Diffie & Hellman Key Exchange

DR.VASUDHAARORA

VASUDHA.ARORA@GDGU.ORG,VASUDHARORA6@GMAIL.COM

DEPARTMENTOFCOMPUTERSCIENCEANDENGINEERING

GDGOENKAUNIVERSITY,GURUGRAM

Introduction

➢ The question of key exchange was one of the first problems addressed by a cryptographic protocol. This was prior to the invention of public key cryptography

➢ The Diffie-Hellman key agreement protocol (1976) was the first practical method for establishing a shared secret over an unsecured communication channel

➢The point is to agree on a key that two parties can use for a symmetric encryption, in such

a way that an eavesdropper cannot obtain the key.

- This algorithm was deviced not to encrypt the data but to generate same private cryptographic key at both ends so that there is no need to transfer this key from one communication end to another.

- This algorithm uses arithmetic modulus as the basis of its calculation

The Diffie-Hellman algorithm

- Suppose a sender Alice and a receiver Bob follow this key exchange procedure.

- First, both Alice and Bob agree upon two large prime numbers say **n** and **g**. These 2 integers need not be kept secret. A and B can use any information channel to agree upon them.

- Alice chooses another large random number x and calculates

$$A = g^x \bmod n$$

- Alice sends the number A to Bob.
- Bob chooses another large random number y and calculates
  $B = g^y \bmod n$
- Bob sends number B to Alice.
- Alice now computes the secret key K1 as follows:
  $K1 = B^x \bmod n$
- Bob now computes the secret key K2 as follows:
  $K2 = A^y \bmod n$

The Diffie-Hellman algorithm

Surprisingly, K1 = K2 !!!

K1 = K2 = K is the shared symmetric key???

Let’s Understand how????

$K1 = B^x \bmod n$

$B = g^y \bmod n$

$K1 = (g^y)^x \bmod n$ Similarly,

$K2 = A^y \bmod n$

$A = g^x \bmod n$

$K2 = (g^x)^y \bmod n$

$\Rightarrow K1 = K2 = K$

Man-in-the-Middle Attack

- Also known as bucket brigade attack.

➢ How can two parties agree on a secret value when all of their messages might be overheard by an eavesdropper?

➢The Diffie-Hellman algorithm accomplishes this, and is still widely used. ➢With sufficiently large inputs, Diffie-Hellman is very secure.