ICS 3

Implementation of Diffie-Hellman key exchange

41323 Gayatri Dhekane

In [1]:

```
# Global variables
P = 23
G = 14

# Private keys
Ra = 3
Rb = 4
```

In [2]:

```
# Public keys
Ua = pow(G, Ra) % P
Ub = pow(G, Rb) % P
```

In [3]:

```
# Symmetric key calculated by A and B
symm_key_a = pow(Ub, Ra) % P # A has access to B's public key and A's private key
symm_key_b = pow(Ua, Rb) % P # B has access to A's public key and B's private key
```

In [4]:

```
assert(symm_key_a == symm_key_b)
```

In [5]:

```
if symm_key_a == symm_key_b:
    print("Agree for communication")
else:
    print("Not Agree for communication")
```

```
Agree for communication
```

In [ ]: