SOLUTIONS FOR ASSIGNMENT-4

HUMESH REDDY VENKATAPURAM **CS 525: INTRO TO CRYPTO**

Question 1:

a)

Considering Z_{17}^*: {1,2,3,4,5,6,7,8,9,10,11,12,13,14,15,16}

$|Z_{17}^*| = 16$

For an element a in Z_{17}^* to be a generator, the powers a^k (where k ranges from 1 to 16) must produce all unique non-zero elements modulo 17, i.e., a^k mod17 must be distinct for all k from 1 to 16.

Given that 17 is prime, Z_{17}^* is a cyclic group of order 16. We will have generators among the numbers from 2 to 16.

Candidate 2:

If 2 is a generator, then every element in Z_{17}^* should be included in the set of elements obtained by 2^x mod 17. This may be computed as shown below.

2^0 mod 17 = 1 mod 17 = 1 - $2^0 \equiv 1$ mod 17

2^1 mod 17 = 2 mod 17 = 2 - $2^1 \equiv 1$ mod 17

$2^2 \equiv 4$ mod 17 = 4

$2^3 \equiv 8$ mod 17 = 8

$2^4 \equiv 16$ mod 17 = 16

$2^5 \equiv 15$ mod 17 = 15

$2^6 \equiv 13$ mod 17 = 13

$2^7 \equiv 9$ mod 17 = 9

$2^8 \equiv 1 \bmod 17 = 1$

The subgroup is 1,2,4,8,16,15,13,9, which misses several components from Z_{17}^*.

As a result, 2 is not a generator.

$H_1 = \{1,2,4,8,9,13,15,16\}$

$| H_1|$ will be the composite of 8

candidate 3:

If 3 is a generator, then every element in Z_{17}^* should be included in the set of elements obtained by 3^x mod 17. This may be computed as shown below

$3^0 \equiv 1 \bmod 17 = 1$

$3^1 \equiv 3 \bmod 17 = 3$

$3^2 \equiv 9 \bmod 17 = 9$

$3^3 \equiv 10 \bmod 17 = 10$

$3^4 \equiv 13 \bmod 17 = 13$

$3^5 \equiv 5 \bmod 17 = 5$

$3^6 \equiv 15 \bmod 17 = 15$

$3^7 \equiv 11 \bmod 17 = 11$

$3^8 \equiv 16 \bmod 17 = 16$

$3^9 \equiv 14 \bmod 17 = 14$

$3^{10} \equiv 8 \bmod 17 = 8$

$3^{11} \equiv 7 \bmod 17 = 7$

$3^{12} \equiv 4 \bmod 17 = 4$

$3^{13} \equiv 12 \bmod 17 = 12$

$3^{14} \equiv 2 \bmod 17 = 2$

$3^{15} \equiv 6 \bmod 17 = 6$

$3^{16} \equiv 1 \bmod 17 = 1$

The subgroup is {1,3,9,10,13,5,15,11,16,14,8,7,4,12,2,6} which has all the components from Z_{17}^*

So, 3 is a generator

H_1= {1,2,3,4,5,6,7,8,9,10,11,12,13,14,15,16}

$|H_1|$ will be the composite of 16

candidate 4:

$4^0 \equiv 1 \bmod 17$

$4^1 \equiv 4 \bmod 17$

$4^2 \equiv 1 \bmod 17$

$4^3 \equiv 13 \bmod 17$

…………………………………………………….

And if we continue to calculate,

We get the subgroup {1,4,13,16}, which misses several Z_{17}^*components. As a result, 4 is not a generator.

H_1= {1,4,13,16}

$|H_1|$ will be the composite of 4

Similarly, if we multiply all of the remaining integers in the set by their powers mod 17, we obtain

- Calculating the powers of 5 modulo 17 gets the subgroup of {1,5,8,6,7,9,13,12,14,10,3,2,11,15,4,16}

- Calculating the powers of 6 modulo 17 gets the subgroup of {1,6,2,12,10,9,4,7,3,5,13,11,14,8,15,16}

- Calculating the powers of 7 modulo 17 gets the subgroup of {1,7,15,3,4,6,13,5,9,10,8,14,11,12,2,16}

- Calculating the powers of 8 modulo 17 gets the subgroup of {1,2,4,8,9,13,15,16}

- Calculating the powers of 9 modulo 17 gets the subgroup of {1,2,4,8,9,13,15,16}

