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

ОТЧЕТ

По лабораторной работе № 6-7
по дисциплине «Криптография и защита информации»
Тема: Исследование алгоритмов хэширования и асимметричного шифрования

Студент гр. 0303 _____ Болкунов В.О.

Преподаватель _____ Племянников А. К.

Санкт-Петербург
2023

Цель работы.

Цель работы: изучить хэш функции MD5, SHA-1, SHA-256, SHA-3, код аутентификации HMAC, протокол согласования ключей Диффи-Хеллмана и ассиметричный шиф 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 проведения 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. Хэш функции

С помощью средств CrypTool 2 (рис. 1) был оценен лавинный эффект для хэш-функций MD5, SHA-1, SHA-256, SHA-3, при добавлении, удалении и замене одного символа в сообщении.

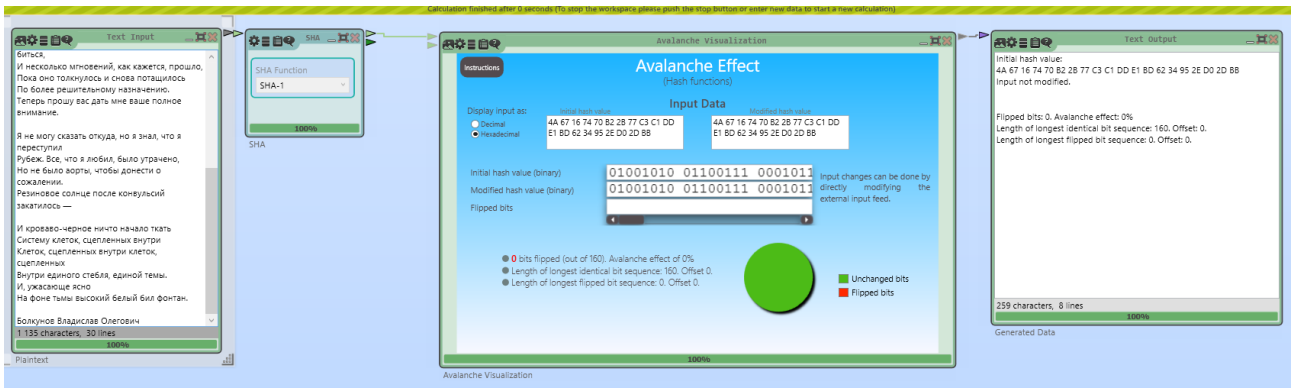

Рисунок 1: измерение лавинного эффекта в CrypTool2

В таблице 1 представлены лавинные эффекты в процентах при добавлении, замене и удаления одного символа в сообщении, и их среднее значение.

Таблица 1 – исследование лавинного эффекта хэш-функций

Хэш-функция	№ измерения	Удаление	Вставка	Замена
MD5	1	44.5	47.7	51.6
	2	41.4	45.3	46.9
	3	60.9	53.9	53.1
	Среднее	**48.93**	**48.96**	**50.53**
SHA-1	1	51.9	54.4	48.1
	2	50.6	59.4	55.6
	3	45.0	55.0	45.0
	Среднее	**49.16**	**56.26**	**49.56**
SHA-256	1	50.8	50.4	46.5
	2	47.7	52.7	49.6
	3	45.7	51.6	52.3
	Среднее	**48.06**	**41.56**	**49.46**
SHA-3	1	49.2	47.3	46.9
	2	47.3	44.5	51.6
	3	48.0	53.5	50.0
	Среднее	**48.16**	**48.43**	**49.5**

В среднем для всех алгоритмов показатель лавинного эффекта оказался близок к 50%.

2. Код аутентификации HMAC

В шаблонной схеме CrypTool для HMAC (на основе MD5) был сгенерирован 64-байтовый ключ и выбрано сообщение (рис. 2).

