

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

Лабораторная работа № 7

Изучение ассиметричных протоколов и шифров

Студент: _____

Чернякова Валерия, группа 1304

Руководитель: _____

Племянников А.К., доцент каф. ИБ

Санкт-Петербург 2024

Цель работы

Повысить компетенции в работе с асимметричными протоколами и шифрами.

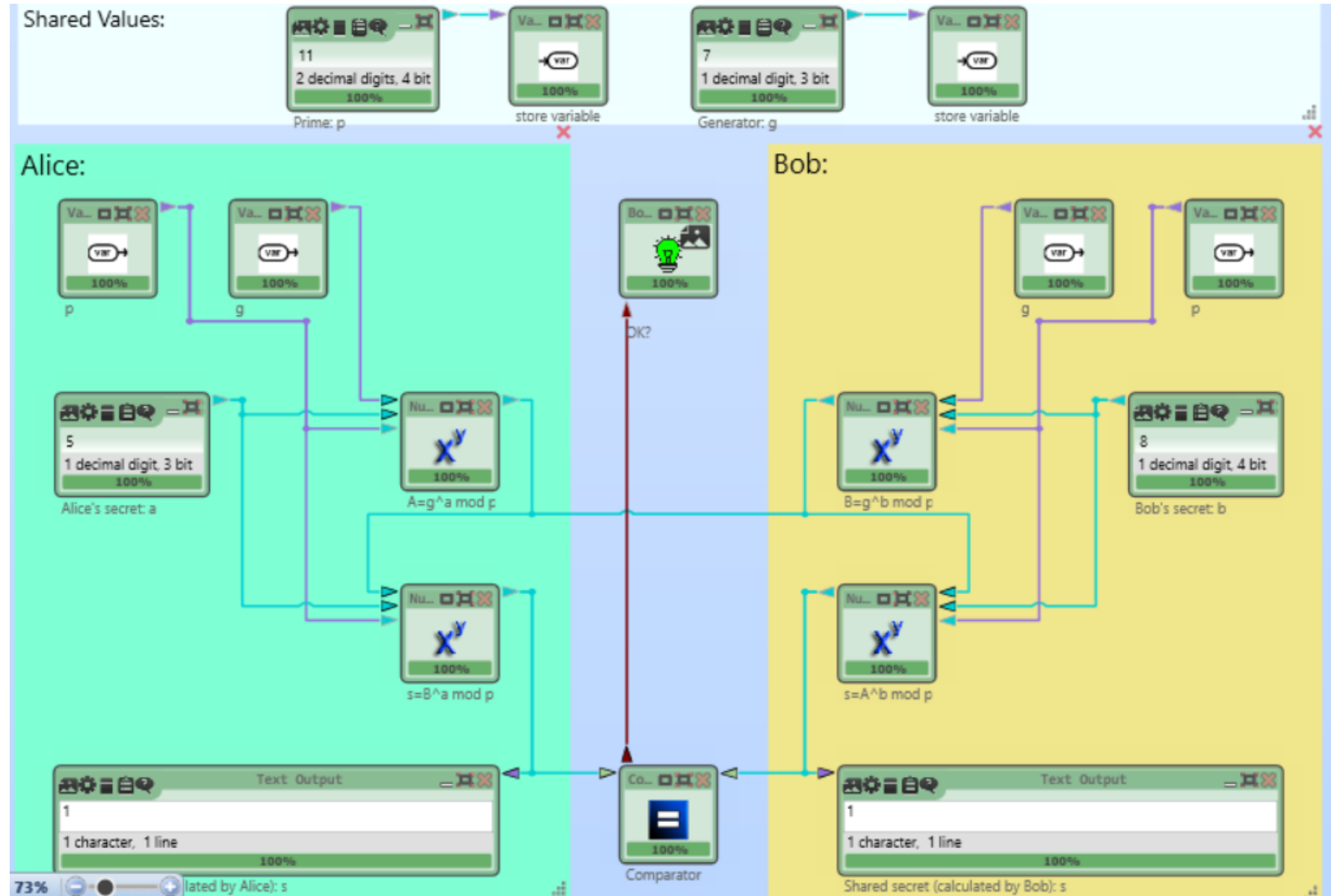
Задачи:

- Изучить протокол согласования ключей Diffie-Hellman Key Exchange и атаку на него "посредником";
- Изучить алгоритм и протокол асимметричного шифрования RSA и атаки методом "малого сообщения" и "посредником";
- Выполнить атаку на шифр RSA факторизацией модуля;
- Выполнить имитацию атаки на гибридную систему шифрования.

Задание

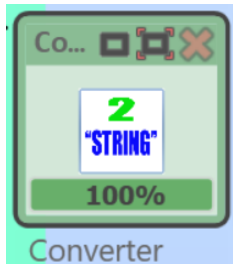
1. Изучить протокол согласования ключей по шаблонной схеме Diffie-Hellman Key Exchange из CrypTool 2 .
2. Выполнить модификацию схемы для преобразования полученного ключевого материала в симметричный ключ длиной 256 бит.
3. В отчет включить скриншот шаблонной схемы и схему, иллюстрирующую атаку протокола " посредником" для случая, когда только одна уполномоченная сторона создает параметры открытого ключа.

