1. Цель

Вариант 25.

Реализовать алгоритм шифрования Blowfish, предусмотреть возможность работы алгоритма в режиме CFB.

Исследовать процесс распространения ошибок в реализуемом режиме шифрования, привести пример распространения ошибок. По результатам анализа сделать выводы о качестве реализованных систем шифрования.

Вычислить коэффициент корреляции для входного и выходного потока алгоритма шифрования, оценить распределение «0» и «1» в выходном потоке.

2. Описание алгоритма

Blowfish — алгоритм 64-битного блочного шифра с ключом переменной длины. Был разработан известным специалистом в области криптографии и защиты информации Брюсом Шнайером в 1993 году.

В общем случае алгоритм состоит из двух этапов — расширение ключа и шифрация/дешифрация исходных данных. Алгоритм шифруется данные 64-битными блоками. Размер ключа алгоритма является переменным – от 32 до 448 битов.

Алгоритм представляет собой сеть Фейстеля (рисунок 1). Шифрование данных выполняется в 16 раундов, в каждом из которых над левым 32-битным субблоком данных производятся следующие действия:

- Значение субблока складывается с ключом *i*-го раунда K*i* операцией XOR, результат становится новым значением субблока;
- Субблок обрабатывается функцией F, результат обработки накладывается на правый субблок операцией XOR;
- Субблоки меняются местами во всех раундах, кроме последнего.

После 16 раундов выполняется наложение на субблоки еще двух подключей: K_{17} и K_{18} складываются операцией XOR с правым и левым

субблоками соответственно.

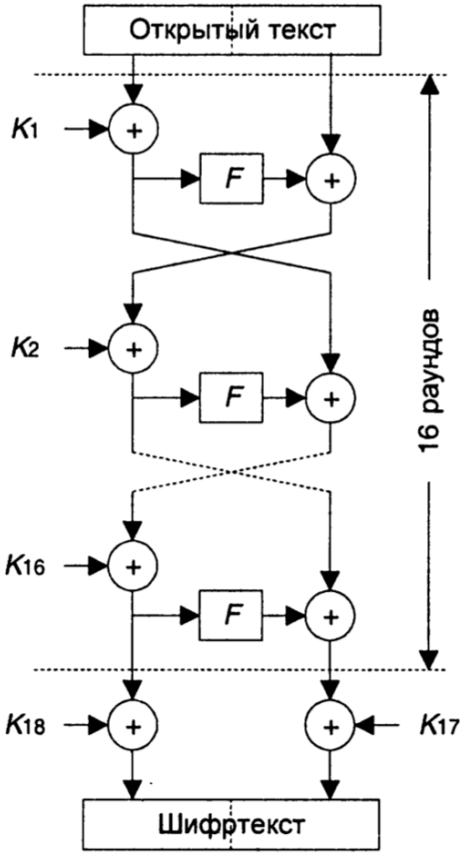

Рисунок 1 – Структура алгоритма Blowfish

Функция F обрабатывает субблок следующим образом (рис. 2):

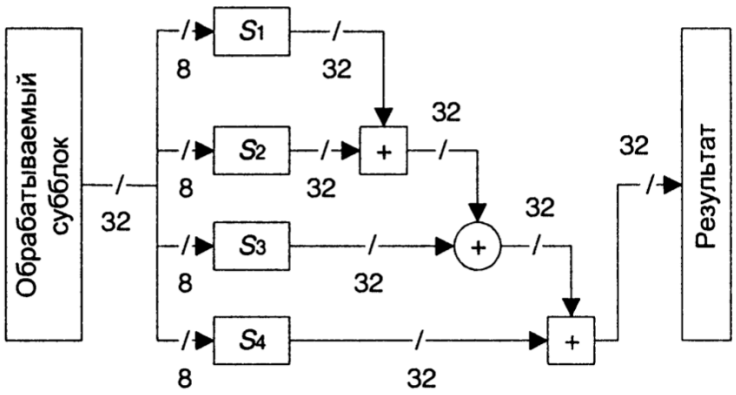

Рисунок 2 - Функция F

Расшифровывание выполняется аналогично зашифровыванию, но ключи используются в обратном порядке.

