Fixed Points of Diffie-Hellman Permutations

Sophia V. Breslavets

Saint Bernard School, Uncasville CT

Yulia's Dream Program
Mentor: Vasily A. Dolgushev

Primes and their primitive roots

Recall that, for every prime p, the multiplicative group $(\mathbb{Z}/p\mathbb{Z})^{\times}$ of units of the ring $\mathbb{Z}/p\mathbb{Z}$ is a cyclic group of order $(p-1)$.

Definition

An integer b coprime to p is called a primitive root modulo p if the residue class $b + p\mathbb{Z}$ *is a generator of* $(\mathbb{Z}/p\mathbb{Z})^{\times}$*.*

It is easy to see that the number of primitive roots modulo p is $\phi(p-1)$. For example the integers $2, 6, 7, 8$ are primitive roots modulo 11. The first 10 primitive roots modulo 101 are $2, 3, 7, 8, 11, 12, 15, 18, 26, 27$.

Notation. For a positive integer N and an integer k, we denote by $\mathrm{rem}(k, N)$ the nonnegative remainder of division of k by N.

The Discrete Logarithm Problem

Consider a “large” prime number p (e.g. p has ≈ 100 decimal digits) and let $1 < b < (p-1)$ be a primitive root modulo p. Since $\langle \bar{b} \rangle = (\mathbb{Z}/p\mathbb{Z})^{\times}$, for every integer $1 \leq y \leq p-1$, there exists exactly one integer $1 \leq x \leq p-1$ such that

$$y \equiv b^x \mod p.$$

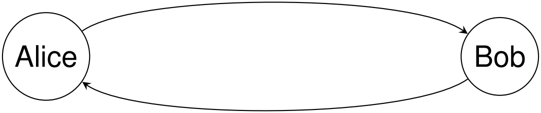
Given y, it is computationally hard to solve the above equation for x. The task of computing an integer x is known as the discrete logarithm problem. There are certain ways to tackle this problem (i.e. ’Baby steps, giant steps’ method). They make the problem easier to solve, however it still remains time consuming.
For the prime $p = 1000958479$ ($> 10^9$) and its primitive root $b = 15$, it took ≈ 5 minutes (on a laptop) to solve the congruence

$$34991890 \equiv b^x \mod p$$

for x. The answer is $x = 10002025$.

The Diffie-Hellman protocol

Let p be a large prime and b be a primitive root modulo p. The pair (p, b) is the **public part** of the key. Alice and Bob place this information in a public channel. Alice chooses an exponent $1 < x_A < p - 1$ and Bob chooses an exponent $1 < x_B < p - 1$. The pair (x_A, x_B) is the **private part** of the key. Alice and Bob make sure that the pair (x_A, x_B) is not publicly available. Then...



$\text{rem}(b^{x_A}, p)$

Alice

Bob

$\text{rem}(b^{x_B}, p)$

Alice can compute the residue class $\left(\overline{b}^{x_B}\right)^{x_A}$ and Bob can compute the residue class $\left(\overline{b}^{x_A}\right)^{x_B}$. Wait! $\left(\overline{b}^{x_B}\right)^{x_A} = \overline{b}^{x_A x_B} = \left(\overline{b}^{x_A}\right)^{x_B}$. After that, Alice and Bob use the remainder $\text{rem}(b^{x_A x_B}, p)$ as their secrete encryption key.

Diffie-Hellman permutations and their fixed points

Let p be a prime number > 3 and $1 < b < p - 1$ be a primitive root modulo p. Since $\langle \bar{b} \rangle = (\mathbb{Z}/p\mathbb{Z})^{\times}$, the assignment $x \mapsto \mathrm{rem}(b^x, p)$ gives us a bijection

$$\{1, \ldots, p-2\} \xrightarrow{\cong} \{2, \ldots, p-1\}.$$

Hence the formula

$$\tau_{p,b}(x) := \mathrm{rem}(b^x, p) - 1$$

defines a bijection $\tau_{p,b} : \{1, \ldots, p-2\} \xrightarrow{\cong} \{1, \ldots, p-2\}$, i.e. a permutation of degree $p - 2$.

Definition

Given a prime number p and a primitive root b modulo p, we call $\tau_{p,b}$ the **Diffie-Hellman (DH) permutation** *corresponding to the pair (p, b).*

The presence of fixed points of the permutation $\tau_{p,b}$ is a weakness of the Diffie-Hellman protocol.

