

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

Лабораторная работа № 7

Изучение и исследование алгоритмов и протоколов
асимметричного шифрования

Студентка:

Усачева Дарья, группа 1384

Руководитель:

Племянников А.К., доцент каф. ИБ

Санкт-Петербург, 2024

Цель работы и задачи

Цель: Повысить свою компетенцию в области алгоритмов и протоколов асимметричного шифрования и в криптографии в целом.

Задачи:

1. Изучить протокол согласования ключей Диффи-Хеллмана.
2. Изучить алгоритм асимметричного шифрования RSA.
3. Изучить протокол асимметричного шифрования RSA.
4. Выполнить атаку на шифр RSA факторизацией модуля.
5. Изучить и выполнить имитацию атаки на гибридный протокол шифрования.

Изучение протокола согласования ключей Диффи-Хеллмана

Изучение протокола согласования ключей Диффи-Хеллмана

Цель протокола – обеспечить двум пользователям возможность получения симметричного секретного ключа путем обмена данными по незащищенному каналу связи. Протокол Диффи-Хеллмана состоит из следующих операций:

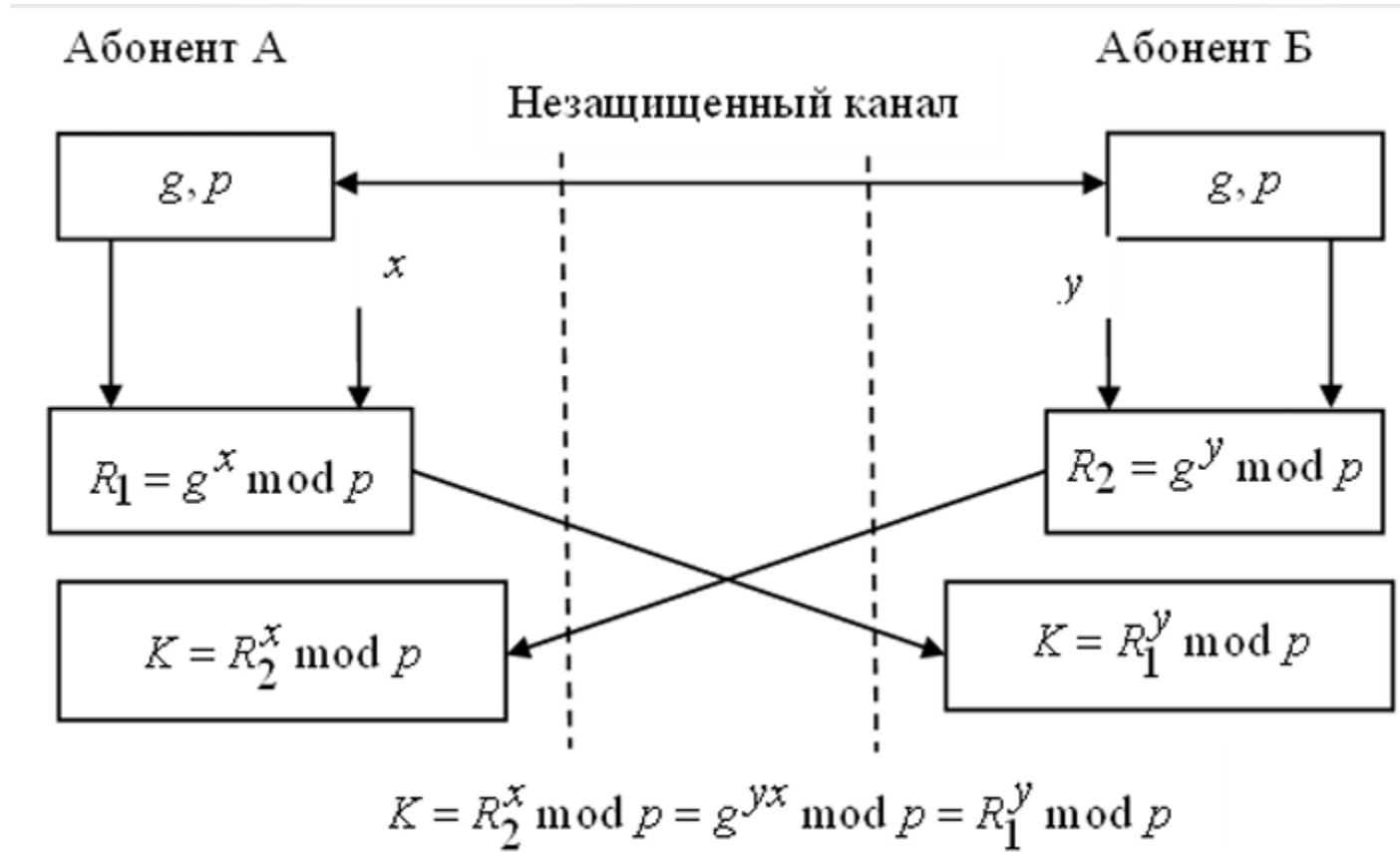
1. Устанавливаются открытые параметры p , g :
 - а) p – большое простое число порядка 300 десятичных цифр (1024 бит);
 - б) g – первообразный корень (генератор) по модулю p .
2. Каждая из сторон генерирует закрытый ключ – большое число x и y соответственно.
3. На каждой стороне вычисляется открытый ключ:

$$\begin{aligned}R_1 &= g^x \bmod p \\ R_2 &= g^y \bmod p\end{aligned}$$

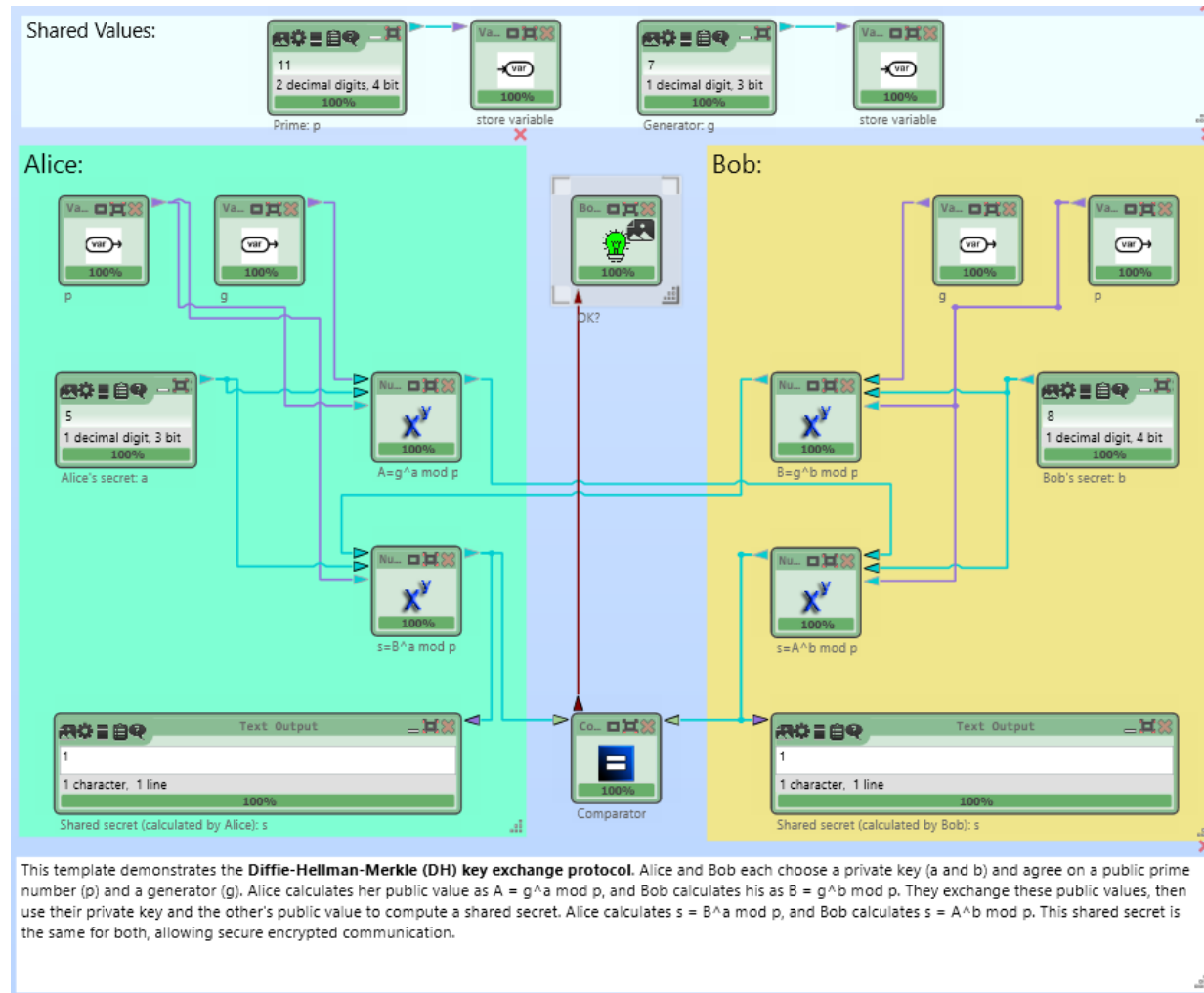
Стороны обмениваются открытыми ключами и вычисляют общие данные K для создания симметричного ключа:

$$K = R_2^x \bmod p = R_1^y \bmod p = g^{xy} \bmod p$$

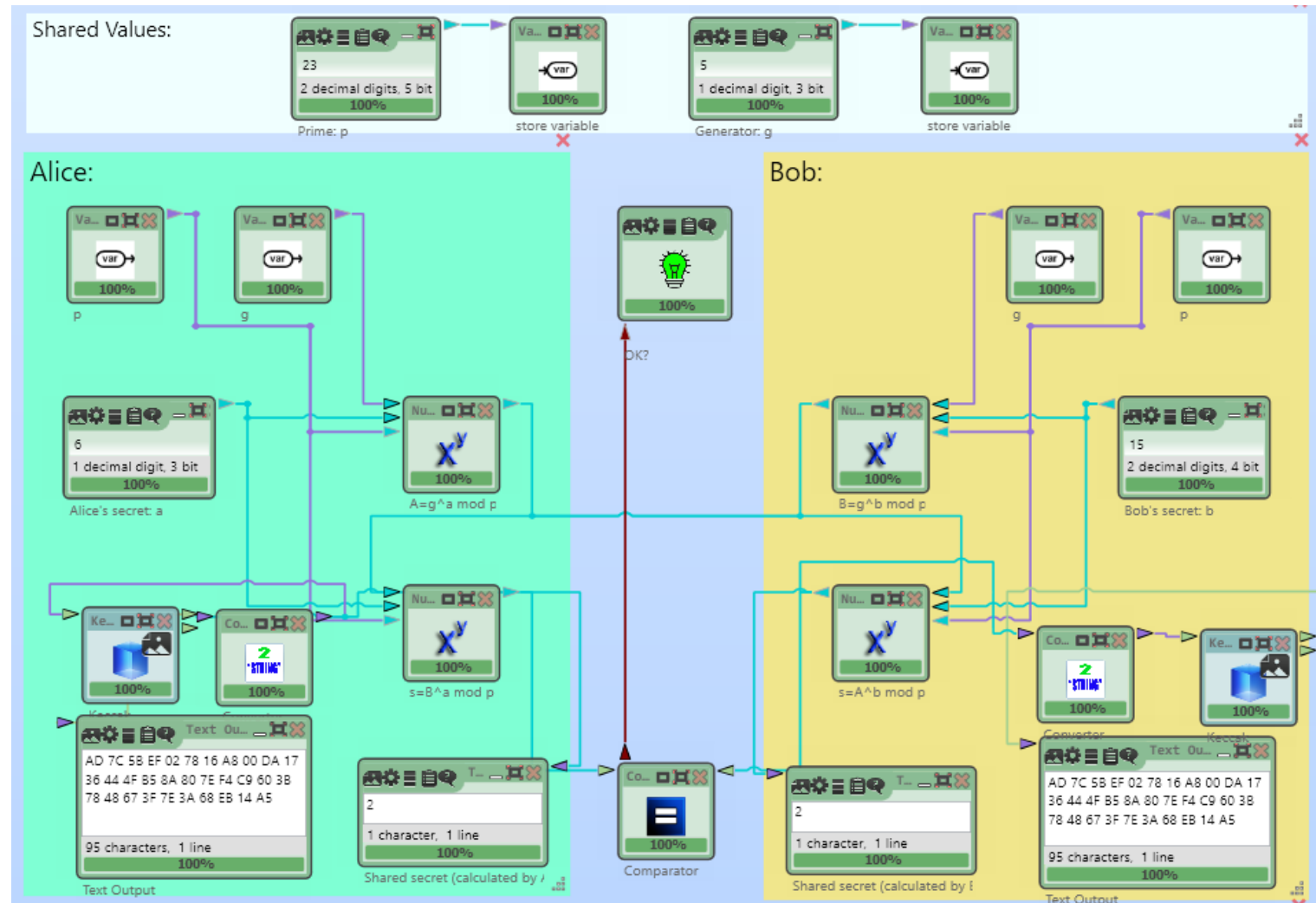
Схема протокола согласования ключа Диффи-Хеллмана