Протокол согласования ключей по шаблонной схеме Diffie-Hellman Key Exchange

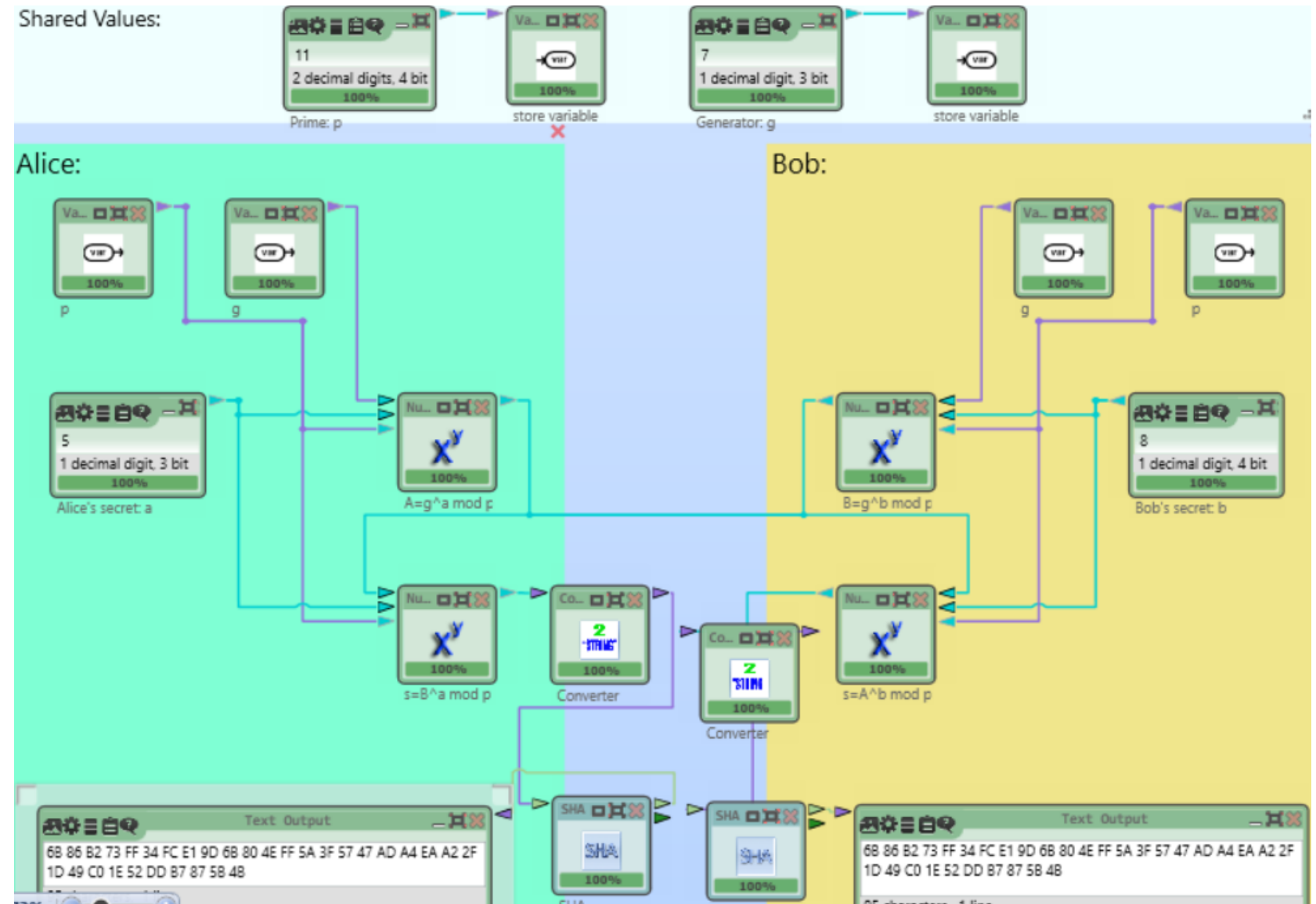
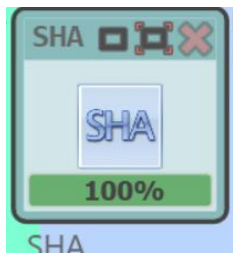


Протокол согласования ключей по шаблонной схеме Diffie-Hellman Key Exchange. Преобразование ключа в симметричный ключ длиной 256 бит

Преобразование данных для дальнейшего использования в блоке SHA-256

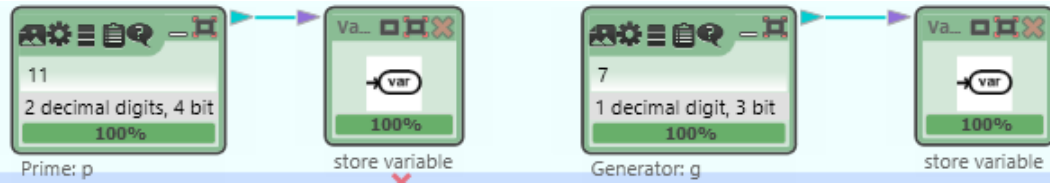


Получение симметричного ключа длиной 256 бит.

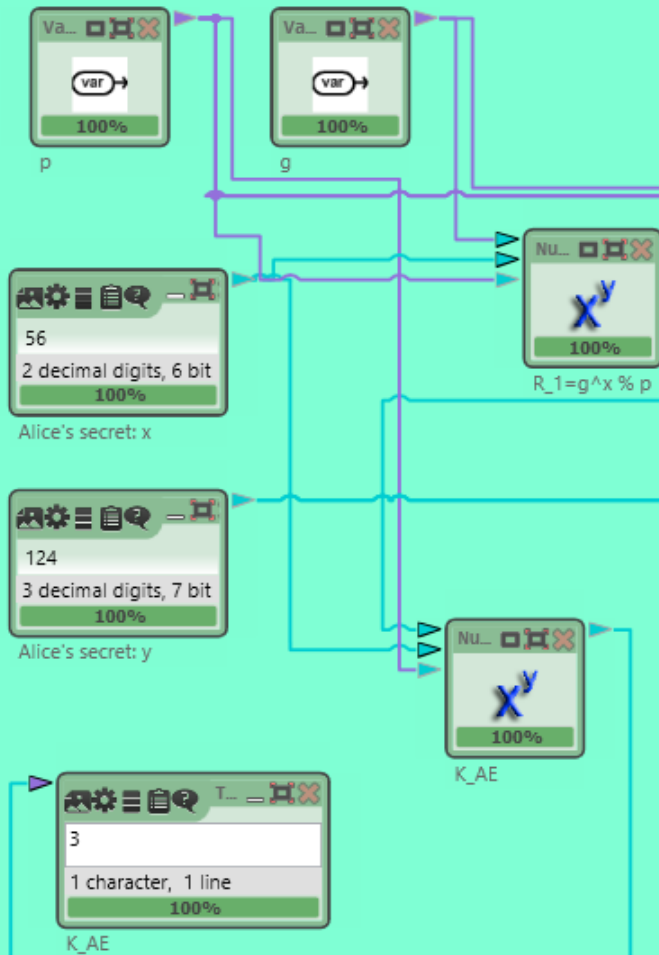


Diffie-Hellman Key Exchange. Атака посредника (man in the middle)

