

Министерство образования Республики Беларусь
Учреждение образования «Белорусский государственный университет
информатики и радиоэлектроники»

Факультет информационных технологий и управления
Кафедра интеллектуальных информационных технологий
Дисциплина «Средства и методы защиты информации в интеллектуальных
системах»

ОТЧЁТ
к лабораторной работе №3
на тему
«РЕЖИМЫ ПРИМЕНЕНИЯ БЛОЧНЫХ ШИФРОВ»

БГУИР 6-05-0611-03 130

Выполнил студент группы 321701
СЕМЕНЯКО Владимир Дмитриевич

(дата, подпись студента)

Проверил
САЛЬНИКОВ Даниил Андреевич

(дата, подпись преподавателя)

Минск 2025

1 ИНДИВИДУАЛЬНОЕ ЗАДАНИЕ

- а) Зашифровать предложенные изображения с использованием алгоритмов AES и DES в режимах ECB, CBC и CTR с помощью программы EModes.exe.
- б) Проанализировать визуальные результаты шифрования и объяснить различия между режимами.
- в) Сформулировать рекомендации по выбору режима шифрования в зависимости от типа изображения и требований к безопасности.
- г) Исследовать влияние размера блока шифра (64 бита у DES, 128 бит у AES) на визуальный результат шифрования.

2 ВЫПОЛНЕНИЕ РАБОТЫ

Для выполнения лабораторной работы использовалась программа EModes.exe, позволяющая визуализировать результаты шифрования изображений различными блочными шифрами (AES, DES) в разных режимах (ECB, CBC, CTR). Были выбраны пять типов изображений: компьютерный рисунок, диаграмма, текстура, фотография с небольшим количеством деталей, фотография с большим количеством деталей

Для каждого изображения выполнялось шифрование всеми комбинациями: AES (128 бит) + ECB / CBC / CTR и DES (64 бит) + ECB / CBC

Результаты шифрования:



Рисунок 1 – Компьютерный рисунок

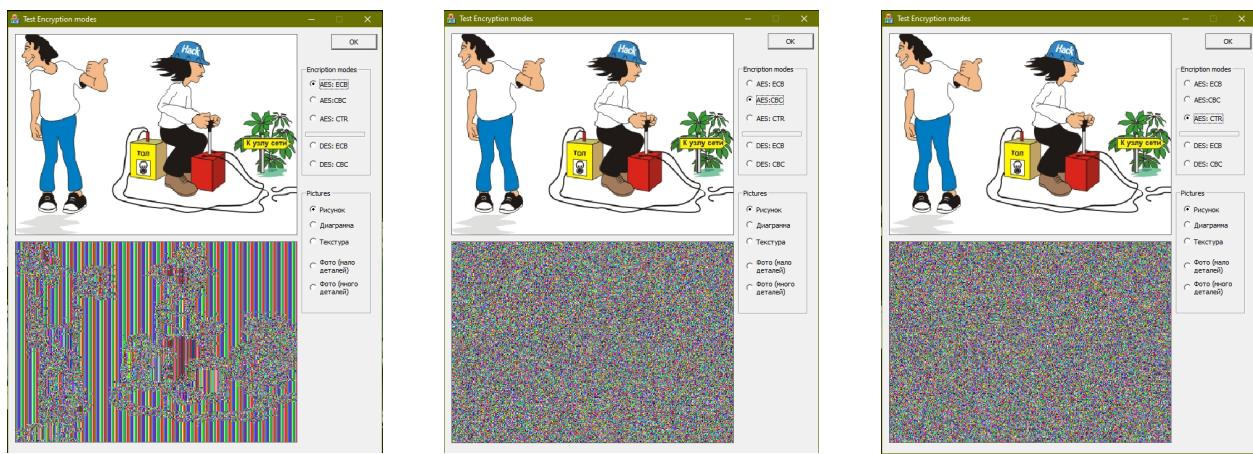


Рисунок 2 – Результат шифрования компьютерного рисунка, используя блочный шифр AES в режимах ECB, CBC, CTR