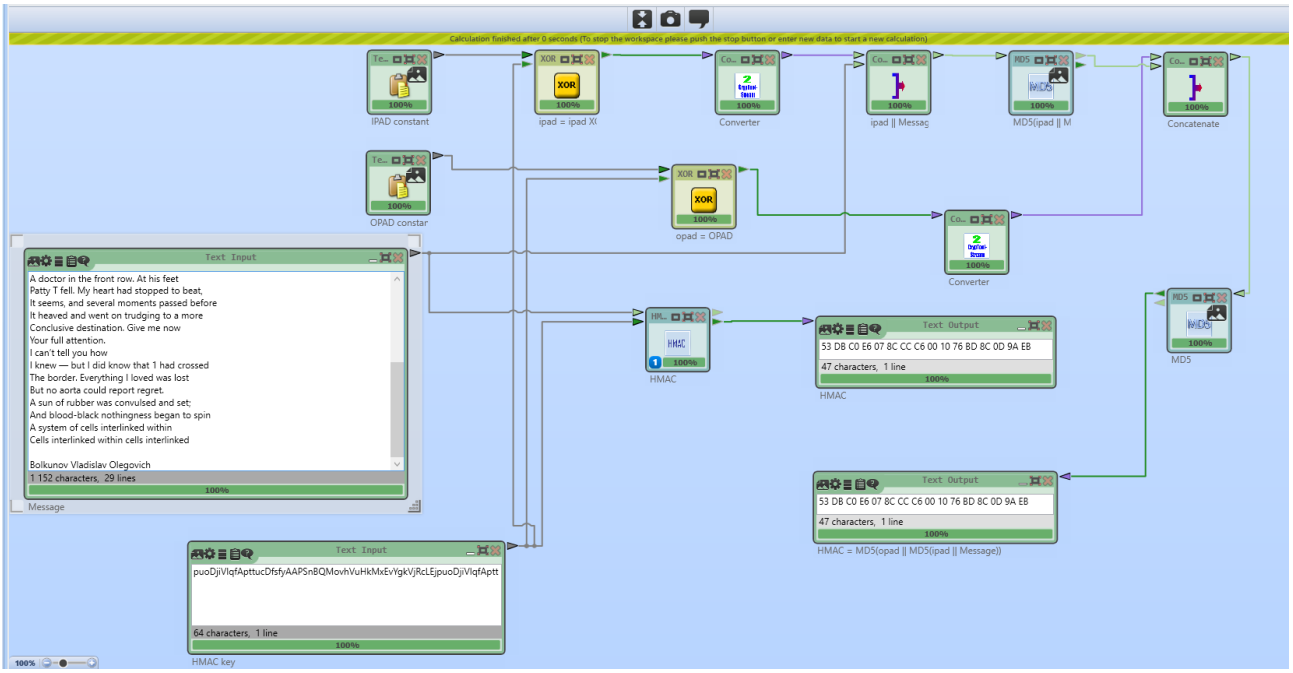

Рисунок 2: HMAC

Полученный код: **53 DB C0 E6 07 8C CC C6 00 10 76 BD 8C 0D 9A EB**

Изменим часть сообщения (рис. 3):

