8

Homework 8 Cryptography

Rick Staals 0716184
Erwin van Duijnhoven 0719562

November 20, 2013

Exercise 1

4/5

Use the schoolbook version of Polard's rho method to attack the discrete logarithm problem given by $g = 3, h = 245$ in $\mathbb{F}_{1013}^*$, i.e. find an integer $0 < a < 1012$ such that $h = g^a$, using the t_i and r_i (the twice as fast walk) as defined in class (also, see below).
Let $t_0 = g, a_0 = 1$, and $b_0 = 0$ and define

$$t_{i+1} = \begin{cases} t_i \cdot g \\ t_i \cdot h \\ t_i^2 \end{cases}, a_{i+1} = \begin{cases} a_i + 1 \\ a_i \\ 2a_i \end{cases}, b_{i+1} = \begin{cases} b_i \\ b_i + 1 \\ 2b_i \end{cases} \text{ for } t_i \equiv \begin{cases} 0 \mod 3 \\ 1 \mod 3 \\ 2 \mod 3 \end{cases}$$

where one takes t_i as an integer.
The twice as fast walk has $r_i = t_{2i}$.
Note that this version offers less randomness in the walk, splitting into more than 3 sets increases the randomness. The walk could start at any $t_0 = g^{a_0}h^{b_0}$ for known a_0 and b_0

Answer 1

0.1 Using t_i

i	t_i	a_i	b_i	$t_i \mod 3$
0	3	1	0	0
1	9	2	0	0
2	27	3	0	0
3	81	4	0	0
4	243	5	0	0
5	729	6	0	0
6	161	7	0	2
7	596	14	0	2
8	666	28	0	0
9	985	29	0	1
10	231	29	1	0
11	693	30	1	0
12	53	31	1	2
13	783	62	2	0
14	323	63	2	2
15	1003	126	4	1
16	589	126	5	1
17	459	126	6	0
18	364	127	6	1
19	36	127	7	0
20	108	128	7	0
21	324	129	7	0
22	972	130	7	0
23	890	131	7	2
24	947	262	14	2
25	304	524	28	1
26	531	524	29	0
27	580	525	29	1
28	280	525	30	1
29	729	525	31	0

We now know that:
$g^{525} \cdot h^{31} \equiv g^{6} \mod 1013$
$\Leftrightarrow g^{519} \equiv h^{981} \mod 1013$
$\Leftrightarrow g^{\frac{519}{981}} \equiv h \mod 1013$
The inverse of 981 is 457 modulo 1012. Therefore $a \equiv 519 \cdot 457 \equiv 375 \mod 1012$.
$3^{375} \equiv 245 \mod 2013$

Instead of detecting cycles by inspection, use Floyd's algorithm with t_i and r_i

0.2 Using r_i

i	r_i	a_i	b_i	$t_i \mod 3$
0	3	1	0	0
1	27	3	0	0
2	243	5	0	0
3	161	7	0	2
4	666	28	0	0
5	231	29	1	0
6	53	31	1	2
7	323	63	2	2
8	589	126	5	1
9	364	127	6	1
10	108	128	7	0
11	972	130	7	0
12	947	262	14	2
13	531	524	29	0
14	280	525	30	1
15	161	526	31	0

We now know that:
$g^{526} \cdot h^{31} \equiv g^{7} \mod 1013$
$\Leftrightarrow g^{519} \equiv h^{981} \mod 1013$
$\Leftrightarrow g^{\frac{519}{981}} \equiv h \mod 1013$
The inverse of 981 is 457 modulo 1012. Therefore $a \equiv 519 \cdot 457 \equiv 375 \mod 1012$.
$3^{375} \equiv 245 \mod 2013$

This only confirmed the answer you already found

Exercise 2

Use factor base $\mathcal{F} = \{2, 3, 5, 7, 11, 13\}$ to solve the DLP $h = 281, g = 2$ in $\mathbb{F}^*_{1019}$. I.e. pick random powers of $g = 2$, check whether they factor into powers of 2,3,5,7,11, and 13; if so, add a relation.

E.g. $2^{291} \equiv 52 \mod 1019$; over the integers $52 = 2^2 \cdot 13$, so we include the relation $291 \equiv 2a_2 + a_{13} \mod 1018$.
Note that you can run into difficulties inverting modulo 1018 since it is not prime.
E.g. $2^{658} \equiv 729 \mod 1019$; over the integers $729 = 3^6$, so we include the relation $658 \equiv 6a_3 \mod 1018$ but 6 is not invertible modulo 1018 and we can only determine $a_3 \equiv 449 \mod 509$ and need to test whether $a_3 = 449$ or $a_3 = 449 + 509$. Here $2^{449} \equiv 1016 \mod 1019$ and $2^{449+509} \equiv 3 \mod 1019$, thus $a_3 = 958$.

Hint: if you're using Pari-GP you'll find

```
factor(lift(Mod(2^i,p)))
```

a usefull command

Answer 2

4/5

i	$g^i \mod 1019$	factor	relation
291	52	$2^2 \cdot 13$	$291 \equiv 2a_2 + a_{13}$
658	729	3^6	$658 \equiv 6a_3$
435	726	$2 \cdot 3 \cdot 11^2$	$435 \equiv a_2 + a_3 + 2a_{11}$
756	11	11	$756 \equiv a_{11}$
123	567	$3^4 \cdot 7$	$567 \equiv 4a_3 + a_7$
369	448	$2^6 \cdot 7$	$369 \equiv 6a_2 + a_7$
989	750	$2 \cdot 3 \cdot 5^3$	$989 \equiv a_2 + a_3 + 3a_5$

From these relations and from the exercise above we get

describe how you solved this (mod 1018) tackling coefficients that don't have an inverse

$$a_2 = 1, \quad a_3 = 958, \quad a_5 = 10, \quad a_7 = 363, \quad a_{11} = 756, \quad a_{13} = 289$$

We then search for a power of g such that $h \cdot g^a$ can be factorized in factors of $\mathcal{F}$ After trying some random a we found $a = 296$

$$h \cdot g^a \equiv 281 \cdot 2^{296} \equiv 2 \cdot 3^2 \cdot 7^2 \equiv 2^{a_2 + 2a_3 + 2a_7} \equiv 2^{607} \mod 1019$$

So we know that $h \cdot g^{296} \equiv g^{607} \mod 1019 \Rightarrow h \equiv g^{311} \mod 1019$.
$a = 311$ is the DLP such that $h \equiv g^a mod 1019$.

als $h \cdot g^2 \equiv 3 \cdot 5 \cdot 7 \ (\text{mod } 1019)$