

Санкт-Петербургский государственный электротехнический университет «ЛЭТИ»  
им. В.И. Ульянова (Ленина)

Лабораторная работа №7

## ИЗУЧЕНИЕ АСИММЕТРИЧНЫХ ПРОТОКОЛОВ И ШИФРОВ

Студент: \_\_\_\_\_

Порошина Алина, группа 0361

Руководитель: \_\_\_\_\_

Племянников А.К., доцент каф. ИБ

Санкт-Петербург 2024

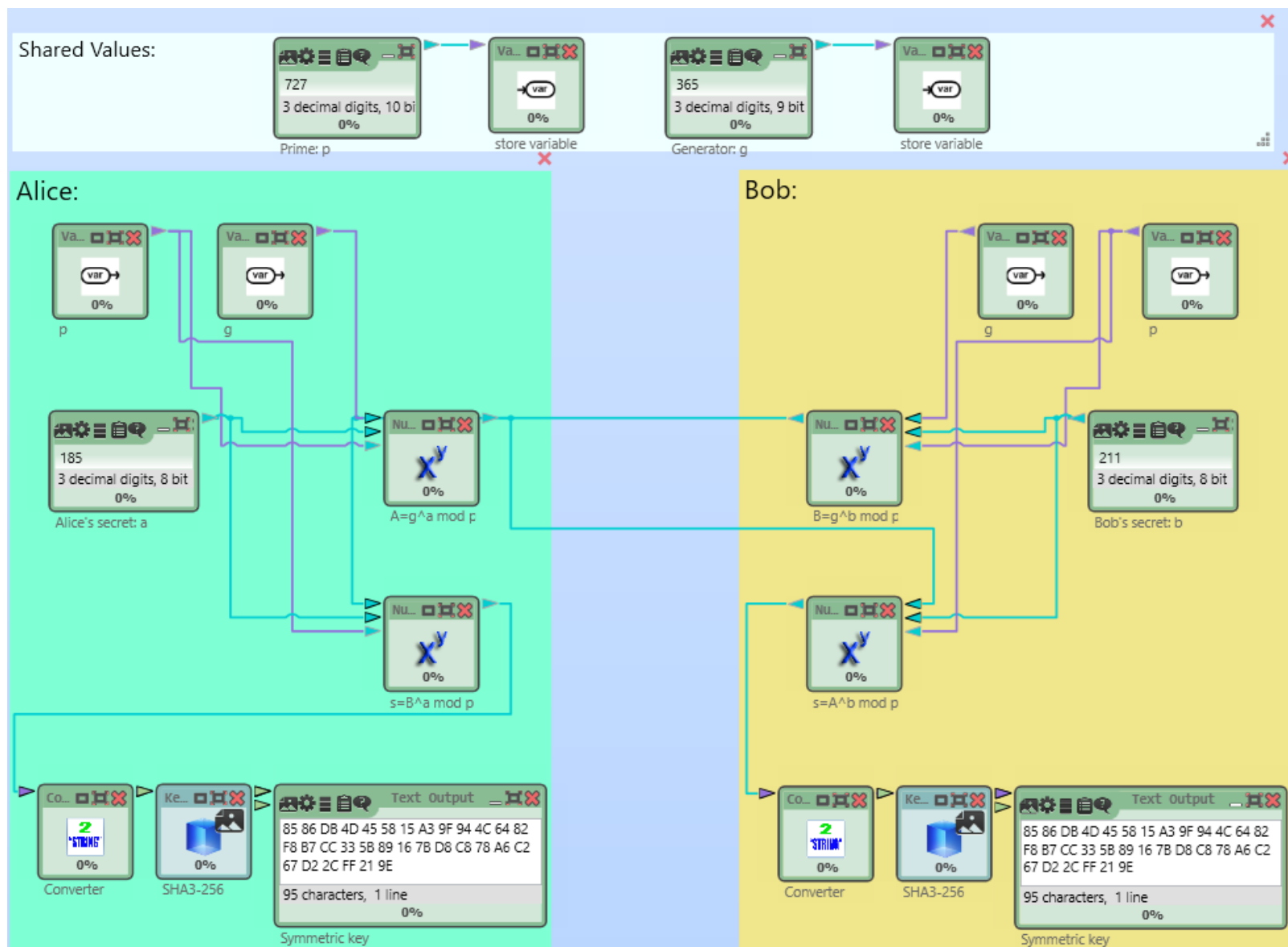
# Цель работы

Цель работы – приобретение знаний и умений в работе с асимметричными протоколами и шифрами: протокол Диффи-Хеллмана, шифр RSA