Шаблонная схема Diffie-Hellman Key Exchange из CrypTool 2

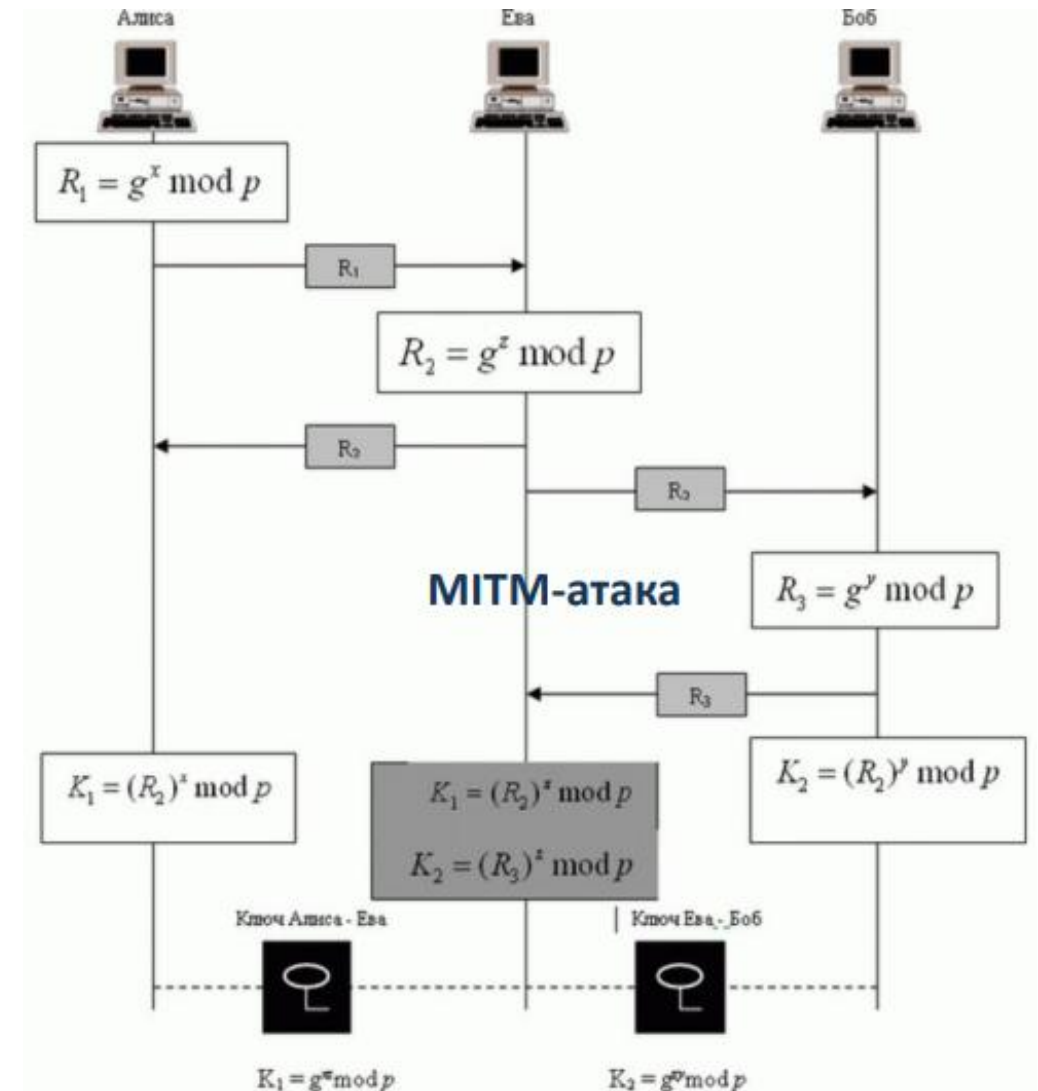


Шаблонная схема Diffie-Hellman Key Exchange из CrypTool 2



Схема, иллюстрирующая атаку протокола "посредником"

- Предполагается, что противник может осуществить активную атаку, т.е. имеет возможность не только перехватывать сообщения, но и заменять их другими.
- Противник может перехватить открытые ключи участников R_1 и R_3 и создать свою пару открытого и закрытого числа (R_2, z) , чтобы послать их каждому из абонентов.
- После этого каждый абонент вычислит ключ, который будет общим с противником, а не с другим участником.
- Если нет контроля подлинности сторон, то законные абоненты не смогут обнаружить подобную подмену.



