SOLUTIONS FOR ASSIGNMENT-5

HUMESH REDDY VENKATAPURAM CS 525: INTRO TO CRYPTO

1) Find discrete logarithm using Baby-Step-Giant-Step algorithm. Show your work:

(a) Given cyclic group Z^*_{29} and 2^x mod 29 = 27. Find x = $\log_2$ 27 in Z^*_{29}

Answer:

Let's find $2^x = 27$ in Z^*_{29}

$|Z^*_{29}| = 28$ ---------------- q

$t \approx \lfloor \sqrt{q} \rfloor \approx \sqrt{28} \approx 5$

Now, we need to find g and h.

$2^x = 27$ is in the form of $g^x = h$

g=2, h=27

Giant Steps:

- 2^0 mod 29 = 1
- 2^5 mod 29 = ($2^2 * 2^2 * 2$) mod 29 = 3
- 2^{10} mod 29 = ($2^5 * 2^5$) mod 29 = 3 * 3 mod 29 = 9
- 2^{15} mod 29 = ($2^{10} * 2^5$) mod 29 = 9 * 3 mod 29 = 27
- 2^{20} mod 29 = ($2^{10} * 2^{10}$) mod 29 = 9 * 9 mod 29 = 23
- 2^{25} mod 29 = ($2^{10} * 2^{10} * 2^5$) mod 29 = 9 * 9 * 3 mod 29 = 11

Baby Steps:

$h*g^i$ mod 37 where i = 1 to t

- 27 * 2^1 mod 29 = 25
- 27 * 2^2 mod 29 = 21
- 27 * 2^3 mod 29 = 13
- 27 * 2^4 mod 29 = 26
- 27 * 2^5 mod 29 = 23

In the above giant and baby step we got similar remainder 23

Now, we need to find $h^* g^i \stackrel{?}{=} g^{k^*t}$ (for some k > 1)

$27 * 2^5 = 23 = 2^{20}$

So, kt = 20

Finally, compute $\log_g h = (k^*t - i) \bmod q$

$\log_2 27 = (20 - 5) \bmod 28 = 15 \bmod 28 = 15$

so, x = 15

Sanity Check:

$2^x \bmod 29 = 27$ --------------- (1)

Substitute x in (1)

$2^{15} \bmod 29 = 2^5 * 2^5 * 2^5 \bmod 29 = 27$

(b) Given cyclic group Z^*_{37}, and $2^x \bmod 37 = 6$. Find $x = \log_2 6$ in Z^*_{37}.

Let's find $2^x = 37$ in Z^*_{37}

$|Z^*_{37}| = 36$ ----------------- q

$t \approx \lfloor\sqrt{q}\rfloor \approx \sqrt{36} \approx 6$

Now, we need to find g and h.

$2^x = 6$ is in the form of $g^x = h$

g=2, h=6

Giant Steps:

- $2^0 \bmod 37 = 1$
- $2^6 \bmod 37 = (2^2 * 2^2 * 2^2) \bmod 37 = 27$
- $2^{12} \bmod 37 = (2^6 * 2^6) \bmod 37 = 27 * 27 \bmod 37 = 26$
- $2^{18} \bmod 37 = (2^{12} * 2^6) \bmod 37 = 26 * 27 \bmod 37 = 36$
- $2^{24} \bmod 37 = (2^{12} * 2^{12}) \bmod 37 = 26 * 26 \bmod 37 = 10$
- $2^{30} \bmod 37 = (2^{18} * 2^{12}) \bmod 37 = 36 * 26 \bmod 37 = 11$
- $2^{36} \bmod 37 = (2^{30} * 2^6) \bmod 37 = 11 * 27 \bmod 37 = 1$

Baby Steps:

$h^*g^i \bmod 37$ where i = 1 to t

$6 * 2^1 \bmod 37 = 12$

$6 * 2^2 \bmod 37 = 24$

$6 * 2^3 \bmod 37 = 11$

$6 * 2^4 \bmod 37 = 22$

$6 * 2^5 \bmod 37 = 7$

$6 * 2^6 \bmod 37 = 14$

In the above giant and baby step we got similar remainder 11

Now, we need to find $h * g^i \stackrel{?}{=} g^{k*t}$ (for some k > 1)

$6 * 2^3 = 11 = 2^{30}$

So, kt = 30

Finally, compute $\log_g h = (k*t - i) \bmod q$

$\log_2 6 = (30-3) \bmod 36 = 27 \bmod 36 = 27$

so, x = 27

Sanity Check:

$2^x \bmod 37 = 6$ --------------- (1)

Substitute x in (1)

$2^{27} \bmod 37 = 2^{10} * 2^{10} * 2^5 * 2^2 \bmod 29 = 6$

(c) Given cyclic group Z^*_{17}, and $3^x \bmod 17 = 7$. Find $x = \log_3 7$ in Z^*_{17}.

