Cruz Chavez

Dr. Bilal Shebarro

COSC 3325-01

7 October 2018

Homework 3

Part I:

My p = 5

My q = 7

My N = pq = 5 * 7 = 35

My e = number relatively prime to (p-1)(q-1) = number relatively prime to (4)(6) = 24

My e = 5 (GCD between 5 & 24 == 1)

My d satisfies the relation ed % (p-1)(q-1) = 1, so it satisfies 5d % (4)(6) = 1

5d % 24 = 1

My d = 5

Public Key = (N,e)

Private Key = (N,d)

My Public Key = (35, 5)

My Private Key = (35, 5)

Part II:

Message = “CRUZ CHAVEZ”

To encrypt Message, we must compute Ciphertext to equal (M^e) % N for M is each character in Message. Note, we are using Alice’s public key (21, 5) N =21 e = 5

ASCII of Message = 34678285903267726586699034

C = (3^5) % 21 = 12

C = (4^5) % 21 = 16

C = (6^5) % 21 = 6

C = (7^5) % 21 = 7

C = (8^5) % 21 = 8

C = (2^5) % 21 = 11

C = (8^5) % 21 = 8

C = (5^5) % 21 = 17

C = (9^5) % 21 = 18

C = (0^5) % 21 = 0

C = (3^5) % 21 = 12

C = (2^5) % 21 = 11

C = (6^5) % 21 = 6

C = (7^5) % 21 = 7

C = (7^5) % 21 = 7

C = (2^5) % 21 = 11

C = (6^5) % 21 = 6

C = (5^5) % 21 = 17

C = (8^5) % 21 = 8

C = (6^5) % 21 = 6

C = (6^5) % 21 = 6

C = (9^5) % 21 = 18

C = (9^5) % 21 = 18

C = (0^5) % 21 = 0

C = (3^5) % 21 = 12

C = (4^5) % 21 = 16

Ciphertext = 121667811817180121167711617866181801216 (We send this to Alice)

Part III:

Message = “CRUZ CHAVEZ”

To sign Message, we must compute Ciphertext to equal (M^e) % N for M is each character in Message. Note, we are using my private key (35, 5) N = 35 e = 5

ASCII of Message = 3467828590326772658669903 4

C = (3^5) % 35 = 33

C = (4^5) % 35 = 9

C = (6^5) % 35 = 6

C = (7^5) % 35 = 7

C = (8^5) % 35 = 8

C = (2^5) % 35 = 32

C = (8^5) % 35 = 8

C = (5^5) % 35 = 10

C = (9^5) % 35 = 4

C = (0^5) % 35 = 0

C = (3^5) % 35 = 33

C = (2^5) % 35 = 32

C = (6^5) % 35 = 6

C = (7^5) % 35 = 7

C = (7^5) % 35 = 7

C = (2^5) % 35 = 32

C = (6^5) % 35 = 6

C = (5^5) % 35 = 10

C = (8^5) % 35 = 8

C = (6^5) % 35 = 6

C = (6^5) % 35 = 6

C = (9^5) % 35 = 4

C = (9^5) % 35 = 4

C = (0^5) % 35 = 0

C = (3^5) % 35 = 33

C = (4^5) % 35 = 9

Ciphertext = 339678328104033326773261086644O339 (This is my name signature)

Part IV:

Message = “CRUZ CHAVEZ”

To encrypt Message, we must compute Ciphertext to equal (M^e) % N for M is each character in Message. Note, we are using Alice’s public key so that only Alice may read its contents in plaintext. (21, 5) N =21 e = 5