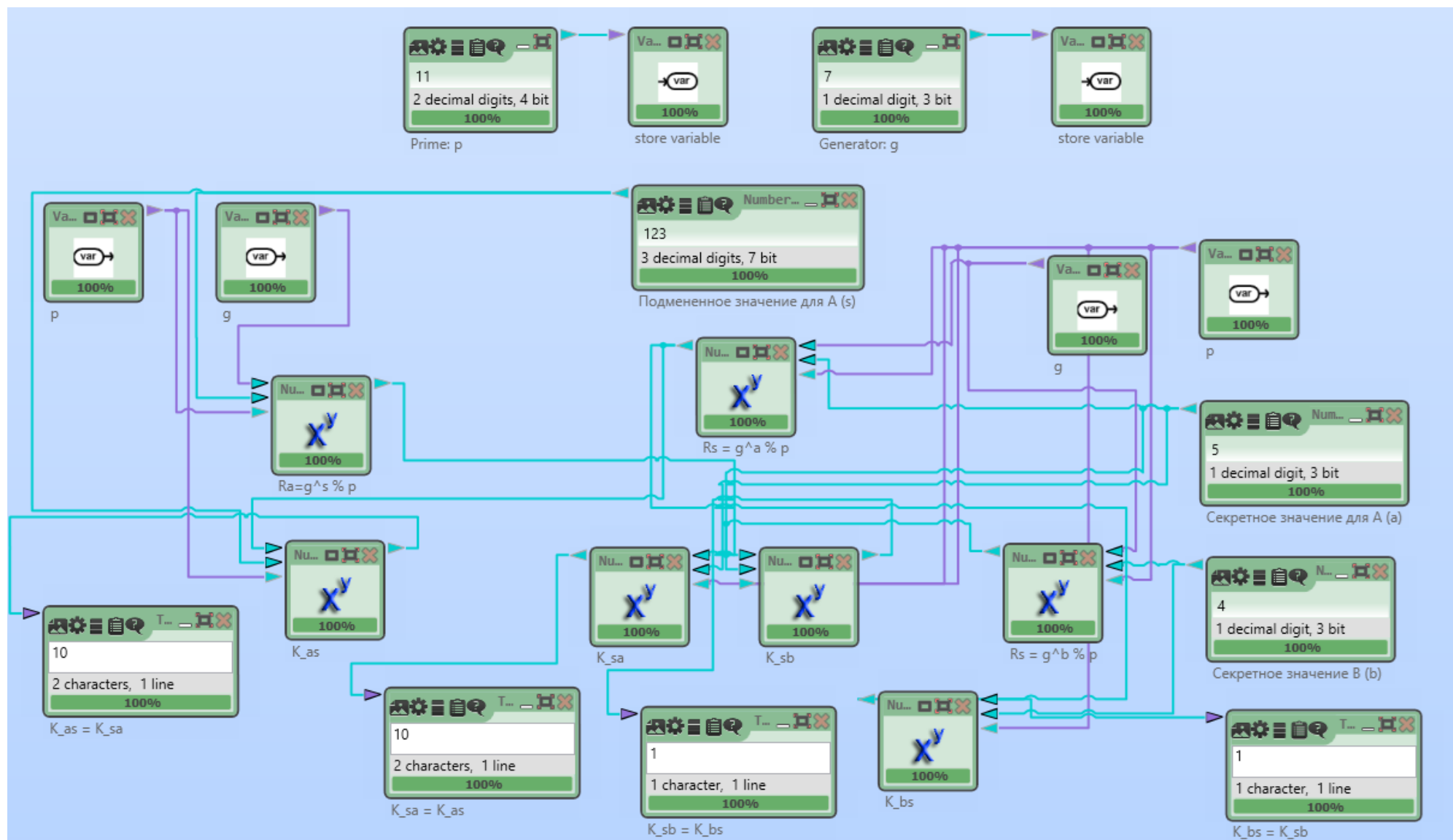
Задачи:

- Изучить протокол согласования ключей Диффи-Хеллмана.
- Изучить алгоритм асимметричного шифрования RSA.
- Изучить протокол асимметричного шифрования RSA.
- Выполнить атаку на шифр RSA факторизацией модуля.
- Выполнить имитацию атаки на гибридную систему шифрования.