Изучение алгоритма асимметричного шифрования RSA

Шаблонная схема алгоритма RSA из CrypTool 2

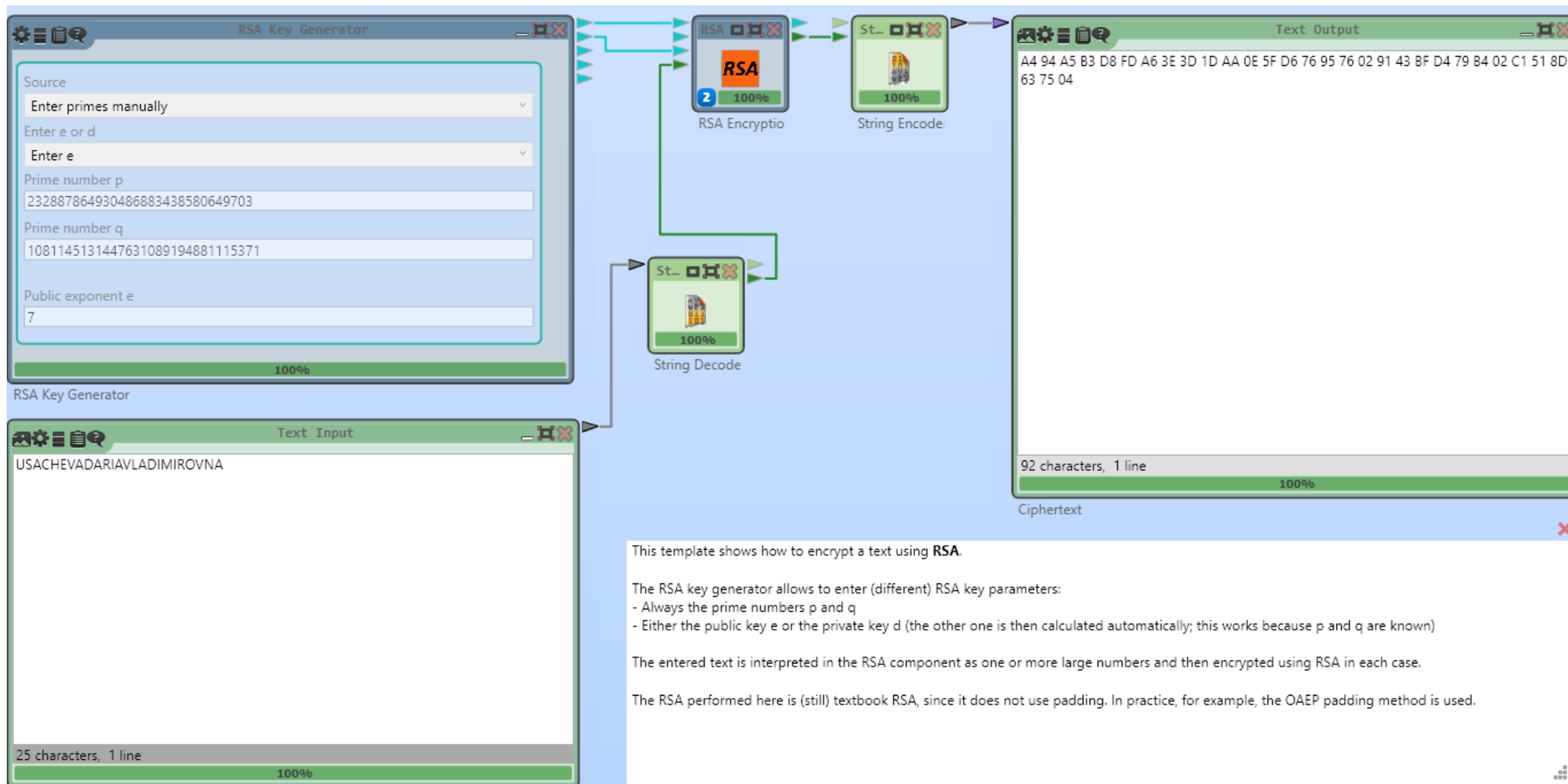
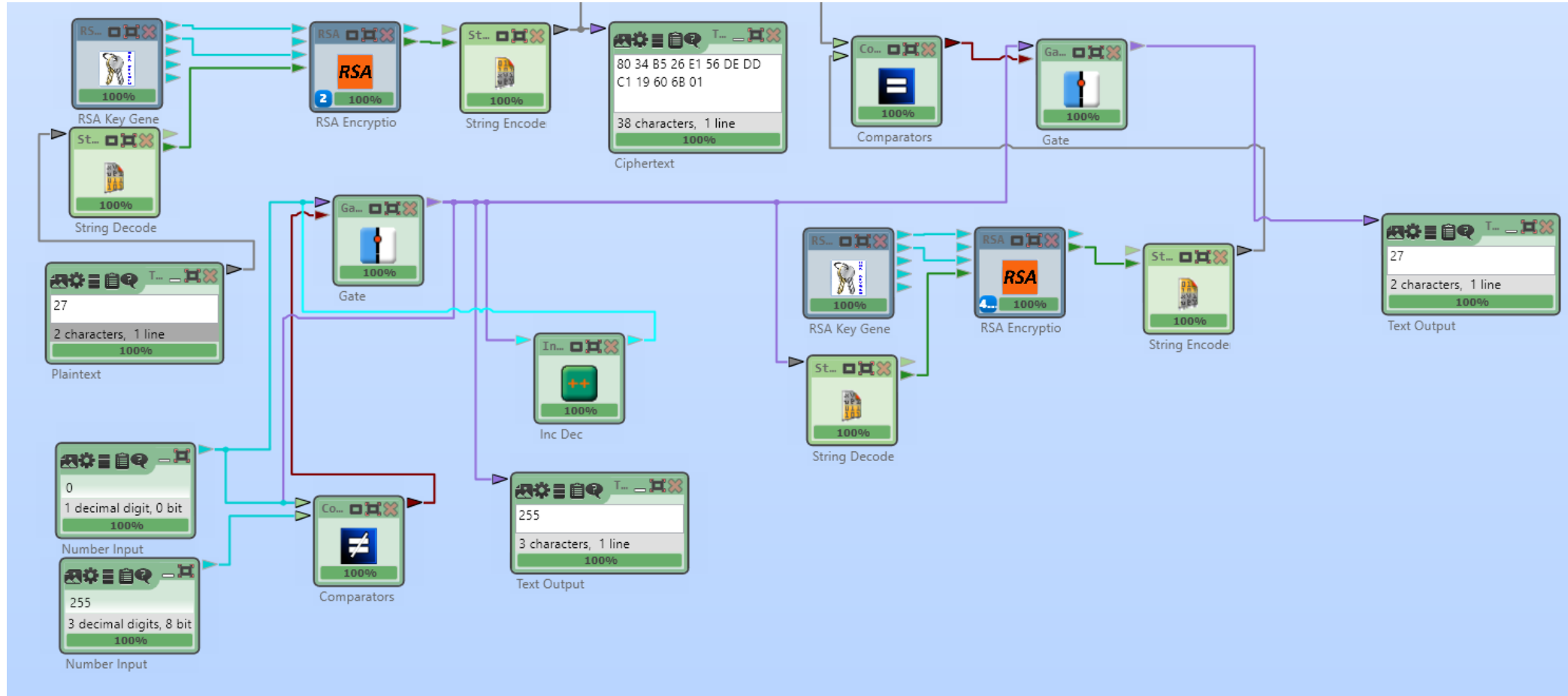


