МИНОБРНАУКИ РОССИИ
САНКТ-ПЕТЕРБУРГСКИЙ ГОСУДАРСТВЕННЫЙ
ЭЛЕКТРОТЕХНИЧЕСКИЙ УНИВЕРСИТЕТ
«ЛЭТИ» ИМ. В.И. УЛЬЯНОВА (ЛЕНИНА)
Кафедра МО ЭВМ

ОТЧЕТ

по лабораторной работе №6-7

по дисциплине «Криптография и защита информации»

ТЕМА: ИЗУЧЕНИЕ И ИССЛЕДОВАНИЕ АЛГОРИТМОВ ХЭШИРОВАНИЯ И АСИММЕТРИЧНОГО ШИФРОВАНИЯ.

Студент гр. 0303 _____ Калмак Д.А.

Преподаватель _____ Племянников А.К.

Санкт-Петербург

2023

Цель работы.

Изучить и исследовать алгоритмы хэширования и асимметричного шифрования, такие как MD5, SHA-1, SHA-256, SHA-3 (Keccak), HMAC, протокол Диффи-Хеллмана и RSA.

Порядок выполнения работы.

1. Изучить хэш-функции MD5, SHA-1, SHA-256 , SHA-3 (Keccak) и оценить их лавинный эффект по шаблонной схеме Avalanche(hash functions) из CrypTool 2 с учетом рекомендаций Методического пособия из задания раздела 6.1 (на с. 32).

2. Изучить код аутентификации сообщения HMAC по одноимённой шаблонной схеме. Выполнить п. 4 задания к разделу 6.3 (с. 34) учебно-методического пособия

3. Изучить протокол согласования ключей по шаблонной схеме Diffie-Hellman Key Exchange из CrypTool 2 . Выполнить модификацию схемы для преобразования полученного ключевого материала в симметричный ключ длиной 256 бит.

4. Изучить алгоритм асимметричного шифрования RSA по шаблонной схеме RSA Encryption из CrypTool 2. Изменить эту шаблонную схему для проведение атаки коротким сообщением. В качестве сообщения использовать две последние цифры студенческого билета.

5. Выполнить имитацию атаки на гибридную систему шифрования в CrypTool 1 по указаниям учебно-методического пособия из раздела 7.5

Выполнение работы.

1. Оценка лавинного эффекта хэш-функций MD5, SHA-1, SHA-256, SHA-3 (Keccak)

Выбран исходный текст на английском языке, в котором количество символов больше тысячи и в конце добавлено ФИО KALMAK DANIIL ANDREEVICH.

Для хэш-функций MD5, SHA-1, SHA-256, SHA-3 (Keccak) повторим следующие действия:

а) изменить (добавлением, заменой, удалением символа) исходный текст

Добавление: символ A

Замена: замена H на A

Удаление: удаление H

б)зафиксировать количество измененных битов в дайджесте модифицированного сообщения;

в) вернуть сообщение в исходное состояние.

Повторим процедуру 3 раза и подсчитаем среднее количество измененных бит дайджеста. Полученные данные представлены в табл. 1.

Таблица 1 – Оценка лавинного эффекта для хеш-функций

Изменение исходного текста	Количество измененных бит дайджеста			
	MD-5 (128)	SHA-1 (160)	SHA-256 (256)	SHA-3 (Keccak)(256)

Добавление символа	58	76	142	137
Замена символа	67	84	130	132
Удаление символа	68	74	124	122
Среднее значение	64,3 50,2 %	78 48,8 %	132 51,6 %	130,3 50,9 %

2. Изучение кода аутентификации сообщения HMAC по одноимённой шаблонной схеме.

Код аутентификации HMAC – механизм проверки целостности информации. Он позволяет гарантировать то, что данные, передаваемые или хранящиеся в ненадежной среде, не были изменены посторонними лицами. Две стороны, использующие HMAC, имеют общий секретный ключ K и используют одинаковую хеш-функцию H(). Алгоритм HMAC в виде формулы:

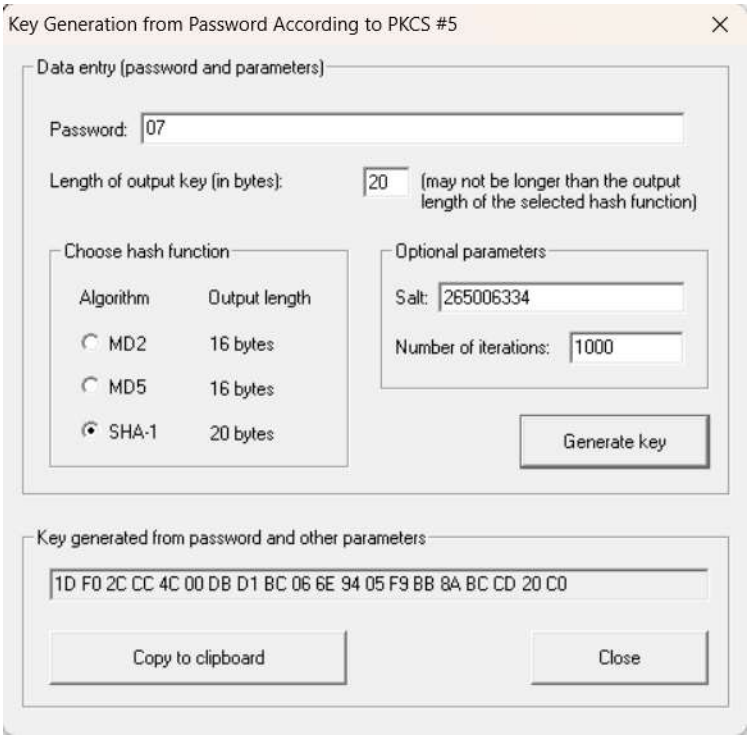
$$\mathrm{HMAC}_K(\mathrm{text}) = H\left\{(K \oplus \mathrm{opad}) \,\|\, H\left[(K \oplus \mathrm{ipad}) \,\|\, \mathrm{text}\right]\right\},$$