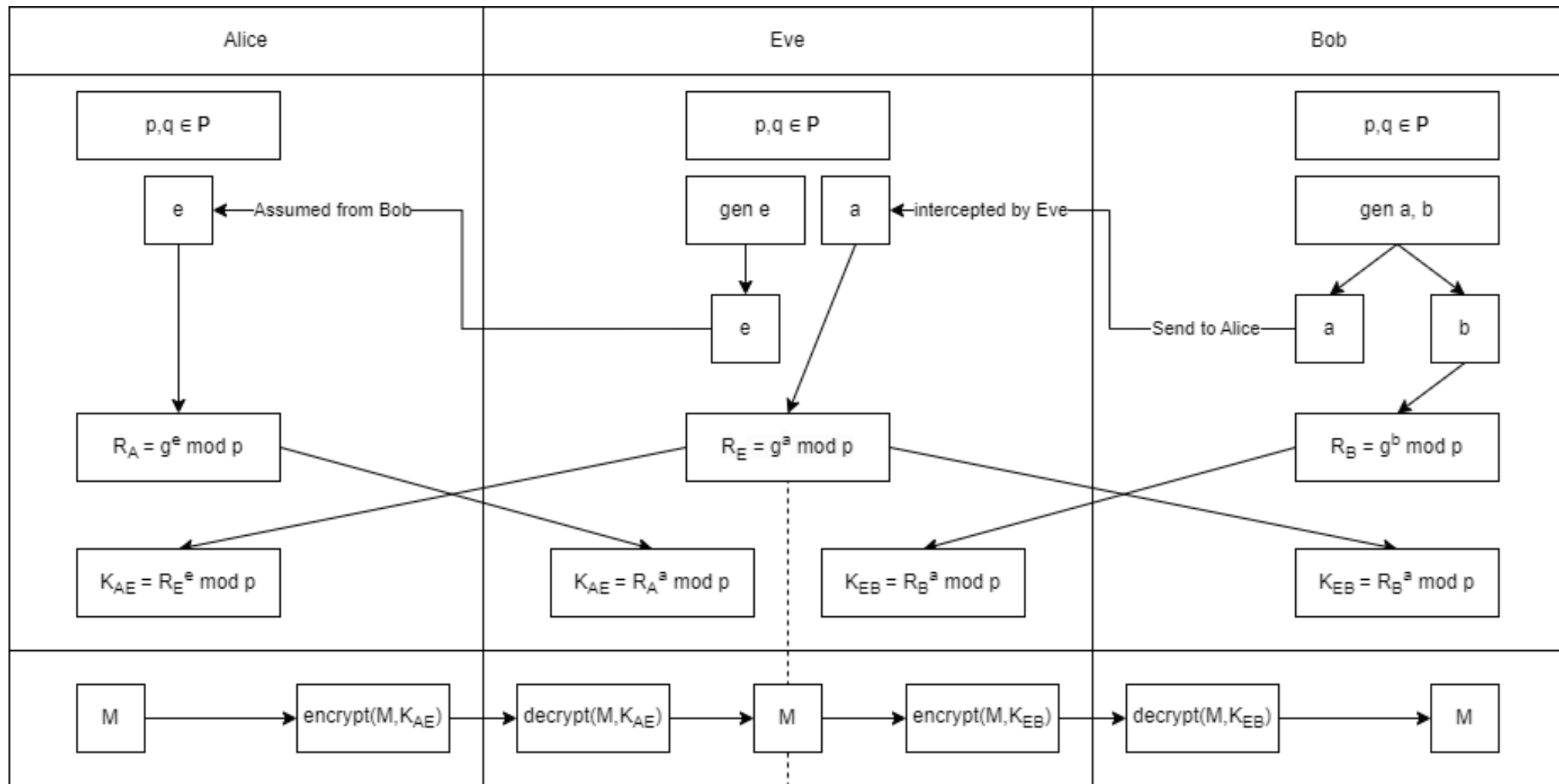
# Протокол согласования ключей Диффи-Хеллмана: шаблонная схема для генерации 256-битного ключа