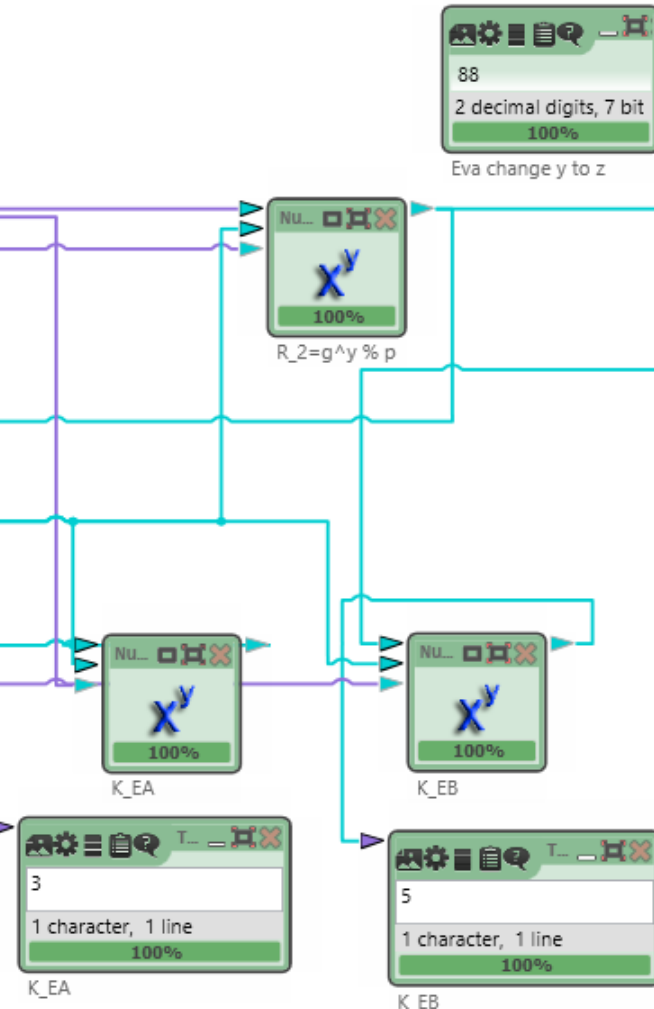
Shared Values:



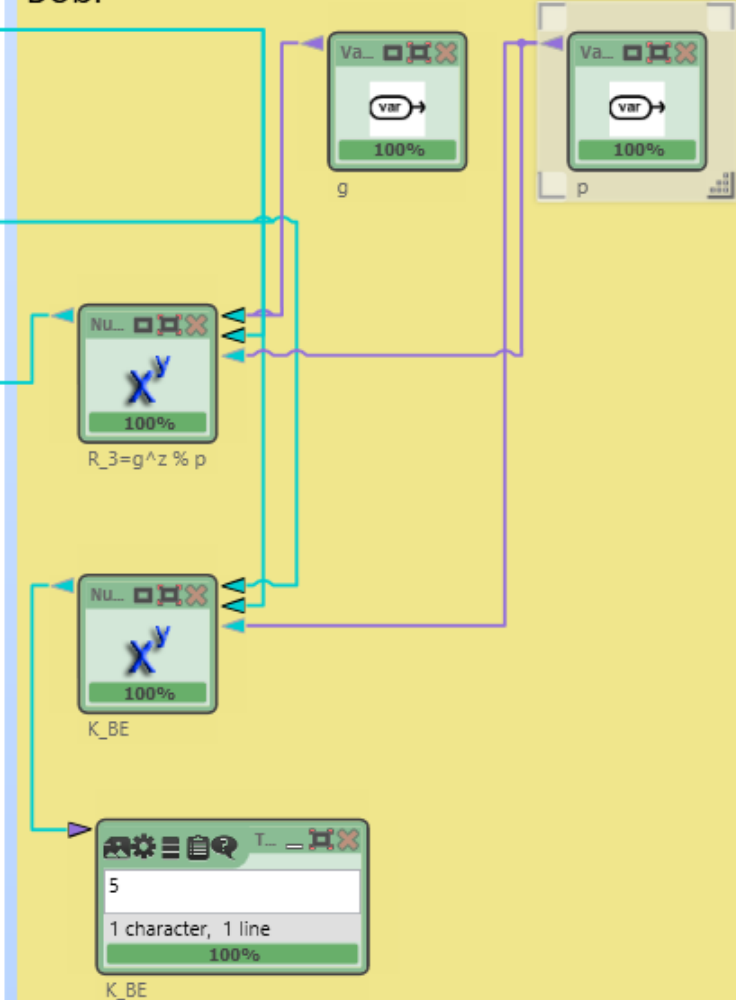
Alice:



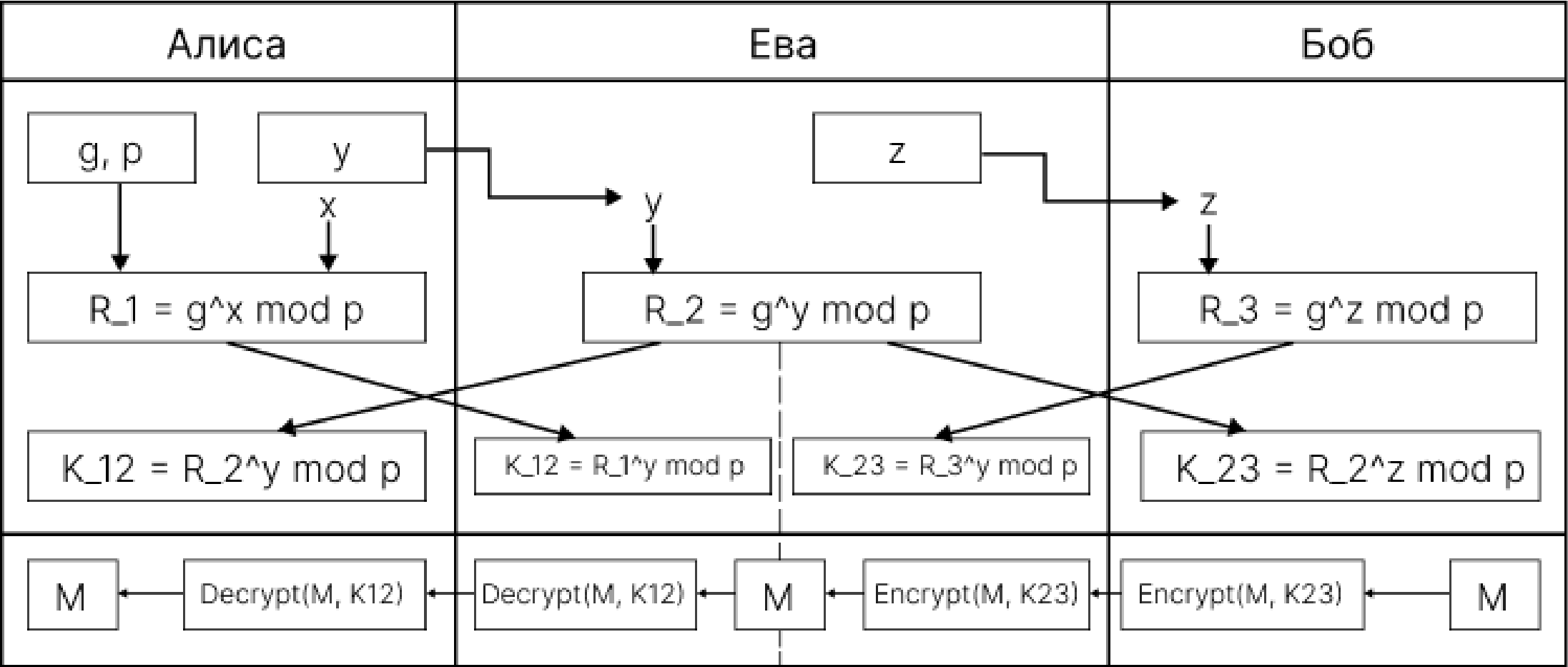
Eva:



