IV International Scientific Practical Conference of graduate and postgraduate students, lecturers «APPLIED ISSUES OF EXACT SCIENCES»
13-14 November 2020, Armavir

ПРИМЕНЕНИЕ КРИПТОГРАФИИ ДЛЯ ЦИФРОВЫХ КОСМИЧЕСКИХ СНИМКОВ

Фазылбекулы З[1)], Б.М. Ахмедов[2)], Ж.Б. Ракишев[3)], А.К. Муханбеткалиева[4)]

1) Магистрант кафедры «Космическая техника и технологии» Евразийского национального университета имени Л. Н. Гумилева, Нур-Султан, Казахстан, zeinbek97@mail.ru

2) Магистрант кафедры «Космическая техника и технологии» Евразийского национального университета имени Л. Н. Гумилева, Нур-Султан, Казахстан, batyrakhmedov@gmail.com

3) Доцент кафедры «Космическая техника и технологии» Евразийского национального университета имени Л. Н. Гумилева, Нур-Султан, Казахстан,
rakishev53@mail.ru

4) Доцент кафедры «Космическая техника и технологии» Евразийского национального университета имени Л. Н. Гумилева, Нур-Султан, Казахстан,
ainur-kanatm@mail.ru

Аннотация: В современных условиях развития общества роль цифровых технологий в различных отраслях неуклонно растет. Значимость информации, хранящейся на носителях, обрабатываемой приложениями или передаваемой по каналам связи для организаций и частных лиц, выходит на передний план. С другой стороны, критичность информации с точки зрения ее безопасности, секретности и потери заставляет применять те или иные методы обработки данных. Поэтому разработка, исследование и реализация систем, обеспечивающих все вышеперечисленное, представляются очень важными. Так же оно является важным для обеспечения безопасности снимкам дистанционного зондирования, так как к изображениям могут произвести несанкционированный доступ. Что может повлечь за собой крупные финансовые потери.

Ключевые слова: криптография, программа безопасности, космические снимки, дистанционное зондирования Земли.

USING CRYPTOGRAPHY FOR DIGITAL SATELLITE IMAGES

Fazylbekuli Z[1)], B. M. Ahmedov[2)], Zh. B. Rakishev[3)], A. K. Mukhanbetkaliyeva[4)]

1) Master's degree student of the Department of Space Engineering and Technologies, L.N. Gumilyov Eurasian National University, Nur-Sultan, Kazakhstan, zeinbek97@mail.ru
2) Master's degree student of the Department of Space Engineering and Technologies, L.N. Gumilyov Eurasian National University, Nur-Sultan, Kazakhstan, batyrakhmedov@gmail.com
3) Associate Professor of the Department of Space Engineering and Technologies, L.N. Gumilyov Eurasian National University, Nur-Sultan, Kazakhstan, rakishev53@mail.ru
4) Associate Professor of the Department of Space Engineering and Technologies, L.N. Gumilyov Eurasian National University, Nur-Sultan, Kazakhstan, ainur-kanatm@mail.ru

Abstract: In modern conditions of society's development, the role of digital technologies in various industries is steadily growing. The importance of information stored on media, processed by applications, or transmitted over communication channels for organizations and individuals comes to the fore. On the other hand, the criticality of information in terms of its security, secrecy, and loss makes it necessary to use certain methods of data processing. Therefore, the development, research and implementation of systems that provide all of the above are very important. It is also important to ensure the security of remote sensing images, as unauthorized access to the images may occur. This can lead to large financial losses.

Keywords: cryptography, security program, satellite images, remote Sensing of the earth.

Введение. Снимки дистанционного зондирования Земли (ДЗЗ) предполагают возможность исследования и непрерывного мониторинга Земли, способствующий результативно применять и использовать ее ресурсы. Снимки, отправленные спутниками ДЗЗ, применяют в многочисленных отраслях — аграрном хозяйстве, геологических и водных исследованиях, лесоводстве, охране окружающей среды, планировке территорий, в учебных и иных целях. Космические системы ДЗЗ дают возможность за быстрый период времени получить требуемые данные с крупных площадей (в том числе малодоступных и небезопасных зон).