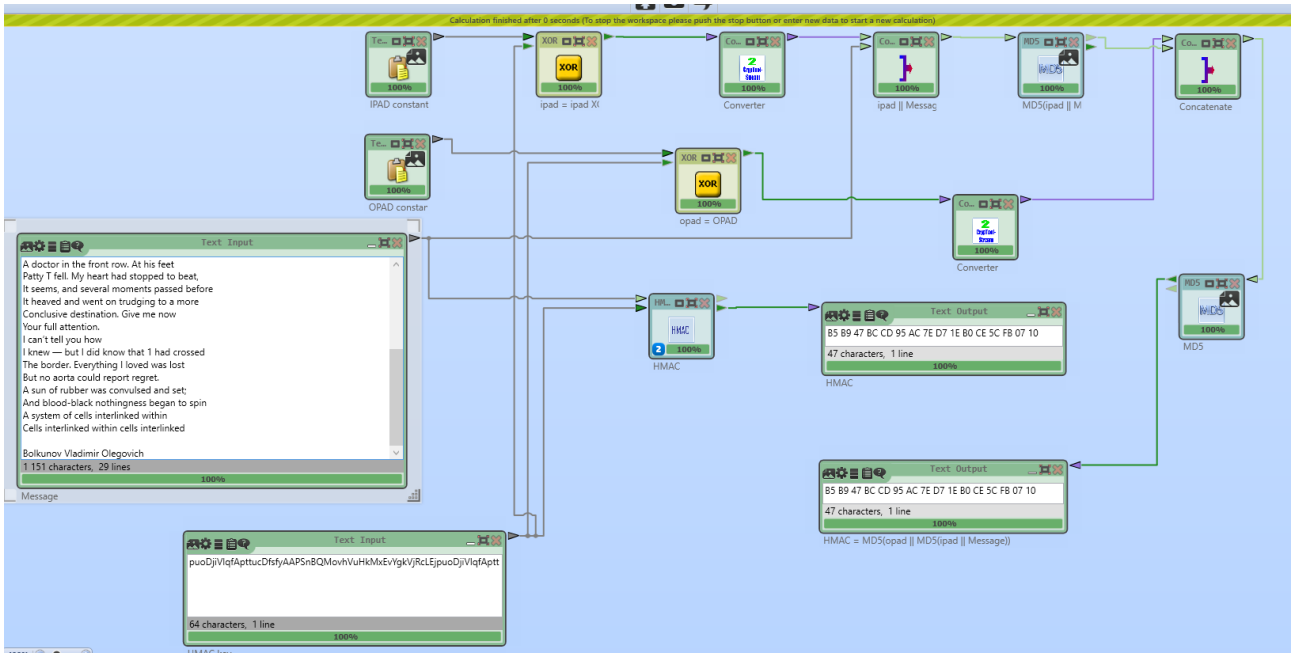

Рисунок 3: модификация сообщения

В результате изменения имени в сообщении был получен следующий хэш-код: **B5 B9 47 BC CD 95 AC 7E D7 1E B0 CE 5C FB 07 10**

Полученные хэш-коды сильно различаются, что свидетельствует о модификации исходного сообщения, в их битовом представлении было изменено **68** бит из **128**.

3. Протокол Диффи-Хеллмана

В шаблонной схеме протокола Диффи-Хеллмана с помощью средств CrypTool2 были выбраны следующие параметры протокола (рис. 4):