Bob:



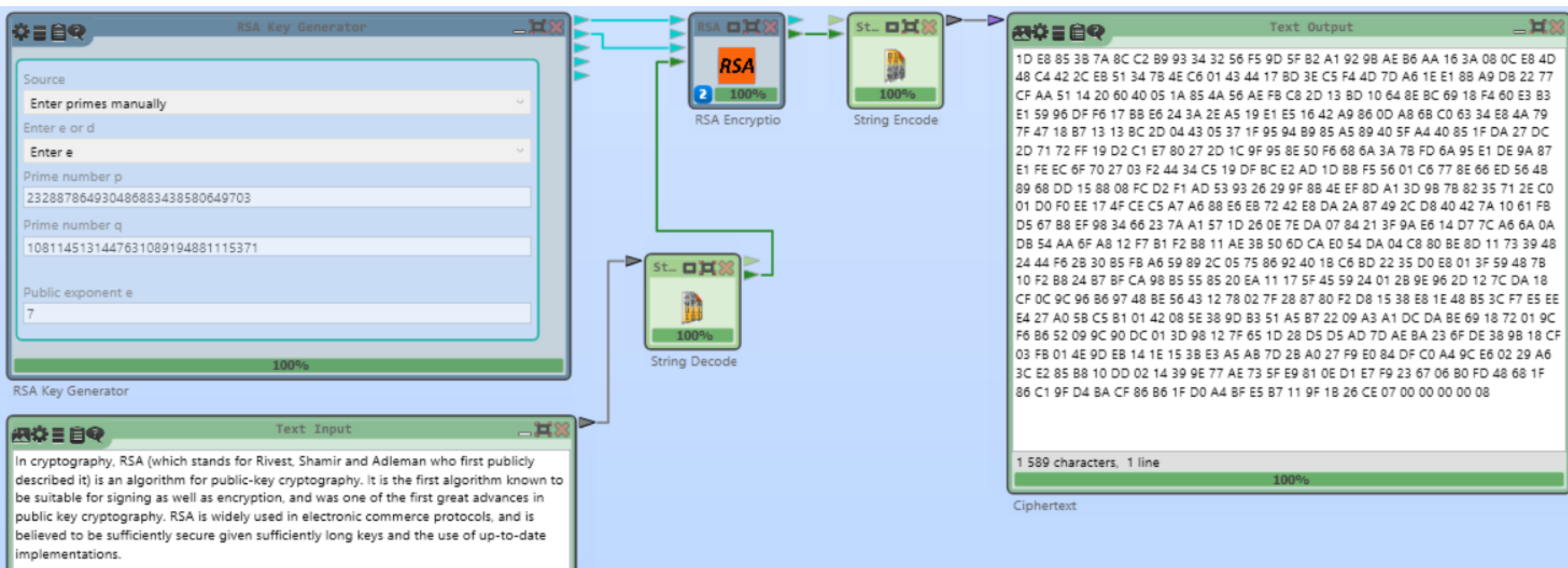
Diffie-Hellman Key Exchange. Атака посредника (main in the middle). Схема