где $\oplus$ – операция xor; $\|$ – конкатенация; K – секретный ключ; ipad – блок вида (0x36 0x36 0x36 ... 0x36), где байт 0x36 повторяется b раз; H – хеш-функция; opad – блок вида (0x5c 0x5c 0x5c ... 0x5c), где байт 0x5c повторяется b раз.

Исходный текст на английском языке, в котором количество символов больше тысячи и в конце добавлено ФИО KALMAK DANIIL ANDREEVICH.

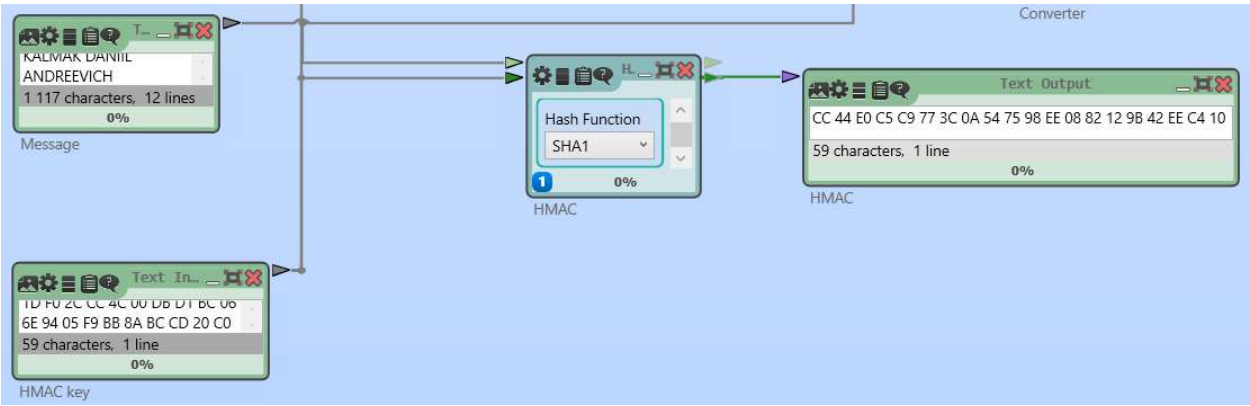
ECONOMIC POLICIES OF INDIVIDUAL COUNTRIES AND INTERNATIONAL ECONOMIC RELATIONS BOTH HAVE GREAT RELEVANCE TO SUSTAINABLE DEVELOPMENT THE REACTIVATION AND ACCELERATION OF DEVELOPMENT REQUIRES BOTH A DYNAMIC AND A SUPPORTIVE INTERNATIONAL ECONOMIC ENVIRONMENT AND DETERMINED POLICIES AT THE NATIONAL LEVEL IT WILL BE FRUSTRATED IN THE ABSENCE OF EITHER OF THESE REQUIREMENTS A SUPPORTIVE EXTERNAL ECONOMIC ENVIRONMENT IS CRUCIAL THE DEVELOPMENT PROCESS WILL NOT GATHER MOMENTUM IF THE GLOBAL ECONOMY LACKS DYNAMISM AND STABILITY AND IS BESET WITH UNCERTAINTIES NEITHER WILL IT GATHER MOMENTUM IF THE DEVELOPING COUNTRIES ARE WEIGHTED DOWN BY EXTERNAL INDEBTEDNESS, IF DEVELOPMENT FINANCE IS INADEQUATE, IF BARRIERS RESTRICT ACCESS TO MARKETS AND IF COMMODITY PRICES AND THE TERMS OF TRADE OF DEVELOPING COUNTRIES REMAIN DEPRESSED THE RECORD OF THE 1980S WAS ESSENTIALLY NEGATIVE ON EACH OF THESE COUNTS AND NEEDS TO BE REVERSED THE POLICIES AND MEASURES NEEDED TO CREATE AN INTERNATIONAL ENVIRONMENT THAT IS STRONGLY SUPPORTIVE OF NATIONAL DEVELOPMENT EFFORTS ARE THUS VITAL KALMAK DANIIL ANDREEVICH

Сгенерируем секретный ключ, используя пароль 07, с помощью Cryptool 1.