Модуль **p = 109**

Генератор **g = 6**

Закрытый ключ стороны А, **q = 31**

Закрытый ключ стороны Б, **r = 47**

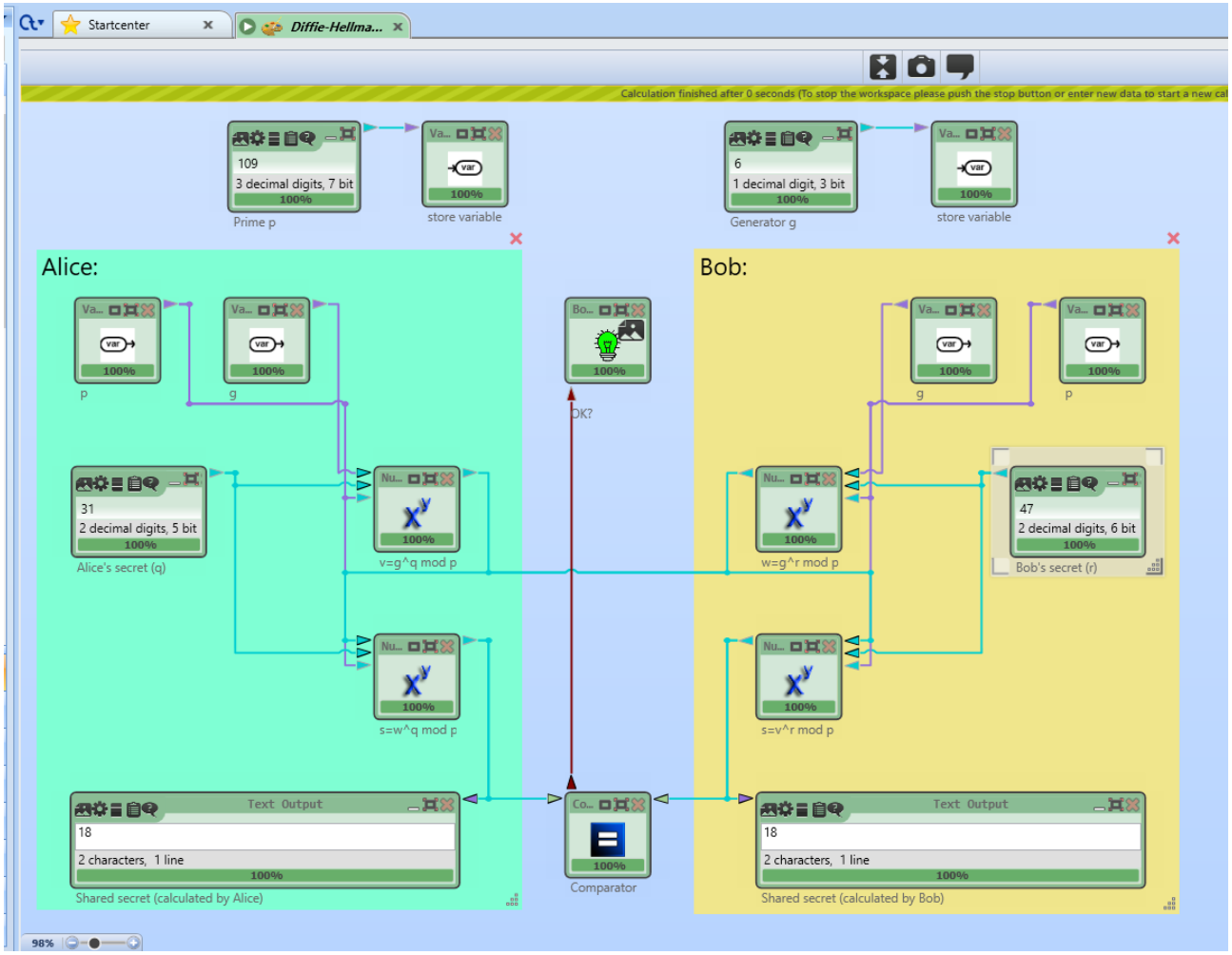

Рисунок 4: схема протокола Диффи-Хеллмана

В результате выполнения протокола был получен общий ключ **K = 18**.

Данная схема была модифицирована (рис. 5) для получения 256-битного ключа с помощью хэш-функции SHA-256.

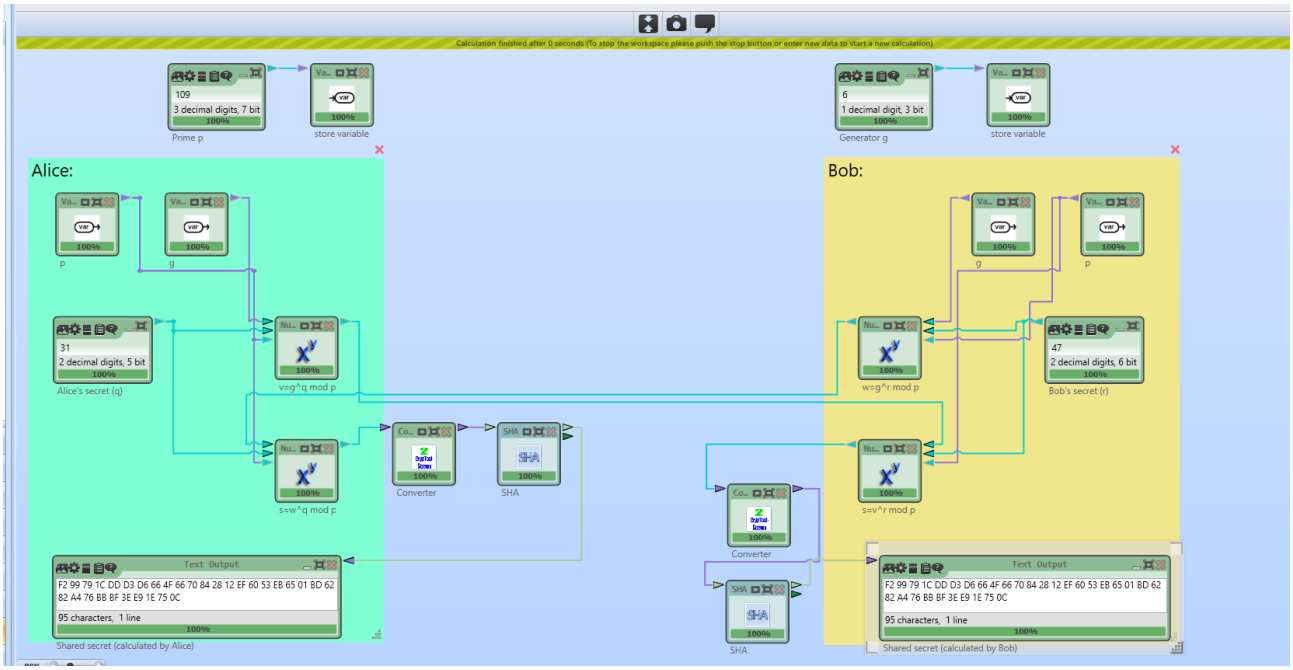

Рисунок 5: Модифицированная схема

Полученные в результате работы протокола Диффи-Хеллмана и хэш-функции SHA-256 ключи:

K_1 = F2 99 79 1C DD D3 D6 66 4F 66 70 84 28 12 EF 60 53 EB 65 01 BD 62 82 A4 76 BB BF 3E E9 1E 75 0C

K_2 = F2 99 79 1C DD D3 D6 66 4F 66 70 84 28 12 EF 60 53 EB 65 01 BD 62 82 A4 76 BB BF 3E E9 1E 75 0C

Полученные ключи идентичны, что позволяет использовать их для симметричного шифрования.

