# Министерство цифрового развития, связи и массовых коммуникаций Федеральное государственное бюджетное образовательное

**учреждение высшего образования**

# «Санкт-Петербургский государственный университет телекоммуникаций

**им. проф. М. А. Бонч-Бруевича»**

Кафедра защищенных систем связи Дисциплина «Основы криптографии»

# Лабораторная работа № 13

**«Исследование криптосистем с открытым ключом»**

Выполнил: ст. гр. ИКТЗ-83

Громов Артем Вариант 4

Проверил: Яковлев В. А.

Санкт-Петербург 2021

**Цель работы**: Приобретение навыков анализа алгоритмов криптосистем с открытыми ключами.

# Ход работы

1. **Моделирование криптографической системы Эль-Гамаля.**

Дано: p = 11, a = 6, x = 9, k = 9.

*Зашифровать сообщение m=(№\*11+4)mod7, расшифровать криптограмму, где № Ваш номер по журналу.*

# Шифрование

Найдем сообщение m: m=(4\*11+4)mod7=48mod7=6

Найдем с1=akmodp и с2=m(y -1)kmodp: с1=akmodp=69mod11=2

A

Воспользуемся быстрым способом возведения: 9=10012

6=6(mod11) 62=3(mod11)

64 =9(mod11)

68=4(mod11)

Y=6\*4(mod11) = 24(mod11) = 2

Найдём yA= axmodp=69mod11 = 2

Воспользуемся быстрым способом возведения: 9=10012

6=6(mod11) 62=3(mod11)

64 =9(mod11)

68=4(mod11)

Y=6\*4(mod11) = 24(mod11) = 2

Найдём yA -1

Найдем НОД(2,11) 11=5\*2+1

НОД(2,11)=1

Найдем х и у удовлетворяющие условию: 1 = (x \* 2 + y \* 11) mod 11 = x \* 2(mod 11)

1=11-2\*5  
 x=-5 y=1

yA -1=p+x=6

Найдем с2=m(y -1)kmodp: с2=m(y -1)kmodp=6\*69mod11=1

A

A

Воспользуемся быстрым способом возведения:

10=10102 6=5(mod11) 62=3(mod11)

64 =9(mod11)

68=4(mod11)

Y=4\*3(mod11) = 12(mod11) = 1

Сформируем криптограмму E(c1c2): E(c1c2)=2\*1=2

# Расшифрование

Найдем b=c1xmodp=akxmodp b=c1xmodp=akxmodp=69\*9mod11=6

Воспользуемся быстрым способом возведения:

81= 10100012 6=6(mod11) 62=3(mod11)

64 =9(mod11)

68=4(mod11)

616=5(mod11)

632=3(mod11)

664=9(mod11)

Y=9\*5\*6(mod11) = 6

Найдем m= c2c1x(modp) m=c2c1x(modp)=1\*29(mod11)=6

Воспользуемся быстрым способом возведения:

9=10012

2=2(mod11) 22=4(mod11)

24 =5(mod11)

28=3(mod11)

Y=3\*2(mod11) = 6(mod11) = 6

Расшифрованное сообщение = зашифрованному => выполнено верно!

*Подписать сообщение, соответствующее Вашему №, используя хэш- функцию вида m=(№\*13+4)mod7. Проверить подпись.*

## Генерирование ключей.

x = 9 - закрытый ключ,

y = ax (mod p) = 69 (mod 11) = 2 – открытый ключ

Воспользуемся быстрым способом возведения: 9=10012

6=6(mod11) 62=3(mod11)

64 =9(mod11)

68=4(mod11)

Y=6\*4(mod11) = 24(mod11) = 2

## Формирование подписи.

Пусть хэшированное сообщение m' = (4\*13+4)mod 7 = 17 mod 7 = 10

Находим первую часть подписи:

r = ak(mod p) = 69(mod 11) = 2

Воспользуемся быстрым способом возведения: 9=10012

6=6(mod11) 62=3(mod11)