- Calculating the powers of 10 modulo 17 gets the subgroup of {1,10,13,9,5,14,9,15,6,2,7,4,12,3,11,16}

- Calculating the powers of 11 modulo 17 gets the subgroup of {1,11,2,5,14,8,9,13,7,6,12,15,3,10,4,16}

- Calculating the powers of 12 modulo 17 gets the subgroup of {1,12,8,4,10,2,11,6,5,7,9,3,13,14,15,16}

- Calculating the powers of 13 modulo 17 gets the subgroup of {1,4,13,16}

- Calculating the powers of 14 modulo 17 gets the subgroup of {1,14,9,11,4,3,6,13,2,15,5,12,7,10,8,16}

- Calculating the powers of 15 modulo 17 gets the subgroup of {1,2,4,8,9,13,15,16}

- Calculating the powers of 16 modulo 17 gets the subgroup of {1,16}

The generators are 3, 5, 6, 7, 10, 11, 12 and 14 for Z_{17}^* because they are all in the order of 16.

All the generators 3, 5, 6, 7, 10, 11, 12 and 14 gives a cyclic subgroup of order 16.

b) From (a), the candidate generators 16 is one and only prime order cyclic subgroup.

- let say:

P = 17

q = 2

so r = (p-1) / q

= 8

The module p is now defined as the subgroups of r^{th}.

G' = {[h^r mod p] | h E Z_p^*}

G' = {1^8 mod 17, ……………………, 16^8 mod 17}

Now if we mod for the above statement

We will get 1,1,16,16,16,1,1,16,16,16,1,16,1,1

G' = {1,1,16,16,16,1,1,16,16,16,1,16,1,1}

G' = {1, 16}

Therefore G' = H_{16}

Question 2: Find the gcd of the following pairs of polynomials. Are they co-prime?

(a) $x^3 - x + 1$ and $x^2 + 1$ over GF(3)

(b) $x^5 + x^4 + x^3 - x^2 - x + 1$ and $x^3 + x^2 + x + 1$ over GF(3)

Answer: a) GF (3) = Z_3 = {0,1,2}

w	Z = w^{-1}(*)	Z = w^{-1} (+)
0	φ	0
1	1	2
2	2	1

$x^3 - x + 1$ and $x^2 + 1$ over GF(3)

__x_______________

x^2+1 | $x^3 - x + 1$

$x^3 + x$

(-)__(-)__________________

x + 1

___x_____________

x + 1 | $x^2 + 1$

$x^2 + x$

_(-)__(-)__________________

2x + 1

___2________________

$2x + 1 \mid x + 1$

$4x + 1$

_(-)_(-)______________________

$-3x + 1$

______x____________________

$2 \mid 2x + 1$

$2x$

_(-)___________________________

1

After using the Euclidean algorithm, the remainder is 1. Since 1 has the degree of 0, it is the gcd of two polynomials.

Therefore $x^3 - x + 1$ and $x^2 + 1$ are co-primes over GF(3).

b) GF(3) = Z_3 = {0, 1, 2}

w	$Z=w^{-1}(*)$	$Z= w^{-1}$ (+)
0	φ	0
1	1	2
2	2	1

$x^5 + x^4 + x^3 - x^2 - x + 1$ and $x^3 + x^2 + x + 1$ over GF(3)

__x^2________________

$x^3 + x^2 + x + 1 \mid x^5 + x^4 + x^3 - x^2 - x + 1$

$x^5 + x^4 + x^3 + x^2$

(-)_(-)__(-)__(-)__________

$x^2 + 2x + 1$

___x__________

$x^2 + 2x + 1 \mid x^3 + x^2 + x + 1$

$x^3 + 2x^2 + x$

_(-)_____(-)_____

$2x^2 + 1$

___2_____________

$2x^2 + 1 \mid x^2 + 2x + 1$

$4x^2 + 2$

_(-)_(-)_________________

$2x - 1$ - **(2x + 2)**

___x_______________

$2x + 2 \mid 2x^2 + 1$

$2x^2 + 2x$

____(-)_________________

$-2x + 1$ – **(x + 1)**

After using the Euclidean algorithm, the remainder is x + 1. Since x + 1 has the degree of 1, it is the gcd of two polynomials.

Therefore $x^5 + x^4 + x^3 - x^2 - x + 1$ and $x^3 + x^2 + x + 1$ are not co-prime over GF(3).

