Homework Assignment 2

Harshitha Chidananda

Winter Quarter 2017

CS 292F Elliptic Curve Cryptography : Discrete Logarithm Problem

Consider the discrete logarithm problem:

y = g^x(mod 2017)

for the primitive g = 5 and y = 1736

1. Write a simple exhaustive search code to find x and verify.

```
#using python for Simple Exhaustive search code to find the value of x

y=1736
for i in range (1,2016):
    z=(5**i)%2017
    if z==y :
        print "Value of x is :" , i
```

Listing 1: Simple Exhaustive search code

Value of x is : 1234

Verification:

5^{1234} = 1736 (mod 2017)

Therefore, value of x is 1234

---

2. Find x using Shank's algorithm. Show the steps, and produce the S and T tables.

m = $\lceil\sqrt{2017}\rceil$ = 45

S = (i, 5^{45*i}) | i = 0, 1, . . . , 45

T = (j, $1736 * 5^j$ | j = 0, 1, . . . , 45

```
#using python for Shank's algorithm

#S Table
print "Shank's algorithm!\n"
print "\n\n S table \n"
for x in range(0,46):
    val = (5**(45*x))%2017;
    print x," ",val,"\n";

#T table
print "\n\n T table \n"
for y in range(0,46):
    val = (1736*(5**y))% 2017;
    print y,"  ",val,"\n";

#Finding values from S and T table to compute x
for x in range(0,46):
    x_val = (5**(45*x))%2017;
    for y in range(0,46):
        y_val = (1736*(5**y))% 2017;
        if x_val==y_val:
            print x," ",y,"\n"
```

Listing 2: Shank's algorithm

S table

i	S	i	S	i	S	i	S	i	S
0	1	10	496	20	1959	30	1487	40	1347
1	45	11	133	21	1424	31	354	41	105
2	8	12	1951	22	1553	32	1811	42	691
3	360	13	1064	23	1307	33	815	43	840
4	64	14	1489	24	322	34	369	44	1494
5	863	15	444	25	371	35	469	45	669
6	512	16	1827	26	559	36	935		
7	853	17	1535	27	951	37	1735		
8	62	18	497	**28**	**438**	38	1429		
9	773	19	178	29	1557	39	1778		

T table

j	T	j	T	j	T	j	T	j	T
0	1736	10	1994	20	1728	30	1455	40	1971
1	612	11	1902	21	572	31	1224	41	1787
2	1043	12	1442	22	843	32	69	42	867
3	1181	13	1159	23	181	33	345	43	301
4	1871	14	1761	24	905	34	1725	44	1505
5	1287	15	737	25	491	35	557	45	1474
6	384	16	1668	**26**	**438**	36	768		
7	1920	17	272	27	173	37	1823		
8	1532	18	1360	28	865	38	1047		
9	1609	19	749	29	291	39	1201		

ith value of 28 in S table has the same value as jth value of 26 in T table. That is 438

x = 28*45 - 26

x = 1234

Verification:

$5^{1234} = 1736 \pmod{2017}$

Therefore, value of x is 1234

---

3. Find x using Pollard Rho algorithm. Show the steps, and produce the sequence

y = 1736 = $5^x \pmod{2017}$

On dividing the set S={1,2,3,...,2016} into 3 sets such that :

S_0 = {1,2,....,672}

S_1 = {673,....,1345}

S_2 = {1346,....,2016}

Choosing a random value for α : $\alpha = 7$

```
#using python for Pollard Rho Algorithm

val = (5**30) % 2017
print "S1 ", val , "\n";
my_list = list()
for i in range (1,10):
    val2 = (val**2)%2017
    if val2 >=1 and val2 <=672 :
        print "S0 ", val2 , "\n";
    elif val2>=673 and val2<=1345 :
        print "S1 ", val2 , "\n";
    elif val2>=1346 and val2<=2016 :
        print "S2 " , val2 , "\n"
    else:
        print "oops \n"

    my_list.append(val)
    my_list.append(val2)
    val = (1736*val2) %2017

    if val >=1 and val <=672 :
        print "S0 ", val , "\n";
    elif val>=673 and val<=1345 :
```

```
        print "S1 ", val , "\n";
    elif val>=1346 and val<=2016 :
        print "S2 " , val , "\n"
    else:
        print "oops \n"

print my_list
map(lambda val: (val, [i for i in xrange(len(my_list)) if my_list[i] == val]), my_list)
```