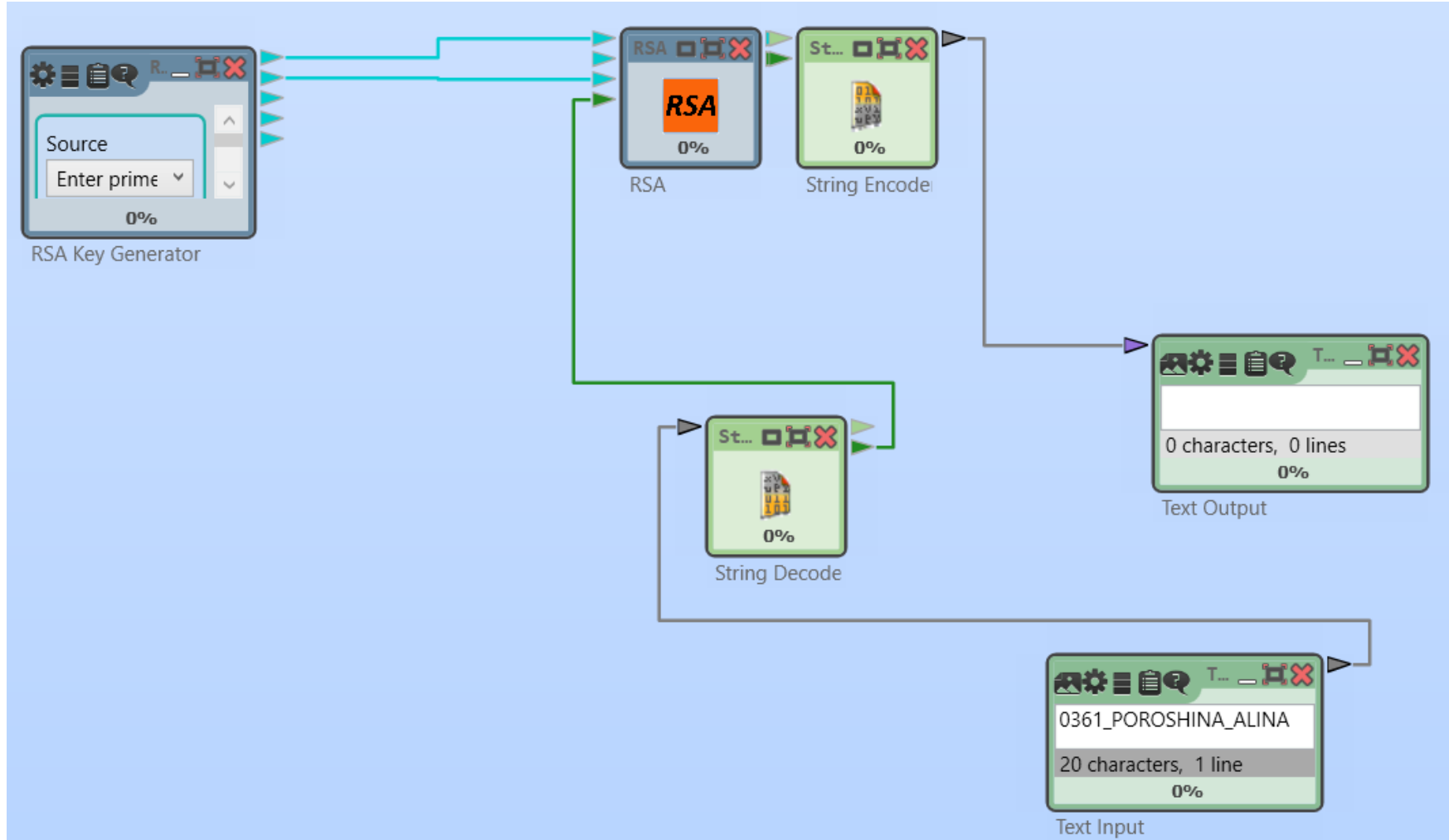
# Протокол согласования ключей Диффи-Хеллмана: Атака посредника