4. Шифр RSA

В схеме шифрования RSA в CrypTool2 было выбрано и зашифровано сообщение (рис. 6).

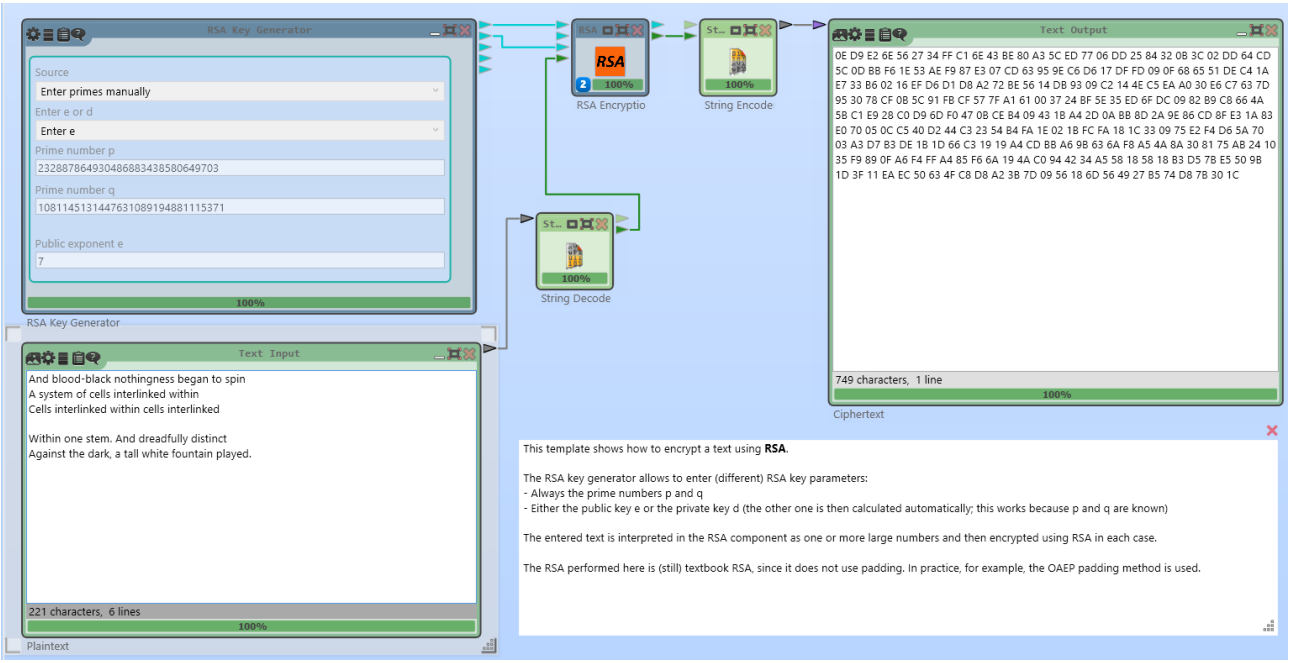

Рисунок 6: шифрование RSA

Данная схема была модифицирована для атаки малым сообщением (рис. 7). В качестве сообщения была выбрана цифра 4. Алгоритм выполнял перебор цифр до тех пор, пока зашифрованные открытым ключом сообщения (исходное и перебираемое) не станут равны.