Одним из методов обеспечения безопасности или секретности космических снимков является использование криптографии. Криптография — это наука о способах предоставления

конфиденциальности и аутентичности данных. Криптография содержит способы сокрытия данных, криптосистемы, несомненно, с открытым шифровальным ключом, системы электронно-цифровой подписи, хеширование, руководство ключами, приобретение тайных данных, а также квантовую криптографию.[1]

В нынешней криптографии применяют открытые ключи шифрования, которые рассчитаны на применение в электронно-вычислительных машинах. В нынешний период имеется около дюжины опробованных алгоритмов шифрования, которые при применении длинных ключей и хорошо реализованных алгоритмов сложно поддаются взлому. Современные системы обработки, передачи и хранения информации нередко используют различные средства шифрования. Повышение эффективности таких систем может быть достигнуто за счет интеграции криптоалгоритмов. Это позволяет уменьшить риск несанкционированного доступа к космическим снимкам, а также заметно повысить быстродействие их передачи, что является особенно актуальным в связи с постоянно увеличивающимся объемом информационных потоков.

Фундаментальным видом криптографического изменения данных является зашифровывание и расшифровывание. Зашифровывание – это изменение данных из раскрытой формы в недоступную (зашифрованную). Имеется также и противоположная процедура – расшифровывание. Весь процесс шифрования показан на рисунке 1.

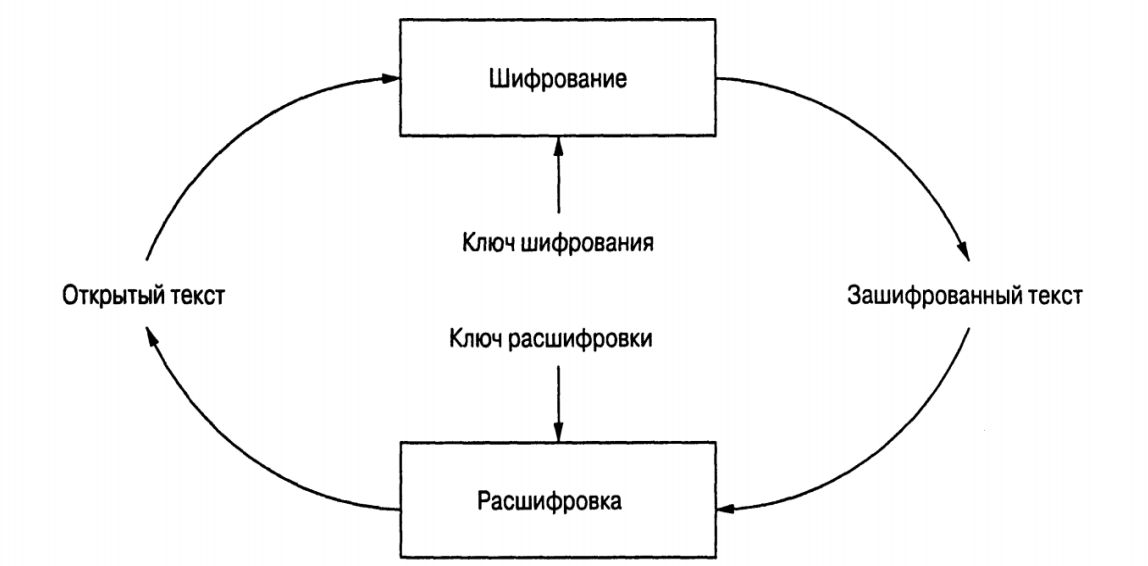

Рис. 1 - Упрощенная схема криптографической системы

В течение многовековой истории шифрования информации человека было создано много методов шифрования или шифров. Метод шифрования или шифр представляет собой набор обратимых преобразований передаваемой открытой информации в закрытый в соответствии с использованным алгоритмом шифрования. После появление компьютеров и CS инициировали процесс разработки новых шифров, которые учитывают возможности использования компьютеров для шифрования или дешифрования информации и для нападения на шифр. Взлом шифра (криптоанализ) - это процесс расшифровки частной информации, не зная ключа и, возможно, отсутствия информации об алгоритме шифрования.

