiality (C), Integrity (I), sender Authentication (A), and Non-Repudiation (NR) for the given protocols.

1. When S generates a random session key k and sends ESpub(sk)-ERpub(sk)-(M PRNGsk) to R: They are using the session key which is randomly generated for the encryption and also the public key which makes sure that Confidentiality is maintained. After that the plain message is XORed with the binary stream from a pseudo-random number generator seeded with sessionKey(sK), which ensures the Integrity is also maintained. In summary this has: A and I

2. When S sends y = Ek1 (x-H(k2-x)) to R: Here as the plain message(x) is concatenated with the Hash of the shared key and also encrypted it insures confidentiality. Since it is hashed it ensures the integrity and since the authentication side of it is also covered since it is technically a shared key which is being used here. In summary this has: C and I

3. When S sends y= ERpub(x-SIGSpri(H(x))) to R: Since the encryption is signed using the public key it ensures that the confidentiality is maintained. The message which is signed with the private key as given means that the R can authenticate the S once message is recieved. Since the message can be verified using the sender's public key, it provides validity that it did come from the sender which provides non-repudiation to it. In summary this has: C, I, A and R

4. When S generates a new symmetric key sk and sends y = ESpub (sk)-ERpub (sk)-SIGSpri (sk)-Esk(x) to R: Here the encryption is done with the public key which means confidentiality is maintained. Since the symmetric key is used to encrypt with the public key authentication can take place. Since the private key is used, it maintains the integrity and the signature has been done with the private key which also provides non-repudiation. In summary this has: C, I, A and R