Fixed points of Diffie-Hellman permutations

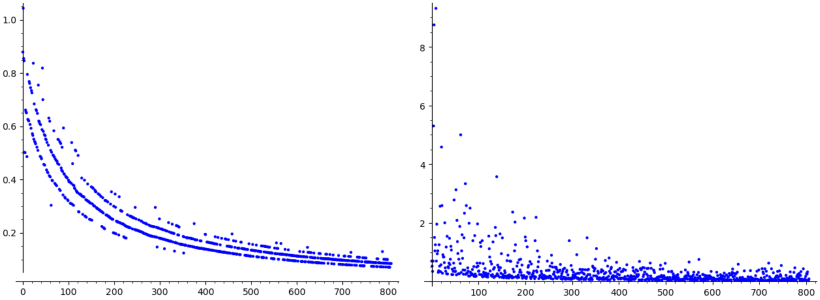
For a prime p, we set

$$\mu(p) := \max(\{fp(\tau_{p,b}) \mid b \in \text{ the set of prim. roots mod } p\}),$$

where $fp(\tau_{p,b})$ is the number of fixed points of the permutation $\tau_{p,b}$. We also denote by $\theta(p)$ the percentage of primitive roots b for which $\tau_{p,b}$ has the largest number of fixed points.

prime p	$100 \cdot \mu(p)/(p-2)$	$\theta(p)$
103	4.95%	3.13%
911	0.55%	0.35%
1009	0.4%	1.04%
1823	0.27%	0.33%
3343	0.15%	0.36%
5557	0.13%	0.05%

Plots of selected lists



The plot to the left shows the percentages of fixed points (in the worse case) for primes $571 \leq p \leq 7109$. The plot to the right shows the percentage of primitive roots b for which $\tau_{p,b}$ has the largest number of fixed points for primes $571 \leq p \leq 7109$. (There are 807 primes in this range.)

Vulnerable exponents

Definition

Let p be prime ≥ 11 and $1 \leq x \leq p-2$ be an integer. We say that x is a **vulnerable exponent** *relative to p if there exists a primitive root b modulo p such that $\tau_{p,b}(x) = x$.*

For example, if $p = 11$, then the exponents $1, 2, 4, 7, 8$ are vulnerable.

Definition

Let x be a vulnerable exponent relative to p. Then a primitive root b is called **distinguished** *if $\tau_{p,b}(x) = x$.*

A Criterion of Vulnerability

Clearly, $\tau_{p,b}(x) = x \iff \overline{b}^x = \overline{x+1}$. Since $\langle \overline{b} \rangle = (\mathbb{Z}/p\mathbb{Z})^\times$, the order of $\overline{b}^x$ is $(p-1)/\gcd(p-1,x)$. Hence we proved "⇒" in the following theorem:

Theorem (A)

Let p be prime ≥ 11. An integer $1 \leq x \leq p-2$ is a vulnerable exponent $\iff$

$$\frac{p-1}{\gcd(p-1,x)} = \operatorname{ord}(\overline{x+1}) \quad \mathit{in} \quad (\mathbb{Z}/p\mathbb{Z})^\times . \tag{1}$$

If x is a vulnerable exponent, $d := \gcd(x, p-1)$, $m := (p-1)/d$ and d_1 is the largest divisor of d coprime to m, then the number of distinguished primitive roots for x is

$$\phi(d_1)d/d_1 .$$

A few words about the proof

For a generator $\overline{b}$ in $(\mathbb{Z}/p\mathbb{Z})^\times$ there exists a unique integer $1 \leq t \leq p-2$ such that $\overline{b}^t = \overline{x+1}$.
In the proof we describe the set of integers k (modulo $(p-1)$) such that $\gcd(k, p-1) = 1$, and $\tau_{p,b^k}(x) = x$.

$$\tau_{p,b^k}(x) = x \iff \overline{b}^{kx} = \overline{b}^t$$

Thus, in the remainder of the proof, we solve the congruence

$$kx \equiv t \mod (p-1)$$

together with the condition $\gcd(k, p-1) = 1$. Finally, we show that the number of such integers k (modulo $(p-1)$) and hence the number of distinguished primitive roots for x is

$$\phi(d_1)d/d_1 \, .$$

Safe primes

Recall that a prime p of the form $2q + 1$ with q being prime is called a **safe prime.** In this case q is called a **Germain prime.** For instance, 911 and 1823 are primes and $1823 = 2 \cdot 911 + 1$.

It is not known whether there are infinitely Germain primes (respectively, infinitely many safe primes). However, according Wolfram MathWorld, the largest known Germain prime (as of Feb 29, 2016) has 388,342 decimal digits!

There are $124, 849$ safe primes between 11 and $50, 000, 747$.