Listing 3: Pollard Rho algorithm

Using Pollard Rho algorithm and using α as 7, we obtain the value of x to be 1234

Verification: (5^{1234}) mod 2017 results in the value of y which is 1736

---

4. Find x using Pohlig-Hellman algorithm. You can use the factorization of 2016 = $2^5 3^2 7$ to create two smaller discrete log problems, for example 2016 = 36 · 56. Show the steps.

y = 1736 = g^x(mod p)

g=5 , p = 2017

p − 1=2016

2016 = 36 . 56

a=36 , b=56

Step 1: Find r

Solve for r in

$(g^a)^r = y^a$(mod p)

g=5 , a=36 , r=? , y=1736 , p = 2017

$(5^{36})^r = 1736^{36}$(mod 2017)

$995^r = 1695$ (mod 2017)

Since 995 is of order b = 56, we solve a smaller DLP.

The solution r is in the set [0, b − 1] = [0, 55]

This DLP gives r = 2 since $995^2 = 1695$ mod 2017

r=2

Step 2: Find s

$(g^b)^s = y.g^{-r}$(mod p)

g = 5 , b = 56 , y = 1736 , r = 2 , p = 2017 , s = ?

$(5^{56})^s = 1736.5^{-2}$(mod 2017)

$284^s = 1736.1775$(mod 2017)

$284^s = 1441$(mod 2017)

This is also a smaller DLP, since s is in the set [0, a − 1] = [0, 55] = [0, 36] We find s = 22,

since $284^{22} = 1441$ (mod 2017)

s=22

Step 3: Find x

x = r + s · b

r = 2 , s = 22 , b = 56

x = 2 + 22.56

Value of x = 1234

Verification:

$g^x = 5^{1234}$ (mod 2017) = 1736 = y

---

5. Find x using the Index Calculus algorithm. Try the prime base $\{2, 3, 5\}$ and if this does not work, try $\{2, 3, 5, 7\}$. Show the steps.

Trying the prime base for $\{2, 3, 5\}$

Step 1:

g^{α}

From the program written below, found 3 smooth values: 75,76 and 106

```
#using python to find the suitable value of alpha

for i in range (1,110):
    smooth = (5**i)%2017
    if smooth%2==0 and smooth%3==0 and smooth%5==0:
        print i," ",smooth,"\n"
```

Listing 4: Finding if the value of alpha leads to smooth

$5^{75} = 90$(mod 2017) = $2^1 * 3^2 * 5$ (mod 2017)

$1.log_5 2 + 2.log_5 3 + 1.log_5 5$ (mod 2016)

$5^{76} = 450$(mod 2017) = $2^1 * 3^2 * 5^2$ (mod 2017)

$1.log_5 2 + 2.log_5 3 + 2.log_5 5$ (mod 2016)

$5^{106} = 900$(mod 2017) $= 2^2 * 3^2 * 5^2$ (mod 2017)

$2.log_5 2 + 2.log_5 3 + 2.log_5 5$ (mod 2016)

Step 2: Solving equations

$1.log_5 2 + 2.log_5 3 + 1.log_5 5$ (mod 2016)

$1.log_5 2 + 2.log_5 3 + 2.log_5 5$ (mod 2016)

$2.log_5 2 + 2.log_5 3 + 2.log_5 5$ (mod 2016)

$$\begin{bmatrix} 1 & 2 & 1 \\ 1 & 2 & 2 \\ 2 & 2 & 2 \end{bmatrix} \begin{bmatrix} \log_5 2 \\ \log_5 3 \\ \log_5 5 \end{bmatrix} = \begin{bmatrix} 75 \\ 76 \\ 106 \end{bmatrix}$$

We find the solution as

$log_5 30$=2(mod 2017)

$log_5 22$=3(mod 2017)

$log_5 1$=5(mod 2017)

Step 3: Finding the value of x

For y=1736

Finding α such that the value is smooth

$\alpha = 690$

Applying the formula $log_g y = -\alpha + \sum_{p_i \in S} \alpha_i log_g p^i (mod$ p-1)

We obtain $log_g 1736 = 1234$ (mod 2016)

