EXP 10: DIFFIE-HELLMAN

PROGRAM:

```
import random

def diffie_hellman_basic(prime, base):
    # Alice's private key
    alice_private = random.randint(1, prime - 1)
    # Alice's public key
    alice_public = pow(base, alice_private, prime)

    # Bob's private key
    bob_private = random.randint(1, prime - 1)
    # Bob's public key
    bob_public = pow(base, bob_private, prime)

    # Shared secret calculation
    alice_shared_secret = pow(bob_public, alice_private, prime)
    bob_shared_secret = pow(alice_public, bob_private, prime)

    return alice_shared_secret, bob_shared_secret

# Example usage
prime = 23
base = 5
shared_secrets = diffie_hellman_basic(prime, base)
print("Shared Secrets:", shared_secrets)
```

OUTPUT: