УДК 004 **Информационные технологии**

Ковтушенко Александр Петрович, *кандидат физико-математических наук, доцент кафедры «Программное обеспечение ЭВМ и информационные технологии», МГТУ имени Н.Э. Баумана, Россия, г. Москва*

E-mail: sasha@bmstu.ru

Сидоров Егор Александрович, *студент магистратуры, 2 курс, кафедра «Программное обеспечение ЭВМ и информационные технологии», МГТУ имени Н.Э. Баумана, Россия, г. Москва*

E-mail: sega-96@mail.ru

ОЦЕНКА ВРЕМЕННОЙ СЛОЖНОСТИ НЕКОТОРЫХ СИММЕТРИЧНЫХ АЛГОРИТМОВ ШИФРОВАНИЯ

Аннотация: В статье представлен обзор временной сложности часто используемых криптографических алгоритмов с длинами ключей от 64 до 256 байт, таких, как Twofish, DES, TDES, AES. Оценка временной сложности производится с помощью замеров времени до и после шифрации и дешифрации. Алгоритмы реализованы на языке C++ в однопоточном режиме.

Ключевые слова: Twofish, DES, TDES, AES, шифрование, дешифрация, временная сложность, криптография, C++.

Abstract: The article provides an overview of the time complexity of frequently used cryptographic algorithms with key lengths from 64 to 256 bytes, such as Twofish, DES, TDES, AES. Evaluation of time complexity is using measurements of time before and after encryption and decryption. Algorithms are implemented by C++ language in single-threaded mode.

Keywords: Twofish, DES, TDES, AES, encryption, decryption, time complexity, cryptography, C++.

Введение

Для безопасной передачи данных в интернет сетях, перед специалистами стоит задача шифрования передаваемых данных. Существует множество алгоритмов шифрования, позволяющих решить эту задачу, но каждый из них требует разных временных затрат.

Для исследования, были выбраны алгоритмы симметричного шифрования [1]: *TwoFIsh, DES, TDES, AES*. Каждый из этих алгоритмов основан на сети Фейстеля [2], и каждый находит применение в различных системах, что говорит об их практической безопасности и применимости.

В рамках данной статьи будет оценена временная сложность алгоритмов на основе замеров времени до и после их работы на основе работы блочного шифра в режиме ECB [3].

Описание используемых алгоритмов

1. TwoFish шифрование Алгоритм представлен в 1997 Национальным Институтом Стандартов и Технологий в результате попытки модифицировать алгоритм Blowfish. Принимает данные блоками, размером 128 бит и ключ любой длины до 256 бит. Обычно, реализуется прием ключей длиной 128, 192 и 256 бит. Twofish работает быстро как на 32-битных и 64-битных, так и на 8-битных процессорах (смарт-картах, встроенных чипах и т. д.). Алгоритм может использоваться в сетевых приложениях, где ключи часто меняются, и в приложениях, где мало ОЗУ и ПЗУ. Входной 128 битный блок разбивается на четыре 32-битных, над которыми, после процедуры отбеливания, происходит 16 раундов преобразования с применением функции g1.

Процедура отбеливания представляет из себя выполнение операции XOR над данными до и после 16 раундов обработки, эта процедура заметно усложняет подбор ключей.

Подробное описание алгоритма можно прочитать в статье [4].

---

[1] 64 – битная перестановка, зависящая от ключа.

2. DES шифрование

Алгоритм был представлен в 1977 году, и в его основе лежит сеть Фейстеля. Алгоритм DES шифрует информацию блоками по 64 бита с помощью 64-битного ключа шифрования, в котором используется только 56 бит, и 8 бит для проверки.

DES основан на двух фундаментальных атрибутах криптографии: замена и транспозиция. DES состоит из 16 раундов, на каждом из которых выполняются шаги замещения и транспонирования.

При расшифровке данных используется тот же ключ, и осуществляется в обратном порядке, по отношению к шифрованию. Подробнее прочитать про алгоритм можно по ссылке [5].

3 TDES шифрование

Симметричный блочный криптографический алгоритм, созданный на основе алгоритма DES с целью устранения главного недостатка — малой длины ключа - 56 бит. Принцип работы TDES не отличается от применяемого в DES: наращивание криптостойкости было достигнуто благодаря трехкратному шифрованию одного блока алгоритмом DES. Три 56-разрядных ключа, используемых в данном процессе, объединяются алгоритмом в один 168-разрядный ключ.

4 AES шифрование

Данный алгоритм является американским стандартом шифрования, опубликован в 2001 году. Имеет возможность задания длины ключа размером 128, 192 и 256 бит. Одной из целью алгоритма была замена DES из-за малой длины ключа, поскольку алгоритм DES уже удавалось взломать [6].

