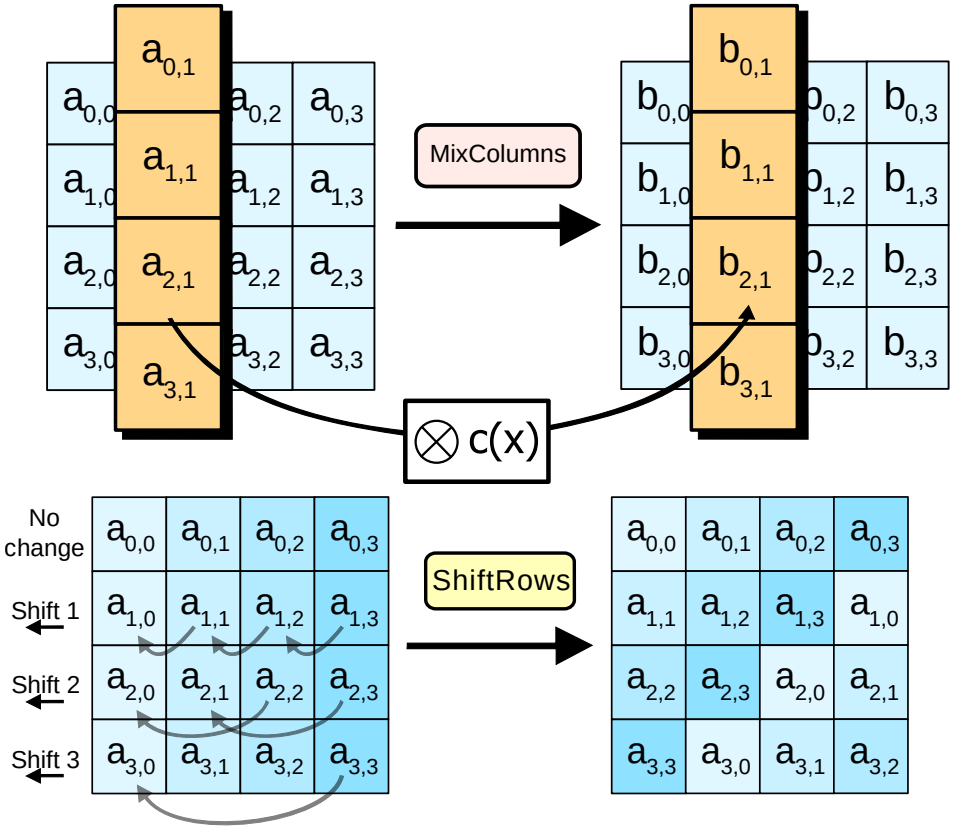
Лабораторная работа 4

Януш Герман
Алексей Ясинецкий
Екатерина Ермолаева

5 мая 2021 г.

Мы реализовали шифр AES на C#.



1 Вывод программы

```
Результаты тестов при случайном ключе и случайном открытом тексте:
Частотный побитовый тест пройден.
```

```
Тест на одинаковые идущие подряд биты пройден.
Тест на самую длинную последовательность из единиц в блоке пройден.

Результаты тестов при случайном ключе и открытом тексте с малым весом:
Частотный побитовый тест пройден.
Тест на одинаковые идущие подряд биты пройден.
Тест на самую длинную последовательность из единиц в блоке пройден.

Результаты тестов при случайном ключе и открытом тексте с большим весом:
Частотный побитовый тест пройден.
Тест на одинаковые идущие подряд биты пройден.
Тест на самую длинную последовательность из единиц в блоке пройден.

Результаты тестов при ключе с малым весом и случайном открытом тексте:
Частотный побитовый тест пройден.
Тест на одинаковые идущие подряд биты пройден.
Тест на самую длинную последовательность из единиц в блоке пройден.

Результаты тестов при ключе с большим весом и случайном открытом тексте:
Частотный побитовый тест пройден.
Тест на одинаковые идущие подряд биты пройден.
Тест на самую длинную последовательность из единиц в блоке пройден.

Результаты тестов при цепочной обработке:
Частотный побитовый тест пройден.
Тест на одинаковые идущие подряд биты пройден.
Тест на самую длинную последовательность из единиц в блоке пройден.

Результаты тестов с размножением ошибки в открытом тексте:
Частотный побитовый тест пройден.
Тест на одинаковые идущие подряд биты пройден.
Тест на самую длинную последовательность из единиц в блоке пройден.

Результаты тестов с размножением ошибки в ключе:
Частотный побитовый тест пройден.
Тест на одинаковые идущие подряд биты пройден.
Тест на самую длинную последовательность из единиц в блоке пройден.

Результаты тестов при исследовании корреляции открытого текста и шифр-текста:
Частотный побитовый тест пройден.
Тест на одинаковые идущие подряд биты пройден.
Тест на самую длинную последовательность из единиц в блоке пройден.
```

2 Тестирование криптосистемы

Сценарий тестирования	Monobits	Runs	Longest Run
О.т. случайный, ключ случайный	Пройден	Пройден	Пройден
О.т. с малым весом, ключ случайный	Пройден	Пройден	Пройден
О.т. с большим весом, ключ случайный	Пройден	Пройден	Пройден
О.т. случайный, ключ с малым весом	Пройден	Пройден	Пройден
Размножение ошибки при изменении ключа	Пройден	Пройден	Пройден
Размножение ошибки при изменении о.т	Пройден	Пройден	Пройден
Корреляция о.т. и шифртекста	Пройден	Пройден	Пройден
Цепочная обработка блоков	Пройден	Пройден	Пройден