

Diffie-Hellman Key Exchange

Whittfield Diffie and Martin Hellman are called the inventors of Public Key Cryptography. Diffie-Hellman Key Exchange is the first Public Key Algorithm published in 1976.

What is Diffie-Hellman?

- A Public Key Algorithm
- Only for Key Exchange
- Does NOT Encrypt or Decrypt
- Based on Discrete Logarithms
- Widely used in Security Protocols and Commercial Products
- Williamson of Britain's CESG claims to have discovered it several years prior to 1976

Discrete Logarithms

- What is a logarithm?
- $\log_{10}100 = 2$ because $10^2 = 100$
- In general if $\log_m b = a$ then $m^a = b$
- Where m is called the **base** of the logarithm
- A **discrete logarithm** can be defined for integers only
- In fact we can define **discrete logarithms mod p** also where p is any prime number

Discrete Logarithm Problem

- The security of the Diffie-Hellman algorithm depends on the difficulty of solving the discrete logarithm problem (DLP) in the multiplicative group of a finite field

Sets, Groups and Fields

- A set is any collection of objects called the elements of the set
- Examples of sets: \mathbf{R} , \mathbf{Z} , \mathbf{Q}
- If we can define an operation on the elements of the set and certain rules are followed then we get other mathematical structures called groups and fields

Groups

- A group is a set G with a custom-defined binary operation $+$ such that:
 - The group is closed under $+$, i.e., for $a, b \in G$:
 - $a + b \in G$
 - The Associative Law holds i.e., for any $a, b, c \in G$:
 - $a + (b + c) = (a + b) + c$
 - There exists an identity element 0 , such that
 - $a + 0 = a$
 - For each $a \in G$ there exists an inverse element $-a$ such that
 - $a + (-a) = 0$
- If for all $a, b \in G$: $a + b = b + a$ then the group is called an Abelian or commutative group
- If a group G has a finite number of elements it is called a finite group

More About Group Operations

- $+$ does not necessarily mean normal arithmetic addition
- $+$ just indicates a binary operation which can be custom defined
- The group operation could be denoted as \cdot
- The group notation with $+$ is called the additive notation and the group notation with \cdot is called the multiplicative notation

Fields

- A field is a set F with two custom-defined binary operations $+$ and \cdot such that:
 - The Field is closed under $+$ and \cdot , i.e., for $a, b \in F$:
 - $a + b \in F$ and $a \cdot b \in F$
 - The Associative Law holds i.e., for any $a, b, c \in F$:
 - $a + (b + c) = (a + b) + c$ and $a \cdot (b \cdot c) = (a \cdot b) \cdot c$
 - There exist identity elements 0 and 1 , such that
 - $a + 0 = a$ and $a \cdot 1 = a$
 - For each $a \in F$ there exist inverse elements $-a$ and a^{-1} such that
 - $a + (-a) = 0$ and $a \cdot a^{-1} = 1$
- If a field F has a finite number of elements it is called a finite field

Examples of Groups

■ Groups

- Set of real numbers \mathbf{R} under $+$
- Set of real numbers \mathbf{R} under $*$
- Set of integers \mathbf{Z} under $+$
- Set of integers \mathbf{Z} under $*?$
- Set of integers modulo a prime number p under $+$
- Set of integers modulo a prime number p under $*$
- Set of 3×3 matrices under $+$ meaning matrix addition
- Set of 3×3 matrices under $*$ meaning matrix multiplication?

■ Fields

- Set of real numbers \mathbf{R} under $+$ and $*$
- Set of integers \mathbf{Z} under $+$ and $*$
- Set of integers modulo a prime number p under $+$ and $*$

Generator of Group

- If for $a \in G$, all members of the group can be written in terms of a by applying the group operation $*$ on a a number of times then a is called a generator of the group G
- Examples
 - 2 is a generator of Z_{11}^*
 - 2 and 3 are generator of Z_{19}^*

m	1	2	3	4	5	6	7	8	9	10
$2^m \text{ mod } 11$	2	4	8	5	10	9	7	3	6	1

m	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18
$2^m \text{ mod } 19$	2	4	8	16	13	7	14	3	6	17	15	11	3	6	12	5	10	1
$3^m \text{ mod } 19$	3	9	8	5	15	7	2	6	18	16	10	11	14	4	12	17	13	1

Primitive Roots

- If $x^n = a$ then a is called the n -th root of x
- For any prime number p , if we have a number a such that powers of $a \bmod p$ generate all the numbers between 1 to $p-1$ then a is called a **Primitive Root** of p .
- In terms of the Group terminology a is the generator element of the multiplicative group of the finite field formed by $\bmod p$
- Then for any integer b and a primitive root a of prime number p we can find a unique exponent i such that
$$b = a^i \bmod p$$
- The exponent i is referred to as the **discrete logarithm** or **index**, of b for the base a .