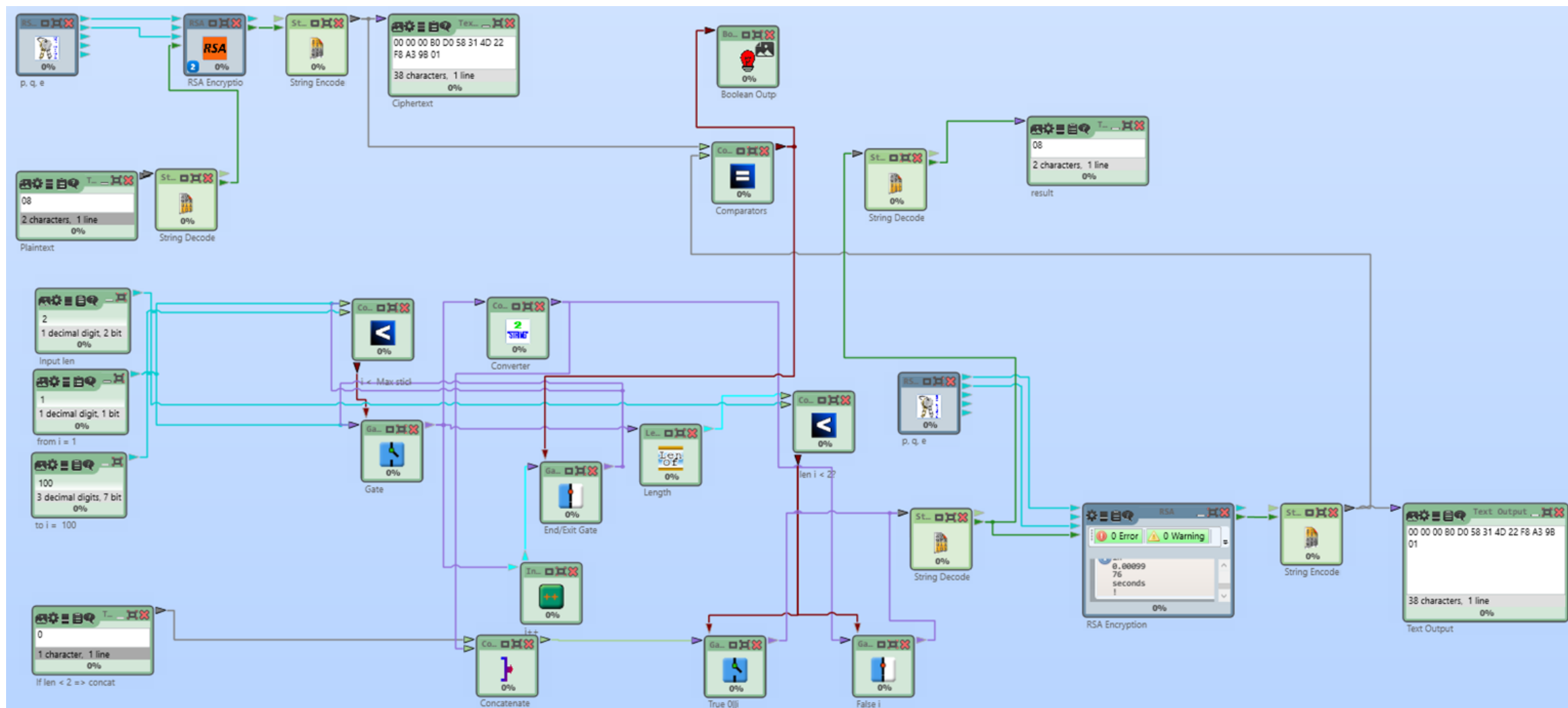
# Протокол согласования ключей Диффи-Хеллмана: Атака посредника