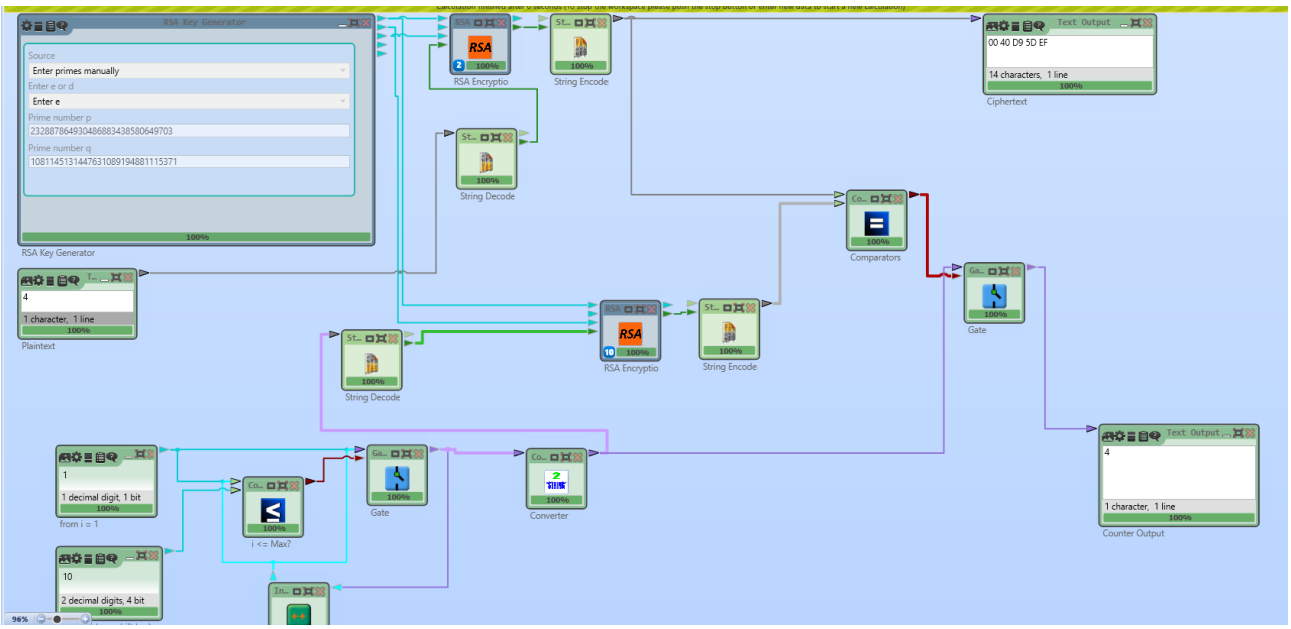

Рисунок 7: Атака малым сообщением

5. Гибридная система шифрования

В среде CrypTool1 было выбрано следующее сообщение (рис. 8)

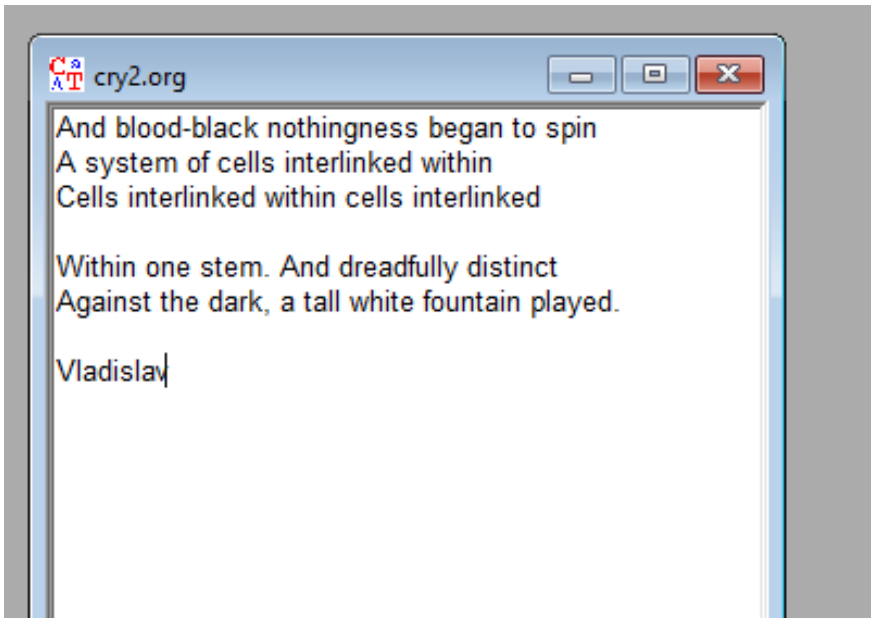

Рисунок 8: выбранное сообщение

Сторона А сгенерировала секретный ключ сессии (рис. 9), после чего с помощью ассиметричного шифра ключ был передан стороне Б (рис. 10). В листинге 1 представлен протокол атаки на систему.