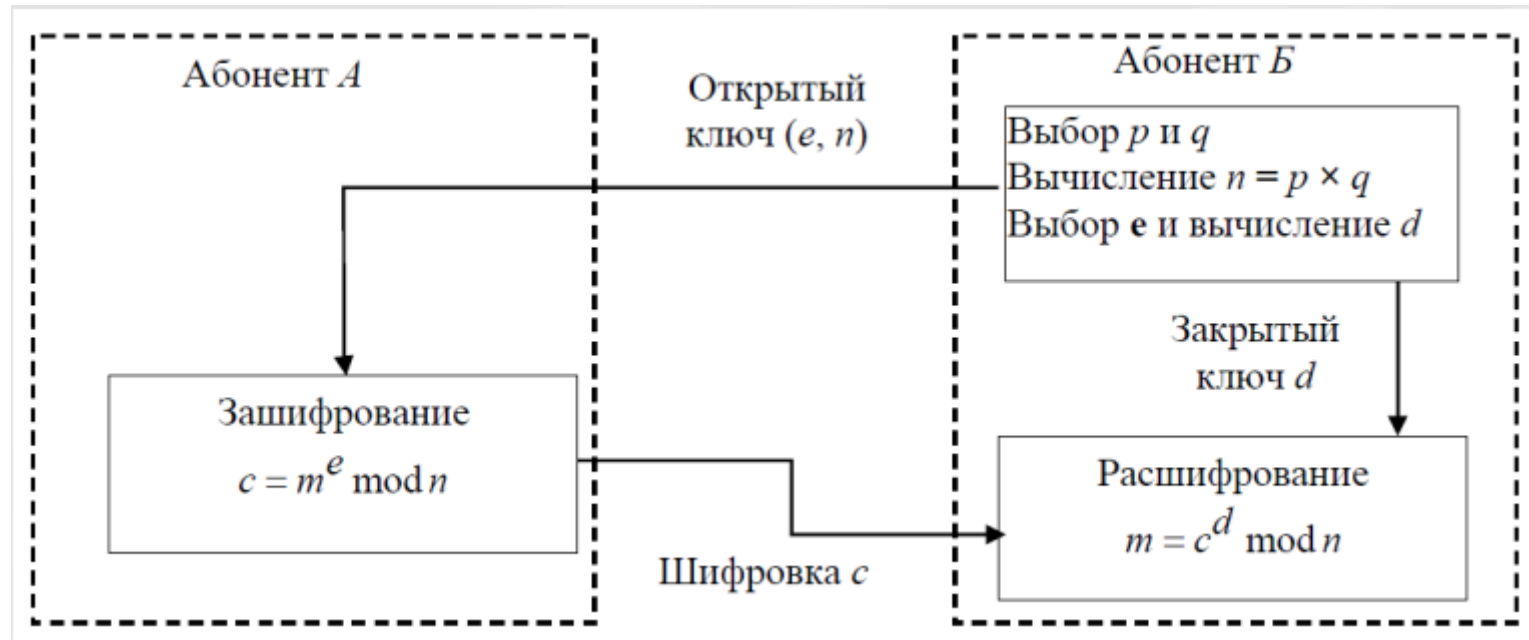
Схема алгоритма атаки шифровки методом "малого сообщения"



Изучение протокола асимметричного шифрования RSA

Протокол шифрования на основе RSA

- Секретный и открытый ключи RSA равноправны - каждый из ключей (d или e) может использоваться как для зашифрования, так и для расшифрования
- Совпадающие блоки зашифровываются одинаково (как в режиме электронной кодовой книги)



