**Diffie Hellman**

**----- Motivation -----------------------------------------------------------------------------------------------**

Diffe-Hellman algorithm is one of the earliest practical examples of public key exchange implemented within the field of cryptography. Traditionally, secure encrypted communication between two parties required that they first exchange keys by some secure physical means, such as paper key lists transported by a trusted courier. The diffie-Hellman key exchange method allows two parties that have no prior knowledge of each other to jointly establish a shared key over an insecure channel. Which was a huge progress in the field of cryptography! This shared key can be used to encrypt subsequent communications using a symmetric key cipher. This algorithm is used for a variety of internet services. The idea of this algorithm is that it's easy to compute powers modulo a prime but hard to reverse the process.
Important note: You're not sharing information during the key exchange, you're creating a key together! This can be used in addition to any other cryptosystem that requires exchanged keys.
An important distinction to make is that the Diffie-Hellman is for exchanging keys over an insecure channel. So, we don't encrypt or decrypt data. But rather we send "encrypted" keys and compute the shared value.
In the encrypt section we will demonstrate creating two keys.

**----- Method -----------------------------------------------------------------------------------------------**

**-- Encrypt -----------------------------------------------------------**

Step 1: Public Parameter Creation
A trusted party must choose and publish a (large) prime p, and an integer g having large prime order in $F_p^*$ (attach popup 3)

Step 2: Private Computations
Alice: Alice chooses a secret integer a to compute A ≡ $g^a$ (mod p)
Bob: Bob chooses a secret integer b to compute B ≡ $g^b$ (mod p)
Now, Alice sends A to Bob, and Bob sends B to Alice. These values will be sent over the channel and are public.
In the decrypt section We will show how Alice and Bob compute the shared secret value.

**-- Decrypt -----------------------------------------------------------**

Recall, Alice and Bob agree on a public prime and the primitive root g.
Alice has sent A ≡ $g^a$ (mod p) to Bob, and Bob has sent B ≡ $g^b$ (mod p) to Alice.
How to decrypt?
Alice: Alice will now compute $B^a \ (mod\, p)$
Bob: Bob will compute $A^b \ (mod\, p)$
The shared secret value is: $B^a \equiv (g^b)^a \equiv g^{ab} \equiv (g^a)^b \equiv A^b \ \ (mod\, p)$
Thus, they managed to create a private key over an insecure channel.

**----- Example-----------------------------------------------------------------------------------------------**

**-- Encrypt -----------------------------------------------------------**

Step 1: Public Parameter Creation
Alice and Bob agree to use the prime p = 941 and the primitive root g = 627.

Step 2: Private Computations
Alice: In our example, Alice chooses 347 and computes: A ≡ $627^{347}$ (mod 941) = 390

<u>Bob:</u> In our example, Bob chooses 781 and computes: B ≡ $627^{781}$ (mod 971) = 691

**-- Decrypt -------------------------------------------------------**

Recall, Alice and Bob agree on a public prime and the primitive root g.
Alice has sent A ≡ $g^a$ (mod p) to Bob, and Bob has sent B ≡ $g^b$ (mod p) to Alice.
In our example, p = 941, g = 627, a = 347, A = 390, b = 781, and B = 691.

The shared secret value is: $B^a \equiv (g^b)^a \equiv g^{ab} \equiv (g^a)^b \equiv A^b \pmod{p}$
In our example, $B^a \equiv A^b \equiv 627^{347*781} \ (mod\ 941) \equiv 470$
Their secret shared value is 470.
Thus, they managed to create a private key over an insecure channel.

****************************************popup 3****************************************************

Primitive Root Theorem:
Let P be a prime number. Then there exists an element g ∈ $F_p^*$ whose powers give every element of $F_p^*$, i.e., $F_p^* = \{\ 1,\ g,\ g^2,\ g^3,\ \ldots,\ g^{p-2}\}$. Elements with this property are called primitive roots of $F_p$ or generators of $F_p^*$. They are the elements of $F_p^*$ having order p-1.
For example, $F_{11}$ has 2 as a primitive root, since $F_{11}$ ,

| | | | | |
|---|---|---|---|---|
| $2^0 = 1$ | $2^1 = 2$ | $2^2 = 4$ | $2^3 = 8$ | $2^4 = 5$ |
| $2^5 = 10$ | $2^6 = 9$ | $2^7 = 7$ | $2^8 = 3$ | $2^9 = 6$ |

**********************************************************************************************************