Федеральное государственное образовательное бюджетное учреждение высшего образования

«ФИНАНСОВЫЙ УНИВЕРСИТЕТ ПРИ ПРАВИТЕЛЬСТВЕ

РОССИЙСКОЙ ФЕДЕРАЦИИ»

(Финансовый университет)

**Колледж информатики и программирования**

Отчёт по практическому занятию№8 по дисциплине

МДК.02.02 «Криптографические средства и методы защиты информации»

На тему: «Программная реализация симметричного криптографического алгоритма Blowfish»

Студентов группы *3ОИБАС-1221*

|  |  |
| --- | --- |
| Бажанов Данила Иванович  Огир Алексей Алексеевич  Бугаев Андрей | «20» января 2024 г. |

Основная профессиональная образовательная программа по специальности

10.02.05 Обеспечение информационной безопасности автоматизированных систем

Форма обучения очная

Проверил: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ Рой А.В.

Москва 2023

### СОДЕРЖАНИЕ

[ВВЕДЕНИЕ 3](#_Toc159333004)

[BLOWFISH 4](#_Toc159333005)

[ПРИМЕНЕНИЕ ПРОГРАММНОЙ РЕАЛИЗАЦИИ СИММЕТРИЧНОГО КРИПТОГРАФИЧЕСКОГО АЛГОРИТМА BLOWFISH 7](#_Toc159333006)

[ЗАКЛЮЧЕНИЕ 9](#_Toc159333007)

[СПИСОК ЛИТЕРАТУРЫ 10](#_Toc159333008)

### ВВЕДЕНИЕ

Симметричное шифрование является одним из основных методов защиты информации от несанкционированного доступа. Одним из наиболее популярных алгоритмов симметричного шифрования является Blowfish. Этот алгоритм был разработан в 1993 году и отличается высокой скоростью работы и хорошей стойкостью к взлому. Программная реализация алгоритма позволяет обеспечить безопасность передаваемой информации и защитить конфиденциальные данные от кибератак.

Целью работы является изучение программной реализация симметричного криптографического алгоритма Blowfish.

Объектом исследования является программная реализация алгоритма Blowfish.

Предметом исследования являются разработка и тестирование программной реализации симметричного криптографического алгоритма Blowfish для защиты данных.

### BLOWFISH

Blowfish (произносится [бло́уфиш]) — криптографический алгоритм, реализующий блочное симметричное шифрование с переменной длиной ключа. Разработан Брюсом Шнайером в 1993 году. Представляет собой сеть Фейстеля. Выполнен на простых и быстрых операциях: XOR, подстановка, сложение. Является незапатентованным и свободно распространяемым.

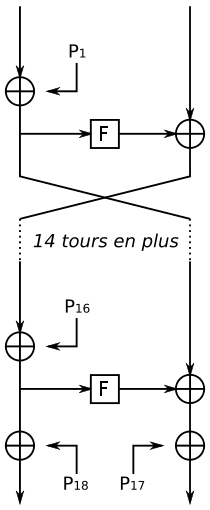


Рисунок 1. Blowfish.

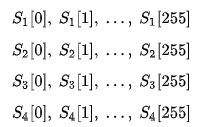
До появления Blowfish существовавшие алгоритмы были либо запатентованными, либо ненадёжными, а некоторые и вовсе держались в секрете (например, Skipjack). Алгоритм был разработан в 1993 году Брюсом Шнайером в качестве быстрой и свободной альтернативы устаревшему DES и запатентованному IDEA. По заявлению автора, критериями проектирования Blowfish были:

* скорость (шифрование на 32-битных процессорах происходит за 26 тактов);
* простота (за счёт использования простых операций, уменьшающих вероятность ошибки реализации алгоритма);
* компактность (возможность работать в менее, чем 5 Кбайт памяти);
* настраиваемая безопасность (изменяемая длина ключа).

Алгоритм состоит из двух частей: расширение ключа и шифрование данных. На этапе расширения ключа исходный ключ (длиной до 448 бит) преобразуется в 18 32-битовых подключей и в 4 32-битных S-блока, содержащих 256 элементов. Общий объём полученных ключей равен (18+256\*4)\*32=33344 бит или 4168 байт

**Параметры**

* секретный ключ K (от 32 до 448 бит)
* 32-битные ключи шифрования 
* 32-битные таблицы замен 



Функция F(x) принимает на вход блок размером в 32 бита и проделывает с ним следующие операции:

32-битный блок делится на четыре 8-битных блока(X\_{{1}},X\_{{2}},X\_{{3}},X\_{{4}}), каждый из которых является индексом массива таблицы замен S\_{{1}}-S\_{{4}}значенияS\_{{1}}[X\_{{1}}] и S\_{{2}}[X\_{{2}}] складываются по модулю 2^{32}, после складываются по модулю 2 с S\_{{3}}[X\_{{3}}] и, наконец, складываются с S\_{{4}}[X\_{{4}}] по модулю 2^{32}.

Результат этих операций — значение F(x).



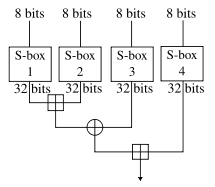


Рисунок 2. Функция F(x) в Blowfish.

Blowfish представляет собой Сеть Фейстеля, состоящую из 16 раундов. Алгоритм шифрования блока X размером 64 бит выглядит следующим образом:

Разделение входного блока X на 2 32-битных блока L\_{{0}},R\_{{0}}

Для i=1\ ...\ 16:

{\displaystyle L\_{i}\ =\ L\_{i-1}\oplus P\_{i}}

{\displaystyle R\_{i}\ =\ R\_{i-1}\oplus F(L\_{i})}

После 16 раунда L\_{{16}}\ ,\ R\_{{16}} меняются местами:

R\_{{16}}\ \leftleftarrows \ L\_{{16}}\ \ L\_{{16}}\ \leftleftarrows \ R\_{{16}}

К получившимся блокам прибавляютсяP\_{{17}} и P\_{{18}}

L\_{{17}}=L\_{{16}}\oplus P\_{{18}}

R\_{{17}}=R\_{{16}}\oplus P\_{{17}}

Выходной блок Y равен конкатенации (объединению) L\_{{17}} и R\_{{17}}.

### ПРИМЕНЕНИЕ ПРОГРАММНОЙ РЕАЛИЗАЦИИ СИММЕТРИЧНОГО КРИПТОГРАФИЧЕСКОГО АЛГОРИТМА BLOWFISH

Изображение выглядит как текст, снимок экрана, программное обеспечение, Мультимедийное программное обеспечение

Автоматически созданное описание

Рисунок 3. Зашифрованный текст.

Изображение выглядит как текст, снимок экрана, программное обеспечение, Значок на компьютере

Автоматически созданное описание

Рисунок 4. Генерация ключей для шифрования Blowfish.

Изображение выглядит как текст, снимок экрана, программное обеспечение, Мультимедийное программное обеспечение

Автоматически созданное описание

Рисунок 5. Инициализация на основе шестнадцатеричной мантиссы числа ПИ.

### ЗАКЛЮЧЕНИЕ

В ходе выполнения данной работы были выполнены следующие задачи:

1. Зашифровали ФИО участников группы;
2. Изучили метод шифрования BLOWFISH;
3. Провели инициализацию ключей для шифрования в Blowfish.

### СПИСОК ЛИТЕРАТУРЫ

Andrey Breeze На пути к Skein: просто и понятно про Blowfish / Andrey Breeze [Электронный ресурс] // habr: [сайт]. — URL: https://habr.com/ru/articles/140394/ (дата обращения: 20.02.2024).

Abhay Bhat Blowfish Algorithm with Examples / Abhay Bhat [Электронный ресурс] // geeksforgeeks: [сайт]. — URL: https://www.geeksforgeeks.org/blowfish-algorithm-with-examples/ (дата обращения: 20.02.2024).

Анастасия Береснева Современные зарубежные шифры / Анастасия Береснева [Электронный ресурс] // xaker: [сайт]. — URL: https://xakep.ru/2016/06/30/crypto-part4/ (дата обращения: 20.02.2024).