AES состоит из ряда связанных операций, некоторые из которых включают замену входов конкретными выходами (подстановки), а другие - перемешивание битов (перестановок). AES выполняет все свои вычисления в байтах, а не в битах. Следовательно, он обрабатывает 128 битов блока открытого текста как 16 байтов. Эти 16 байтов расположены в четыре столбца и четыре строки для обработки в виде матрицы. В отличие от DES, количество раундов в AES

является переменным и зависит от длины ключа. AES использует 10 раундов для 128-битных ключей, 12 раундов для 192-битных ключей и 14 раундов для 256-битных ключей. Каждый из этих раундов использует различный 128-битный ключ раунда, который рассчитывается из исходного ключа AES. Подробная информация об алгоритме в статье [7].

Результаты работы

Для сравнения результатов шифрования были созданы три текстовых файла размерами 1, 10 и 100 кбайт (рисунок 1,2,3) и реализованы 4 рассмотренных алгоритма шифрования на языке C++ с вычислением затраченного времени. Учитывалось время непосредственно работы алгоритма, без загрузки данных. С исходным кодом для измерений можно ознакомиться по ссылке [8].

Каждый из алгоритмов работает в однопоточном режиме.

В таблице 1 представлены результаты тестирования для каждого алгоритма.

Таблица 1 - Время, затрачиваемое на шифрование и дешифрацию

Размер входного файла	Время, мс					
	AES 128 bit	AES 192 bit	AES 256 bit	DES 64 bit	TDES 192 bit	Twofish 256 bit
1 кбайт	716	825	954	678	1971	227
10 кбайт	7093	8440	9379	6713	18881	2165
100 кбайт	71358	82618	93753	64389	190340	22411

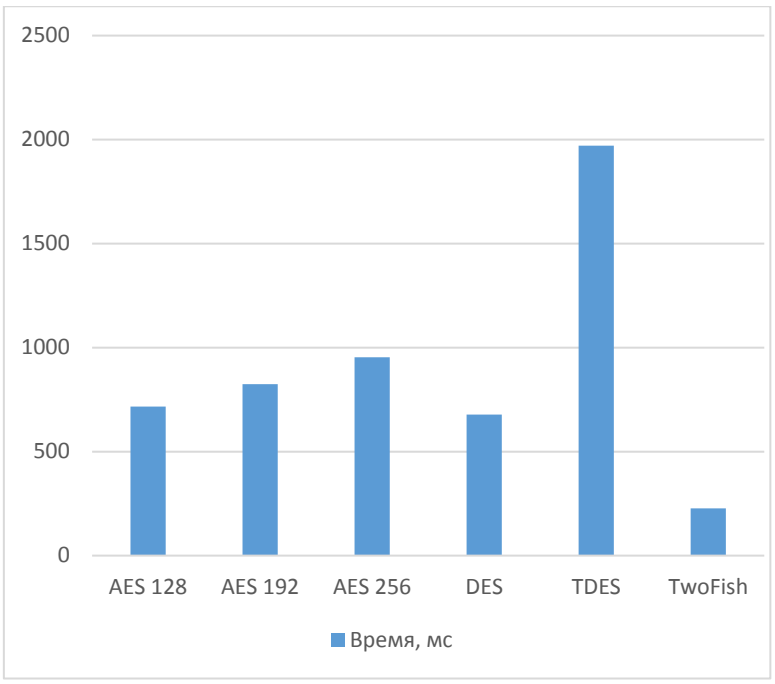

Рисунок 1 - График распределения времени шифровании и дешифрации входного файла 1 кбайт.