Let's find $3^x = 17$ in Z^*_{17}

$|Z^*_{17}| = 16$ -------------------- q

$t \approx \lfloor \sqrt{q} \rfloor \approx \sqrt{16} \approx 4$

Now, we need to find g and h

$g^x = h$

$3^x = 7$ is in the form of $g^x = h$

g=3, h=7

Giant Steps:

- $3^0 \bmod 17 = 1$

- 3^4 mod 17 = (3^2 * 3^2) mod 17 = 13

- 3^8 mod 17 = (3^4 * 3^4) mod 17 = 13 * 13 mod 17 = 16

- 3^{12}mod 17 = (3^4 * 3^4) mod 17 = 16 * 16 mod 17 = 4

- 3^{16}mod 17 = (3^4 * 3^4 * 3^4) mod 17 = 16 * 16 * 16 mod 17 = 1

Baby Steps:

h*g^i mod 17 where i = 1 to t

- 7 * 3^1 mod 17 = 4

- 7 * 3^2 mod 17 = 12

- 7 * 3^3 mod 17 = 2

- 7 * 3^4mod 17 = 6

In the above giant and baby step we got similar remainder 4

Now, we need to find h* $g^i \stackrel{?}{=} g^{k*t}$ (for some k > 1)

7 * 3^1 = 4 = 3^{12}

So, kt = 12

Finally, compute $\log_g$ h = (k*t - i) mod q

$\log_3 7$ = (12 - 1) mod 16 = 11 mod 16 = 11

so, x = 11

Sanity Check:

3^x mod 17 = 7 --------------- (1)

Substitute x in (1)

3^{11} mod 17 = 3^5 * 3^5 * 3 mod 17 = 7

2) Find discrete logarithm using Pohlig-Hellman algorithm. Show your work:

(a) Given cyclic group Z^*_{11}, and 2^x mod 11 = 10. Find x = $\log_2$ 10 in Z^*_{11}

Answer:

$|Z^*_{11}|$ = 10 --------------------- q

Let q = 10 = 5 * 2

So, q1 = 5 and q2 = 2

Now, we need to find g and h

$g^x = h$

$2^x = 10$ is in the form of $g^x = h$

g=2, h=10

Now we use $(g^{q/qi})^2 = (g^x)^{q/qi} = h^{q/qi}\ \forall\ i \in 1..k$

$H_1 \rightarrow$

$(g^{q/q1})^{x1}$ mod 11 = $(h^{q/q1})$ mod 11

- $(2^{10/5})^{x1}$ mod 11 - $(2^2)^{x1}$ mod 11 – (4 mod 11) $^{x1} = 4^{x1}$

- $(10^{10/5})$ mod 11 – 10^2 mod 11 - 1

So, $(4)^{x1} \equiv 1 \pmod{11}$

$H_2 \rightarrow$

$(g^{q/q2})^{x2}$ mod 11= $(h^{q/q2})$ mod 11

- $(2^{10/2})^{x2}$ mod 11 - $(2^5)^{x2}$ mod 11 - $(32 \bmod 11)^{x2}$ - $(10)^{x2}$

- $(10^{10/2})$ mod 11 – 10^5 mod 11 = 10

So, $(10)^{x2} \equiv 10 \pmod{11}$

We know |H1| = q1 = 5, |H2| = q2 = 2

Using Extended CRT:

X = [(x_1 mod q_1), (x_2 mod q_2)]

x = [($4^{x1} \equiv 1$ (mod11)), ($10^{x2} \equiv 10$ (mod11))]

= [(0 mod 5), (1 mod 2)]

Solving, x = 5

Sanity Check:

2^x mod 11 = 10 --------------- (1)

Substitute x in (1)

2^5 mod 11 = $2^2 * 2^2 * 2$ mod 11 = 10

(b) Given cyclic group Z^*_{31}, and 3^x mod 31 = 12. Find x = $\log_3 12$ in Z^*_{31}.

