mobilefish.com

BLOCKCHAIN TUTORIAL 9

Discrete logarithm

$$8 = 2^x \pmod{13}$$

BLOCKCHAIN TUTORIAL 9

Discrete logarithm

mobilefish.com

DISCRETE LOGARITHM

- The goal of exponentials is to calculate the product: $x = 2^3$
- The goal of logarithms is to calculate the exponent: $x = \log_2 (8)$ $(8 = 2^x)$
- In discrete logarithm, you need to apply a modulo operation in the latter:
  - $x = \log_2 8 \pmod{13}$
  - Other way of notation: $x = \text{dlog}_{2,13} (8)$
  - where: x = exponent, 2 = base, 13 = modulus, 8 = remainder
  - If you find this confusing, you can also rewrite it this way: $8 = 2^x \pmod{13}$

mobilefish.com

DISCRETE LOGARITHM

- Example:
  - $2^x \pmod 7 = 4$
  - $x = 2$ or 5 $x = \{1,..,6\}$
  - $4 \pmod 7 = 4$ and $32 \bmod 7 = 4$
- There are two solutions. In the world of cryptography we are only interested in discrete logarithms where each exponent has a distinct remainder.
- If seems that if the modulus (p) is a prime number there are certain base values (b) which generate distinct remainders for different exponents ($x = 1,\ldots, p-1$). A prime number is a number that is divisible only by itself and 1. For example: 2, 3, 5, 7, 11, …

mobilefish.com

DISCRETE LOGARITHM

- Lets calculate $b^x \pmod 7$ = remainder $x = \{1,\ldots,6\}$ modulus p = 7

b	b^1mod7	b^2mod7	b^3mod7	b^4mod7	b^5mod7	b^6mod7
1	1	1	1	1	1	1
2	2	4	1	2	4	1
3	**3**	**2**	**6**	**4**	**5**	**1**
4	4	2	1	4	2	1
5	**5**	**4**	**6**	**2**	**3**	**1**
6	6	1	6	1	6	1

- The discrete logarithm for modulus 7 generates distinct remainders when using base value 3 or 5 and the remainders are in the range {1,…,6}

mobilefish.com

DISCRETE LOGARITHM

- The base values 3 and 5 are called the *primitive roots of* 7 or *generators*, often indicated by symbol α. It is called generator because applying the multiplication operation on one single element (α^x), generates all elements in the discrete group {1, … p -1}

- The word *discrete* in discrete logarithm refer to the aspect that we are working in a discrete group {1, … p -1} and not any real numbers (meaning fractions 2.58)

- Calculating 3^{11} mod 17 = x is very easy, but doing the opposite, calculating the discrete logarithm 11 = 3^x mod 17 is very difficult. Especially if the modulus is at least 309 digits long. *REMEMBER: CALCULATING A DISCRETE LOGARITHM IS HARD.*
To solve 11 = 3^x mod 17 a computer needs to try each exponent x = 0, 1, 2, 3 … until the equation matches.

mobilefish.com

DISCRETE LOGARITHM

- Example: α (generator) = 2 and p (modulus) = 11   discrete group {1, …, p -1}

$2^1 \bmod 11 = 2$	$2^6 \bmod 11 = 9$	$2^{11} \bmod 11 = 2$	$2^{16} \bmod 11 = 9$
$2^2 \bmod 11 = 4$	$2^7 \bmod 11 = 7$	$2^{12} \bmod 11 = 4$	$2^{17} \bmod 11 = 7$
$2^3 \bmod 11 = 8$	$2^8 \bmod 11 = 3$	$2^{13} \bmod 11 = 8$	$2^{18} \bmod 11 = 3$
$2^4 \bmod 11 = 5$	$2^9 \bmod 11 = 6$	$2^{14} \bmod 11 = 5$	$2^{19} \bmod 11 = 6$
$2^5 \bmod 11 = 10$	$2^{10} \bmod 11 = \mathbf{1}$	$2^{15} \bmod 11 = 10$	$2^{20} \bmod 11 = \mathbf{1}$

- This is called a *cyclic group* of generator α. After a certain number of exponentiations and modulus operations, we have loop.

- If the remainder has value 1, the cycle starts all over again in the same order.

mobilefish.com

DISCRETE LOGARITHM

- In the previous example (p=11) the cyclic group is referred to with notation: $\mathbb{Z}^*_p$
- For example: $\mathbb{Z}^*_{11}$
  - the * means no zero,
  - the discrete group is {1, …, p -1} = {1, …, 10}
  - the number of elements in the discrete group is p -1 = 10
- Cyclic groups are the basis of discrete logarithm crypto systems.