В рамках данных требований, рассматриваются симметричные криптографические алгоритмы шифрования. Алгоритмы данной группы по сравнению с асимметрическими алгоритмами показывают наибольшую скорость, позволяют наращивать безопасность путем изменения параметров алгоритмов и многие из них имеют серьезное математическое обоснование, что позволяет доказать отсутствие возможных атак в ближайшем будущем.

Симметрический алгоритм шифрования - способ шифрования, в котором для шифрования и расшифровывания применяется один и тот же криптографический ключ. Ключ алгоритма должен сохраняться в секрете обеими сторонами.

В задаче архивации, вся необходимая информация будет храниться локально, передач ключа не потребуется, что повышает безопасность системы в целом и ещё раз подтверждает в необходимости использования именно симметричных алгоритмов.

Для сравнения были отобраны наиболее распространенные алгоритмы симметрического шифрования, основываясь на исследованиях NIST от 2 января 1997 года и существующих наработок для отечественных стандартов:

1. Rijndael (англ. Advanced Encryption Standard) - американский стандарт шифрования
2. DES (англ. Data Encryption Standard) - стандарт шифрования данных в США до AES
3. RC6 (Шифр Ривеста)
4. BlowFish

Некоторые из вышеперечисленных алгоритмов: DES,3DES, Rigndael, RC6 были реализованы программно. Интерфейс программы показан на рисунке 2.

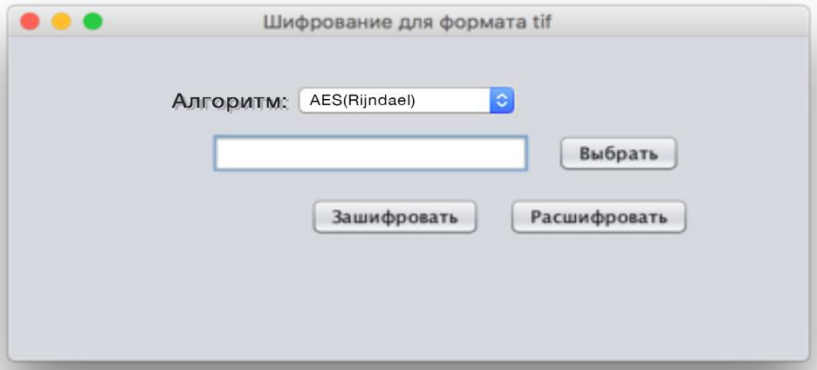

Рис. 2 - Интерфейс программы «Демонстрация симметричных шифров»

В поле алгоритм имеется возможность выбора алгоритма из предложенного списка: DES, Rijndael, 3DES, RC6. В поле размер ключа пользователь может выбрать длину ключа. Пароль был записан в программу для полного сокрытия ключа, так как ключ алгоритма должен сохраняться в секрете обеими сторонами. В поле входной файл выбирается директория местонахождения файла, который необходимо зашифровать, в поле выходной файл прописываем директорию зашифрованного файла и даем ему имя.

Программа была разработана на языке программирования Java на среде разработки IntelliJIDEA. Для использования разработанной программы необходимо иметь операционную систему Windows или macOS, а также установленный JDK не ниже десятой версии.

Интерфейс программы был выполнен с минимальными количеством кнопок для удобства. На рисунке №3 показан интерфейс в котором находится кнопка «Выбрать» предназначенная для указания пути нахождения цифрового космического снимка формата .tiff. Ниже имеются две кнопки «Зашифровать» и «Расшифровать» которые имеют одноименные функции.