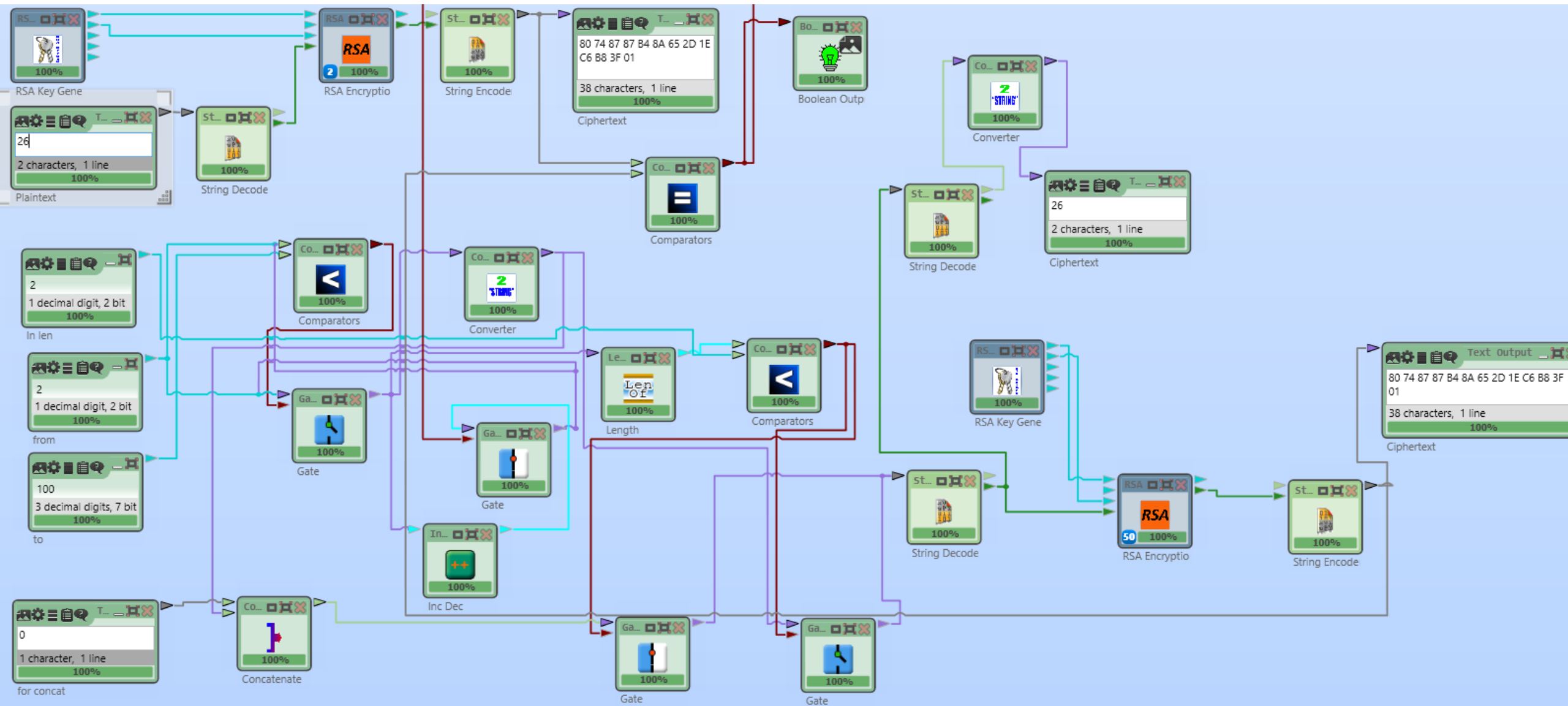
Задание

1. Изучить алгоритм асимметричного шифрования RSA по шаблонной схеме RSA Encryption из CrypTool 2.
2. Изменить эту шаблонную схему для проведение атаки коротким сообщением. В качестве сообщения использовать две последние цифры студенческого билета.
3. В отчет включить скриншот шаблонной схемы и схему алгоритма атаки шифровки методом "малого сообщения"

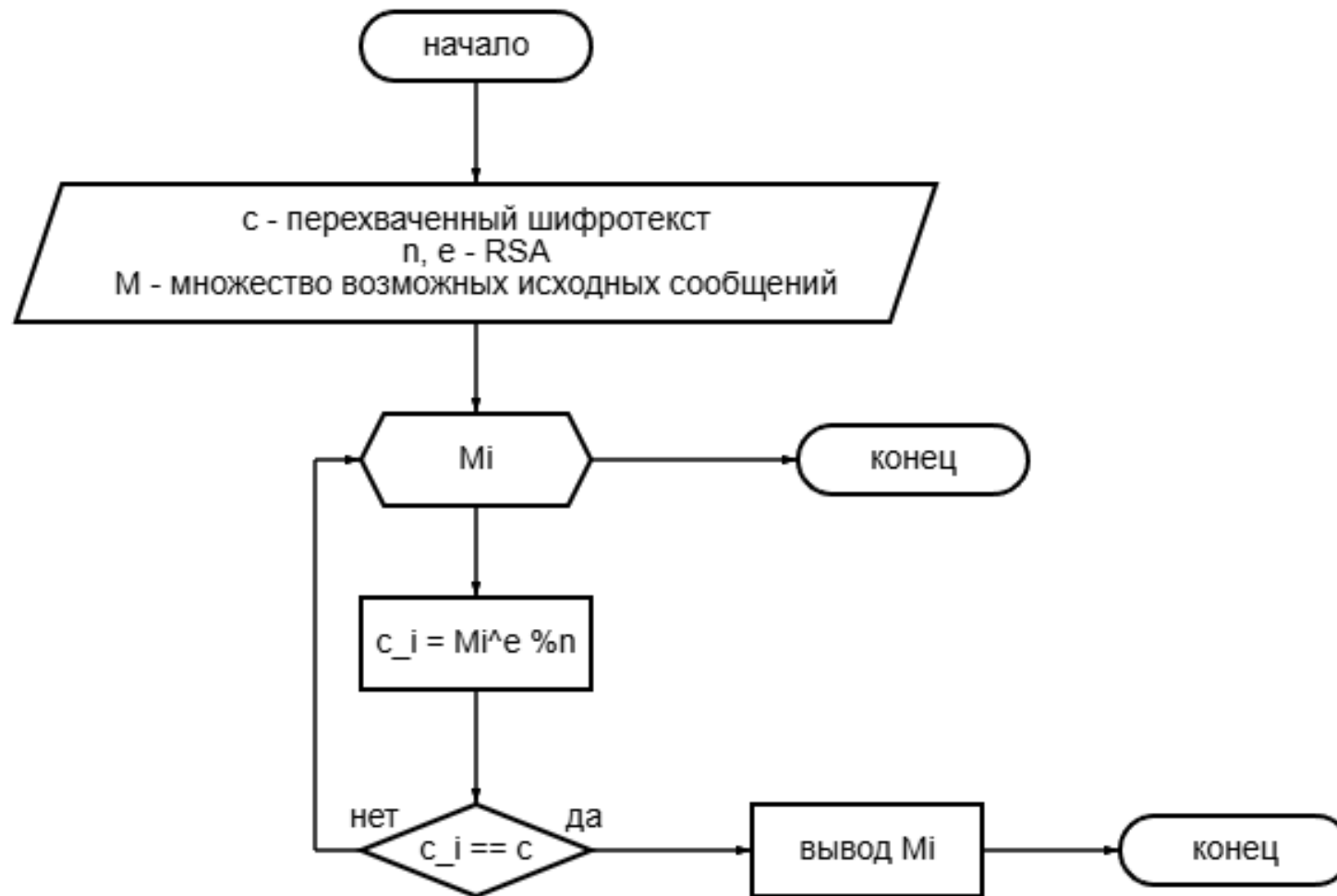
Алгоритм асимметричного шифрования RSA



RSA. Атака «коротким сообщением»