$|Z^*_{31}| = 30$ ---------------------- q

Let q = 30 = 5 * 3 * 2

So, q1 = 5, q2 = 3 and q3 = 2

Now, we need to find g and h

$g^x = h$

$3^x = 12$ is in the form of $g^x = h$

G = 3, h = 12

Now we use $(g^{q/qi})^2 = (g^x)^{q/qi} = h^{q/qi}$ $\forall$ i $\in$ 1..k

$H_1 \rightarrow$

$(g^{q/q1})^{x1}$ mod 31 = $(h^{q/q1})$ mod 31

- $(3^{30/5})^{x1}$ mod 31 - $(3^6)^{x1}$ mod 31 – $(3^3 * 3^3 \text{ mod } 31)^{x1} = 16^{x1}$

- $(12^{30/5})$ mod 31 – 12^6 mod 31 – $(12^3 * 12^3$ mod 31) - 2

So, $(16)^{x1} \equiv 2 \pmod{31}$

$H_2 \rightarrow$

$(g^{q/q2})^{x2}$ mod 31= $(h^{q/q2})$ mod 31

- $(3^{30/3})^{x2}$ mod 31 - $(3^{10})^{x2}$ mod 31 - $(3^5 * 3^5 \text{ mod } 31)^{x2}$ - $(25)^{x2}$

- $(12^{30/3})$ mod 31 – 12^{10} mod 31 = $(12^5 * 12^5$ mod 31) - 25

So, $(25)^{x2} \equiv 25 \pmod{31}$

$H_3 \rightarrow$

$(g^{q/q3})^{x3}$ mod 31= $(h^{q/q3})$ mod 31

- $(3^{30/2})^{x2}$ mod 31- $(3^{15})^{x2}$ mod 31 - $(3^5 * 3^5 * 3^5 \text{ mod } 31)^{x2}$ - $(30)^{x2}$

- $(12^{30/3})$ mod 31 – 12^{15} mod 31 = $(12^5 * 12^5 * 12^5$ mod 31) = 25

So, $(30)^{x3} \equiv 25 \pmod{31}$

We know |H 1 | = q1 = 5, |H2 | = q2 = 3, |H 3 | = q3 = 2

Using Extended CRT:

x = [(x_1 mod q_1), (x_2 mod q_2), (x_3 mod q_3)]

$x = [(16^{x1} = 2 \ (mod31)\ ), (25^{x2} = 25\ (mod31)), (30^{x3} = 25\ (mod31)]$

$= [(4 \bmod 5), (1 \bmod 3), (1 \bmod 2)]$

Solving, x = 19

Sanity Check:

$3^x \bmod 31 = 12$ --------------- (1)

Substitute x in (1)

$3^{19} \bmod 31 = 3^6 * 3^6 * 3^6 * 3 \bmod 11 = 12$

(c) Given cyclic group Z^*_{23}, and $5^x \bmod 23 = 15$. Find $x = \log_5 15$ in Z^*_{23}.

$|Z^*_{23}| = 22$ ---------------------- q

Let q = 22 = 11 * 2

So, q1 = 11, q2 = 2

Now, we need to find g and h

$g^x = h$

$5^x = 15$ is in the form of $g^x = h$

g = 5, h = 15

Now we use $(g^{q/qi})^2 = (g^x)^{q/qi} = h^{q/qi}\ \forall\ i \in 1..k$

$H_1 \rightarrow$

$(g^{q/q1})^{x1} \bmod 23 = (h^{q/q1}) \bmod 23$

$- (5^{22/11})^{x1} \bmod 23 - (5^2)^{x1} \bmod 23 – (5 * 5 \bmod 23)^{x1} = 2^{x1}$

$- (15^{22/11}) \bmod 23 – 15^2 \bmod 23 – (15 * 15 \bmod 23) - 18$

So, $(2)^{x1} \equiv 18 \pmod{23}$

$H_2 \rightarrow$

$(g^{q/q1})^{x1} \bmod 23 = (h^{q/q1}) \bmod 23$

$- (5^{22/2})^{x1} \bmod 23 - (5^{11})^{x1} \bmod 23 – (5^5 * 5^5 * 5 \bmod 23)^{x1} = 22^{x1}$

