Semih Balki
Yildiz Technical University

semihbalki@sabanciuniv.edu

Assignment 2

BLM 5153 : Fall 2019 : Prof. Koc
Due Sunday, November 3, 2019

Problem 1 - Carefully read the notes on Index calculus algorithm and demonstrate the solution of the DLP $2^x = 3(mod 2029)$

Solution

- **Step 1**: Try $\alpha = 799$:$g^\alpha = 2^{799} = 250 = 2.5^3$ (mod 2029): Smooth
- Thus, we find

$$1.\log_2 2 + 3.\log_2 5 = 799\ (mod 2028)$$

- Try $\alpha = 389$:$2^{389} = 1250 = 2.5^4$ (mod 2029): Smooth
- Thus, we find

$$1.\log_2 2 + 4.\log_2 5 = 389\ (mod 2028)$$

- **Step 2**: We solve these two equations

$$1.\log_2 2 + 3.\log_2 5 = 799\ (mod 2028)$$

$$1.\log_2 2 + 4.\log_2 5 = 389\ (mod 2028)$$

- Expressed in matrix form as

$$\begin{bmatrix} 1 & 3 \\ 1 & 4 \end{bmatrix} . \begin{bmatrix} \log_2 2 \\ \log_2 5 \end{bmatrix} = \begin{bmatrix} 799 \\ 389 \end{bmatrix} (mod 2028)$$

- We find solutions as $\log_2 2 = 1$ and $\log_2 5 = 1618$
- These are verified as $2^1 = 2$ (mod 2029) and $2^{1618} = 5$(mod 2029)
- **Step 3**: Suppose we want to find $\log_2 3$(mod 2029)
- We are trying to solve the DLP: y = 3 = 2^x (mod 2029)

- Try $\alpha = 848$: y.g^{α} = 3.2^{848} = 500 (mod 2029): Smooth
- This number factors as 500 = 2^2 . 5^3, thus, we find

$$log_g y = -\alpha + \Sigma_{p_i \in S}(\alpha_i . \log_g p_i(mod p - 1))$$

$$\log_2 3 = -848 + 2. \log_2 2 + 3. \log_2 5(mod 2028)$$

$$= 4008(mod 2028)$$

$$= 1980$$

- The solution is x = 1980 in 3 = 2^x (mod 2029) since 2^{1980} = 3 (mod 2029)

Problem 2 - Also solve for $2^x = 2019(mod 2029)$.

Solution

- **Step 1**: Try $\alpha = 389$: $\mathrm{g}^\alpha = 2^{389} = 1250 = 2.5^4$ (mod 2029): Smooth
- Thus, we find

$$1.\log_2 2 + 4.\log_2 5 = 799\ (mod 2028)$$

- Try $\alpha = 799$: $2^{799} = 250 = 2.5^3$ (mod 2029): Smooth
- Thus, we find

$$1.\log_2 2 + 3.\log_2 5 = 389\ (mod 2028)$$

- **Step 2**: We solve these two equations

$$1.\log_2 2 + 4.\log_2 5 = 389\ (mod 2028)$$

$$1.\log_2 2 + 3.\log_2 5 = 799\ (mod 2028)$$

- Expressed in matrix form as

$$\begin{bmatrix} 1 & 4 \\ 1 & 3 \end{bmatrix} . \begin{bmatrix} \log_2 2 \\ \log_2 5 \end{bmatrix} = \begin{bmatrix} 389 \\ 799 \end{bmatrix} (mod 2028)$$

- We find solutions as $\log_2 2 = 1$ and $\log_2 5 = 1618$
- These are verified as $2^1 = 2$ (mod 2029) and $2^{1618} = 5$(mod 2029)
- **Step 3**: Suppose we want to find $\log_2 3$(mod 2029)
- We are trying to solve the DLP: y = 2019 = 2^x (mod 2029)
- Try $\alpha = 609$: $y.\mathrm{g}^\alpha = 2019.2^{609} = 1600$ (mod 2029): Smooth
- This number factors as $1600 = 2^6.5^2$, thus, we find

$$log_g y = -\alpha + \Sigma_{p_i \in S}(\alpha_i . \log_g p_i (mod p - 1))$$

$$\log_2 2019 = -609 + 6.\log_2 2 + 2.\log_2 5\ (mod 2028)$$

$$= 2633\ (mod 2028)$$

$$= 605$$

- The solution is x = 605 in 2019 = 2^x (mod 2029) since $2^{605} = 2019$ (mod 2029)

Note that: Could check my code as in the following link:
https://nbviewer.jupyter.org/gist/smhblk04/481462d7d2077faee834083d2373696b