Diffie-Hellman

Key exchange and discrete log problem

Saturday, 7 December 2019 10:38 AM

Alice — PUBLIC PARAMETERS ← p, α → — Bob

$a = K_{PrA} \in \{2,3,\dots,p-2\}$ $\quad b = K_{PrB} \in \{2,3,\dots,p-2\}$

$A = \alpha^a \bmod p = K_{pubA}$ $\xrightarrow{A}$ $\quad B = \alpha^b \bmod p = K_{pubB}$ $\xleftarrow{B}$

KEY EXCHANGE

$K_{AB} = B^a \bmod p \Leftarrow$ same value $\Rightarrow K_{AB} = A^b \bmod p$

How they got same key over an insecure connection:

Use case → $y = AES(x)$ $\xrightarrow{y}$ $AES^{-1}(y) = x$

K_{AB} $\quad$ K_{AB}

Proof of correctness:

Alice computes: $B^a = (\alpha^b)^a = \alpha^{ab} \bmod p$

Bob computes: $A^b = (\alpha^a)^b = \alpha^{ab} \bmod p$

FINITE GROUPS:

group ≈ "set with elements and 1 group operation".

Definition 8.2.1 Group

A group is a set of elements G together with an operation ∘ which combines two elements of G. A group has the following properties.

1. *The group operation ∘ is* closed. *That is, for all $a, b, \in G$, it holds that $a \circ b = c \in G$.*
2. *The group operation is* associative. *That is, $a \circ (b \circ c) = (a \circ b) \circ c$ for all $a, b, c \in G$.*
3. *There is an element $1 \in G$, called the* neutral element *(or* identity element*), such that $a \circ 1 = 1 \circ a = a$ for all $a \in G$.*
4. *For each $a \in G$ there exists an element $a^{-1} \in G$, called the* inverse *of a, such that $a \circ a^{-1} = a^{-1} \circ a = 1$.*
5. *A group G is* abelian (or commutative) *if, furthermore, $a \circ b = b \circ a$ for all $a, b \in G$.*

In short:

ABELIAN GROUP = all groups +

① closeness $a \circ b = c \in G$

② Associativity $(a \circ b) \circ c = a \circ (b \circ c)$

③ NEUTRAL ELEMENT $a \circ 1 = a$

④ Inverse element $a \circ a^{-1} = 1$

⑤ Commutativity: $a \circ b = b \circ a$

Experiment:

Is $(\mathbb{Z}_9, \times)$ a group? × → multiply.

Definition 8.2.3 Order of an element

The order *ord(a) of an element a of a group $(G, \circ)$ is the smallest positive integer k such that*

$$a^k = \underbrace{a \circ a \circ \dots \circ a}_{k \text{ times}} = 1,$$

where 1 is the identity element of G.

A group which contains an element α with maximum order $ord(\alpha) = |G|$ is said to be CYCLIC. Elements with maximum order are called PRIMITIVE ELEMENT or GENERATORS.

Eg: $\alpha = 2$ is a generator for $\mathbb{Z}_{11}^*$.

cyclic groups are basis of discrete logarithmic cryptosystem.

For every prime p, $(\mathbb{Z}_p^*)$ is an abelian finite cyclic group.

Properties of cyclic group:

Let $a \in G$, G is a cyclic group

① $a^{|G|} = 1$, 1 → neutral element

② ord(a) divides $|G|$.

① Fermat's little theorem for $\mathbb{Z}_p^*$

proof ↳ $a^p = a \bmod p$

$\Rightarrow a^{p-1} = 1 \bmod p$

$|\mathbb{Z}_p^*| = p-1$

$\Rightarrow a^{p-1} = a^{|\mathbb{Z}_p^*|} = 1 \bmod p$

② Let's look at an example:

$\mathbb{Z}_{11}^* = \{1,2,3,\dots,10\}$

$|\mathbb{Z}_{11}^*| = 10$

what are the possible element orders in $\mathbb{Z}_{11}^*$?

possible orders $\in \{1, 2, 5, 10\}$

element a	1	2	3	4	5	6	7	8	9	10
ord(a)	1	10	5	5	5	10	10	10	5	2

∴ 2, 6, 7, 8 are primitive elements or generators

THE USE CASE:

⇒ CYCLIC GROUPS make "NICE" DISCRETE LOGARITHMIC PROBLEMS.

$\mathbb{Z}_{47}^*$, $a = 5$ is a generator

Is $(\mathbb{Z}_9, \times)$ a group? $\times \rightarrow$ multiply.

$\mathbb{Z}_9 = \{0, 1, 2, 3, \ldots\ldots 8\}$

$0 \stackrel{?}{=} x \bmod 9$

No, because INVERSES only exist for element a s.t. $\gcd(a, 9) = 1$

Def $\mathbb{Z}_9^* = \{1, 2, 4, 5, 7, 8\}$

$\stackrel{k}{=} \mathbb{Z}_9 - \{x : \gcd(x, 9) \neq 1\}$

are where INVERSE ELEMENTS EXIST.

→ is a MULTIPLICATIVE GROUP

$\mathbb{Z}_{47}^*$, $a = 5$ is a generator

$\therefore \exists x$ s.t. $5^x \equiv 47 \bmod 47$

$x \rightarrow$ this a hard to compute value (dd)

Theorem 8.2.1
The set $\mathbb{Z}_n^*$ which consists of all integers $i = 0, 1, \ldots, n-1$ for which $\gcd(i, n) = 1$ forms an abelian group under multiplication modulo n. The identity element is $e = 1$.

note: $\mathbb{Z}_p^*$, p is prime, forms a multiplicative group as follows:

$\mathbb{Z}_p^* = \{1, 2, 3, \ldots\ldots\ldots, p-1\}$

CYCLIC GROUPS :

Experiment:

$\mathbb{Z}_{11}^* = \{1, 2, 3, 4, 5, 6, 7, 8, 9, 10\}$

Q: what happens if we compute all powers of $a = 3$?

$a^1 = 3$

$a^2 = 9$

$a^3 = 27 = 5 \bmod 11$

$a^4 = a^3 a = 81 = 4 \bmod 11$

$a^5 = 243 = 1 \bmod 11$

$a^6 = 3 \bmod 11$

REPEATS

#CYCLIC

what is $3^{7812245763} \bmod 11$??

I know that it will be one of $\{3, 1, 9, 5, 4\}$

$\Rightarrow$ order(3) = 5 → 5 possible values (d)

experiment:

$\mathbb{Z}_{11}^* = \{1, 2, 3, \ldots\ldots 10\}$

experiment:

$Z_{11}^* = \{1, 2, 3, \ldots\ldots 10\}$

$\text{ord}(2) = 22.$

$a^1 = 2$
$a^2 = 4$
$a^3 = 8$
$a^4 = 5$
$a^5 = 10$
$a^6 = 9$
$a^7 = 7$
$a^8 = 3$
$a^9 = 6$
$a^{10} = 1$

#CYCLE
$\text{ord}(2) = 10$
2 generates all possible member of Z_{11}^*.