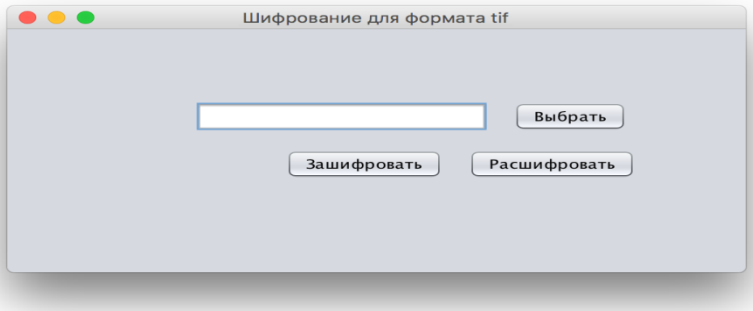

Рис. 3 - Интерфейс программы для шифрования цифровых космических снимков

При нажатии на кнопку «Выбрать» появляется окно в котором необходимо указать путь расположения цифрового космического снимка и выбрать его кликнув на необходимый файл и нажать на кнопку «Open» расположенный ниже. Рис № 4

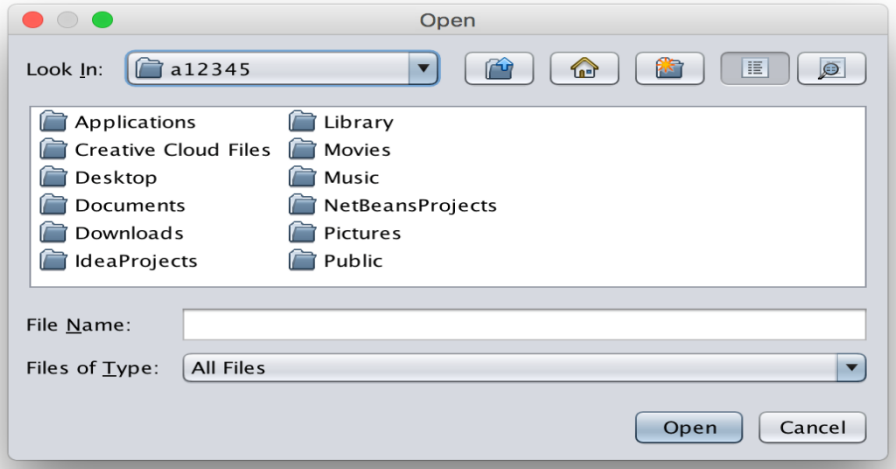

Рис. 4 - Выбор цифрового космического снимка.

Вывод. Изучив теоретические аспекты о криптографии, проведя полный анализ существующих алгоритмов, рассмотрев вопросы по технологии разработки программы, техники безопасности и охране труда, были сделал выводы о необходимости внедрения программы по защите цифровых космических снимков.

Проведя анализ существующих алгоритмов шифрования, было выбрано четыре симметричных алгоритмов. Симметричные алгоритмы показывают более высокое быстродействие чем алгоритмы с открытым ключом шифрования. Был выбран алгоритм шифрования AES(Rijndael) который совпадал по требованиям безопасности, скорости и криптостойкости.

Список использованных источников:

1. Введение в криптографию. Под общей редакцией В. В. Ященко. Издание 4-е, дополненное. МЦНМО, М., 2012.
2. О. Н. Василенко. Теоретико-числовые алгоритмы в криптографии. МЦНМО, М., 2003 (1-е изд.), 2006 (2-е изд.).
3. Х. К. А. Ван Тилборг. Основы криптологии. Профессиональное руководство и интерактивный учебник. Мир, М., 2006.
4. Т. В. Кузьминов. Криптографические методы защиты информации. Наука, Сибирское предприятие РАН, Новосибирск, 1998.
5. Ю. Лифшиц. Курс лекций «Современные задачи криптографии».
6. Савитч, Уолтер Язык Java. Курс программирования / Уолтер Савитч. - М.: Вильямс, 2015. - 928 с.
7. Шилдт, Герберт Java 8. Руководство для начинающих / Герберт Шилдт. - М.: Вильямс, 2015. - 720 с.
8. Эккель, Брюс Философия Java / Брюс Эккель. - М.: Питер, 2016. - 809 с.