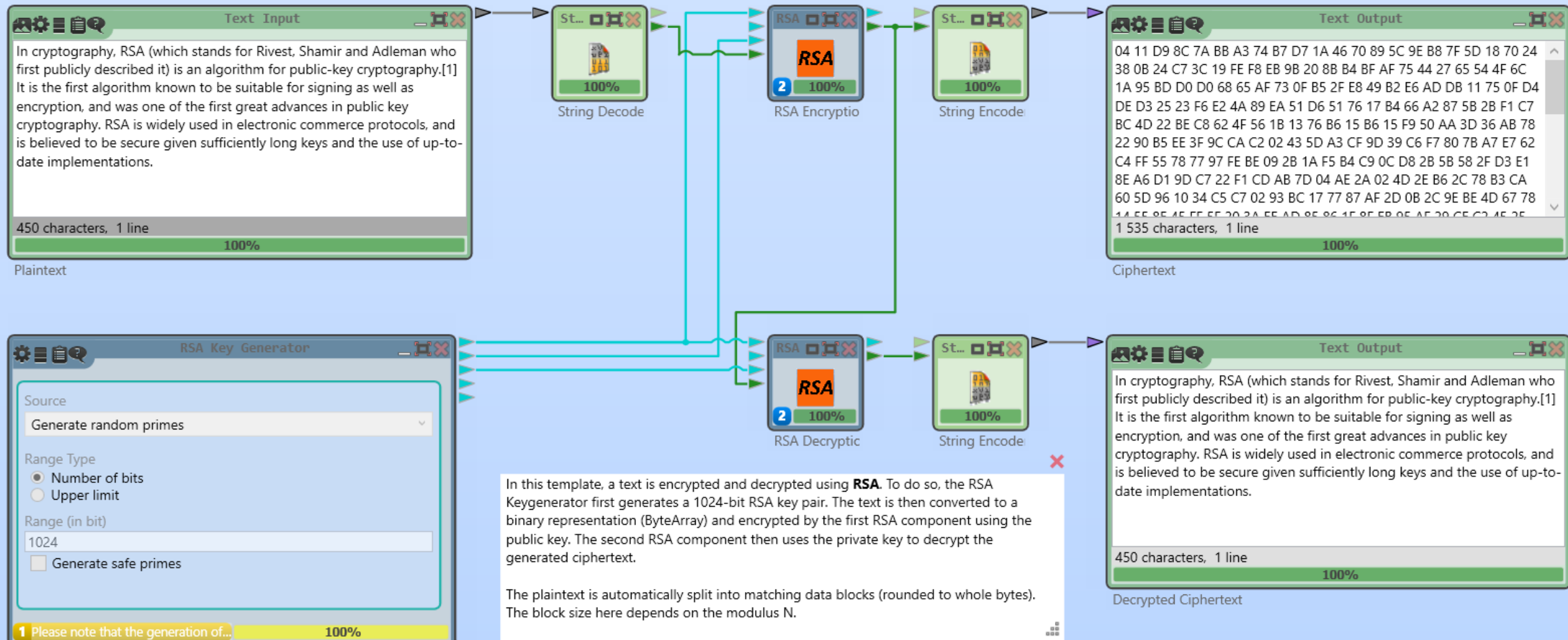
RSA. Атака «коротким сообщением». Схема



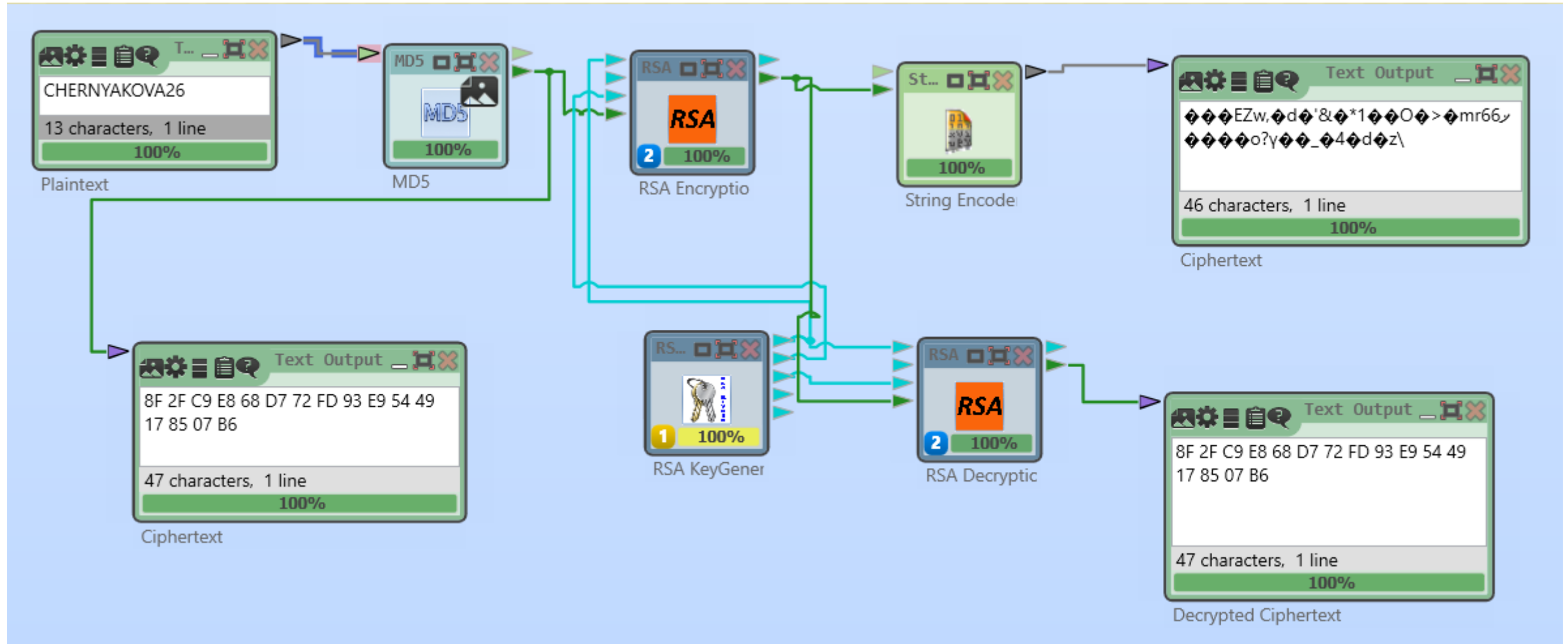
Задание

1. Изучить протокол асимметричного шифрования RSA по шаблонной схеме RSA Cipher из CrypTool 2.
2. Изменить эту шаблонную схему для зашифрования и расшифрования симметричного ключа размером 128 бит, полученного из парольной фразы. В качестве парольной фразы использовать Фамилию и две последние цифры студенческого билета.
3. В отчет включить скриншот шаблонной схемы и схему, иллюстрирующую атаку протокола "посредником".

