EECE 455/632 – Cryptography and Network Security

HWK4 - SOLUTION

Question 1

Let *n* be an integer and *p* be a prime number. Explain why for all such *n* and *p*:

$$gcd(n, n+p) = 1 \text{ or } p$$

Answer:

If a number divides n+p and n, this implies that this number divides n+p-n= p.

- ⇨ Since p is prime, gcd (n+p,n) = 1 or p., depending on whether p divides n or not.

Question 2

Using Fermat Theorem, find 5^{301} mod 11.

Answer:

11 is prime, so $a^{10}= 1(\text{mod}11)$, for every a greater than 0.

So $5^{301}= 5^{30*10}*5= 1^{30} * 5= 5 \ (\text{mod}11)$

Question 3

Use Fermat Theorem to find a number *X* between 0 and 36, such that X^{109} is congruent to 8 modulo 37 (Don't use brute force to find x).

Answer:

$x^{109}= x^{(36*3)+1}= 1^3\ x= x(\text{mod}37)$: Fermat's little theorem

Hence, x=8(mod37), x=8

Question 4

Use Euler Theorem to find a number *a* between 0 and 9 such that *a* is congruent to 3^{500} modulo 10 (Note that this is the same as the last digit of the decimal expansion of 3^{500}).

Answer:

$A=3^{500}(\text{mod}10)$. $\Phi(10)= \varphi(2)\ \Phi(5)= 1*4= 4$

Hence, $a= (3^4)^{125}= 1^{125}= 1 \ (\text{mod } 10)$

Therefore, a=1.

Question 5

Prove the following:

If *p* is prime, then $\phi(p^i) = p^i - p^{i-1}$.

Hint: what numbers have a factor in common with p^i?

Answer:

Only the multiple of p have common factors with p_i given that p is prime

Then in p^i's residues, there are p^{i-1} multiples of p

Hence, $\varphi(p^i)= p^i-p^{i-1}$

Question 6

If gcd(m,n) = 1, then we can show that $\phi(mxn) = \phi(m)x\phi(n)$.

Also, we know that for a prime p, $\phi(p) = p-1;$ and $\phi(p^i) = p^i - p^{i-1}$

Given these properties, we can easily determine $\phi(n)$ for any n.

Determine: $\phi(61); \phi(62); \phi(63); \phi(64)$

Answer:

$\Phi(61) = 61-1 = 60$ since 61 is prime.

$\Phi(62) = \Phi(31) * \Phi(2) = 30*1=30$.

$\Phi(63) = \Phi(3^2) * \Phi(7)$

$\Phi(3^2)=3^2-3^1=6$

$\Phi(7)=6$, since 7 is prime

$\Phi(63)=6*6=36$

$\Phi(64) = \Phi(2^6)=2^6-2^5=32$

Question 7

Use Chinese Remainder Theorem to solve for *X*.

$X \equiv 2 \pmod 3; \quad X \equiv 3 \pmod 5; \quad X \equiv 2 \pmod 7$

Answer:

$M_1 = \frac{3*5*7}{3} = 35$

$M_1^{-1} = 2^{-1} \equiv 2 \pmod 3$

$c_1 = 35 * 2 = 70$

$M_2 = \frac{3*5*7}{5} = 21$

$M_2^{-1} = 1^{-1} \equiv 1 \pmod 5$

$c_2 = 21 * 1 = 21$

$M_3 = \frac{3*5*7}{7} = 15$

$M_3^{-1} = 1^{-1} \equiv 1 \pmod 7$

$c_3 = 15 * 1 = 15$

then $X \equiv 2 * 70 + 3 * 21 + 2 * 15 \bmod 105$

therefore, X=2

Question 8

Perform encryption and decryption using RSA for the following:

a. p=3; q=13; e=5; M=10
b. p=11; q=7; e=11; M=7

Answer:

a- PU{e,n}, PR{d,n}. p=3, q=13. n=p*q=39 φ(n)=(p-1)*(q-1)=2x12=24
e=5, e.d= 1 mod24; d is multiplicative inverse of e mod24. d=5.