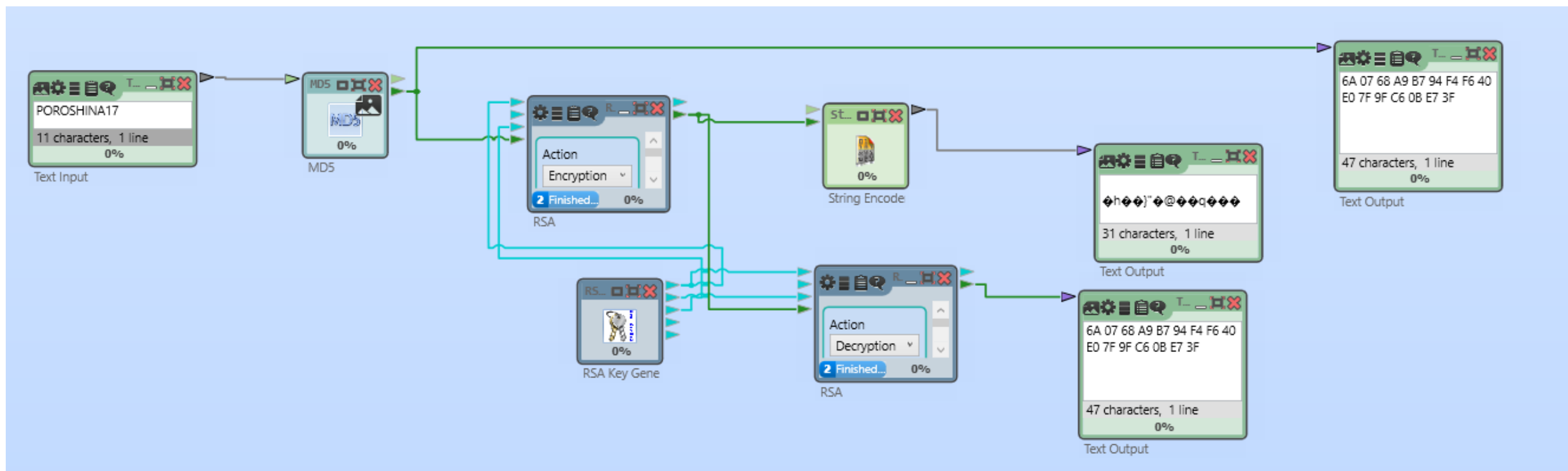
# RSA: Шаблонная схема



# RSA: Атака короткого сообщения

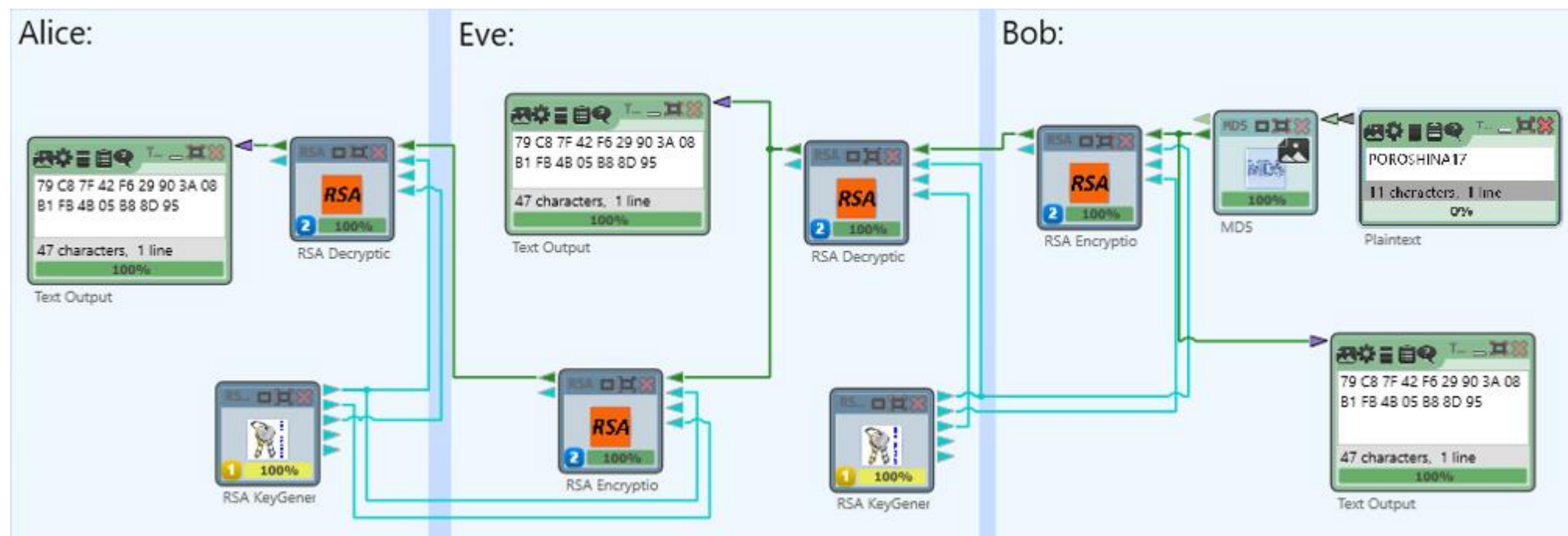


# RSA: Шифрование ключа 128 бит





# RSA: Атака посредником



# RSA: Атака факторизацией модуля

Factorization of a Number

Algorithms for factorization

☒ Brute-force  
☐ Brent  
☐ Pollard  
☐ Williams  
☐ Lenstra  
☐ Quadratic sieve

Input

Enter the number to be factorized:

Factorization (stepwise)

Click "Continue" to factor the input number. If the result (shown below) can be factored further, click the button again to execute the factorization.

Factorization

The factorization is represented in the format  $\langle z_1^{a_1} * z_2^{a_2} * \dots * z_n^{a_n} \rangle$ . Composite numbers are highlighted in red.

Last factorization through:  Found 2 factors in 0.006 seconds.

Factorization result:

RSA Demonstration

☒ RSA using the private and public key -- or using only the public key  
☐ Choose two prime numbers p and q. The composite number  $N = pq$  is the public RSA modulus, and  $\phi(N) = (p-1)(q-1)$  is the Euler totient. The public key e is freely chosen but must be coprime to the totient. The private key d is then calculated such that  $d = e^{-1} \pmod{\phi(N)}$ .  
☐ For data encryption or certificate verification, you will only need the public RSA parameters: the modulus N and the public key e.

Prime number entry

Prime number p

Prime number q

RSA parameters

RSA modulus N (public)

$\phi(N) = (p-1)(q-1)$  (secret)

Public key e

Private key d

RSA encryption using e / decryption using d [alphabet size: 256]

Input as ☒ text ☐ numbers

Input text


The Input text will be separated into segments of Size 1 (the symbol '#' is used as separator).

Numbers input in base 10 format.

Decryption into plaintext  $m[i] = c[i]^d \pmod{N}$

# RSA: Имитация атаки на гибридную криптосистему

Current Status of Trudy



