Assignment 3 – ECE 1155

Rayan Hassan 4511021

Question 1

a) Let's say we have two people Amir and Bassem. They both agree on a large prime number and a primitive root (p and g respectively). They both randomly generate a number (less than p), x for Amir and y for Bassem. Amir sends (g^x mod p) to Bassem, and the later sends (g^y mod p) to Amir. Then, Amir computes (g^y mod p)^x mod p and Bassem computes (g^x mod p)^y mod p. These are both equal to K=g^{xy} mod p, which is the shared secret key.

b) p = 13 and g = 2. Let's say x=2 for Amir and y=4 for Bassem.

Amir will get (g^y mod p) = 2^4 mod 13 = 16 mod 13 = 3 from Bassem.

Bassem will get (g^x mod p) = 2^2 mod 13 = 4 mod 13 = 4 from Amir.

Amir will calculate (g^y mod p)^x mod p = 3^2 mod 13 = 9 mod 13 = 9

Bassem will calculate (g^x mod p)^y mod p = 4^4 mod 13 = 256 mod 13 = 9

So as expected, these are equal. The secret key is K=9.

Question 2

Since p is a large prime number and g is a primitive root of p, it is extremely hard to find x from g^x mod p

Question 3

a) Let's find the private key 'd' such that (ed) mod totient(n) = 1.

n = p x q = 3 x 11 = 33.

Totient(n) = (p-1)(q-1) = (3-1)(11-1) = 2 x 10 = 20

Now let's find d such that (ed) mod totient(n) = 1 ⇔ 7d = 20k + 1. d=3 and k = 1 (7 x 3 = 21)

Plaintext is M=5. Ciphertext is M^e mod n = 5^7 mod 33 = 14. (encryption)

Now to retrieve the plaintext: M = C^d mod n = 14^3 mod 33 = 5 (decryption)

b) n = p x q = 11 x 13 = 143.

Totient(n) = (11-1)(13-1) = 10 x 12 = 120

(ed) mod totient(n) = 1 ⇔ 11d = 120k + 1. d = 11 and k =1 (11 x 11 = 121)

Plaintext is M=7. Ciphertext is M^e mod n = 7^{11} mod 143 = 106 (encryption)

To retrieve plaintext: M = C^d mod n = 106^{11} mod 143 = 7

Question 4

P=59 and q=61 using the table.

Totient(n) = (59-1)(61-1) = 58 x 60 = 3480

(ed) mod totient(n) = 1 ⇔ 31d = 3480k + 1

k = -4 and private key is d=449

Question 5

M = C^d mod n.

n = 35 so p=5 and q=7.

Totient(n) = 4 x 6 = 24

(ed) mod totient(n) = 1 ⇔ 5d = 24k + 1

Private key d is 5 (5 x 5 = 24 + 1), with k=1

So M = 10^5 mod 35 = 5

Question 6

P=3 and q=11, n=33

Totient(n) = 2 x 10 = 20

(ed) mod totient(n) = 1 ⇔ 3d = 20k + 1

So d = 7 and k=1

Question 7

Totient(n) = 16 x 12 = 192.

Gcd(e,totient(n)) = gcd(3,192) = 3 ≠1. So e and totient(n) are not relatively prime, so no we can't choose e=3.

Question 8

a) n= 17 x 31 = 527

totient(n) = 16 x 30 = 480

(ed) mod totient(n) = 1 ⇔ 7d = 480k + 1

So private key d is 137, with k=-2

b) C=M^e mod n = 2^7 mod 527 = $2^{3 \times 2 +1}$mod 527 = $(2^2)^3$ x 2 mod 527 = [$(2^2)^3$ mod 527][2 x mod 527]

= $[4 \text{ mod } 527]^3$[2 x mod 527] = 4^3 x 2 = 64 x 2 = 128.

c) $M = C^d \bmod n = 128^{137} \bmod 527 = 128^{2x68+1} \bmod 527$

$= (128^2)^{68} \times 128 \bmod 527 = [(128^2)^{68} \bmod 527][128 \bmod 527]$

$= [(128^2 \bmod 527)^{68} \bmod 527] \times [128 \bmod 527]$

$= [47^{68} \bmod 527]\ [128 \bmod 527] = (47^{2 \times 34} \bmod 527)\ [128 \bmod 527]$

$= [(47^2 \bmod 527)^{34} \bmod 527]\ [128 \bmod 527]$

$= (101^{34} \bmod 527)\ [128 \bmod 527]$

$= ((101^2 \bmod 527)^{17} \bmod 527)\ [128 \bmod 527] = (188^{17} \bmod 527)\ [128 \bmod 527]$

$= (188^{2x8+1} \bmod 527)\ [128 \bmod 527] = [(188^2 \bmod 527)^8 \bmod 527]\ [128 \bmod 527]\ [128 \bmod 527]$

$= (35^8 \bmod 527) \times [128^2 \bmod 527] = (35^{4x2} \bmod 527) \times 47 = (256^2 \bmod 527) \times 47 = 128$