BLM 5153 Homework Assignment 1

Semih Balki

October 15, 2019

Problem 1 - Carefully read the notes on Shank's algorithm and demonstrate the solution of the DLP

$$5^x = 3(mod 2027) \tag{1}$$

Choose m and create the S and T tables, and finally show how x is obtained.

Solution 1 Consider the solution of

$$5^x = 3(mod 2027)$$

$$m = \sqrt{2027} = 46$$

Therefore, the giant step and baby steps tables:

$S = (i, 5^{46i})|i = 0, 1, ..., 46$

[1, 1960, 435, 1260, 714, 810, 459, 1679, 1019, 645, 1379, 849, 1900, 401, 1511, 113, 537, 507, 490, 1629, 315, 1192, 1216, 1635, 1940, 1775, 668, 1865, 719, 475, 607, 1898, 535, 641, 1647, 1136, 914, 1599, 298, 304, 1929, 485, 1964, 167, 973, 1700]

$T = (j, 46.5^j)|i = 0, 1, ..., 46$

[3, 15, 75, 375, 1875, 1267, 254, 1270, 269, 1345, 644, 1193, 1911, 1447, 1154, 1716, 472, 333, 1665, 217, 1085, 1371, 774, 1843, 1107, 1481, 1324, 539, 668, 1313, 484, 393, 1965, 1717, 477, 358, 1790, 842, 156, 780, 1873, 1257, 204, 1020, 1046, 1176]

The 26^{th} element of S and 28^{th} element of T are same. Therefore, x = 26.46 - 28 = 1168, i.e, $5^{1168} = 3(mod 2027)$

Problem 2 - Repeat the solution of the same DLP in (1) above using Pollard rho algorithm.

Solution 2 Consider the solution of

$$5^x = 3(mod 2027)$$

We divide the set S = 1, 2, ..., 2026 into 3 sets such that;
S_0 = {1, 2, ..., 675}
S_1 = {676, 677, ..., 1351}
S_2 = {1352, 1353, ..., 2026}

We start with $a_0 = g^a(mod p)$ for a random a.
Taking a = 1311, we obtain $a_0 = 5^{1311} = 1171(mod 2027)$

I will not show iterations as a table since I have implemented the algorithm in python to solve the problem. Therefore,

$$a_{94} = a_{162} \tag{2}$$

- Power of y at a_{94} is 8573720
- Power of g at a_{94} is 43996235994
- Power of y at a_{162} is 8990199648823
- Power of g at a_{162} is 46133397155065752

The equality (2) implies

$y^{8573720}.g^{43996235994} = y^{8990199648823}.g^{46133397155065752}$

We have an equality over the exponents

$8573720.x + 43996235994 = 8990199648823.x + 46133397155065752$

$-46133353158829758 = x.8990191075103(mod 2026)$

$x.1461 = 556(mod 2026)$

Since gcd(1461, 2026) = 1. Therefore, there is exactly one solution.

$x = 556.1461^{-1}(mod 2026)$

$x = 556.1671(mod 2026)$

x = 1168, i.e, $5^{1168} = 3(mod 2027)$

Note that: Could check my code as in the following link:
https://nbviewer.jupyter.org/gist/smhblk04/d9807711aed87a976ed954e893e01c85