Table 7.6 Powers of Integers, Modulo 19

a	a^2	a^3	a^4	a^5	a^6	a^7	a^8	a^9	a^{10}	a^{11}	a^{12}	a^{13}	a^{14}	a^{15}	a^{16}	a^{17}	a^{18}
1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1
2	4	8	16	13	7	14	9	18	17	15	11	3	6	12	5	10	1
3	9	8	5	15	7	2	6	18	16	10	11	14	4	12	17	13	1
4	16	7	9	17	11	6	5	1	4	16	7	9	17	11	6	5	1
5	6	11	17	9	7	16	4	1	5	6	11	17	9	7	16	4	1
6	17	7	4	5	11	9	16	1	6	17	7	4	5	11	9	16	1
7	11	1	7	11	1	7	11	1	7	11	1	7	11	1	7	11	1
8	7	18	11	12	1	8	7	18	11	12	1	8	7	18	11	12	1
9	5	7	6	16	11	4	17	1	9	5	7	6	16	11	4	17	1
10	5	12	6	3	11	15	17	18	9	14	7	13	16	8	4	2	1
11	7	1	11	7	1	11	7	1	11	7	1	11	7	1	11	7	1
12	11	18	7	8	1	12	11	18	7	8	1	12	11	18	7	8	1
13	17	12	4	14	11	10	16	18	6	2	7	15	5	8	9	3	1
14	6	8	17	10	7	3	4	18	5	13	11	2	9	12	16	15	1
15	16	12	9	2	11	13	5	18	4	3	7	10	17	8	6	14	1
16	9	11	5	4	7	17	6	1	16	9	11	5	4	7	17	6	1
17	4	11	16	6	7	5	9	1	17	4	11	16	6	7	5	9	1
18	1	18	1	18	1	18	1	18	1	18	1	18	1	18	1	18	1

Table 7.7 Tables of Discrete Logarithms, Modulo 19

(a) Discrete logarithms to the base 2, modulo 19

a	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18
$\text{Ind}_{2,19}(a)$	18	1	13	2	16	14	6	3	8	17	12	15	5	7	11	4	10	9

(b) Discrete logarithms to the base 3, modulo 19

a	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18
$\text{Ind}_{3,19}(a)$	18	7	1	14	4	8	6	3	2	11	12	15	17	13	5	10	16	9

(c) Discrete logarithms to the base 10, modulo 19

a	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18
$\text{Ind}_{10,19}(a)$	18	17	5	16	2	4	12	15	10	1	6	3	13	11	7	14	8	9

(d) Discrete logarithms to the base 13, modulo 19

a	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18
$\text{Ind}_{13,19}(a)$	18	11	17	4	14	10	12	15	16	7	6	3	1	5	13	8	2	9

(e) Discrete logarithms to the base 14, modulo 19

a	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18
$\text{Ind}_{14,19}(a)$	18	13	7	8	10	2	6	3	14	5	12	15	11	1	17	16	14	9

(f) Discrete logarithms to the base 15, modulo 19

a	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18
$\text{Ind}_{15,19}(a)$	18	5	11	10	8	16	12	15	4	13	6	3	7	17	1	2	12	9

Diffie-Hellman Algorithm

- Five Parts
 1. Global Public Elements
 2. User A Key Generation
 3. User B Key Generation
 4. Generation of Secret Key by User A
 5. Generation of Secret Key by User B

Global Public Elements

- q Prime number
- α $\alpha < q$ and α is a primitive root of q
- The global public elements are also sometimes called the domain parameters

User A Key Generation

- Select private X_A $X_A < q$
- Calculate public Y_A $Y_A = \alpha^{X_A} \bmod q$

User B Key Generation

- Select private X_B $X_B < q$
- Calculate public Y_B $Y_B = \alpha^{X_B} \bmod q$

Generation of Secret Key by User A

- $K = (Y_B)^{X_A} \bmod q$

Generation of Secret Key by User B

- $K = (Y_A)^{X_B} \bmod q$

Diffie-Hellman Key Exchange

User A

Generate
random $X_A < q$;
Calculate
 $Y_A = \alpha^{X_A} \text{ mod } q$

Calculate
 $K = (Y_B)^{X_A} \text{ mod } q$

User B

Generate
random $X_B < q$;
Calculate
 $Y_B = \alpha^{X_B} \text{ mod } q$;
Calculate
 $K = (Y_A)^{X_B} \text{ mod } q$

Y_A

Y_B

Diffie-Hellman Example

- $q = 97$
- $\alpha = 5$
- $X_A = 36$
- $X_B = 58$
- $Y_A = 5^{36} = 50 \pmod{97}$
- $Y_B = 5^{58} = 44 \pmod{97}$
- $K = (Y_B)^{X_A} \pmod{q} = 44^{36} \pmod{97} = 75 \pmod{97}$
- $K = (Y_A)^{X_B} \pmod{q} = 50^{58} \pmod{97} = 75 \pmod{97}$

Why Diffie-Hellman is Secure?

- Opponent has q , α , Y_A and Y_B
- To get X_A or X_B the opponent is forced to take a discrete logarithm
- The security of the Diffie-Hellman Key Exchange lies in the fact that, while it is relatively easy to calculate exponentials modulo a prime, it is very difficult to calculate discrete logarithms. For large primes, the latter task is considered infeasible.