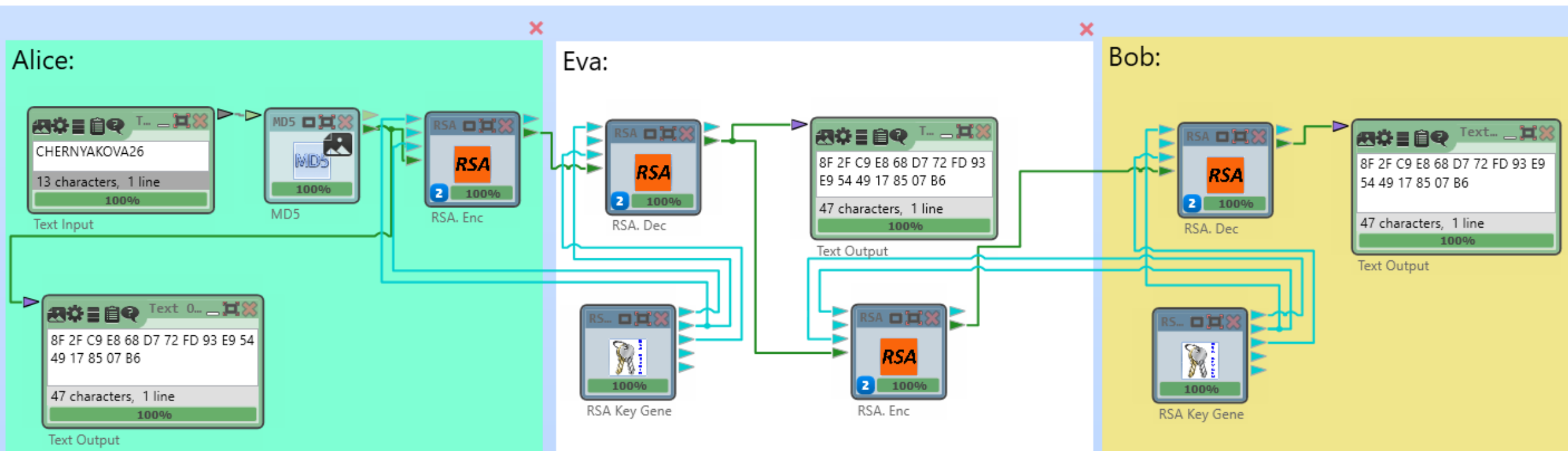
Протокол асимметричного шифрования RSA



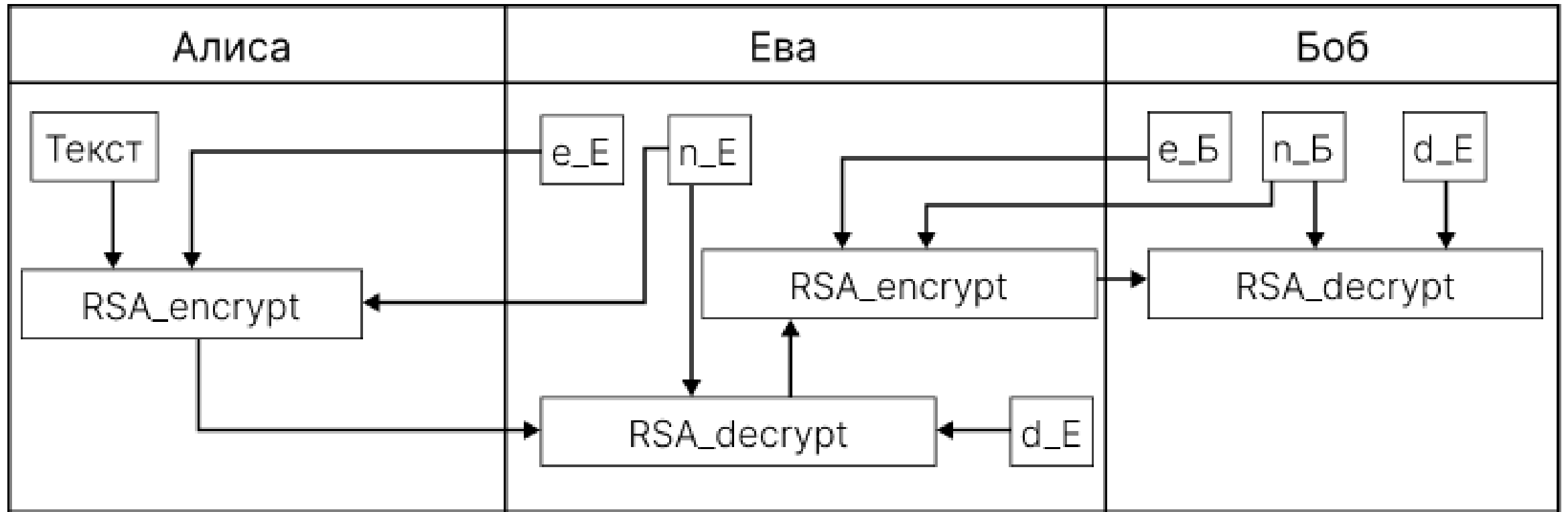
Зашифрование и расшифрование симметричного ключа размером 128 бит, полученного из парольной фразы



RSA. Атака посредника (main in the middle)



RSA. Атака посредника (main in the middle). Схема



Задание

1. Выполнить атаку на шифр RSA факторизацией модуля, используя CrypTool 1
2. Запустить утилиту `Indiv.Procedures` → `RSACryptosystem` → `RSA Demonstration`.
3. Установить переключатель в режим «Choose two prime...».
4. Выбрать параметры p и q так, чтобы $n = pq > 256$.
5. Задать открытый ключ e .
6. Зашифровать произвольное сообщение и передать его вместе с открытым ключом (n, e) коллеге. В ответ получить аналогичные данные.
7. Запустить утилиту `Indiv.Procedures` → `RSACryptosystem` → `RSADemonstration` и установить переключатель в режим «For data encryption...».
8. Выполнить факторизацию модуля n командой `Factorize...`

RSA. Атака факторизацией модуля

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	<input type="text" value="173"/>	<input type="button" value="Generate prime numbers..."/>
Prime number q	<input type="text" value="181"/>	

RSA parameters

RSA modulus N	<input type="text" value="31313"/>	(public)
$\phi(N) = (p-1)(q-1)$	<input type="text" value="30960"/>	(secret)
Public key e	<input type="text" value="2^16+1"/>	<input type="button" value="Update parameters"/>
Private key d	<input type="text" value="23633"/>	

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.

