Учреждение образования
“БЕЛОРУССКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ
ИНФОРМАТИКИ
И РАДИОТЕХНИКИ
Кафедра Интеллектуальных Информационных технологий

Отчет по лабораторной работе №4
по дисциплине “Средства и методы защиты информации в интеллектуальных системах”

Выполнил ст. группы 121701
МУлярчик Д.С.

Проверил
Сальников Д.А.

Для решения лабораторной работы были использована одна функция, которая позволяет найти примитивный элемент поля размером P:

```python
def primitive_element(modul):
    for g in range(2, modul):
        powers = set()
        for i in range(1, modul):
            power = pow(g, i, modul)
            if power in powers:
                break
            powers.add(power)
        else:
            return g
    return None
```

```python
P = 9011

g = primitive_element(P)
print("Примитивный элемент g в GF({}): {}".format(P, g))
```

```
Примитивный элемент g в GF(9011): 2
```

В основной части кода выполняются действия для протокола Диффи-Хеллмана:

```python
A = random.randint(1000, 9999)
print("Сектрет A:", A)
public_A = pow(g, A, P)
print("Отправляемое A:", public_A)

B = random.randint(1000, 9999)
print("Секрет B:", B)
public_B = pow(g, B, P)
print("Отправляемое B:", public_B)

shared_secret_A = pow(public_B, A, P)

shared_secret_B = pow(public_A, B, P)

shared_secret = pow(g, A*B, P)

print("Общий секрет A:", shared_secret_A)
print("Общий секрет B:", shared_secret_B)

print("Общий секрет:", shared_secret)
```

```
Сектрет A: 2610
Отправляемое A: 7949
Секрет B: 1074
Отправляемое B: 6147
Общий секрет A: 4821
Общий секрет B: 4821
Общий секрет: 4821
```