Alona Trubchaninova 150502

Algorytm Diffiego-Helmana

- Implementacja algorytmu:

```
Comment Code
def diffie_hellman_key_exchange(n, g):
    privKeyA = randint(10000, 100000)       #2)generujemy prywatny klucz dla A
    privKeyB = randint(10000, 100000)       #generujemy prywatny klucz dla B
    print("A's private key: " + str(privKeyA))
    print("B's private key: " + str(privKeyB))

    x = (g ** privKeyA) % n         #3) A oblicza wartość x i wysyłą ją do B
    y = (g ** privKeyB) % n         #B oblicza wartość y i wysyłą ją do A

    keyA = x ** privKeyA % n        #4) B oblicza klusz A
    keyB = y ** privKeyB % n        #4) A oblicza klusz B

    print("Public key generated by A: " + str(keyA) + "\nPublic key generated by B: " + str(keyB))

if __name__ == '__main__':
    try:
        n = int(input("n (large prime number): "))      #1)podajemy znaczenie n i g
        g = int(input("g (prime smaller than n): "))

        #n = 170141183460469231731687303715884105727
        #g = 2305843009213693951

        if n <= 0 or g <= 0 or not (2 < g < n):
            raise ValueError("Invalid values for n or g.")

        diffie_hellman_key_exchange(n, g)

    except ValueError as e:
        print(f"Error: {e}")
```

2. Ograniczenia dla parametrów

- n powinno być dużą liczbą pierwszą, a g powinno być liczbą całkowitą taką, że 1 < g < n.
- g i n powinny być względnie pierwsze (nie mają wspólnych dzielników).
- g powinno być pierwiastkiem pierwotnym modulo n.

3. Danych, które można podsłuchać:

- Klucze publiczne A i B są przesyłane otwarcie, ale są bezpieczne, ponieważ trudno jest obliczyć klucz prywatny na ich podstawie bez znajomości tajnych liczb x i y.

4. Schemat ataku:

- Atak Man-in-the-Middle (MITM): Ktoś podsłuchuje klucze publiczne A i B, a następnie udaje obie strony, aby uzyskać współdzielony klucz. Rozwiązaniem jest użycie metod weryfikacji tożsamości.

5. Dodatkowe wnioski:

- Implementacja algorytmu D-H pozwala na bezpieczną wymianę kluczy, ale wymaga odpowiednich środków zabezpieczających, takich jak uwierzytelnianie stron i ochrona przed atakami typu MITM.