Секретный ключ: 1D F0 2C CC 4C 00 DB D1 BC 06 6E 94 05 F9 BB 8A BC CD 20 C0

Сгенерирован HMAC для имеющегося текста и ключа с использованием хеш-функции SHA-1.



HMAC: CC 44 E0 C5 C9 77 3C 0A 54 75 98 EE 08 82 12 9B 42 EE C4 10

Модифицированный текст получен путем изменения последнего символа H на A.

Отправитель:

1. Генерирует секретный ключ на основе пароля, который известен получателю, и алгоритма, например, таких хеш-функций, как MD-5, SHA-1 и т.д.

2. Генерирует HMAC для имеющегося текста и ключа.

3. Передает HMAC и исходный открытый текст.

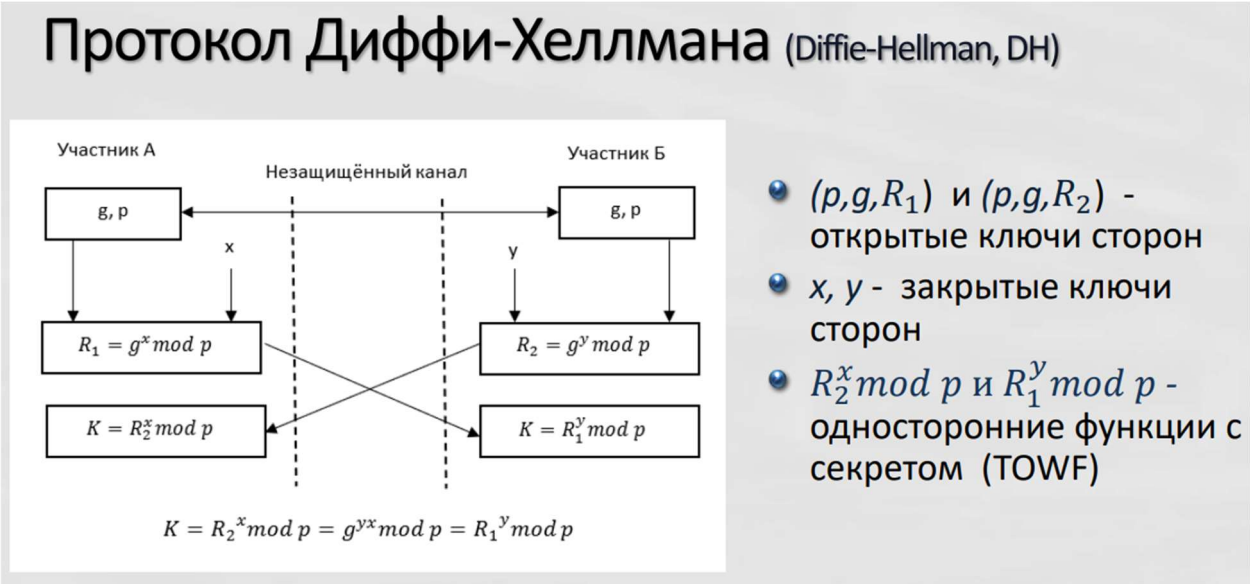
Получатель:

1. Получает текст и его HMAC от отправителя.

2. Вычисляет HMAC полученного текста на основе секретного ключа, который сгенерирован на основе пароля, который заранее известен от получателя, и алгоритма, например, таких хеш-функций, как MD-5, SHA-1 и т.д, который заранее известен от получателя.

3. Сравнивает вычисленный и полученный HMAC. Если HMAC совпадают, то текст подлинный.

3. Изучение протокола согласования ключей по шаблонной схеме Diffie-Hellman Key Exchange из CrypTool 2. Модификация схемы для преобразования полученного ключевого материала в симметричный ключ длиной 256 бит.