Шаблонная схема RSA Cipher из CrypTool2

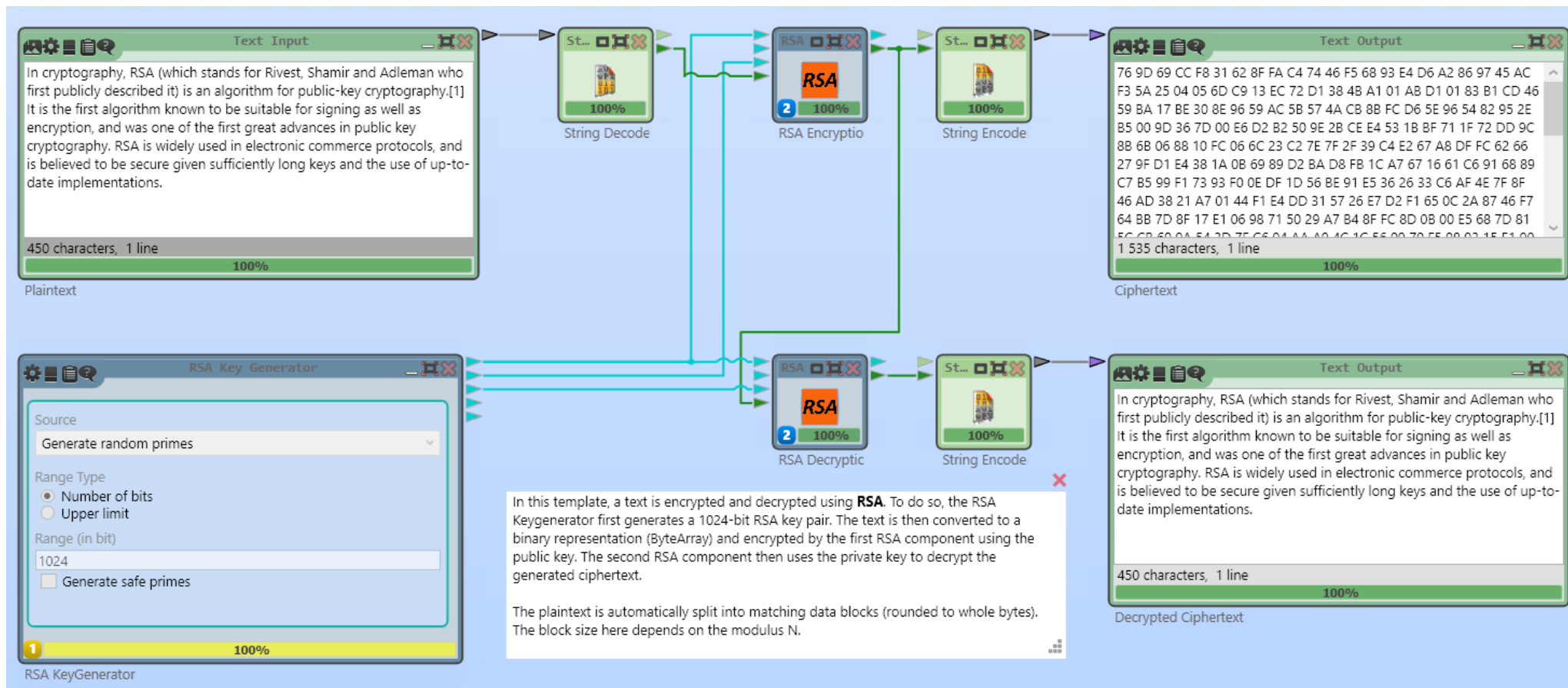
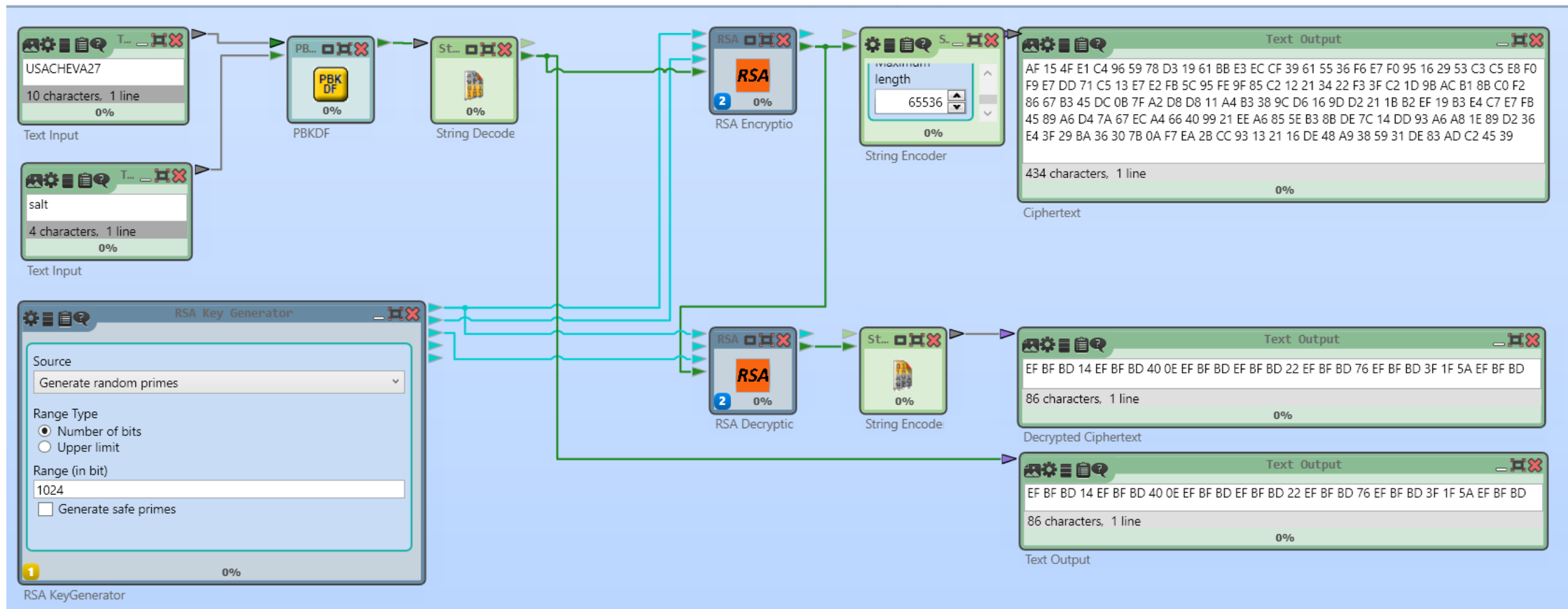
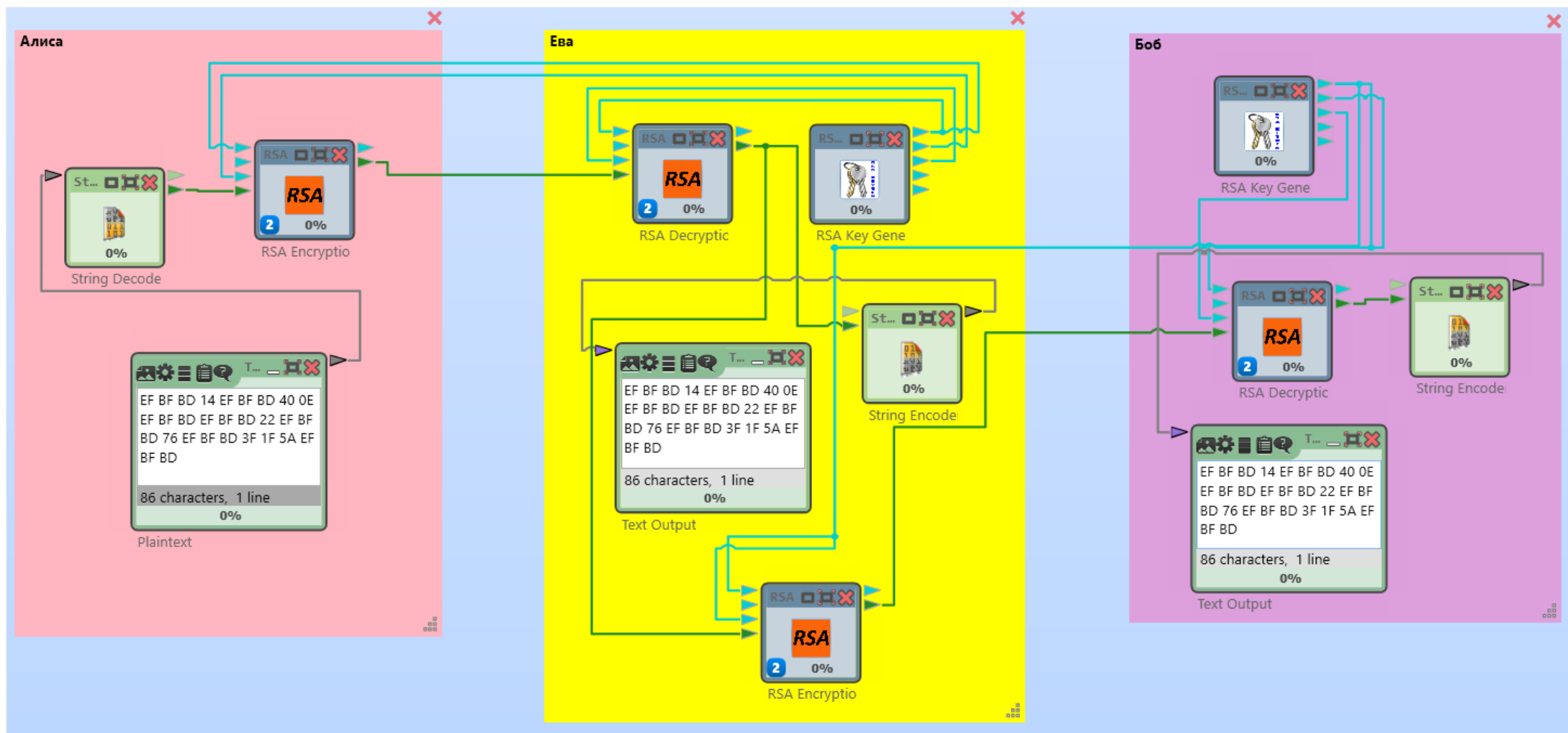


