I ОСНОВНАЯ ЧАСТЬ

№1 Зашифровать сообщение «КИБЕРНЕТИКА» ключом «ДИСК».

|  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| ДАННЫЕ ДЛЯ ШИФРОВАНИЯ | | | | | | | | | | |
| К | И | Б | Е | Р | Н | Е | Т | И | К | А |
| №СИМВОЛОВ В АЛФАВИТЕ | | | | | | | | | | |
| 12 | 10 | 2 | 6 | 18 | 15 | 6 | 20 | 10 | 12 | 1 |
| КЛЮЧ | | | | | | | | | | |
| Д | И | С | К | Д | И | С | К | Д | И | С |
| 5 | 10 | 19 | 12 | 5 | 10 | 19 | 12 | 5 | 10 | 19 |
| ПРОЦЕСС ШИФРОВАНИЯ | | | | | | | | | | |
| К+Д | И+И | Б+С | Е+К | Р+Д | Н+И | Е+С | Т+К | И+Д | К+И | А+С |
| 17 | 20 | 21 | 18 | 23 | 25 | 25 | 32 | 15 | 22 | 20 |
| ИТОГ ШИФРОВАНИЯ | | | | | | | | | | |
| 17 | 20 | 21 | 18 | 23 | 25 | 25 | 32 | 15 | 22 | 20 |
| П | Т | У | Р | Х | Ч | Ч | Ю | Н | Ф | Т |

Ответ: ПТУРХЧЧЮНФТ

Задание №2. Между абонентами A и B установлен секретный канал связи без передачи ключей при заданных p = 167 и их первых ключах 15 и 21. Описать процесс передачи сообщений 22 (от A к B ) и 17 (от B к A)

Решение:

p = 167 (φ(167)=166; a=15,b=21

15a = 1 (mod φ(167))

15a = 1 (mod 166) /166-1

15a = 164 (mod 166) /15

a = 11 (mod 166)

a = 11

21β = 1(mod 166) /166+1

21β = 167(mod 166) /167+1

21β = 168(mod 166) /21

β = 8 (mod 166)

β = 8

mn = m2 (mod p); ma>b = 22; mb>a = 17

m1 = 2215 (mod 167)

m1 = 58

m2 = 1715 (mod 167)

m2 = 16

m3 = 2221 (mod 167)

m4 = 1721 (mod 167)

Задание №3. Нужно послать секретные сообщения 25 и 2 для JB и 14 для CIA, используя следующие записи открытой книги паролей криптосистемы RSA:

JB: 77,7;

CIA: 667,15.

Решение:

A1=7; A2=11; B1=15; B2= 44 (667 mod 15)

M1= 25; M2=2; M1=257 (mod 77); M1 = 69

15 β=1 (mod φ (667))

15 β=1 (mod 666)/666 - 1

15 β=665 (mod 666)/665-1

15 β=664 (mod 666)/664-1

15 β=663 (mod 666)/663-1

15 β=662 (mod 666)/662-1

15 β=661 (mod 666)/661-1

15 β=660(mod 666)/15

β=44 (mod 666)

β=44

m1 β = m (mod 667)

6914=25 (mod 667)

Задание №4. Пользователь системы RSA выбрал p1=11и p2=47. Какие из чисел 12, 33, 125, 513 он может выбрать для открытого ключа? Вычислить для них закрытый ключ.

Решение:

Задание №5. Пользователь системы RSA, выбравший p1=17, p2=11 и a= 61, получил шифрованное сообщение m1 = 3. Дешифровать m1.

Решение:

rA = 17\*11=187

φ(187) = 186

17a=1(mod 186) /186+1

17a = 187 (mod 186) /17

17a = 11(mod 186)

a = 11

m1= 317 (mod 187)

m=13011 (mod 187)