64 =9(mod11)

68=4(mod11)

Y=6\*4(mod11) = 24(mod11) = 2

Найдём k-1:

Найдем НОД(9,10):

10=1\*9+1

НОД(9,10)=1

Найдем х и у удовлетворяющие условию: 1 = (x \* 9 + y \* 10) mod 10 = x \* 9 (mod 10)

1=10-9\*1

x=-1 y= 1

k-1 = 10+x=9

k\*k-1 = 9\*9(mod 10) = 1(mod 10)

Находим вторую часть подписи: s = k-1(m –xr) (mod p-1)

s = 9(10 – 9\*2) (mod 10) = -72 mod 10 = 8

Подпись (r = 2, s = 8).

# Проверка подписи.

Проверяем выполнение сравнения:

yrrs (mod p) = am’(mod p).

yrrs (mod p) = 2228 (mod 11) = 210 (mod 11)=1

Воспользуемся быстрым способом возведения: 10 = 10102

2=2(mod11) 22=4(mod11)

24=5(mod11) 28=3(mod11)

Y=3\*4(mod11)=1

am’(mod p) = 610 (mod 11) = 1

1 = 1, значит подпись верна

# Моделирование криптографической системы РША.

Дано: p = 5, q = 7, e = 13, m = 4.

# Сформировать закрытый ключ d.

Найдем y = me (mod p):

y = me (mod p) = 413 (mod 5) = 4

Воспользуемся быстрым способом возведения: 13 = 11012

4=4(mod5) 42=1(mod5)

44=1(mod5)

48=1(mod5) Y=1\*1\*4(mod5)=4

# Генерирование ключа в криптосистеме

* N = p \* q = 5 \* 7 = 35- модуль
* (N)= (p-1)(q-1) = (5-1)(7-1) = 24 – функция Эйлера
* е = 13 - из таблицы
* НОД(13, 24) = 1

24 = 13 \* 1 + 11

13 = 11 \* 1 + 2

11 = 2 \* 5 + 1 → НОД = 1

* de = 1(mod (N)) – обратный элемент к е

1 = (x \* 13 + y \* 24) mod 24 = x \* 13 (mod 24)

1 = 11 - 5 \* 2

2 = 13 – 1 \* 11

11 = 24 – 1 \* 13

1 = 11 – 5 \* 2 = (24 – 1 \* 13) – 5 \* (13 – 1 \* 11) =

= (24 – 1 \* 13) – 5 \* (13 – 1 \*(24 – 1 \* 13)) = 24 – 13 – 5 \* (13 – 24 + 13) =

24 – 13 – 5 \* (2 \* 13 – 24) = 24 – 13 – 10 \* 13 + 5 \* 24 = 4 \* 24 – 11 \* 13

x = -11, y = 4

d = 24+x = 13

Проверка: 13 \* 13(mod 24) = 1 - верно

* d = 13 = SK – приватный ключ
* (e, N) = (13, 35) = PK – публичный ключ

# Формирование подписи.

m = h(M) = 4 – хэшированное сообщение

Используя закрытый ключ d подпишем m s = md(mod N)

s = 413 (mod 35) = 4

Воспользуемся быстрым способом возведения:

13 = 11012

4=4(mod35) 42=16(mod35)

44=11(mod35)

48=16(mod35) Y=16\*11\*4(mod35) = 4

# Проверка подписи.

m’ = h(M) = 4 – хэшированное сообщение

Используя открытый ключ, осуществим проверку подписи, вычисляя m = se(mod N)

m = 413(mod 35) = 4

m = m’ = 4 → Подпись верна! Проверка выполнена успешно.

# Вывод:

В ходе данной лабораторной работы были изучены способы формирования и проверки подписи в системах РША и Эль-Гамаля. Для этого были использованы алгоритмы быстрого возведения в степень и нахождения НОД с помощью алгоритма Евклида.