Action log:

- Trudy has intercepted the message Alice sent to Bob
- Trudy has isolated the encrypted session key from the message
- Trudy has created 130 modified session keys up to now
- 73 of 130 modified messages were successfully decrypted by Bob's server

Intercepted, encrypted session key:

C86EFB5762714227095E5B891320F658990C9545F344006B3D0D6C9E890CAF9F7A0F0F8EC6A96DAB897E11

Modified and encrypted session keys:

Modified and encrypted session key (hexadecimal):

B58F030548815C32E88C71D6FD0749B2846FB96FA5C8C76D4BCD1A38B423464AF8B5ED1E92A79E814  
AA5F8003DFD34E541CD15B813C498D35A917137DCB3732C8882845F181B8CB3DF4684BFB91FF68292  
FD098F5106B06E0B54039F8D4F442FFA1F60FD69500A466B606FFF436891B02E992A86349D62B7391AC  
A05721EC44DC51D72710222A1E0B419C07D0D74E9EDEC4EA2CE772A77C211A21E66E9EACEEA4C42E01

Decrypted session key (calculated by Trudy, based on Bob's responses):

6242D7BD5A18CBB170085A5EF9649DE3

Message (calculated by Trudy using the decrypted session key):

Starting example for the CrypTool version family 1.x (CT1)

Remark:  
The successor versions of CT1 (called CT2, JCT and CTO) now offer a significantly wider range of functionality than CT1. In CT1 only errors will be corrected. Please use the newer versions of CrypTool little by

OK

# Заключение

- Был исследован протокол согласования ключей Диффи-Хеллмана и рассмотрена атака посредником в случае нарушения протокола. На обеих сторонах были получены одинаковые симметричные ключи.
- Был исследован алгоритм асимметричного шифрования RSA, в результате была получена схема.
- Исследован протокол асимметричного шифрования RSA, была выполнена модификация шаблонной схемы, в результате получена схема для передачи ключа и для атаки посредника.
- Были рассмотрены атака на короткое сообщение и атака факторизацией модуля на RSA.
- Была проведена имитация атаки по побочному каналу на гибридную криптосистему