Public Ciphers

Caleb Dennis

CPE321-03

## Task 1: Implement Diffie-Helman key exchange

The Diffie-Helman key exchange allows users to create a shared secret without communicating any information that would make the secret insecure. In task 1 Alice and Bob independently compute the same shared secret which can be used as a key to securely exchange information. To find the shared secret an adversary must find the prime number that Alice or Bob each chose. To find this number the adversary needs to compute the log base g of Alice’s public key. An adversary could check all primes, but if Alice has chosen a reasonably large prime this process takes a lot of computing.

from Crypto.Util.number import getPrime

from Crypto.Util.Padding import pad, unpad

from Crypto.Random import get\_random\_bytes

from Crypto.Hash import SHA256

from Crypto.Cipher import AES

from Crypto.Cipher import AES

def main():

    p = 37

    g = 5

    Alice\_prime = getPrime(16)

    Bob\_prime = getPrime(16)

    print(f"Alice's prime: {Alice\_prime}")

    print(f"Bob's prime: {Bob\_prime}")

    Alice\_public = pow(g, Alice\_prime) % p

    Bob\_public = pow(g, Bob\_prime) % p

    Alice\_shared\_secret = bytes(pow(Bob\_public, Alice\_prime) % p)

    Bob\_shared\_secret = bytes(pow(Alice\_public, Bob\_prime) % p)

    Alice\_hasher = SHA256.new()

    Alice\_hasher.update(Alice\_shared\_secret)

    alice\_key = Alice\_hasher.digest()

    Bob\_hasher = SHA256.new()

    Bob\_hasher.update(Bob\_shared\_secret)

    bob\_key = Bob\_hasher.digest()

    iv = get\_random\_bytes(16)

    print(f"Bob's key {alice\_key}\nAlice's key {bob\_key}\n")

    Alice\_msg = pad(bytes("Hi Bob, i'm Alice", "ascii"), 16)

    print(f"Alice: {unpad(Alice\_msg, 16)}")

    Alice\_encrypter = AES.new(alice\_key, AES.MODE\_CBC, *iv*=iv)

    Alice\_sends\_to\_Bob = Alice\_encrypter.encrypt(Alice\_msg)

    Bob\_encrypter = AES.new(bob\_key, AES.MODE\_CBC, *iv*=iv)

    Bob\_received\_from\_Alice = Bob\_encrypter.decrypt(Alice\_sends\_to\_Bob)

    print(f"Bob received: {unpad(Bob\_received\_from\_Alice, 16)}")

if \_\_name\_\_ == "\_\_main\_\_":

    main()