Introduction to Cryptography: Assignment 13

Group number 57

Elwin Tamminga
s1013846

Lucas van der Laan
s1047485

A

$p = 179$
$g = 5$
$m = \lfloor \sqrt{89} \rfloor = 9$
$g^{-m} = g^{-9} = 5^{-9} = 56^{-1} = 56^{\varphi(179)-1} = 56^{179-2} \equiv 16 \pmod{179}$

Baby steps:

i	0	1	2	3	4	5	6	7	8	9
5^i	1	5	25	125	88	82	52	81	47	56

Giant steps:

j	0	1	2
$107 \cdot 5^{-mj}$	107	101	5

The result of the giant step is 5 with $j = 2$, which is the same result as the baby step with $i = 1$. According to the algorithm $x = i + m \cdot j$. We can know calculate x:

$i = 1$
$j = 2$
$x = i + m \cdot j = 1 + 9 \cdot 2 = 19$

We now can check if this is correct by doing $g^{i+m \cdot j} \mod p = 5^{1+9\cdot 2} \mod 179 = 5^{19} \mod 179 \equiv 107$

B

Starting point: $(a_0 = 5, b_0 = 1, c_0 = 0)$
$g = 5$
$h = 107$

We know that the order of the subgroup $\langle 5 \rangle = 89 = l$.

computations for a_i is done mod 179, b_i and c_i are done mod 89

$a_0 \mod 3 = 2$
$(a_1, b_1, c_1) = (a_0 \cdot h, b_0, c_0 + 1) = (5 \cdot 107, 1, 0 + 1) \equiv (177, 1, 1)$

$a_1 \mod 3 = 0$
$(a_2, b_2, c_2) = (a_1^2, 2 \cdot b_1, 2 \cdot c_1) = (177^2, 2 \cdot 1, 2 \cdot 1) \equiv (4, 2, 2)$

$a_2 \mod 3 = 1$
$(a_3, b_3, c_3) = (a_2 \cdot g, b_2 + 1, c_2) = (4 \cdot 5, 2 + 1, 2) \equiv (20, 3, 2)$

$a_3 \mod 3 = 2$
$(a_4, b_4, c_4) = (a_3 \cdot h, b_3, c_3 + 1) = (20 \cdot 107, 3, 2 + 1) = (171, 3, 3)$

$a_4 \mod 3 = 0$
$(a_5, b_5, c_5) = (a_4^2, 2 \cdot b_4, 2 \cdot c_4) = (171^2, 2 \cdot 3, 2 \cdot 3) = (64, 6, 6)$

$a_5 \mod 3 = 1$
$(a_6, b_6, c_6) = (a_5 \cdot g, b_5 + 1, c_5) = (64 \cdot 5, 6 + 1, 6) = (141, 7, 6)$

$a_6 \mod 3 = 0$
$(a_7, b_7, c_7) = (a_6^2, 2 \cdot b_6, 2 \cdot c_6) = (141^2, 2 \cdot 7, 2 \cdot 6) = (12, 14, 12)$

$a_7 \mod 3 = 0$
$(a_8, b_8, c_8) = (a_7^2, 2 \cdot b_7, 2 \cdot c_7) = (12^2, 2 \cdot 14, 2 \cdot 12) = (144, 28, 24)$

$a_8 \mod 3 = 0$
$(a_9, b_9, c_9) = (a_8^2, 2 \cdot b_8, 2 \cdot c_8) = (144^2, 2 \cdot 28, 2 \cdot 24) = (151, 56, 48)$

$a_9 \mod 3 = 1$
$(a_{10}, b_{10}, c_{10}) = (a_9 \cdot g, b_9 + 1, c_9) = (151 \cdot 5, 56 + 1, 48) = (39, 57, 48)$

$a_{10} \mod 3 = 0$
$(a_{11}, b_{11}, c_{11}) = (a_{10}^2, 2 \cdot b_{10}, 2 \cdot c_{10}) = (39^2, 2 \cdot 57, 2 \cdot 48) = (89, 25, 7)$

$a_{11} \mod 3 = 2$
$(a_{12}, b_{12}, c_{12}) = (a_{11} \cdot h, b_{11}, c_{11} + 1) = (89 \cdot 107, 25, 7 + 1) = (36, 25, 8)$

$a_{12} \mod 3 = 0$
$(a_{13}, b_{13}, c_{13}) = (a_{12}^2, 2 \cdot b_{12}, 2 \cdot c_{12}) = (36^2, 2 \cdot 25, 2 \cdot 8) = (43, 50, 16)$

$a_{13} \mod 3 = 1$
$(a_{14}, b_{14}, c_{14}) = (a_{13} \cdot g, b_{13} + 1, c_{13}) = (43 \cdot 5, 50 + 1, 16) = (36, 51, 16)$

i	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14
a_i	5	177	4	20	171	64	141	12	144	151	39	89	36	43	36
b_i	1	1	2	3	3	6	7	14	28	56	57	25	25	50	51
c_i	0	1	2	2	3	6	6	12	24	48	48	7	8	16	16

We found a a_i and a_j with $i \neq j$ that are the same, namely $a_{12} = a_{14} = 36$.
So we can find x by solving $a \equiv \frac{b_i - b_j}{c_j - c_i} \pmod{l}$.
$x \equiv \frac{25-51}{16-8} \equiv \frac{63}{8} \equiv 63 \cdot 8^{-1} \equiv 63 \cdot 8^{\varphi(89)-1} \equiv 63 \cdot 8^{89-2} \equiv 63 \cdot 78 \equiv 19 \pmod{89}$

We can verify this, by comparing it against the answer of question A, which was also 19, thus we know that $x = 19$ is correct.