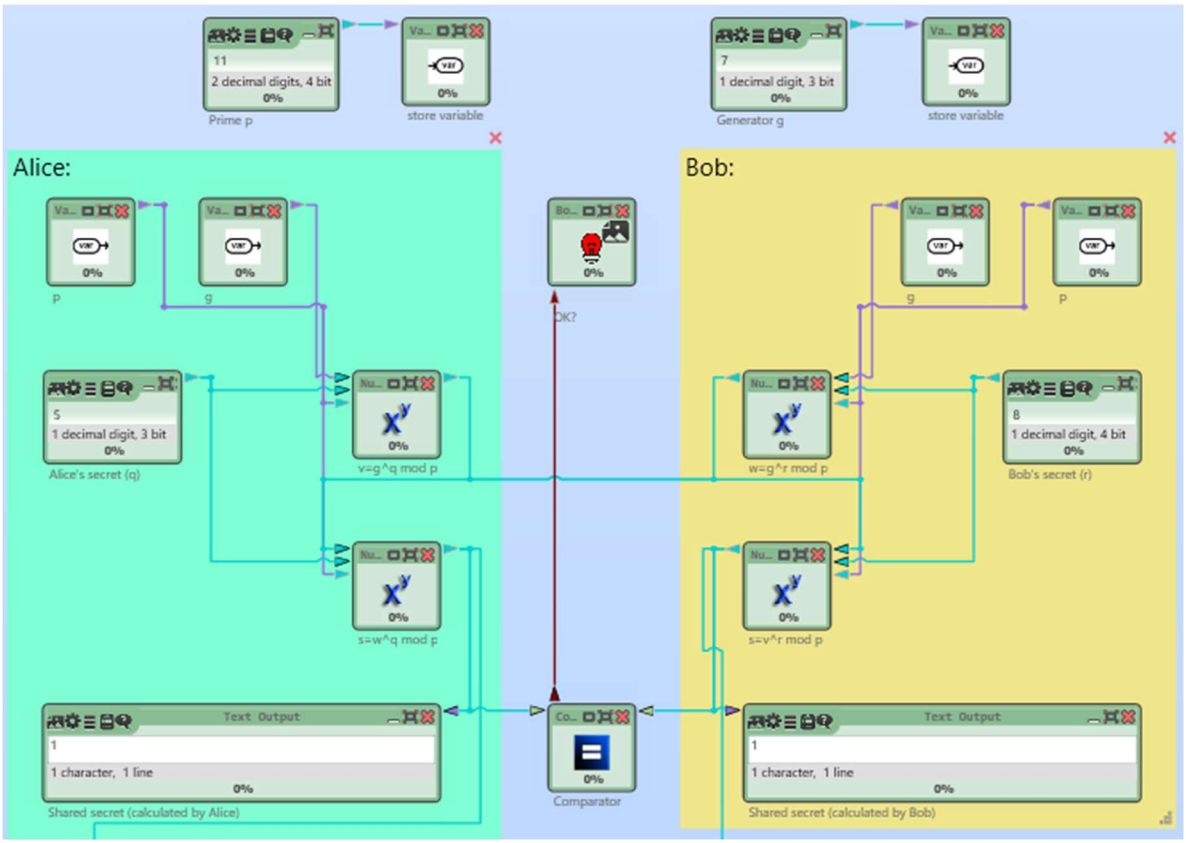
Математическая модель протокола

- p -большое простое число порядка 300 десятичных цифр (1024 бита)
- g – порождающий элемент циклической группы (генератор) порядка p, для которого справедливо:
  $g \bmod p, g^2 \bmod p, g^3 \bmod p \ldots g^{p-1} \bmod p$ являются различными целыми из $[1,p-1]$
- x, y - большие случайные числа такие, что $0 < x < p-1, 0 < y < p-1$
- Поскольку:

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

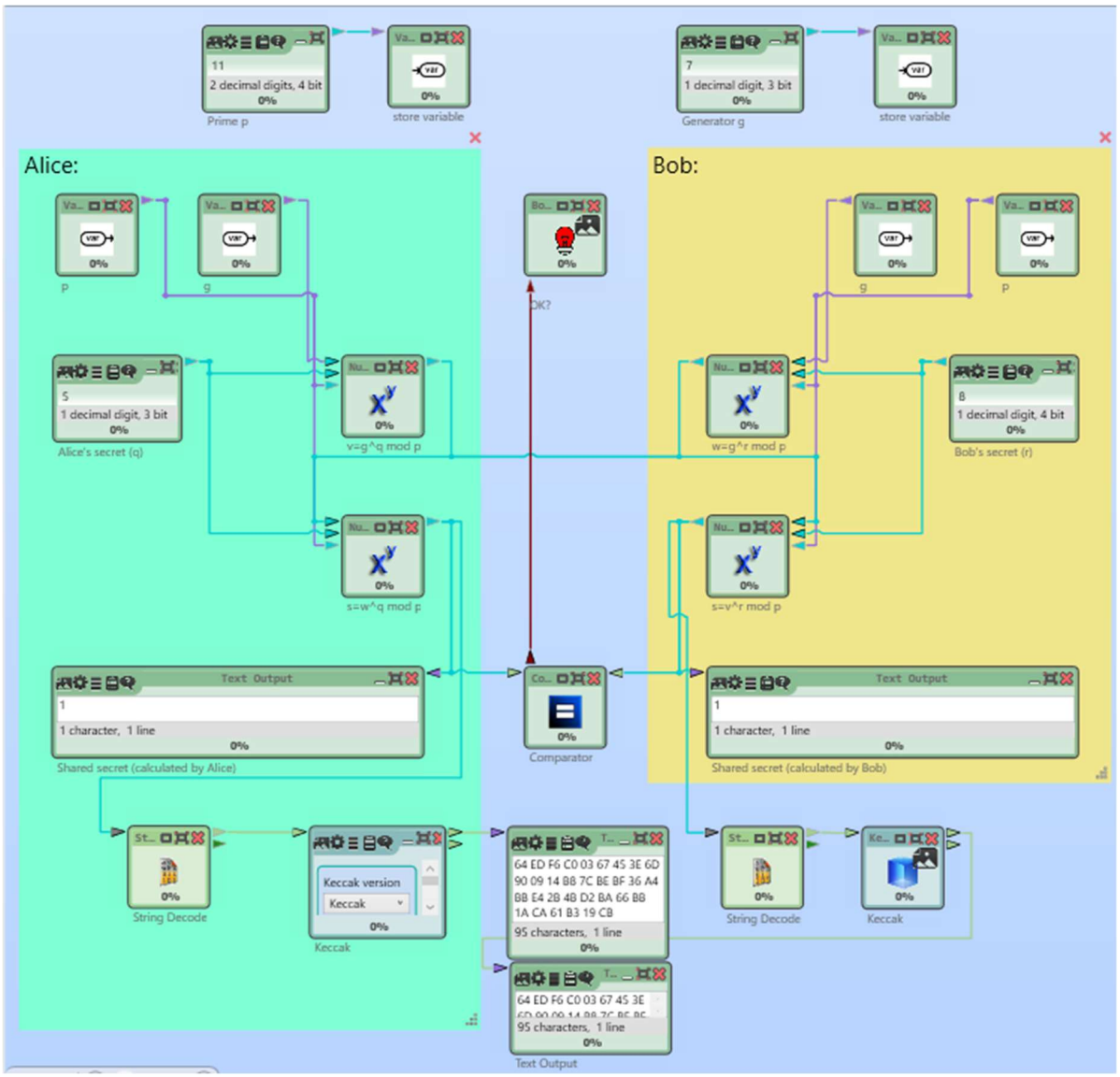
- Стороны создают материал для симметричного ключа и этот материал используется для генерации сеансового ключа без посредничества Центра распределения ключей (KDC)