$C=M^e \bmod n = 10^5 \bmod 39 = 4$

$M=C^d \bmod n= 4^5 \bmod 39 = 10$

b- p=11, q=7
n=p*q=11*7=77
φ(n)=(p-1)(q-1)=60
e=11
e.d=1 mod 60; d is multiplicative inverse of e mod 60
d = 11.
$C=M^e \bmod n = 7^{11} \bmod 77=7$

$M=C^d \bmod n= 7^{11} \bmod 77 = 7$

Question 9

In RSA you intercepted the ciphertext C = 8 sent to a user whose public key e = 13, n=33. What is the plaintext M?

Answer:

$M \equiv C^d \pmod n$, with $d \equiv e^{-1} \pmod{\emptyset (n)} \equiv 13^{-1} \pmod{\emptyset (33)}$
≡ 13-1 (mod 20) ≡ 17 (mod 20)
$M \equiv 8^{17} \pmod{33} \equiv 2 \pmod{33}$

Question 10

In RSA, the public key of a user is e=31 and n=3599. What is the private key of the user? (Use trial and error to find p and q)

Answer:

N=3599, iterating we find that p=59 and q=61
Therefore, ϕ(n)=(59-1)(61-1)=3480
d is the multiplicative inverse of e mod3480 ; e=31
Then d=3031
PU{31,3599}
PR{3031,3599}

Question 11

Use the fast exponentiation algorithm to determine $6^{477} \bmod 2345$.

Answer:

477 = 111011101

i	8	7	6	5	4	3	2	1	0
b_i	1	1	1	0	1	1	1	0	1
c	1	3	7	14	29	59	119	238	477
f	6	316	881	2311	2246	181	1931	211	2141

Question 12

Consider a Diffie-Hellman scheme with a common prime q = 13, and a primitive root $\alpha = 7$.

a. Show that 7 is a primitive root of 13.

b. If Alice has a public key $Y_A = 5$, what is Alice's private key X_A?

c. If Bob has a public key $Y_B = 12$, what is the secret key shared with Alice?

Answer:

7 is a primitive root modulo 13 if and only if $7^{12} \equiv 1 \pmod{13}$ and 7^d not congruent to 1 (mod 13) for every d such that d divides 12.

$7^1 \equiv 7 \pmod{13}$

$7^2 \equiv 10 \pmod{13}$

$7^3 \equiv 5 \pmod{13}$

$7^4 \equiv 9 \pmod{13}$

$7^6 \equiv 12 \pmod{13}$

$7^{12} \equiv 1 \pmod{13}$

So 7 is a primitive root modulo 13.

b- $Y_A = 5$, $Y_A = \alpha^x$ modq

$5 = 7^x \bmod 13$

Using the above table, we find out that $x_A = 3$

a- $Y_B = 12$

$K_{AB} = Y_B^{Xa}$ modq

$K^{AB} = 12^3 \bmod 13 = 12$

Question 13

Consider ElGamal scheme with a common prime q = 71 and a primitive root α = 7.

a. If B has public key Y_B = 3 and A chose the random integer k = 2, what is the ciphertext of M = 30?

b. If A now chooses a different value of k so that the encoding of M = 30 is C = (59, C_2), what is the integer C_2?

Answer:

One time key K=YBr modq
K=32mod71= 9 mod71
C1=a^r modq =7^2 mod 71= 49 mod71 =49
C2=K*M modq ; where M=30
C2=9*30 mod71 = 57
M is encrypted to (C1,C2) = (49,57)

b- C1 = 59 = ar mod q = 7k mod 71
k = 3
K = YBk mod q = 33 mod 71 = 27
So C2 = k × M mod q = 27 × 30 mod 71 = 29
C2 = 29

Question 14

The cryptosystem parameters of ECC scheme are $E_{11}(1, 6)$ and G = (2, 7). B's secret key is n_B = 3.

a. Find B's public key P_B.

b. A wishes to encrypt the message P_m = (10, 9) and choose a random value k = 4. Determine the ciphertext C_m.

c. Show how to recover P_m from C_m.