Схема для зашифрования и расшифрования симметричного ключа размером 128 бит, полученного из парольной фразы



Схема, иллюстрирующая атаку протокола "посредником"



Выполнение атаки на шифр RSA факторизацией модуля

Метод факторизации Ферма

Если найдены x и y такие, что $N = x^2 - y^2$,
то найдено и разложение $N = a \cdot b$, где $a = (x + y)$, $b = (x - y)$.

Пусть у числа N есть два натуральных делителя: $a, b : a \leq b$, тогда меньший из них $a \leq \sqrt{N}$

Тогда ищем $y^2 = x^2 - N$, изменяя значение x :

Вход : нечетное положительное целое N

Выход : положительные целые a и b , такие что $a \cdot b = N$

```
x ← √N                                // наименьшее целое, большее, чем √N
while (x < N) {
    w ← x2 - N
    If (w полный квадрат числа) {
        y ← √w
        a ← x + y
        b ← x - y
        return a, b }
    x ← x + 1 }                        // сложность метода o(√N)
```

Атака на шифр RSA 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: 131

Prime number q: 11

Generate prime numbers...

RSA parameters

RSA modulus N: 1441 (public)

$\phi(N) = (p-1)(q-1)$: 1300 (secret)

Public key e: 27

Private key d: 963

Update parameters

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

Input as: ☒ text ☐ numbers

Alphabet and number system options...

Input text

Dear Friend, I hope this letter finds you well. I wanted to share something that brings me immense joy and warmth

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

D # e # a # r # # F # r # i # e # n # d # , # I # # h # o # p # e # # t # h # i # s # # I # e # t # t # e #

Numbers input in base 10 format.

068 # 101 # 097 # 114 # 032 # 070 # 114 # 105 # 101 # 110 # 100 # 044 # 032 # 073 # 032 # 104 # 111 #

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

0854 # 1129 # 0642 # 0797 # 0032 # 0995 # 0797 # 0437 # 1129 # 0946 # 0254 # 1243 # 0032 # 0435 # 0

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:

1441

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 0.005 seconds.

Factorization result:

11 * 131

Details

Close

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: 131

Prime number q: 11

Generate prime numbers...

RSA parameters

RSA modulus N: 1441 (public)

$\phi(N) = (p-1)(q-1)$: 1300 (secret)

Public key e: 27

Private key d: 963

Update parameters

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

Input as: ☐ text ☒ numbers

Alphabet and number system options...

Ciphertext coded in numbers of base 10

0854 # 1129 # 0642 # 0797 # 0032 # 0995 # 0797 # 0437 # 1129 # 0946 # 0254 # 1243 # 0032 # 0435 # 0

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

0068 # 0101 # 0097 # 0114 # 0032 # 0070 # 0114 # 0105 # 0101 # 0110 # 0100 # 0044 # 0032 # 0073 # 0

Output text from the decryption (into segments of size 1; the symbol '#' is used as separator).

D # e # a # r # # F # r # i # e # n # d # , # I # # h # o # p # e # # t # h # i # s # # I # e # t # t # e #

Plaintext

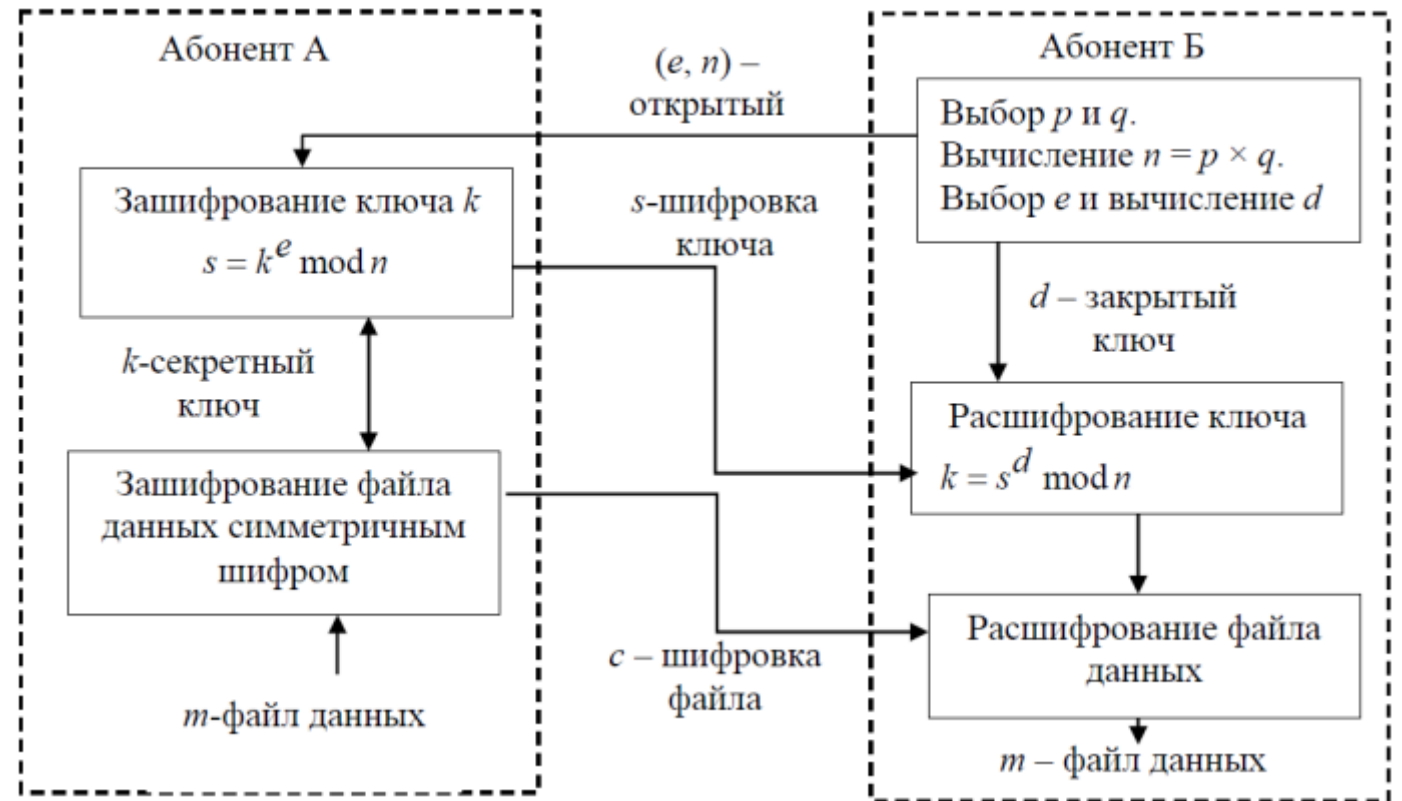
Dear Friend, I hope this letter finds you well. I wanted to share something that brings me immense joy and warmth