3. Процедура расширение ключа

Задача процедуры расширения ключа состоит в вычислении на основе

ключа шифрования значений ключей раундов $K_1 \ldots K_{18}$ и таблиц замены $S_1 \ldots S_4$. Для этого используется процедура расширения ключа, состоящая из следующих шагов:

- Исходные значения ключей раундов и таблиц замен инициализируются фиксированной псевдослучайной строкой, в качестве которой используется шестнадцатеричная запись дробной части числа pi;
- Операцией XOR на K_1 накладываются первые 32 бита ключа шифрования, на K_2 – следующие 32 бита и т.д. до K_{18}. Если используется более короткий ключ шифрования, то ключ шифрования накладывается циклически;
- С использованием полученных ключей раундов и таблиц замены выполняется шифрования алгоритмом Blowfish блока данных, состоящего из 64 нулевых битов. Результат становится новым значением ключей K_1 и K_2;
- Результат предыдущего этапа снова шифрует алгоритмом Blowfish (причём уже с изменёнными значениями ключей K_1 и K_2), в результате получаются новые значения ключей K_3 и K_4;
- Шифрование выполняется до тех пор, пока новыми значениями не будут заполнены все ключи раундов и таблицы замен.

4. Режим шифрования CFB

В режиме CFB *i*-й блок шифротекста формируется путем шифрования (*i - 1*)-го блока шифротекста и его суммированием (операция XOR) с *i*-м блоком открытого текста.

Шифрование может быть описано следующим образом:

$$C_0 = IV$$
$$C_i = E_k\left(C_{i-1}\right) \oplus P_i$$
$$P_i = E_k\left(C_{i-1}\right) \oplus C_i$$

Где i - номер блоков, IV - вектор инициализации, C_i и P_i - блоки зашифрованного и открытого текстов соответственно, а E_k - функция блочного шифрования.

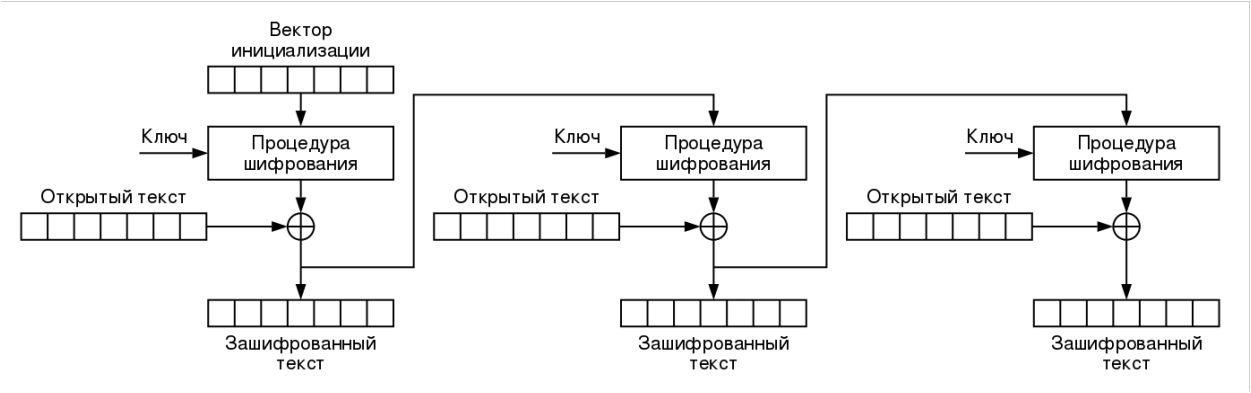

Рисунок 3 - Шифрование в режиме CFB

Криптостойкость CFB определяется криптостойкостью используемого шифра. Фиксируемые блоки открытого текста «маскируются» блоками шифротекста. Скорость шифрования CFB-режима с полноблочной обратной связью та же, что и у блочного шифра, причем возможности распараллеливания процедуры шифрования ограничены.