Question 3 Answer:

The Extended Euclidean Algorithm is used to find the multiplicative inverses of non-zero polynomials in GF(24) with the irreducible polynomial x4 + x + 1. We've previously found the set of non-zero polynomials and started inverting the polynomial x3 + x. The steps below outline the process to find its inverse:

The division of x^4 + x + 1 by x^3 + x gives a quotient q_1(x) = x and a remainder r_1(x) = x^2 + x + 1.

The division of x^3 + x by x^2 + x + 1 yields a quotient q_2(x) = x + 1 and a remainder r_2(x) = x + 1.

The division of x^2 + x + 1 by x + 1 gives a quotient q_3(x) = x and a remainder r_3(x) = 1.

We now express the remainder 1 as a linear combination of the polynomial x^3 + x and the remainder sequence.

We find that r_2(x) is obtained from r_0(x) - q_2(x) * r_1(x), which simplifies to x + 1 = (x^3 + x) - (x + 1)(x^2 + x + 1).

Using the Extended Euclidean Algorithm:

W_1(x) = W_{-1}(x) - q_1(x) * W_0(x) = 1 since W_{-1}(x) = 1 and W_0(x) = 0.

W_2(x) = W_0(x) - q_2(x) * W_1(x) = x^2 as q_2(x) = x + 1 and W_1(x) = 1.

W_3(x) = W_1(x) - q_3(x) * W_2(x) = 1 + x^3 given that q_3(x) = x.

Therefore, W_3(x) = 1 + x^3 serves as the multiplicative inverse of x^3 + x in GF(2^4), satisfying the condition that (x^3 + x) * (1 + x^3) = 1 mod (x^4 + x + 1).

The procedure shown for x3 + x would be used systematically to all other non-zero polynomials in GF(24) to obtain their multiplicative inverses. It is important to remember that polynomial arithmetic in GF (2) requires coefficients to be reduced modulo 2.

Question 4: Consider Z^*_n for n = 15. Using Fermat's little theorem, how many witnesses can you find? Which ones? Are there any strong liars? Which ones? (See class notes for a worked-out example, Z^*_9).

Answer: When checking for witnesses in the context of Fermat's Little Theorem and its applications to primality testing.

We use the equation:

$a^{n-1} \bmod n = 1$

For composite numbers n, number a such that $1 < a < n-1$ is a Fermat witness if it does not satisfy the congruence.

We need to test if n = 15 is prime

$Z^*_{15} = \{1,2,4,7,8,11,13,14\}$

$| Z^*_{15}| = 8$

If $a^{n-1} \bmod n = 1$ for a composite number n, then a is called a Fermat liar because it falsely suggests that n might be prime.

For n = 15 we check:

(i) a = 2

$2^{14} \bmod 15 = 4$

(ii) a = 4

$4^{14} \bmod 15 = 1$

(iii) a = 7

$7^{14} \bmod 15 = 4$

(iv) a = 8

$8^{14} \bmod 15 = 4$

(v) a = 11

$11^{14} \bmod 15 = 1$

(vi) a = 13

13^{14} mod 15 = 4

(vii) a = 14

14^{14} mod 15 = 1

Now we're looking for any of these results not being equal to 1, which would indicate a witness to the compositeness of 15.

- 2, 7, 8, and 13 are the witnesses because 2^{14} mod 15, 7^{14} mod 15, 8^{14} mod 15, and 13^{14} mod 15 are not congruent to 1.

- 4, 11, and 14 are strong liars because 4^{14} mod 15, 11^{14} mod 15, and 14^{14} mod 15 are congruent to 1, which doesn't reveal the compositeness of 15.

So, the witnesses are 2, 7, 8 and 13

The strong liars are 4, 11 and 14

Question 5: Let's say, instead of using a composite N = pq in the RSA cryptosystem, we just use a prime modulus p. As in RSA, we will have an encryption exponent e, and the encryption of a message m mod p would be m^e mod p. Is this modified RSA secure? Either argue why it is or give a counter-example that breaks it (i.e., an adversary given only public parameters p, e, C = m^e mod p, can easily decrypt C to get plaintext m).

Answer: The security of the RSA is based on the difficulty of factoring the product of the two large prime numbers.

N = pq – (when using the composite numbers as modules)

The RSA cryptosystem significantly weakens the system. If an attacker knows N and the encryption exponent e, they cannot efficiently determine the decryption exponent d without factoring N into p and q to calculate Euler's totient function $\varphi(N)$.