Получен секретный ключ при p = 11, g = 7, секретном числе Алисы x = 5 и секретном числе Боба y = 8.



Секретный ключ: 1

Модифицирована схема для преобразования полученного ключевого материала в симметричный ключ длиной 256 бит с помощью хеш-функции Keccak.



Симметричный ключ длиной 256 бит: 64 ED F6 C0 03 67 45 3E 6D 90 09 14 B8 7C BE BF 36 A4 BB E4 2B 4B D2 BA 66 BB 1A CA 61 B3 19 CB

4. Изучение алгоритма асимметричного шифрования RSA по шаблонной схеме RSA Encryption из CrypTool 2. Изменение шаблонной схемы для проведения атаки коротким сообщением.

Шифр RSA

- Шифр RSA базируется на следующих двух фактах из теории чисел:
  - задача проверки числа на простоту является сравнительно легкой;
  - задача разложения чисел вида $n = p*q$ (p и q — простые числа) на множители является очень трудной, если мы знаем только n, а p и q — большие числа (это так называемая задача факторизации)
- Шифр RSA представляет собой блочный алгоритм шифрования, где зашифрованные и незашифрованные данные должны быть представлены в виде целых чисел между 0 и $n-1$

RSA генерация ключей

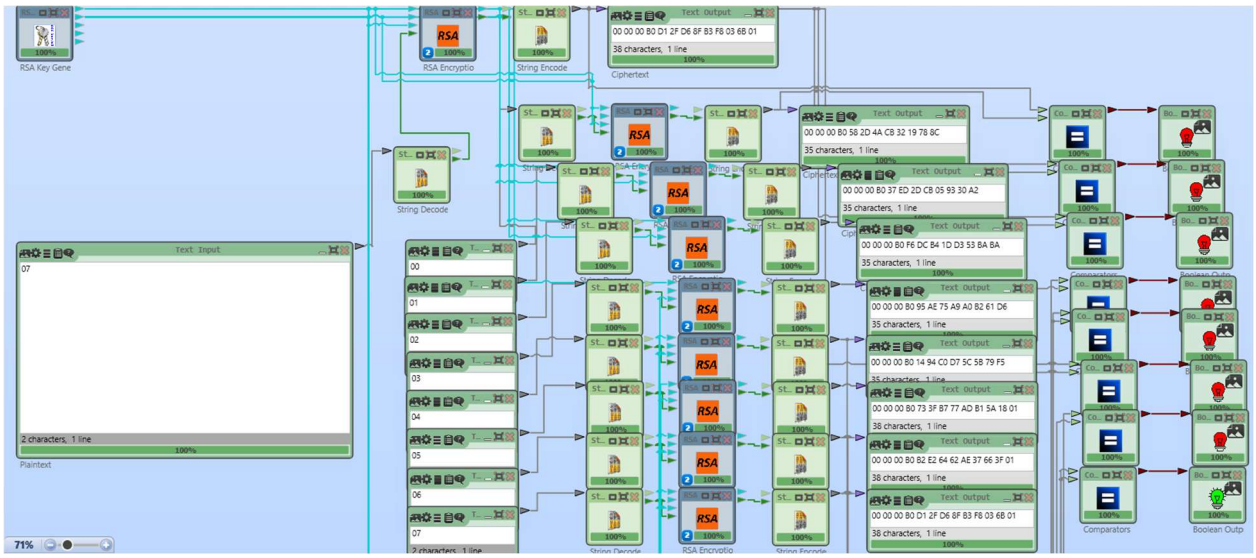
- Выбираются два больших простых числа p и q
- Вычисляется $n=p*q$
- Выбирается произвольное число e ($e<n$), взаимно простое с $(p-1)\times(q-1)$
- Вычисляется d, такое, что $e \times d \equiv 1\ mod(p-1)\times(q-1)$ решением в целых числах уравнения (расширенный алгоритм Евклида) относительно d и y :

$$e \times \boldsymbol{d} + (p-1)\times(q-1)\times \boldsymbol{y} = \text{НОД}\big(e,(p-1)*(q-1)\big) = 1$$