Encryption into ciphertext $c[i] = m[i]^e \pmod{N}$

Encrypt
Decrypt
Close

Factorization of a Number

Algorithms for factorization

☒ Brute-force

☒ Brent

☒ Pollard

☒ Williams

☒ Lenstra

☒ Quadratic sieve

Input

Enter the number to be factorized:

31313

Load number from file

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.

Continue

Complete factorization into primes

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: Brute Force Found 2 factors in 0.003 seconds.

Factorization result:

173 * 181

Details

Close

Задание

1. Изучить и выполнить имитацию атаки на гибридную систему шифрования , используя CrypTool 1
2. Подготовить текст передаваемого сообщения на английском с вашим именем в конце.
3. Запустить утилиту Analysis → Asymmetric Encr... → Side-Channel attack on «Textbook RSA»...
4. Настроить сервер, указав в качестве ключевого слова ваше имя, используемое в конце текста.
5. Выполнить последовательно все шаги протокола.
6. Сохранить лог-файлы участников протокола для отчета.

Имитация атаки на гибридную систему шифрования

Current Status of Alice



Action log:

- Alice has composed a message for Bob
- Alice chose a random session key
- Alice has encrypted the message symmetrically with
- Alice chose Bob's public RSA key e
- Alice encrypted the session key with Bob's public R

Randomly chosen session key:

50B5BDADFD761EFF768FE9041EC1BBD9

Current Status of Bob



Action log:

- Bob could successfully decrypt the message
- Bob received 1 message up to now

Actually, Bob cannot decide whether the messages he received were sent by Alice or Trudy. To decide, Bob can use a keyword. If he knows a certain keyword, Bob can decide if a message was sent by Alice. Please specify the keyword.

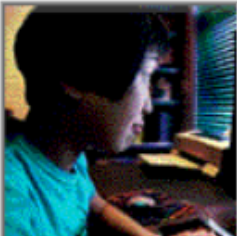
Keyword:

Received session keys and decryption results:

N...	Decryption:	Decrypted session key (hexadecimal):
1	Correct	50B5BDADFD761EFF768FE9041EC1BBD9

Имитация атаки на гибридную систему шифрования

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
- 60 of 130 modified messages were successfully decrypted by Bob's server

Intercepted, encrypted session key:

E6A148EC677D2BFB059BEDDEBEF9A154DAF5558F86B9A6BBD A07AFA2D6B3D50A90E03236A99A87973E

Modified and encrypted session keys:

Modified and encrypted session key (hexadecimal):

1356D05AA9E6A2364999E067E35651316BF0FC38EC326275EF75A647781B59452FF26BC6B90D5BE7...
D5C03FFB611EA382D5B2185698F474CDC5820636B1C111DDFA3B4FDC91FE31BBA2D6434C6430032...
FD3E2C92F4E1B02C383D29B245BE9AC29EF2131E550EAB96B9478DB80192BF6F235B29D1EDE5738...
1F5A439BFF74F66CE37CD7CB81CCD2410C673653287DF872FEB78563A4C438BBB7E319D328CFB09...
418C374529FCC33F30558D76C87B89FCC4783DA057F7C349434D41B6FF220C5930432B5947A770F0

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

50B5BDADFD761EFF768FE9041EC1BBD9

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

In cryptography, RSA (which stands for Rivest, Shamir and Adleman who first publicly described it) is an algorithm for public-key cryptography. It is the first algorithm known to be suitable for signing as well as encryption, and was one of the first great advances in public key cryptography. RSA is widely used in electronic commerce protocols, and is believed to be sufficiently secure given sufficiently long keys and the use of up-to-date implementations.

Имитация атаки на гибридную систему шифрования

I. PREPARATIONS

Alice composes a message M, addressed to Bob.

Alice chooses a random session key S:
50B5BDADFD761EFF768FE9041EC1BBD9

Alice symmetrically encrypts the message M with the session key S.

Alice chooses Bob's public key e:
010001

Alice asymmetrically encrypts the session key S with Bob's public RSA key e:
E6A148EC677D2BFB059BEDDEBEF9A154DFAF5558F86B9A6BBDA07AFA2D6B3D50A90E03236A99A8797366C90027A1EF379EF81
B4434755CFAD6ECEAEE6853700B

II. MESSAGE TRANSMISSION

Alice sends the hybrid encrypted file to Bob over an insecure channel.

III. MESSAGE INTERCEPTION

Trudy intercepts the hybrid encrypted file and isolates the encrypted session key S:
E6A148EC677D2BFB059BEDDEBEF9A154DFAF5558F86B9A6BBDA07AFA2D6B3D50A90E03236A99A8797366C90027A1EF379EF81
B4434755CFAD6ECEAEE6853700B

IV. BEGINNING OF THE ATTACK CYCLE

She sends an exact copy of the original, encrypted message to Bob and extends it with the session key S' (encrypted with Bob's public key). Compared to the message sent by Alice, Trudy simply replaces the encrypted session key [ENC(S, PubKeyBob) is replaced by ENC(S', PubKeyBob)].
Trudy repeats this step 130 times, whereas the step count depends on the bit length of the used session key (step count = bit length + 2).

Заключение

- Исследован протокол согласования ключей Диффи-Хеллмана. Рассмотрена и проведена атака протокола "посредником" для случая, когда только одна уполномоченная сторона создает параметры открытого ключа. Были получены одинаковые значения ключа для стороны отправителя и посредника, а также посредника и получателя.
- Исследован алгоритм ассиметричного шифрования RSA. Средствами CrypTool2 была составлена схема атаки коротким сообщением. Атака успешно сработала, были найдены верные значения исходного Plaintext и его модификации Ciphertext.
- Исследован протокол ассиметричного шифрования RSA. Средствами CrypTool2 была составлена схема атаки протокола «посредником». Атака успешно сработала, значение зашифрованного текста, наданного посредником, совпала с тем, что было у получателя.
- Изучена атака факторизацией модуля на шифр RSA. Она заключается в разложении модуля n на простые множители p и q , что позволяет вычислить приватный ключ и взломать шифр.
- Была проведена атака на гибридную систему, основанная на том, что злоумышленник перехватывает цифровой конверт с зашифрованным сообщением и зашифрованным секретным ключом. Модифицируя полученные данные и анализируя ответы сервера, можно побитово восстановить целиком секретный ключ.