# Diffie-Hellman key exchange

## Theory:

The Diffie-Hellman algorithm is being used to establish a shared secret that can be used for secret communications while exchanging data over a public network using the elliptic curve to generate points and get the secret key using the parameters.

* For the sake of simplicity and practical implementation of the algorithm, we will consider only 4 variables, one prime P and G (a primitive root of P) and two private values a and b.
* P and G are both publicly available numbers. Users (say Alice and Bob) pick private values a and b and they generate a key and exchange it publicly. The opposite person receives the key and that generates a secret key, after which they have the same secret key to encrypt.

## Procedure:

| **Alice** | **Bob** |
| --- | --- |
| Public Keys P=23, G=9 | |
| Private Key Selected = a | Private Key Selected = b |
| Key generated = | Key generated = |
| Exchange of generated keys takes place | |
| Key received = y | Key received = x |
| Generated Secret Key, | Generated Secret Key, |
| Show that, = | |