$- (15^{22/2}) \bmod 23 – 15^{11} \bmod 23 – (15^5 * 15^5 * 15 \bmod 23) - 22$

So, $(22)^{x1} \equiv 22 \pmod{23}$

We know |H 1 | = q1 = 11, |H2 | = q2 = 2

Using Extended CRT:

$x = [(x_1 \bmod q_1), (x_2 \bmod q_2)]$

$x = [(2^{x1} \equiv 18 \pmod{23}), (22^{x2} \equiv 22 \pmod{31})]$

$x = [(6 \bmod 11), (1 \bmod 2)]$

Solving, $x = 17$

Sanity Check:

$5^x \bmod 23 = 15$ --------------- (1)

Substitute x in (1)

$5^{17} \bmod 23 = 5^5 * 5^5 * 5^5 * 5 \bmod 23 = 15$

3) Consider a group Z^*_{23}, and a message M = 10. Encrypt M using ElGamal encryption scheme (you'll have to pick the PK, SK before encryption) to obtain ciphertext C. Now decrypt C to verify you get M back. Show your steps.

We need to choose a cyclic group of order q with generator g

$G = Z^*_{23} = \{1,2,3,4,5,6,7,8,9,10,11,12,13,14,15,16,27,18,19,20,21,22\}$

Let q = 23.

Let's find g

- candidate generator 2

$2^x \bmod 23 = \{1,2,4,8,16,9,18,13,3,6,12,1,2,4,8,16,9,18,13,3,6,12\} \neq G$

- candidate generator 3

$3^x \bmod 23 = \{1,3,9,4,12,13,16,2,6,18,8,1,3,9,4,12,13,16,2,6,18,8\} \neq G$

- candidate generator 4

$4^x \bmod 23 = \{1,4,16,18,3,12,2,8,9,13,6,1,4,16,18,3,12,2,8,9,13,6\} \neq G$

- candidate generator 5

$5^x \bmod 23 = \{1,5,2,10,4,20,8,17,16,11,9,22,18,21,13,19,3,15,6,7,12,14\} = G$

Since 5 is a primitive root modulo 23

Now, choose a private key randomly from {1, ………………, q-1}

I choose x = 2

Let's compute with the private key $h = g^x = 5^2 = 25$

Now we need to return PK = (G,g,q,h), SK = (G,g,q,x)

So, PK = (G,5,23,25)

SK = (G,5,23,2)

Encryption:

Choose a random integer y from {1, ……………., q-1}

y = 1

c = (c1,c2)

$c1 = g^y$, $c2 = h^y . m$

$c = (g^y, h^y . m) = (5^1, 25^1 . 10) = (5, 250)$

(c1, c2) = (5, 250)

Decryption:

Compute $m = c2 / c1^x = h^y . m / g^{yx} = 250 / 5^2$

$= 250 / 25 = 10$

We retrieved the original message M = 10

Therefore, the encryption and decryption process preserve the message M = 10

4) Compute 4^{23} mod 187, and 9^{36} mod 101, using square-and-multiply method.

- 4^{23} mod 187

We need to convert 23 to binary - 10111

Now we will rewrite the converted binary:

1	10	101	1011	10111
↓	↓	↓	↓	↓
1	2	5	11	23

Now calculate the following:

- 4^1 mod 187 = 4

- 4^2 mod 187 = 16

- 4^5 mod 187 = (4^2 * 4^2 * 4) mod 187 = (16 * 16 * 4) mod 187 = 89

- 4^{11} mod 187 = (4^5 * 4^5 * 4) mod 187 = (89 * 89 * 4) mod 187 = 81

- 4^{23} mod 187 = (4^{11}* 4^{11} * 4) mod 187 = (81 * 81 * 4) mod 187 = 64

- 9^{36} mod 101

We need to convert 36 to binary - 100100

Now we will rewrite the converted binary:

1	10	100	1001	10010	100100
↓	↓	↓	↓	↓	↓
1	2	4	9	18	36

Now calculate the following:

- 9^1 mod 101 = 9

- 9^2 mod 101 = 81

- 9^4 mod 101 = (9^2 * 9^2) mod 101 = (81 * 81) mod 101 = 97

- 9^9 mod 101 = (9^4 * 9^4 * 9) mod 101 = (97 * 97 * 9) mod 101 = 43

- 9^{18} mod 101 = (9^9 * 9^9) mod 101 = (43 * 43) mod 101 = 31

- 9^{36} mod 101 = (9^{18} * 9^{18}) mod 101 = (31 * 31) mod 101 = 52