- Пара чисел (e, n) объявляются открытым ключом,
- Закрытым ключом выбирается d , p и q нужно уничтожить

Зашифрованы последние две цифры 07 студенческого билета при p = 232887864930486883438580649703, q = 10811451314476310891948811153 71 и e = 7.

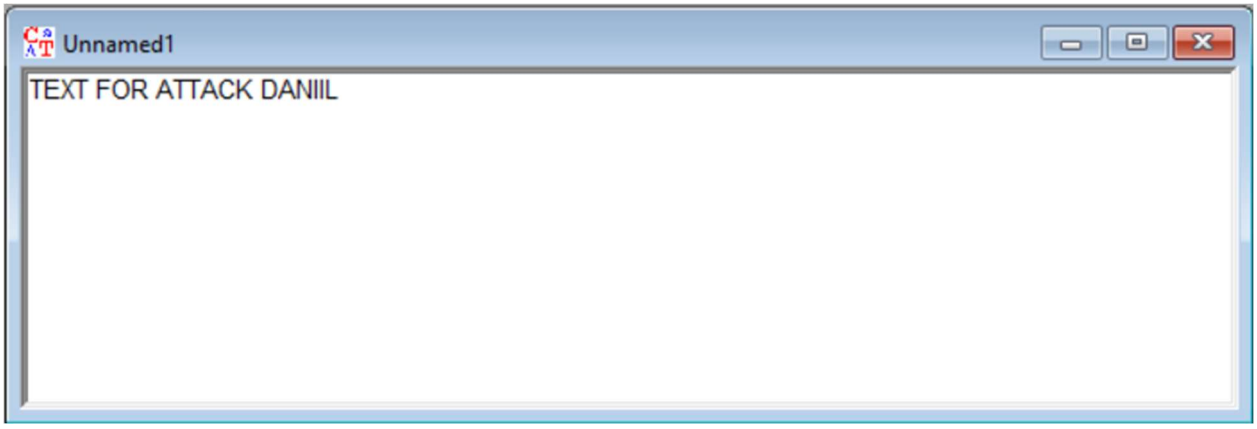
Проведена атака короткого сообщения по известным N, e и шифротексту. Перебраны сообщения, пока шифротекст подобранного сообщения не совпал с известным шифротекстом.



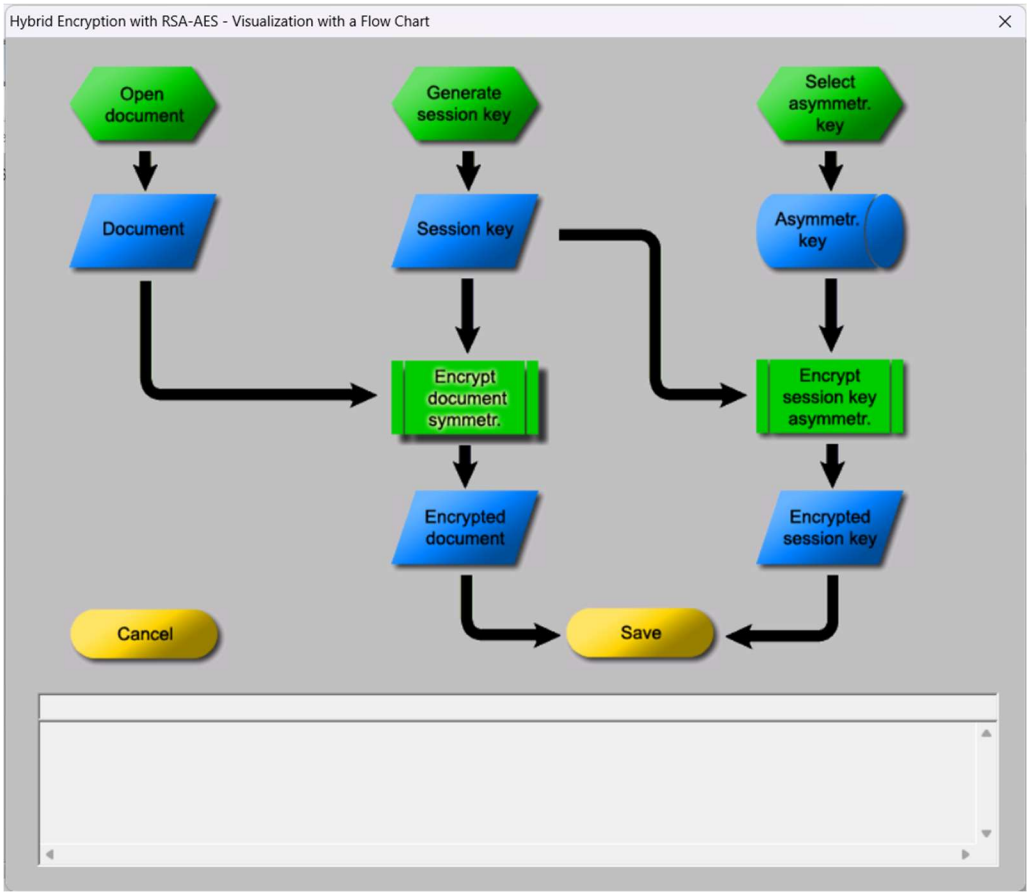
5. Имитация атаки на гибридную систему шифрования в CrypTool 1.