Encrypt Decrypt Close

Изучение и выполнение имитации атаки на гибридный протокол шифрования


Пример гибридного шифрования на основе асимметричного шифра

- Файл данных шифруется симметричным секретным ключом
- Секретный ключ шифруется открытым ключом получателя
- Зашифрованное сообщение и зашифрованный ключ составляют цифровой конверт (digital envelope), который отправляется получателю
- Получатель сначала расшифровывает секретный ключ, а затем расшифровывает секретным (сеансовым) ключом шифровку файла данных



Лог файлы участников протокола

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 the session key
- Alice chose Bob's public RSA key e
- Alice encrypted the session key with Bob's public RSA key
- Alice sent the hybrid encrypted file to Bob

Randomly chosen session key:

727E8140D55010025AE1B3990AD7F546

Current Status of Bob



Action log:

- Bob could successfully decrypt 65 of 131 messages
- Bob received 131 messages up to now

Actually, Bob cannot decide whether the messages he received were sent by Alice or Trudy. However, given a certain keyword, Bob can decide if a message was sent by Alice. Please specify the keyword below:


Keyword:

Received session keys and decryption results:

N...	Decryption:	Decrypted session key (hexadecimal):
1	Correct	727E8140D55010025AE1B3990AD7F546
2	Correct	727E8140D55010025AE1B3990AD7F546
3	Correct	727E8140D55010025AE1B3990AD7F546
4	Incorrect	DB4E13D60DD954C85B2E633B64CA330F
5	Incorrect	DB4E13D60DD954C85B2E633B64CA330F
6	Incorrect	DB4E13D60DD954C85B2E633B64CA330F
7	Incorrect	DB4E13D60DD954C85B2E633B64CA330F
8	Correct	727E8140D55010025AE1B3990AD7F546
9	Correct	727E8140D55010025AE1B3990AD7F546
10	Correct	727E8140D55010025AE1B3990AD7F546

OK

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

Intercepted, encrypted session key:

A4118FA96FEF933851302B9F591D6ACD5B82BB5C8B161952F392F96FFC12EAC55ED92AC960A98FBC788E1

Modified and encrypted session keys:

Modified and encrypted session key (hexadecimal):

C1D76344E32AE75238C493505DE3B49E1DD8834A599F94535B85131A021D1E368A3B6F832D27979...
041BE023204301B980C7B88BF53B46C9C51747FF643FBABE4AA64D95CB221CA63F3DFF2205386D...
9136F31428C24377D03740CB86768DE03DD9E2F22D3A30891913FC9D511D52FCB04A7367D52024B...
9026E171F20CFF47AC8088E3F419A9599DDC5560AF57D8F01552AC1C86AAFF0D8D12804FA1F0AA4...
R3A8633C8C5R610D9F59C5565AFAFD302A1R202A19211R3F59A52FARRRRRC2RD55AC25379F5R3CF3

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

727E8140D55010025AE1B3990AD7F546

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

care for them the most. I feel incredibly lucky to have shared my life with several feline friends over the years.
Each one has left a lasting impression on my heart.
Thank you for letting me share my love for cats with you. I hope you have a wonderful day!

Warm regards, Daria

Заключение

1. Изучен протокол согласования ключей Диффи-Хеллмана, который позволяет пользователям получить секретный ключ без его непосредственной передачи. Модификация схемы привела к преобразованию ключевого материала в симметричный ключ длиной 256 бит. Также была изучена атака протокола «посредником».
2. Изучен алгоритм асимметричного шифрования RSA. Шаблонная схема RSA Encryption из CrypTool 2 была изменена для проведения атаки коротким сообщением. В ходе атаки нарушитель может зашифровать открытым ключом все возможные исходные сообщения, пока результат не будет совпадать с перехваченным зашифрованным текстом. Для предотвращения этой атаки рекомендуется дополнять исходный текст случайными битами до начала шифрования.
3. Изучен протокол асимметричного шифрования RSA. Модификация схемы шаблонная схемы из CrypTool 2 позволяет зашифровать и расшифровать симметричный ключ, полученный из парольной фразы. Также была изучена атака протокола «посредником».
4. Выполнена атака на шифр RSA факторизацией модуля. Для модуля N равного 1441 было найдено верное разложение менее чем за 1 секунду.
5. Изучена и выполнена имитация атаки на гибридный протокол шифрования. Установлено, что злоумышленник может перехватить цифровой конверт, содержащий зашифрованные данные и ключ, модифицировать сообщения и направлять их серверу. Анализируя ответы сервера, злоумышленник может бит за битом восстановить секретный ключ.