Национальный исследовательский университет «МЭИ» Институт автоматики и вычислительной техники

Кафедра вычислительных машин, систем и сетей

Лабораторная работа № 8

«Криптосистема RSA»

по курсу «Защита информации»

Выполнил: Кутузов И.Г.

Группа: А-08-16

Подпись:

Преподаватель: Рытов А.А.

Москва, 2020 г.

In[ ]:=
```
Nomer = 10;
(*1. Разработать программный модуль для формирования системных параметров RSA
  (модуль,открытый ключ,секретный ключ) на основе заданных номеров простых чисел:Q=
 Prime[10000-N],P=Prime[10000+N],где N-номер по списку в группе.*)
Q = Prime[10 000 - Nomer]
P = Prime[10 000 + Nomer]
```

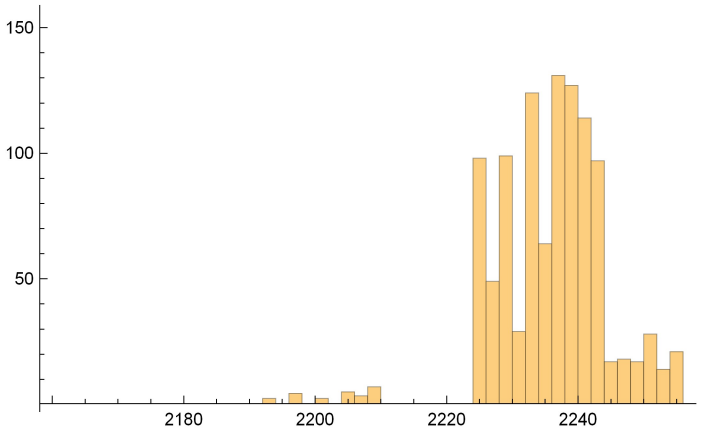
Out[ ]= 104 659

Out[ ]= 104 831

In[ ]:=
```
(*2. Импортировать текстовый файл с номером по списку в группе
 из папки Plaintext1RSA.Провести анализ кодов текста и привести к
 виду:1XXX или 2XXX-четыре десятичных цифры,представляющие собой блок
  для шифрования в RSA.Например:код пробела 32 представляем как 2000+32=
 2032. Построить гистограмму распределения кодов символов открытого текста.*)
codes = Import["Z:\\Develop\\SEM8\\ЗИ\\LAB8\\work task\\Plaintext1RSA\\Text-10.txt",
   "Byte"];
RsaCodes = codes + 2000;
```

In[ ]:=
```
Histogram[RsaCodes]
```

Out[ ]=



In[ ]:=
```
(*3. Зашифровать текст на открытом ключе и определить энтропию шифртекста*)
n = P * Q
eul = (P - 1) * (Q - 1)
e = NextPrime[eul, -100]
    следующее простое число
GCD[e, eul]
НОД

Clear[d]
очистить
d = Solve[e * d == 1, d, Modulus → eul][[1]][[1]][[2]]
    решить уравнения    модуль
Mod[d * e, eul]
остаток от деления
cript = PowerMod[RsaCodes, e, n];
        степень по модулю
N[Entropy[cript]]
.. энтропия
```

Out[ ]= 10 971 507 629

Out[ ]= 10 971 298 140

Out[ ]= 10 971 295 883

Out[ ]= 1

Out[ ]= 636 792 227

Out[ ]= 1

Out[ ]= 3.25386

In[ ]:=

In[ ]:=
```
(*4. Провести расшифрование на секретном ключе.*)
decripted = PowerMod[cript, d, n];
                    степень по модулю
FromCharacterCode[decripted - 2000, "WindowsCyrillic"]
символ по его коду
```

Out[ ]= разрушение информации, вызванное вирусными воздействиями;

- разрушение архивной банковской информации, хранящейся на магнитных носителях;

- кража оборудования [39].

Несанкционированный доступ (НСД) является наиболее распространенным и многообразным видом компьютерных нарушений. Суть НСД состоит в получении пользователем (нарушителем) доступа к объекту в нарушение правил разграничения доступа, установленных в соответствии с принятой в организации политикой безопасности. НСД использует любую ошибку в системе защиты и возможен при нерациональном выборе средств защиты, их некорректной установке и настройке. НСД может быть осуществлен как штатными средствами АСОИ, так и специально созданными аппаратными и программными средствами.

Перечислим основные каналы несанкционированного доступа, через которые нарушитель может получить доступ к компонентам АСОИ и осуществить хищение, модификацию и/или разрушение информации:

- все штатные каналы доступа к информации (терминалы пользователей, оператора, администратора системы; средства отображения и документирования информации; каналы связи) при их использовании нарушителями, а также законными пользователями вне пределов их полномочий;

- технологические пульты управления;

- линии связи между аппаратными с

In[ ]:=
```
(*5. Сформировать из модифицированных блоков открытого текста
  (см.п.2) десятичные эквиваленты биграмм:{1079,2032}→{10792032}.*)
parts = Partition[RsaCodes, 2];
        разбиение на блоки
bigrams = {};
Do[AppendTo[bigrams, parts[[i]][[1]] * 10000 + parts[[i]][[2]]], {i, Length[parts]}]
... добавить в конец к                                          длина
```

In[ ]:=
```
(*6. Провести шифрование блоков биграмм
 на открытом ключе.Определить энтропию шифр текста*)
criptbigrams = PowerMod[bigrams, e, n];
               степень по модулю
N[Entropy[criptbigrams]]
  энтропия
```

Out[ ]= 5.20375

In[ ]:=
```
(*7. Расшифровать полученный шифртекст и вывести его в виде строки.*)
decriptedbigrms = PowerMod[criptbigrams, d, n];
                  степень по модулю
letters = {};
Do[AppendTo[letters, Floor[decriptedbigrms[[i]] / 10000] - 2000];
…  добавить в конец к    округление вверх
 AppendTo[letters, Mod[decriptedbigrms[[i]], 10000] - 2000],
 добавить в конец к    остаток от деления
 {i, Length[decriptedbigrms]}]
     длина
FromCharacterCode[letters, "WindowsCyrillic"]
символ по его коду
```

Out[ ]=

разрушение информации, вызванное вирусными воздействиями;

- разрушение архивной банковской информации, хранящейся на магнитных носителях;
- кража оборудования [39].

Несанкционированный доступ (НСД) является наиболее распространенным и многообразным видом компьютерных нарушений. Суть НСД состоит в получении пользователем (нарушителем) доступа к объекту в нарушение правил разграничения доступа, установленных в соответствии с принятой в организации политикой безопасности. НСД использует любую ошибку в системе защиты и возможен при нерациональном выборе средств защиты, их некорректной установке и настройке. НСД может быть осуществлен как штатными средствами АСОИ, так и специально созданными аппаратными и программными средствами.

Перечислим основные каналы несанкционированного доступа, через которые нарушитель может получить доступ к компонентам АСОИ и осуществить хищение, модификацию и/или разрушение информации:

- все штатные каналы доступа к информации (терминалы пользователей, оператора, администратора системы; средства отображения и документирования информации; каналы связи) при их использовании нарушителями, а также законными пользователями вне пределов их полномочий;
- технологические пульты управления;
- линии связи между аппаратными с