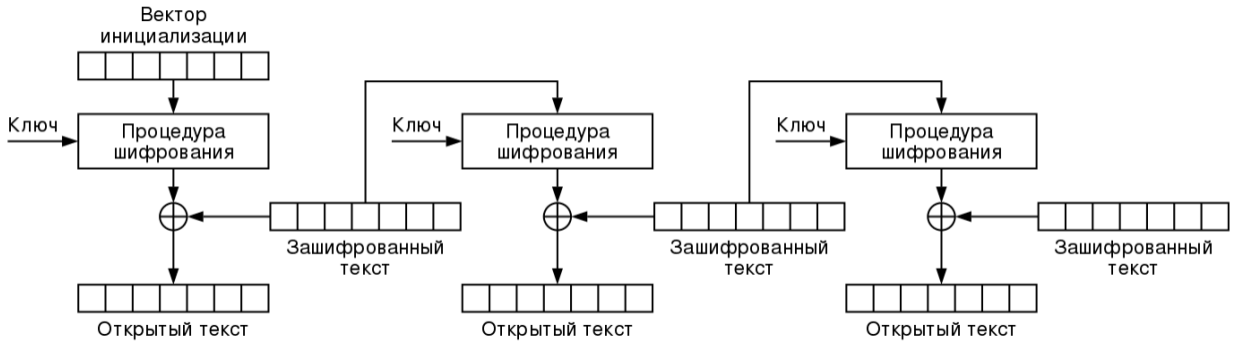

Рисунок 4 - Дешифрование в режиме CFB

5. Описание реализации

На входе программа просит сгенерировать рандомный ключ или задать ключ самостоятельно. Затем программа считывает из файла поблочно данные и шифрует/дешифрует его, в зависимости от того, в каком режиме программа работает на данный момент. После этого, программа выводит в файл

шифрованные/дешифрованные данные (текст/изображение).

6. Примеры

Пример шифрования текста в CFB режиме шифрования.

Ключ шифрования: blowfish

Исходный текст в файле:

```
I try to enjoy each season. But my favourite season is autumn. Beautiful autumn flowers make the
first cool days more pleasant. The early autumn is often called "Indian Summer". The silver gossamer
is flying in the air, the trees are gold and brown, and the sky looks extremely blue. Many people
like these last warm days of the year. The fruit trees are heavy with juicy apples, almost all fruits
and vegetables could be seen in the market. It is pleasant to stay at home with an interesting book
and a cup of coffee on an autumn gloomy day. Late autumn sometimes brings frost and soon soft, white
snow covers everything around.
```

Рисунок 5 - Исходный текст

Зашифрованный текст:


```
E^pЌ^n2m^•∗€Ksf69§цЯIE§эГЃ,оп8Ќ`CЇ©≤ЏЫr"ΔЌcc:lu€JZЉxXЋqёШщ
ЬiƒTA№:шцЫ]K?`—ЬAF8BXjC3∞ЎЁпрGLЮeY≥Pue]√¬Cz$Q>`08Ї—BK£»'cEњ'oЌr\6л¬бФTLФCeAЋIЩe§п#cз:KCH/h…
9JHЊй89Эn<Э2soҐ{ЪчUOOY7г¬њЬ√      ƒ»
&i:µтЂRpћч£4ЪI€zЭ∗qП1qҐzымc2Iт.&I eВљXeќK§Q_Bfё PЯЖ°EI®m§(Hя∗)ўPv±S7Б i8з_мрЪёKxтнTЖїЉЯноV%ON#bbxgSs5
4]1љґ ҐcЋ≈}_){л`
√zJ>Ъ°ќsћ|'n€ЖC©E)%FH£ї[∞Ё'Fљ|≥3VOьm\"H€еnIA/ЎX8cГїБvч0"ЩВ'Бy7Bs„iЎ3'Wш+5c≈[<Ѓdк$Ѓќзящ:њїў8!їэt¶|ct"
≤xЊ"^tиA–fjO+O†н'Mґ"N©йИµ(Eъp"°NO`;лS≠_R`RiЫд_Z]®;Xф…0p≈ыy\£_KЁxΔxЗЫУЙ№У(oУЛ1Ш…gвC&'I%|Ѓ/@wmЧЂJф"
O3tpҐмиас√∗Δ_≈_
T≠≥Jy–¶Љ]}]Д№iX√M2N†~BЉ~Oh€p√
```


Рисунок 6 - Зашифрованный текст

Расшифрованный текст:

```
I try to enjoy each season. But my favourite season is autumn. Beautiful autumn flowers make the
first cool days more pleasant. The early autumn is often called "Indian Summer". The silver gossamer
is flying in the air, the trees are gold and brown, and the sky looks extremely blue. Many people
like these last warm days of the year. The fruit trees are heavy with juicy apples, almost all fruits
and vegetables could be seen in the market. It is pleasant to stay at home with an interesting book
and a cup of coffee on an autumn gloomy day. Late autumn sometimes brings frost and soon soft, white
snow covers everything around.
```

Рисунок 7 - Расшифрованный текст

Рисунок 8 - Исходное изображение

Проведем шифрование, используя режим CFB. Результат шифрования представлен на рисунке 9.