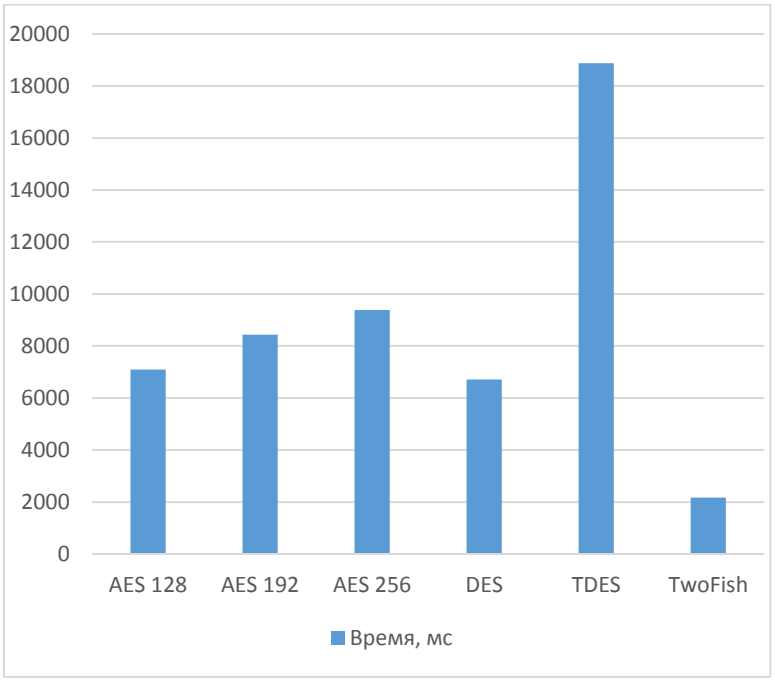

Рисунок 2 - График распределения времени шифровании и дешифрации входного файла 10 кбайт

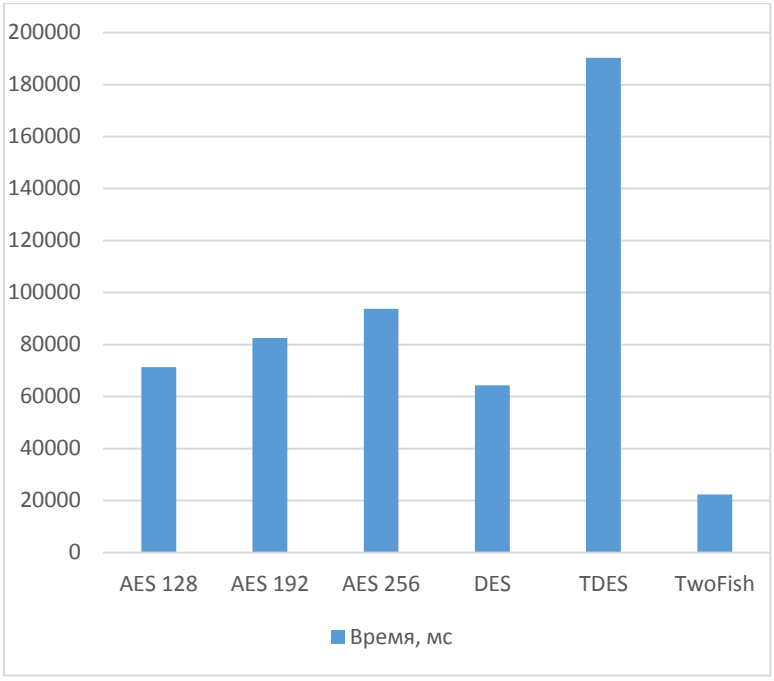

Рисунок 3- График распределения времени шифровании и дешифрации входного файла 100 кбайт

Заключение

Использование нескольких тестов с различными текстами для шифрования показало одинаковое соотношение. Twofish значительно быстрее всех рассматриваемых алгоритмов, разница с самым медленным, TDES приблизительно в 9 раз. Алгоритм DES примерно в 3 раза медленнее алгоритма Twofish, и примерно в 3 раза быстрее TDES, при их разнице в размере ключа в 3 раза. Алгоритмы AES с длинами ключей 128,192 и 256 бит отличаются между собой по скорости приблизительно на 15%, но AES 128 бит медленнее DES примерно на 5%.

Библиографический список:

1. Симметричные алгоритмы шифрования [Электронный ресурс] URL: https://studme.org/94398/informatika/simmetrichnye_algoritmy_shifrovaniya (дата обращения: 03.05.2020).

2. Сеть Фейстеля [Электронный ресурс] URL: https://xakep.ru/2016/04/21/crypto-part3/#toc04 (дата обращения: 03.05.2020).

3. Описание ECB [Электронный ресурс] URL: http://cryptowiki.net/index.php?title=Electronic_Code_Book (дата обращения: 03.05.2020).

4. Описание алгоритма Twofish [Электронный ресурс] URL: https://studfile.net/preview/2807205/page:23/ (дата обращения: 03.05.2020).

5. Описание алгоритма DES [Электронный ресурс] URL: http://protect.htmlweb.ru/des.htm (дата обращения: 03.05.2020).

6. Взлом шифра алгоритма DES за 3 дня [Электронный ресурс] URL: https://www.osp.ru/cw/1998/28-29/30844/ (дата обращения: 03.05.2020).

7 Описание алгоритма AES [Электронный ресурс] URL: https://ru.bmstu.wiki/AES_(Advanced_Encryption_Standard) (дата обращения: 03.05.2020).

8. Исходный код сравнения алгоритмов шифрования [Электронный ресурс] URL: https://github.com/EgorSidorov/-EncryptionAlgorithmComparison (дата обращения: 03.05.2020).