ASCII of Message = 34678285903267726586699034

C = (3^5) % 21 = 12

C = (4^5) % 21 = 16

C = (6^5) % 21 = 6

C = (7^5) % 21 = 7

C = (8^5) % 21 = 8

C = (2^5) % 21 = 11

C = (8^5) % 21 = 8

C = (5^5) % 21 = 17

C = (9^5) % 21 = 18

C = (0^5) % 21 = 0

C = (3^5) % 21 = 12

C = (2^5) % 21 = 11

C = (6^5) % 21 = 6

C = (7^5) % 21 = 7

C = (7^5) % 21 = 7

C = (2^5) % 21 = 11

C = (6^5) % 21 = 6

C = (5^5) % 21 = 17

C = (8^5) % 21 = 8

C = (6^5) % 21 = 6

C = (6^5) % 21 = 6

C = (9^5) % 21 = 18

C = (9^5) % 21 = 18

C = (0^5) % 21 = 0

C = (3^5) % 21 = 12

C = (4^5) % 21 = 16

Ciphertext (Plaintext encryption) = 121667811817180121167711617866181801216

We now sign this ciphertext using my private key (35, 5) N = 35 e = 5

C = (1^5) % 35 = 1

C = (2^5) % 35 = 32

C = (1^5) % 35 = 1

C = (6^5) % 35 = 6

C = (6^5) % 35 = 6

C = (7^5) % 35 = 7

C = (8^5) % 35 = 8

C = (1^5) % 35 = 1

C = (1^5) % 35 = 1

C = (8^5) % 35 = 8

C = (1^5) % 35 = 1

C = (7^5) % 35 = 7

C = (1^5) % 35 = 1

C = (8^5) % 35 = 8

C = (0^5) % 35 = 0

C = (1^5) % 35 = 1

C = (2^5) % 35 = 32

C = (1^5) % 35 = 1

C = (1^5) % 35 = 1

C = (6^5) % 35 = 6

C = (7^5) % 35 = 7

C = (7^5) % 35 = 7

$C = (1^5) \% 35 = 1$

$C = (1^5) \% 35 = 1$

$C = (6^5) \% 35 = 6$

$C = (1^5) \% 35 = 1$

$C = (7^5) \% 35 = 7$

$C = (8^5) \% 35 = 8$

$C = (6^5) \% 35 = 6$

$C = (6^5) \% 35 = 6$

$C = (1^5) \% 35 = 1$

$C = (8^5) \% 35 = 8$

$C = (1^5) \% 35 = 1$

$C = (8^5) \% 35 = 8$

$C = (0^5) \% 35 = 0$

$C = (1^5) \% 35 = 1$

$C = (2^5) \% 35 = 32$

$C = (1^5) \% 35 = 1$

$C = (6^5) \% 35 = 6$

Ciphertext (Plaintext encryption signiture) =

132166781181718013211677116178661818013216 (We send this to Alice)

Part V:

Message = “CRUZ CHAVEZ”

To sign Message, we must compute Ciphertext to equal (M^e) % N for M is each character in Message in order to verify I am the sender. Note, we are using my private key (35, 5) N = 35 e = 5

ASCII of Message = 346782859032677265866990 34

C = (3^5) % 35 = 33

C = (4^5) % 35 = 9

C = (6^5) % 35 = 6

C = (7^5) % 35 = 7

C = (8^5) % 35 = 8

C = (2^5) % 35 = 32

C = (8^5) % 35 = 8

C = (5^5) % 35 = 10

C = (9^5) % 35 = 4

C = (0^5) % 35 = 0

C = (3^5) % 35 = 33

C = (2^5) % 35 = 32

C = (6^5) % 35 = 6

C = (7^5) % 35 = 7

C = (7^5) % 35 = 7

C = (2^5) % 35 = 32

C = (6^5) % 35 = 6

C = (5^5) % 35 = 10

C = (8^5) % 35 = 8

C = (6^5) % 35 = 6

C = (6^5) % 35 = 6

C = (9^5) % 35 = 4

C = (9^5) % 35 = 4

C = (0^5) % 35 = 0

C = (3^5) % 35 = 33

C = (4^5) % 35 = 9

Ciphertext = 33967832810403332677326108664403339 (This is my name signature)

We now encrypt this signed message using Alice’s public key (21, 5) N =21 e = 5

C = (3^5) % 21 = 12

C = (3^5) % 21 = 12

C = (9^5) % 21 = 18

C = (6^5) % 21 = 6

C = (7^5) % 21 = 7

C = (8^5) % 21 = 8

C = (3^5) % 21 = 12

C = (2^5) % 21 = 11

C = (8^5) % 21 = 8

C = (1^5) % 21 = 1

C = (0^5) % 21 = 0

C = (4^5) % 21 = 16

C = (0^5) % 21 = 0

C = (3^5) % 21 = 12

$C = (3^5) \% 21 = 12$

$C = (3^5) \% 21 = 12$

$C = (2^5) \% 21 = 11$

$C = (6^5) \% 21 = 6$

$C = (7^5) \% 21 = 7$

$C = (7^5) \% 21 = 7$

$C = (3^5) \% 21 = 12$

$C = (2^5) \% 21 = 11$

$C = (6^5) \% 21 = 6$

$C = (1^5) \% 21 = 1$

$C = (0^5) \% 21 = 0$

$C = (8^5) \% 21 = 8$

$C = (6^5) \% 21 = 6$

$C = (6^5) \% 21 = 6$

$C = (4^5) \% 21 = 16$

$C = (4^5) \% 21 = 16$

$C = (0^5) \% 21 = 0$

$C = (3^5) \% 21 = 12$

$C = (3^5) \% 21 = 12$

$C = (9^5) \% 21 = 18$

Ciphertext (Encrypted name signature) =

121218678121181016012121211677121161086616160121218 (We send this to Alice)

Problem 2:

p = 541 g = 10

In order to generate a symmetric key using the above numbers and the private values of Alice (a = 11) and Bob (b = 13) via Diffie Helman, both Alice and Bob must compute (g^sercret value) % p and send the result to the other person

Alice’s calculation is as follows

(10^11) % 541 = 297 (She sends this to Bob)

Bob’s calculation is as follows

(10^13) % 541 = 486 (He sends this to Alice)

Upon receiving these values, both parties calculate (received value^secret value) % p

Alice’s calculation is as follows

(486^11) % 541 = 511

Bob’s calculation is as follows

(297^13) % 541 = 511

In this case, the symmetric key used by Alice and Bob for a symmetric cryptographic algorithm is 511