Introduction to the Diffie-Hellman Key Exchange

by Elsa Frankel

February 2023

Prerequisites

Multiplicative Group of Integers Modulo *n*
Primitive Roots
Euler's Totient Function

Multiplicative Group of Integers Modulo *n*

DEFINITION: the multiplicative group of integers modulo n is the set of all relatively prime positive integers $n-1$ for a given n. We can express this group as $\{0, 1, ..., n-1\}$

EX: let $n = 6$, we have that 1 and 5 are relative primes, so the multiplicative group of integers modulo 6 is $\{1, 5\}$

note: these can also be referred to as the the "residues modulo n"

(we'll see a more detailed explanation of finding relative primes in the next section)

***

Euler's Totient Function

DEFINITION: Euler's totient function counts the number of relatively prime integers $n \geq 1$ and is expressed as $\phi(n)$

relatively prime: two integers which only share 1 as a common divisor

EX: let $n = 6$

first we must list all factors of 6 and preceding values,

$$\text{factors of } 6 = \{1, 2, 3, 6\}$$

$$\text{factors of } 1 = \{1\}$$
$$\text{factors of } 2 = \{1, 2\}$$
$$\text{factors of } 3 = \{1, 3\}$$
$$\text{factors of } 4 = \{1, 2, 4\}$$
$$\text{factors of } 5 = \{1, 5\}$$

next, we remove values who share a common factor other than 1 with n,

$$\text{factors of } 1 = \{1\}$$
$$\boxed{\text{factors of } 2 = \{1,\ 2\}}$$
$$\boxed{\text{factors of } 3 = \{1,\ 3\}}$$
$$\boxed{\text{factors of } 4 = \{1,\ 2,\ 4\}}$$
$$\text{factors of } 5 = \{1, 5\}$$

we now have our set of relative primes for $n = 6$: $\{1, 5\}$ (recall multiplicative groups of integers!). since there are four relative primes, $\phi(6) = 2$

since primes p only have factors of $\{1, p\}$, every positive integer $n < p$ is a relative prime for some given p, so we have that $\phi(p) = p - 1$

Activity #1: Computing the Totient of n

$\phi(6)$	$\phi(8)$ n	$\phi(13)$

we'll use the totient of n to make determining primitive roots significantly more efficient!

***

Primitive Roots

DEFINITION: an integer g is a primitive root modulo n if every integer a relatively prime to n is congruent to g to some power. We can express this as: $g^k \equiv a(\text{mod } n)$

note: not all positive integers have primitive roots!

EX: let $n = 6$

first, let's calculate $\phi(6)$ and find the residues modulo 6. These will help cut down our work in future steps. (methods in prior sections)

$$\phi(6) = 2$$
$$\text{residues modulo } 6 = \{1, 5\}$$

now, let's check for primitive roots. The relative primes are the only values we need to check for g, and we only need to check positive powers $k \leq \phi(6)$

also, $1^k = 1$ for any $k > 0$, so 1 will never be a primitive root, and is a trivial check

thus, lets check the next and final relative prime, 5

$$5^1 \equiv 5^1(\text{mod } 6) = 5(\text{mod } 6) = 5$$
$$5^2 \equiv 5^2(\text{mod } 6) = 25(\text{mod } 6) = 1$$

since we were able to find all relative primes of 6 congruent to some $5^k(\text{mod } 6)$, we have that 5 is a primitive root modulo 6

Activity #2: Finding Primitive Roots

$n = 14$	$n = 8$	$n = 13$

Diffie-Hellman Key Exchange

cryptographic explanation

DEF: The Diffie-Hellman key exchange uses two secret numbers, and modifies them with public values including a prime integer p and primitive root modulo p, defined as g. This creates a shared private encryption key between two parties

EX: let public values $p = 29$, $g = 2$

Alice and Bob both define private values a and b for themselves respectively

$$a = 6$$
$$b = 3$$

Alice then shares $2^6 \pmod{29}$ with Bob, and Bob shares $2^3 \pmod{29}$ with Alice. Lets call these values A and B respectively. These are also public

$$A = 2^6 \pmod{29} = 64 \pmod{29} = 6$$
$$B = 2^3 \pmod{29} = 8 \pmod{29} = 8$$

Then, Alice computes $B^a \pmod{29}$, and Bob computes $A^b \pmod{29}$

$$A^b \pmod{29} = 262144 \pmod{29} = 13$$
$$B^a \pmod{29} = 216 \pmod{29} = 13$$

Alice and Bob now have a shared private value 13 for an encryption key

Activity #3: Create Your Own Encryption Key

choose any positive prime integer p and check whether it has a primitive root. If so, find a friend, choose your private numbers, and follow the protocol!

$$p = \_\_\_, \; q = \_\_\_,$$

$$a \text{ or } b = \_\_\_$$