Answer:

PB = 3(2,7)

$m2 = \frac{3x_1^2 + a}{2y_1} = \frac{3 \times 2^2 + 1}{2 \times 7} = \frac{13}{14} \equiv 2 \times 3\text{-}1 \equiv 2 \times 4 = 8$

$x2 = m2^2 - x1 - x1 = 8^2 - 2 \times 2 = 60 \equiv 5$

$y2 = m2\ (x1 - x2) - y1 = 8 \times (2\text{-}5) - 7 = -31 \equiv 2$

PB = (2,7) + (5,2)

$m3 = \frac{y_2 - y_1}{x_2 - x_1} = \frac{2-7}{5-2} = \frac{-5}{3} \equiv -5 \times 3\text{-}1 \equiv -5 \times 4 \equiv 2$

$x3 = m3^2 - x1 - x2 = 2 \times 2 - 2 - 5 = -3 \equiv 8$

$y3 = m3\ (x1 - x3) - y1 = 2(2\text{-}8) - 7 = -19 \equiv 3$

PB = 3(2,7) = (8,3)

b- $kG = 4(2,7) = 2(5,2)$

$m = \frac{3 \times 5^2 + 1}{2 \times 2} = 76 \times 4^{-1} \equiv 10 \times 3 \equiv 8$

$x = 8^2 - 2 \times 5 = 54 \equiv 10$

$y = 8 \times (5-10) - 2 = -42 \equiv 2$

$kG = (10,2)$

$kPB = 4(8,3)$

$m = \frac{3 \times 8^2 + 1}{2 \times 3} \equiv 6 \times 6^{-1} = 1$

$x = 1^2 - 8 - 8 = -15 \equiv 7$

$y = 1(8-7) - 3 = -2 \equiv 9$

$kPB = 2(7,9)$

$m = \frac{3 \times 7^2 + 1}{2 \times 3} \equiv 5 \times 7^{-1} = 40 \equiv 7$

$x = 7^2 - 7 - 7 = 35 \equiv 2$

$y = 7(7-2) - 9 = 26 \equiv 4$

$kPB = (2,4)$

$Pm + kPB = (10,9) + (2,4)$

$m = \frac{4-9}{2-10} = \frac{-5}{-8} \equiv 6 \times 3^{-1} = 6 \times 4 \equiv 2$

$x = 2^2 - 10 - 2 = -8 \equiv 3$

$y = 2(10-3) - 9 = 5$

$Pm + kPB = (3,5)$

$Cm = \{(10,2), (3,5)\}$

c- $Pm = (Pm + kPB) - nB(kG) = (3,5) - 3(10,2)$

$m = \frac{3 \times 10^2 + 1}{2 \times 2} \equiv \frac{4}{4} = 1$

$x = 1^2 - 10 - 10 = -19 \equiv 3$

$y = 1(10-3) - 2 = 5$

$2(10,2) = (3,5)$

$m = \frac{5-2}{3-10} \equiv \frac{3}{4} = 3 \times 3 = 9$

$x = 9^2 - 10 - 3 = 68 \equiv 2$

$y = 9(10-2) - 2 = 70 \equiv 4$

$3(10,2) = (2,4)$

$-3(10,2) = -(2,4) = (2,-4) \equiv (2,7)$

$Pm = (3,5) + (2,7)$

$m = \frac{7-5}{2-3} = \frac{2}{-1} = -2 \equiv 9$

$x = 9^2 - 3 - 2 = 76 \equiv 10$

$y = 9(3-10) - 5 = -68 \equiv 9$

$Pm = (10,9)$