Results related to safe primes

For every safe prime $p = 2q + 1$, the set of divisors of $p - 1 = 2q$ is $\{1, 2, q, 2q\}$. Using this fact and Theorem A, we proved:

Corollary

Let $p = 2q + 1$ be a safe prime ≥ 11. If x is a vulnerable exponent relative to p, then there is exactly one primitive root b_x modulo p such that $\tau_{p,b_x}(x) = x$.

Theorem (B)

Let $p = 2q + 1$ be a safe prime ≥ 11. Then the ratio of the vulnerable exponents to the total number of exponents (relative to p) is greater of equal to

$$\frac{q-5}{4q-2}.$$

Note that, for large Germain primes q, the above ratio is $\approx 1/4$.

A few words about the proof

First, we prove that the total number of vulnerable exponents relative to p is greater or equal to

$$2v_{even} - 1,$$

where v_{even} is the number of even vulnerable exponents. Second, we reduce the question of counting even vulnerable exponents to the question of counting odd integers $3 \le y \le 2q - 1$ satisfying

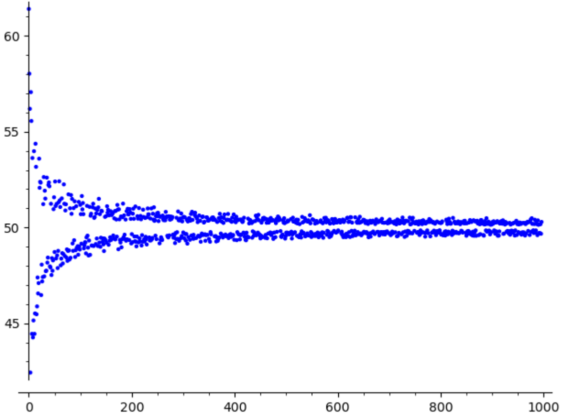
$$\mathrm{ord}(\overline{y}) = q.$$

It is easy to show that every such $\overline{y}$ is of the form $\overline{a}^2$ for some integer a.

Thus the question of counting such odd integers boils down to counting odd integers > 1 on $(0, \sqrt{p})$, even integers on $(\sqrt{p}, \sqrt{2p})$, odd integers on $(\sqrt{2p}, \sqrt{3p})$ and so on...

Finally, it is easy to take care of the issue of overcounting.

Percentages of vulnerable exponents for safe primes



This is the plot of the list of percentages of vulnerable exponents among all exponents for 997 **safe primes**

$$59 \le p \le 165,059.$$

Open questions

- Let p be a prime ≥ 11. Is this true that p has a primitive root b such that the DH permutation $\tau_{p,b}$ has a fixed point?
- Let p be a prime ≥ 11. Is this true that the percentage of vulnerable exponents relative to p is $> 5\%$? For example, for all primes $11 \leq p < 180181$, the percentage of vulnerable exponents is $> 7\%$. However, for $p = 180181$, the percentage of vulnerable exponents is 6.99%.
- Is this true that for every safe prime $p \geq 59$, the percentage of vulnerable exponents is $> 42\%$? This is true for all safe primes $59 \leq p \leq 1,276,103$.
- *Please feel free to suggest your own open question! :-)*

Future Plans

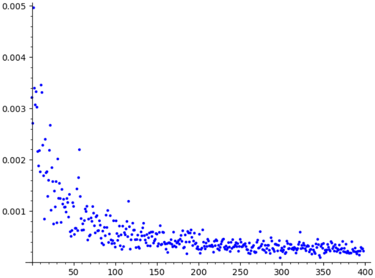
We are planning to build a GitHub repository with the SageMath script for working with Diffie-Hellman permutations, their fixed points, and with vulnerable exponents of primes. The repository will also contain results of our computer experiments.

Let p be a safe prime ≥ 11. Recall that, for every vulnerable exponent x relative to p, there is a unique primitive root b_x (modulo p) such that $\tau_{p,b_x}(x) = x$. We have an algorithm for finding the root b_x and this algorithm works fast. It seems that the function that sends a vulnerable exponent x to the primitive root b_x is pre-image resistant. Moreover, the ability to factor large integers fast does not seem to help finding the pre-image of this function.

THANK YOU!

DH permutations behave like random permutations

Recall that the probability of a random permutation to have exactly k fixed points is $e^{-1}/k!$ (a particular case of the Poisson distribution). Below is the plot of the list of distances (in the sense of the cab metric) between the distribution of fixed points for DH permutations and the above theoretical distribution.



This plot is for 399 **safe primes** $107 \leq p \leq 53,003$.