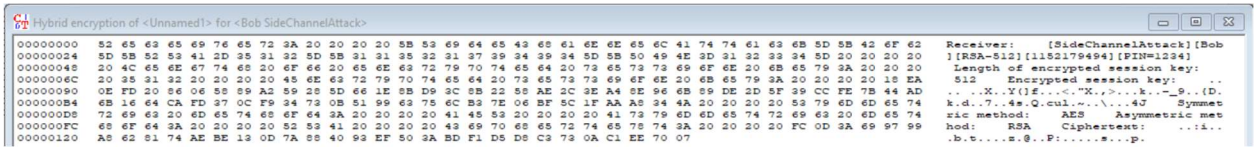
Атака на модель гибридной криптосистемы основана на том, что злоумышленник сначала перехватывает цифровой конверт, содержащий зашифрованное сообщение и секретный ключ, затем специальным образом модифицирует шифровку ключа из конверта и восстанавливает бит за битом зашифрованный секретный ключ с помощью анализа положительных и отрицательных ответов сервера, которые злоумышленник получает по побочным каналам.

Исходный текст:

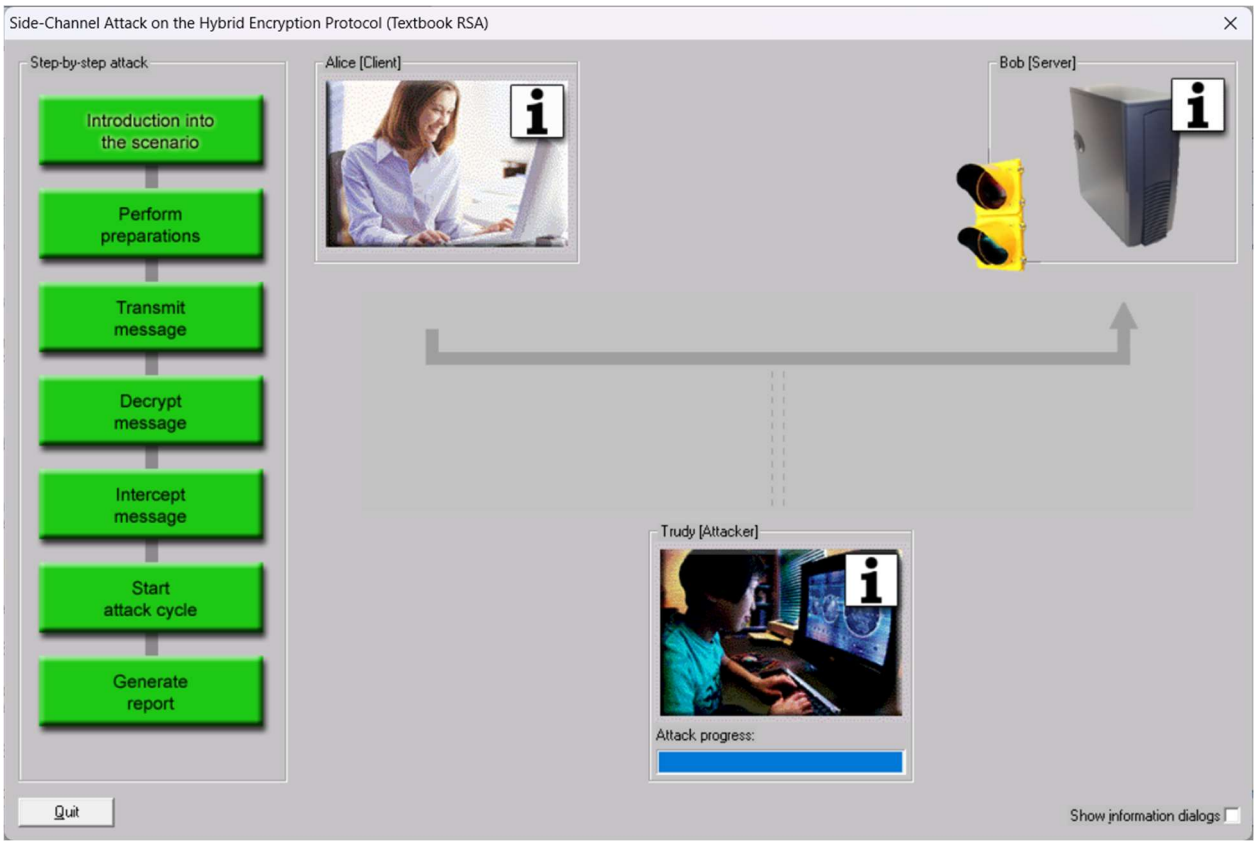


Шифрование исходного текста и ключа.