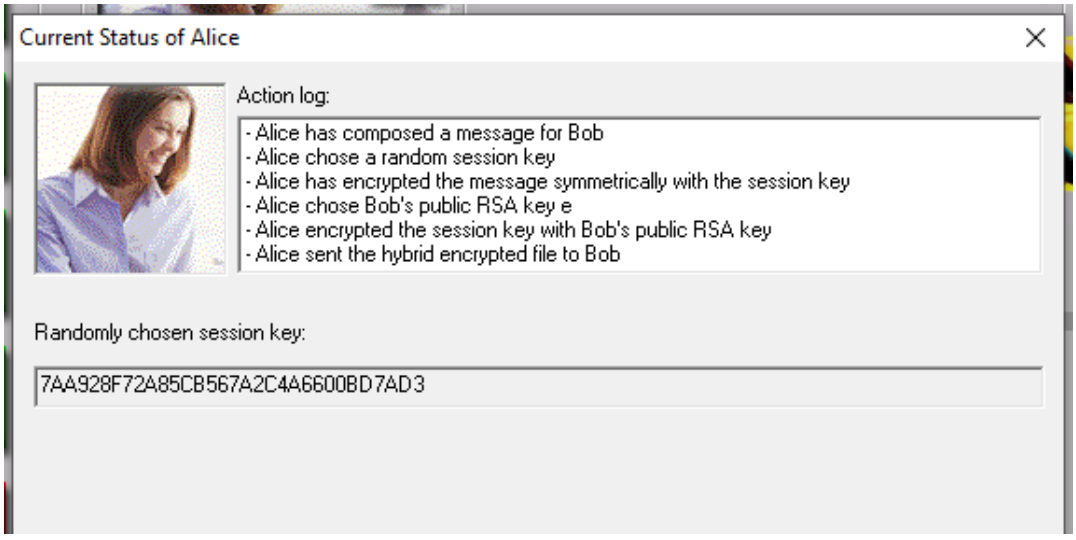

Рисунок 9: симметричный ключ сессии

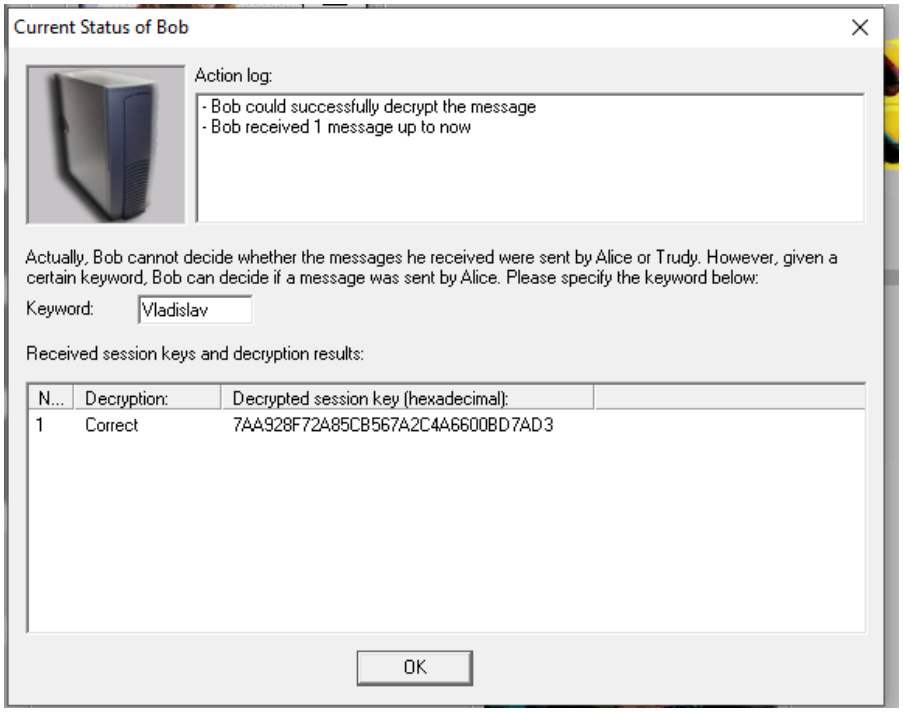

Рисунок 10: расшифрованный симметричный ключ

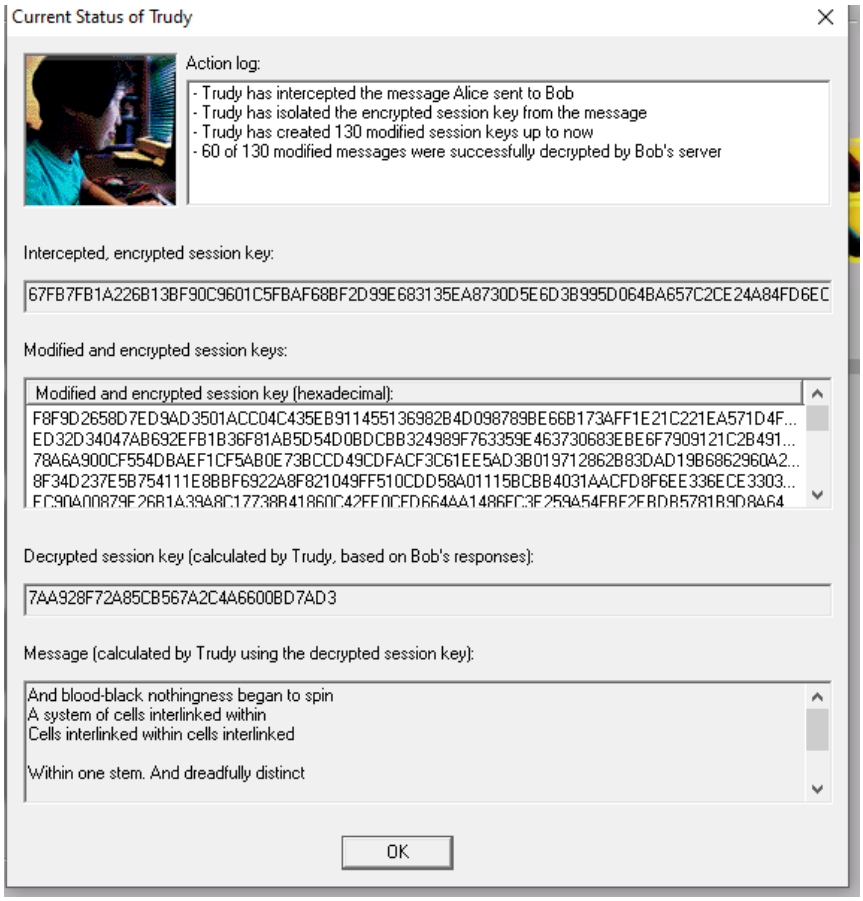

Рисунок 11: атака на систему

Листинг 1. Протокол работы атаки на гибридный шифр

```
I. PREPARATIONS
```

Alice composes a message M, addressed to Bob.

Alice chooses a random session key S:
7AA928F72A85CB567A2C4A6600BD7AD3

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:
67FB7FB1A226B13BF90C9601C5FBAF68BF2D99E683135EA8730D5E6D3B995D064B
A657C2CE24A84FD6EC7B0E9B03A45000946E4F77E3F96442F1269B416E8952

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:
67FB7FB1A226B13BF90C9601C5FBAF68BF2D99E683135EA8730D5E6D3B995D064B
A657C2CE24A84FD6EC7B0E9B03A45000946E4F77E3F96442F1269B416E8952

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).

Выводы:

В ходе лабораторной работы были исследованы хэш-функции MD-5, SHA-1, SHA-256, SHA-3; код аутентификации HMAC; протокол согласования ключей Диффи-Хеллмана и алгоритм ассиметричного шифрования RSA.

- Для хэш-функций MD-5, SHA-1, SHA-256, SHA-3 с помощью средств CrypTool2 был измерен лавинный эффект в результате операций преобразования исходного текста; в среднем лавинный эффект составил около 50%, что является хорошим показателем.

- С помощью средств CrypTool2 был изучен код аутентификации HMAC на основе хэш-функции MD-5. В результате небольшой модификации исходного сообщения было замечено сильное изменение HMAC кода, что позволило определить модификацию сообщения.

- На основе схемы протокола согласования ключей Диффи-Хеллмана были выбраны открытые константы и секретные ключи каждой из двух сторон, в результате удалось сгенерировать общий секретный ключ.
  Была произведена модификация схемы, в ходе которой к полученному секретному ключу применялась хэш-функция SHA-256, в результате которой был получен 256-битный секретный ключ возможный для использования в симметричном шифровании.

- В среде CrypTool2 был изучен ассиметричный шифр RSA, была создана схема для атаки коротким сообщением, в результате которой было успешно подобрано исходное сообщение.

- В программе CrypTool1 была проведена атака по побочному каналу на гибридную систему шифрования, что в результате позволило подобрать секретный ключ симметричного шифра, которым было зашифровано исходное сообщение отправителя.