Министерство образования Республики Беларусь

Учреждение образования

БЕЛОРУССКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ
ИНФОРМАТИКИ И РАДИОЭЛЕКТРОНИКИ

Факультет информационный технологий и управления

Кафедра интеллектуальных информационных технологий

Дисциплина: «Средства и методы защиты информации в интеллектуальных системах»

Лабораторная работа №3 по теме: «Режимы применения блочных шифров»

Студент гр. 121702

Колтович Д.С.

Проверил:

Сальников Д.А.

Минск 2023

Тема

Режимы применения блочных шифров

Задание

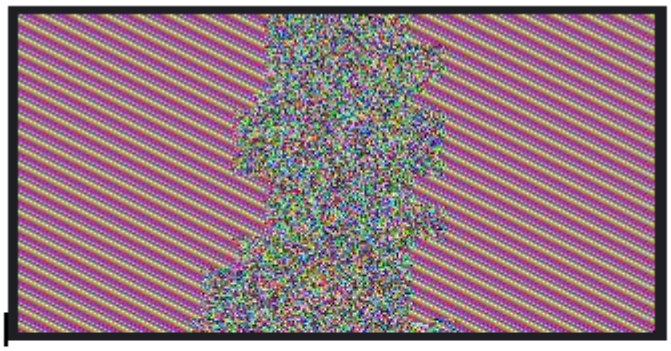
Разработать программу, реализующую следующие функции:

1. Реализовать программу, шифрующую изображения всеми возможными алгоритмами во всех возможных режимах. Результаты шифрования отразить в отчете в виде скриншотов.
2. Оценить полученные результаты и объяснить их причины.
3. Дать рекомендации по применению алгоритмов шифрования и их режимов в зависимости от типов изображения, шифрования и особенностей применения.
4. Дать ответ на вопрос: как влияет размер блока шифра на результат шифрования и почему?

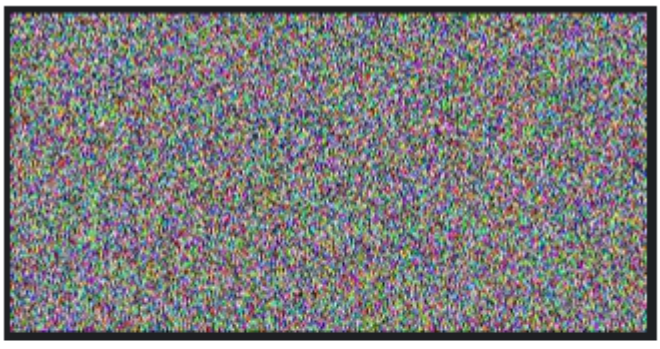
Выполнение задания

Оригинальные картинки:

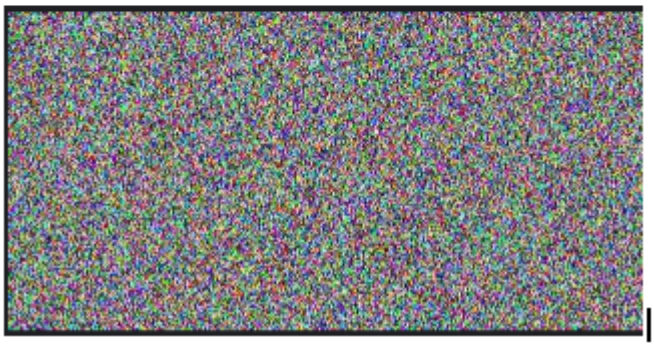
Алгоритм AES режим ECB



Алгоритм AES режим CBC



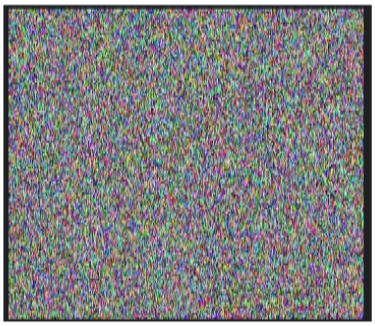
Алгоритм AES режим CFB

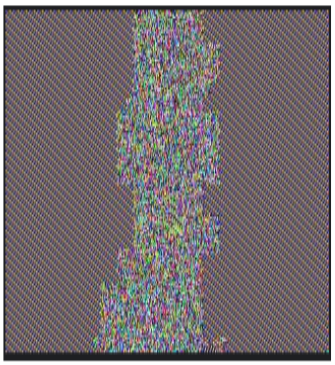


Алгоритм AES режим OFB

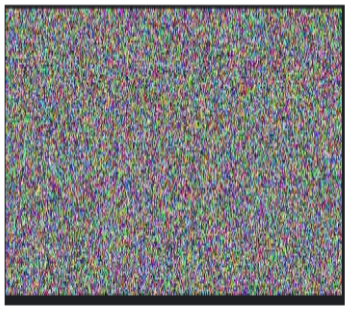
Алгоритм AES режим CTR

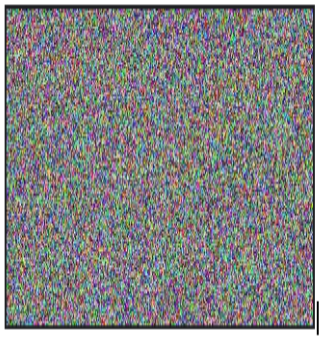
Алгоритм DES режим ECB



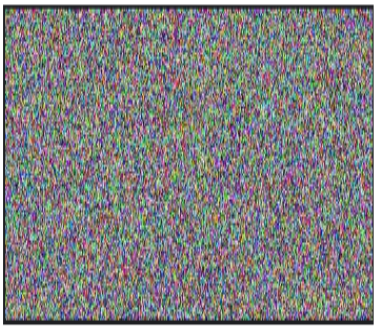


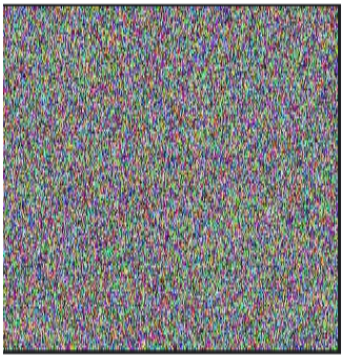
Алгоритм DES режим CBC



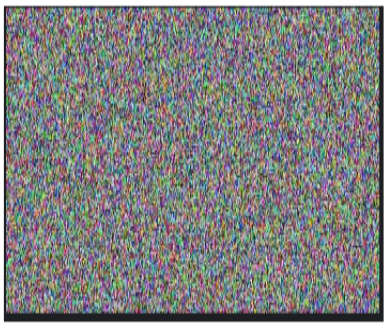


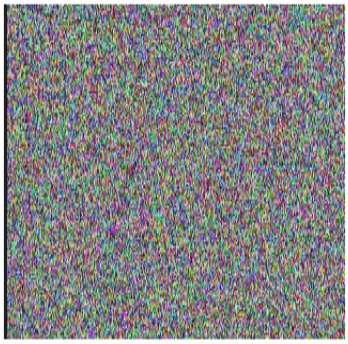
Алгоритм DES режим CFB





Алгоритм DES режим OFB





Как видно, явное отличие при использовании различных алгоритмов шифрования изображений не наблюдается. Однако наблюдаются отличия при использовании режима ECB и остальных. Это объясняется тем, что в силу специфики алгоритма режима ECB, одинаковые блоки будут зашифрованы одинаковый шифротекст. В целом, на данный момент ECB считается самым небезопасным режимом шифрования, поэтому предпочтительно использовать другой.

Различия же алгоритмов хотя и не так видны, всё же рекомендуется использовать алгоритм AES, ибо увеличение размера блока ведёт к увеличению ключа, а его в свою очередь становится сложнее подобрать методом перебора.

Вывод

В ходе лабораторной работы были реализованы программные средства шифрования изображений при помощи алгоритмов AES и DES в различных режимах. Явных отличий в зашифрованных изображениях, зашифрованных по алгоритмам AES и DES обнаружено не было (но стоит отметить, что режим AES более устойчив к взлому посредством перебора из-за увеличенного ключа). В целом, различные режимы также не дают отличных изображений (кроме режима ECB). Это объясняется тем, что одинаковые блоки в ECB шифруются одинаково, что позволяет определить смысл даже зашифрованного изображения.