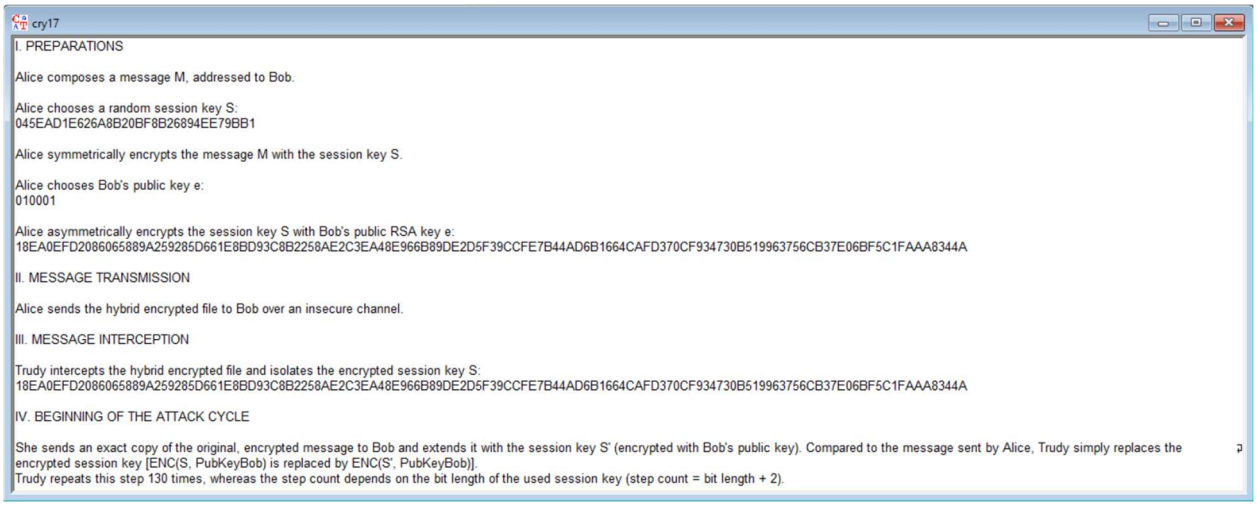

Hybrid Encryption with RSA-AES - Visualization with a Flow Chart
Open document
Generate session key
Select asymmetr. key
Document
Session key
Asymmetr. key
Encrypt document symmetr.
Encrypt session key asymmetr.
Encrypted document
Encrypted session key
Cancel
Save


Hybrid encryption of <Unnamed1> for <Bob SideChannelAttack>
Receiver: [SideChannelAttack][Bob][RSA-512][1152179494][PIN=1234]
Length of encrypted session key:
512 Encrypted session key:
Symmetric method: AES Asymmetric method: RSA Ciphertext:

Атака.



Отчет по атаке.



Выводы.

Таким образом, были исследованы алгоритмы хэширования и асимметричного шифрования.

1. Хеш-функция для строки произвольной длины вычисляет другую строку определенной длины: SHA-256 – 256 бит, SHA-3 Keccak – 256 бит, MD5 – 128 бит, SHA-1 – 160 бит. Лавинный эффект должен быть 50 %. Лидером стал SHA-256 с 51,6 % лавинного эффекта, SHA-3 Keccak – 50,9 %, MD5 – 50,2 % и SHA-1 – 48,8 %.

2. HMAC - код аутентификации сообщения, механизм, который обеспечивает проверку целостности сообщения и гарантию, что сообщение не было изменено. HMAC вычисляется с использованием ключа и хеш-функции. Получен ключ по паролю, создано модифицированное сообщение и сгенерирован HMAC для исходного сообщения.

3. Протокол Диффи-Хелмана обеспечивает двум сторонам возможность получения общего симметричного секретного ключа с помощью обмена данными по незащищенному каналу. Получен секретный ключ и с помощью хеш-функции Keccak получен симметричный ключ длиной 256 бит.

4. RSA - ассиметричный блочный шифр, основанный на проблеме разложения больших целых чисел на простые множители - задаче факторизации. С помощью двух больших простых чисел генерируются открытый и закрытый ключи. Было зашифровано сообщение, а затем проведена успешная атака коротким сообщением.

5. Гибридная система шифрования содержит симметричное шифрование для открытого текста и ассиметричное шифрование для ключа, с помощью которого был зашифрован открытый текст. При атаке на гибридную систему шифрования злоумышленник пытается получить секретный ключ с помощью ответов сервера, а затем секретным ключом расшифровать шифротекст. Выполнена имитация атаки на гибридную систему шифрования в CrypTool 1.