**Введение**

**Целью** данной работы является изучение различных видов шифрования сообщений. В своей работе я использую симметричное и асимметричное. С помощью них я передаю информацию своему собеседнику так, чтобы никто не мог прочитать содержание.

Асимметричное шифрование — это метод шифрования данных, предполагающий использование двух ключей — открытого и закрытого. Открытый ключ применяется для шифрования информации и может передаваться по незащищенным каналам. Закрытый ключ применяется для расшифровки данных, зашифрованных открытым ключом. Алгоритм шифрования, который используется – RSA.

Симметричное шифрование — это криптографический метод, предполагающий шифрование и расшифровку данных с помощью одного и того же секретного ключа.

Для того, чтобы нам передать сообщение с помощью асимметричного шифрования, нам потребуется скачать приложение *OpenKeychain* на андроид.



Это Бесплатное мобильное приложение, которое позволяет пользователям шифровать, расшифровывать, подписывать и проверять подписи для текста, электронных писем и файлов.

Для того, чтобы нам передать сообщение с помощью симметричного шифрования, нам потребуется сайт *AES.*

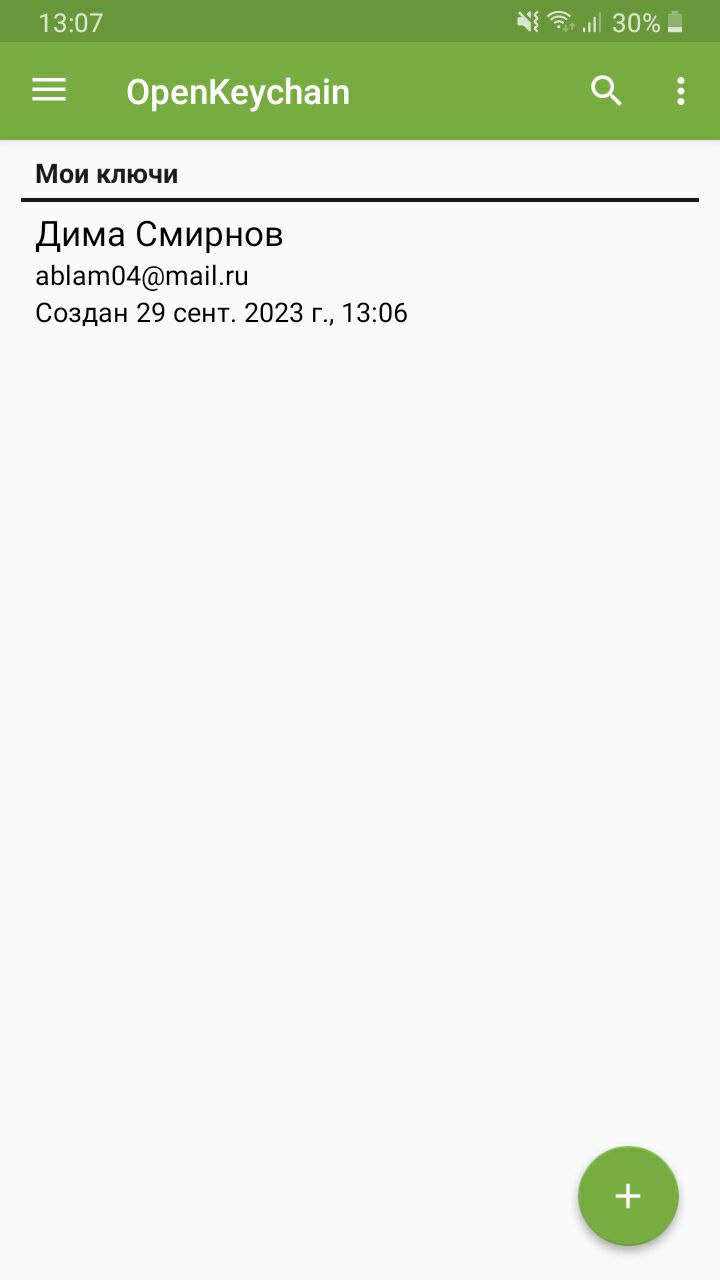
****

Работу выполнили студенты группы КТСО-03-22 Абламская Ксения Денисовна и Виноградова Полина Ильинична.

**Асимметричное шифрование**

Для начала нам потребуется создать ключ:

|  |  |
| --- | --- |
| 1.1 | 1.2 |
| 1.3 | 1.4 |



После этого мы можем поделиться открытым ключом с собеседником:

|  |  |
| --- | --- |
| 2.1 Копируем открытый ключ. | * 1. Делимся им с собеседником. |
| * 1. Собеседник делает то же самое. | 2.4 После обмена потребуется добавить этот открытый ключ себе. |
| 2.5 | 2.6 |
| 2.7 | 2.8 Ключ добавлен. |



Можем перейти к зашифровке сообщения,дальше к передаче и расшифровке:

|  |  |
| --- | --- |
| 3.1 | 3.2 |
| 3.3 | 3.4 |
| 3.5 | 3.6 |

Сообщение расшифровано

**Симметричное шифрование**

Позже с помощью асимметричного шифрования мы договорились о ключе, который будем использовать в дальнейших передачах сообщений.



Рис 4.1. Передача сообщения с помощью

Вывод: с помощью RSA и AES можно безопасно передавать сообщения по публичным каналам. Но поскольку AES работает быстрее RSA, рациональней договориться о ключе AES, шифруя сообщения с помощью RSA, а затем передавать сообщения, зашифрованные с помощью AES.