The value of x is 1234

The solution is x = 1234 in 1736 = 5^x (mod 2017),

since $5^{1234} = 1736$ (mod 2017)

Also trying the prime base for $\{2, 3, 5, 7\}$

Step 1: Finding α in g^α

From the program written below, found 4 α which lead to smooth values: 673, 889 , 919 and 1875

```
#using python to find the suitable value of alpha

for i in range (1,110):
    smooth = (5**i)%2017
    if smooth%2==0 and smooth%3==0 and smooth%5==0 and smooth%7==0:
```

```
        print i," ",smooth,"\n"
```

Listing 5: Finding if the value of alpha leads to smooth

$5^{673} = 1470(\text{mod } 2017\ ) = 2^1 * 3^1 * 5^1 * 7^2\ (\text{mod } 2017)$

$1.log_5 2\ +\ 1.log_5 3\ +\ 1.log_5 5\ +\ 2.log_5 7\ (\text{mod } 2016)$

$5^{889} = 630(\text{mod } 2017\ ) = 2^1 * 3^2 * 5^1 * 7^1(\text{mod } 2017)$

$1.log_5 2\ +\ 2.log_5 3\ +\ 1.log_5 5\ +\ 1.log_5 7\ (\text{mod } 2016)$

$5^{919} = 1260(\text{mod } 2017\ ) = 2^2 * 3^2 * 5^1 * 7^1\ (\text{mod } 2017)$

$2.log_5 2\ +\ 2.log_5 3\ +\ 1.log_5 5+\ 1.log_5 7\ (\text{mod } 2016)$

$5^{1875} = 210(\text{mod } 2017\ ) = 2^1 * 3^1 * 5^1 * 7^1\ (\text{mod } 2017)$

$1.log_5 2\ +\ 1.log_5 3\ +\ 1.log_5 5+\ 1.log_5 7\ (\text{mod } 2016)$

Step 2: Solving equations

$1.log_5 2\ +\ 1.log_5 3\ +\ 1.log_5 5\ +\ 2.log_5 7\ (\text{mod } 2016)$

$1.log_5 2\ +\ 2.log_5 3\ +\ 1.log_5 5\ +\ 1.log_5 7\ (\text{mod } 2016)$

$2.log_5 2\ +\ 2.log_5 3\ +\ 1.log_5 5+\ 1.log_5 7\ (\text{mod } 2016)$

$1.log_5 2\ +\ 1.log_5 3\ +\ 1.log_5 5+\ 1.log_5 7\ (\text{mod } 2016)$

$$\begin{bmatrix} 1 & 1 & 1 & 2 \\ 1 & 2 & 1 & 1 \\ 2 & 2 & 1 & 1 \\ 1 & 1 & 1 & 1 \end{bmatrix} \begin{bmatrix} \log_5 2 \\ \log_5 3 \\ \log_5 5 \\ \log_5 7 \end{bmatrix} = \begin{bmatrix} 673 \\ 889 \\ 919 \\ 1875 \end{bmatrix}$$

We find the solution as

$log_5 2 = 30$

$log_5 3 = 1030$

$log_5 5 = 1$

$log_5 7 = 814$

These are verified as:

5^{30}=2(mod 2017)

5^{1030}=3(mod 2017)

5^{1}=5(mod 2017)

5^{814}=7(mod 2017)

Step 3: Finding the value of x

For y = 1736:

Finding α such that the value is smooth

$\alpha = 641$

y.g^{α} = 1736.5^{641} (mod 2017)

=210 (mod 2017)

The number factors as 210 are $2^1.3^1.5^1.7^1$

$log_g y = -\alpha + \sum_{p_i \in S} \alpha_i log_g p^i (mod$ p-1)

$log_5 1736 = -641 + \sum_{p_i \in S} \alpha_i log_5 p^i$ (mod 2016)

log_g1736 = -641 + 1.$log_5$2 + 1.$log_5$3 + 1.$log_5$5 + 1.$log_5$7 (mod 2016)

log_g1736 = -641 + 30 + 1030 + 1 + 814 (mod 2016)

log_g1736 = 1234 (mod 2016)

The value of x is 1234

The solution is x = 1234 in 1736 = 5^x (mod 2017), since 5^{1234} = 1736 (mod 2017)

Thank You