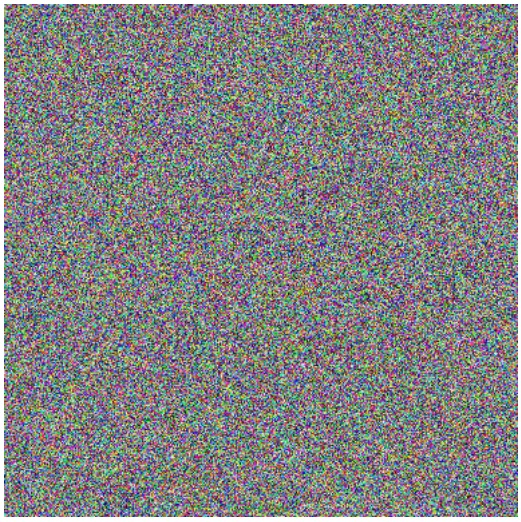

Рисунок 9 - Зашифрованное изображение

Результат дешифрования представлен на рисунке 10. Как можно заметить, он идентичен входному изображению.

Рисунок 10 - Дешифрованное изображение

Если зашифрованный файл будет как-либо повреждён (рисунок 11), то и дешифрованный файл будет отличаться от исходного (рисунок 12).

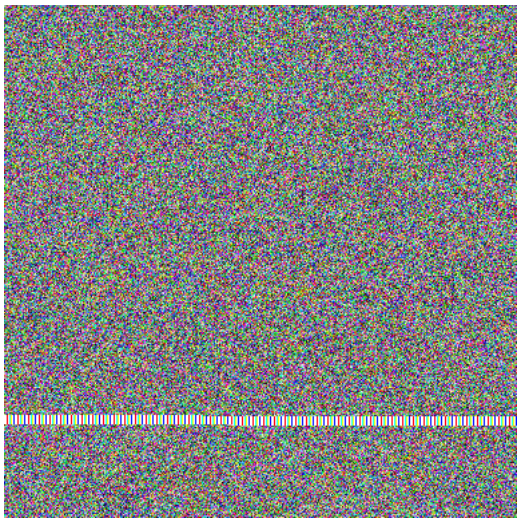

Рисунок 11 - Поврежденное зашифрованное изображение

Рисунок 12 - Восстановленное изображение

7. Коэффициент корреляции для входного и выходного потока алгоритма шифрования

Вычислим коэффициент корреляции для красной компоненты исходного и закодированного изображения.

Формула для подсчета коэффициента корреляции представлена ниже:

$$\hat{r}_{A,B} = \frac{\hat{M}[(A - \hat{M}[A])(B - \hat{M}[B])]}{\hat{\sigma_A}\hat{\sigma_B}},$$

где A и B – компоненты изображения;

M[.] – оценка математического ожидания в соответствии с формулой:

$$\hat{M}[I^{(A)}] = \frac{1}{WH}\sum_{i=1}^{H}\sum_{j=1}^{W} I_{i,j}^{(A)},$$

где σ_A и σ_A – оценки среднеквадратичного отклонения компонент A и B, вычисляемого по формуле:

$$\hat{\sigma_A} = \sqrt{\frac{1}{WH-1}\sum_{i=1}^{H}\sum_{j=1}^{W}\left(I_{i,j}^{(A)} - \hat{M}[I^{(A)}]\right)^2}.$$

По результатам вычислений, коэффициент корреляции для красной компоненты исходного и закодированного изображения составил 0.003268387771232692.

8. Оценка распределения «0» и «1» в выходном потоке

Оценим распределение «0» и «1» на примере зашифрованного изображения, представленного на рисунке 9:

- 0 – 50.0562 %
- 1 – 49.9438 %

9. Вывод

Реализован алгоритм шифрования Blowfish, а также режим шифрования CFB. Исследован процесс распространения ошибок в реализуемом режиме шифрования. Вычислен коэффициент корреляции.

Достоинства алгоритма:

- Высокая скорость шифрования на развернутом ключе;
- Простота алгоритма, снижающая вероятность ошибок при его реализации;
- Отсутствие известных успешных атак на полнораундовую версию алгоритма.

Недостатки алгоритма:

- Алгоритм не годится для применения в случаях, где требуется частая смена ключей, так как процедура расширения ключа является достаточно ресурсоемкой;
- Невозможность расширения ключа параллельно процессу шифрования;
- Небольшой по современным меркам размер блока шифруемых данных.

10. Список литературы

[1] Б. Я. Рябко и А. Н. Фионов, Основы современной криптографии для специалистов информационных технологиях, Москва: Научный мир, 2004.

[2] С. П. Панасенко, Алгоритмы шифрования. Специальный справочник, Санкт-Петербург: БХВ-Петербург, 2009.

[3] А.Л. Чмора Современная прикладная криптография, Гелиос АРВ, 2002