Fermat's little theorem states that for any prime p and any integer a that is not divisible by p, we have $a^{(p-1)} = 1 \bmod p$.

Therefore, if we know p and e, we can easily find the decryption exponent d by computing d = (p-1)/e mod p-1. This works because ed = 1 mod p-1, which is the condition for RSA decryption.

Suppose, the encryption of the message m is $C = m^e \bmod p$

P is prime and the public key will be (p,e)

$\varphi(p) = p-1$

If the attacker can compute d such that $de \equiv 1 \bmod (p-1)$ because $\varphi(p)$ is known.

Once the attacker has d, they can decrypt C by computing:

$m = c^d \bmod p$

So, this effectively breaks the encryption, since m will be the plaintext message. The modified RSA is not secure.

For example,

Suppose p = 17, e = 3, and C = 10.

We can find d by computing d = (17-1)/3 mod 16 = 5.

Now we can decrypt C by computing $M = C^d \bmod p = 10^5 \bmod 17 = 15$.

This attack works for any prime p and any e that is relatively prime to p-1.

Therefore, using a prime modulus p in RSA is not secure. A counter-example that breaks it is given above.

Question 6: Consider an RSA system with the following parameters: p = 17, q = 23, N = 391, e = 3. Find d. Encrypt M = 55, showing the resulting ciphertext C. Now, decrypt C (using the d you computed), and verify we get back M.

Answer: In the RSA system, the parameters p and q are the prime numbers

It is used to generate the modules N

From the question, the parameters are:

p = 17

q = 23

N = 391

e = 3

Now we need to find d such that:

$ed \equiv 1(\bmod\ \varphi(N))$ ---------------------------- (1)

We don't know the value $\varphi(N)$

So, $\varphi(N)$ is Euler's totient function

$(p-1)\,(q-1) = (17-1)\,(23-1) = 16 * 22 = 352$

Therefore $\varphi(N) = 352$

Now let's find the d using the above equation (1)

$ed \equiv 1(\text{mod } \varphi(N))$

substitute all the values

$3d \equiv 1(\text{mod } 352)$

Now if we use the Extended Euclidean Algorithm

$d \equiv e^{-1} (\text{mod } \varphi(N))$

$d \equiv 3^{-1} (\text{mod } 352)$

$3 * d \text{ mod } 352 = 1$

$d = 235$ (this will be the private key)

Next, to encrypt a message M using the public key (N,e), we use the encryption function:

$C = M^e \text{ mod } N$

$M = 55$

$C = 55^3 \text{ mod } 391 = 166375 \text{ mod } 391 = 200$

Finally, to decrypt the ciphertext C using the private key d, we use the decryption function:

$M = C^d \text{ mod } N$

$= 200^{235} \text{ mod } 391 = 55$

The above process verifies that the RSA encryption and decryption work correctly with the given parameters.

7th Question Answer:

The encryption scheme presented in the question is to be similar to the El Gamal encryption system. In El Gamal, the discrete logarithm problem is the underlying hard problem which ensures the security of the system. This system is set in a cyclic group G of order p, where p is prime.

In the Decryption process Decrypt (SK, C):

Public key PK = (g_1, g_2, g_3)

The secret key SK = (a,b)

the ciphertext C = $(c_1, c_2, c_3) = (g_1^x, g_2^y, m.g_3^{x+y})$

To decrypt C, we do

Compute $s_1 = c_1^a – g_1^a = g_3$, $s_1 = g_3^x$

Compute $s_2 = c_2^b – g_2^a = g_3$, $s_2 = g_3^y$

Let's compute the inverse of g_3^{x+y} by multiplying the s_1 and s_2 as

$g_3^x.g_3^y = g_3^{x+y}$ and then to find the inverse of the result within the group G.

Now multiply c_3 by this inverse to obtain the original message m.

i.e., $m = c_3 . (g_3^{x+y})^{-1}$

So, the description of the decryption function is:

$M = Decrypt((a,b), (g_1^x, g_2^y, m.g_3^{x+y})) = c_3 . (c_1^a . c_2^b)^{-1}$

Here, $(c_1^a . c_2^b)^{-1}$ is the multiplicative inverse of g_3^{x+y} in the group G. The secret key (a,b) to compute inverse of the shared secret g_3^{x+y}.

So, it is used to decrypt the ciphertext c_3 to retrieve the message m.