Национальный исследовательский университет «МЭИ» Институт автоматики и вычислительной техники

Кафедра вычислительных машин, систем и сетей

Лабораторная работа № 10

«Схемы разделения секрета»

по курсу «Защита информации»

Выполнил: Кутузов И.Г.

Группа: А-08-16

Подпись:

Преподаватель: Рытов А.А.

Москва, 2020 г.

In[ ]:=
```
nstd = 10;
(*1. Решить уравнение ax+b=
 c (mod p) обычным методом с использованием обратного элемента:a=5;
b=9;
p=31;
c=29.*)
```

In[ ]:=
```
a = 5; b = 9; p = 31; c = 29;
Mod[Mod[c - b, p] * PowerMod[a, -1, p], p]
```
ос··· | остаток от дел··· | степень по модулю

Out[ ]= 4

In[ ]:=
```
(*2. Решить это же уравнение ax+b=
 c (mod p) с применением функции Solve[a*x+b==c,{x},Modulus→31].*)
```
решить уравнения | модуль

```
Solve[a * x + b == c, {x}, Modulus → p]
```
решить уравнения | модуль

Out[ ]= {{x → 4}}

In[ ]:=
```
(*3. Восстановить сообщение M в пороговой схеме (3,5) по трем долям:*)
Mod[nstd, 4] + 1
```
остаток от деления
```
k = {, , 7, 12, 5}
Solve[
```
решить уравнения
```
 a1 * 3^2 + b1 * 3 + m == k[[3]] &&
  a1 * 4^2 + b1 * 4 + m == k[[4]] &&
  a1 * 5^2 + b1 * 5 + m == k[[5]]
 , {a1, b1, m}, Modulus → 13
```
модуль
```
]
```

Out[ ]= 3

Out[ ]= {Null, Null, 7, 12, 5}

Out[ ]= {{a1 → 7, b1 → 8, m → 11}}

In[ ]:=
```
(*4. Провести оценку числа возможных решений при наличии только двух долей.*)
(*бесконечное количество*)
```

In[ ]:=
```
SeedRandom[nstd]
инициализация генератора псевдослучайны
pA = RandomPrime[nstd * 10 000]
    случайное простое число
qA = RandomPrime[nstd * 10 000]
    случайное простое число
nA = pA * qA
eul = (pA - 1) * (qA - 1)
k1 = RandomPrime[eul]
    случайное простое число
k2 = RandomPrime[eul]
    случайное простое число

k3 = PowerMod[k1 * k2, -1, eul]
    степень по модулю
While[GCD[k1 * k2 * k3, eul] ≠ 1,
цикл··· НОД
 k1 = RandomPrime[eul];
     случайное простое число
 k2 = RandomPrime[eul];
     случайное простое число
 k3 = PowerMod[k1 * k2, -1, eul];]
     степень по модулю
Mod[k1 * k2 * k3, eul]
остаток от деления
```

Out[ ]= 21 599

Out[ ]= 86 029

Out[ ]= 1 858 140 371

Out[ ]= 1 858 032 744

Out[ ]= 354 150 353

Out[ ]= 375 532 903

Out[ ]= 97 185 383

Out[ ]= 1

In[ ]:=
```
(*6. Представить свою фамилию в числовом эквиваленте,
подписать на первом ключе и выполнить проверку.*)
fam = ToCharacterCode[ToUpperCase["аКутузовя"], "WindowsCyrillic"] -
      код символа          перевести в верхний регистр
  ToCharacterCode["A", "WindowsCyrillic"][[1]] + 1
  код символа
fam = Take[fam, {2, Length[fam] - 1}]
      извлечь        длина
grant = PowerMod[fam, k1, nA]
        степень по модулю
fam == PowerMod[grant, k2 * k3, nA]
       степень по модулю
grant2 = PowerMod[grant, k2, nA]
         степень по модулю
```

Out[ ]= {1, 11, 20, 19, 20, 8, 15, 3, 32}

Out[ ]= {11, 20, 19, 20, 8, 15, 3}

Out[ ]= {1 580 675 821, 313 985 414, 851 220 910, 313 985 414, 1 107 771 359, 1 577 260 697, 1 724 097 077}

Out[ ]= True

Out[ ]= {312 150 563, 1 040 234 732, 1 080 285 531, 1 040 234 732, 773 848 552, 225 347 116, 1 259 945 508}

In[ ]:=

In[ ]:=
```
(*7. Подписать свою фамилию на втором ключе и представить результат для проверки.*)
grant2 = PowerMod[grant, k2, nA]
         степень по модулю
FromCharacterCode[PowerMod[grant2, k3, nA] +
символ по его коду      степень по модулю
  ToCharacterCode["A", "WindowsCyrillic"][[1]] - 1, "WindowsCyrillic"]
  код символа
```

Out[ ]= {312 150 563, 1 040 234 732, 1 080 285 531, 1 040 234 732, 773 848 552, 225 347 116, 1 259 945 508}

Out[ ]= КУТУЗОВ