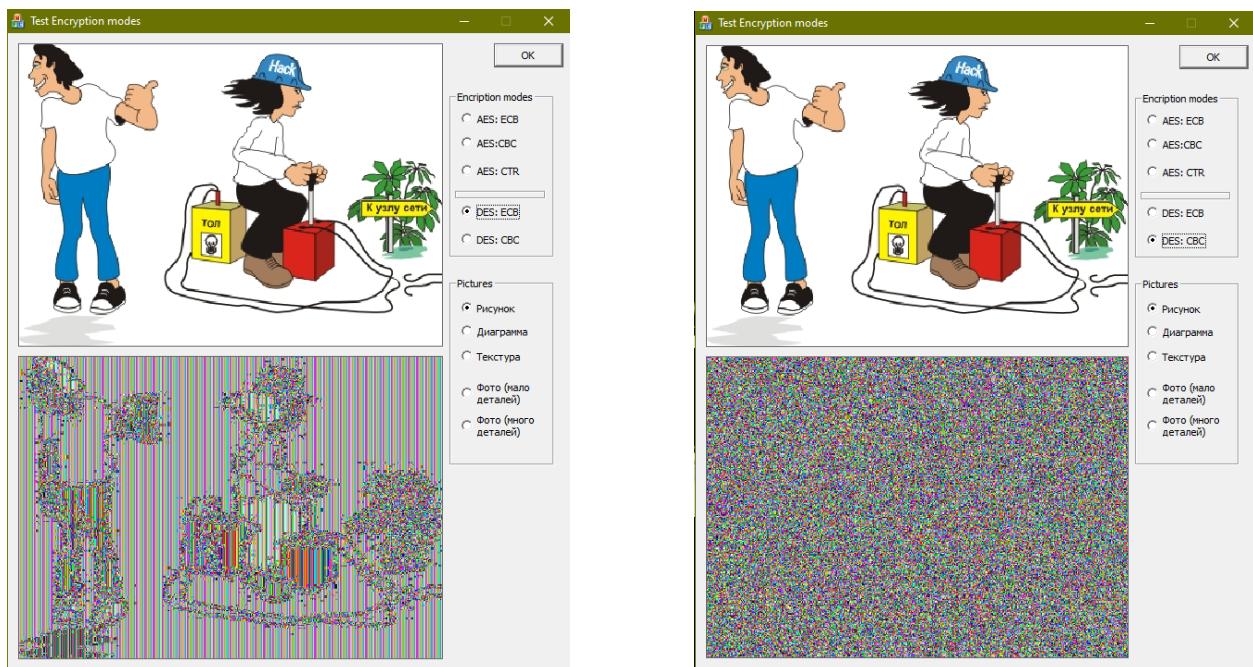


Рисунок 3 – Результат шифрования компьютерного рисунка, используя блочный шифр DES в режимах ECB, CBC

Какой процент от расходов на ИТ занимают финансовые затраты на защиту информации?

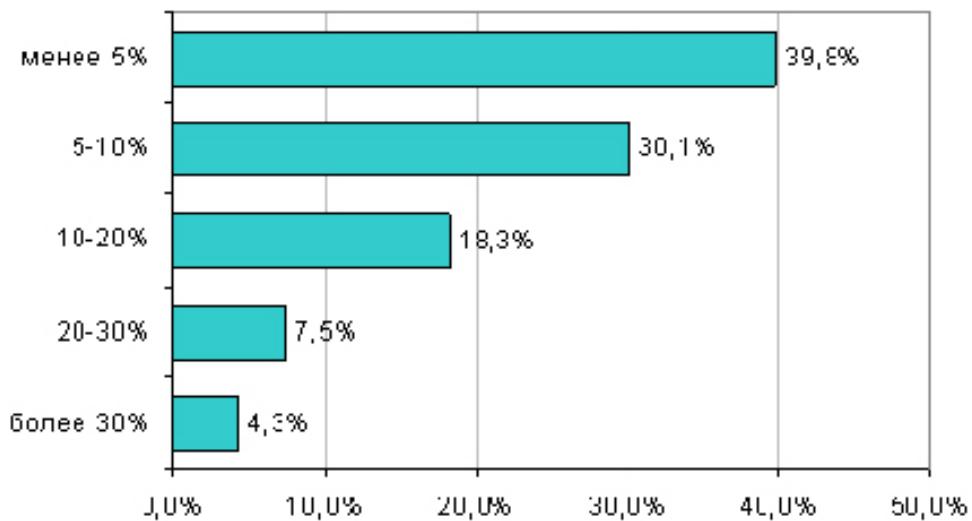


Рисунок 4 – Диаграмма

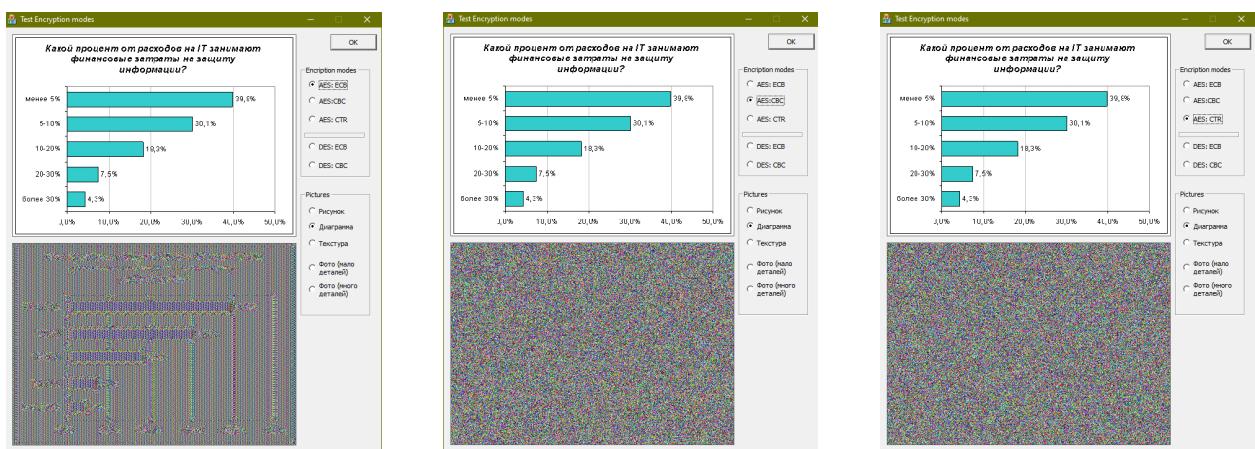


Рисунок 5 – Результат шифрования диаграммы, используя блочный шифр AES в режимах ECB, CBC, CTR

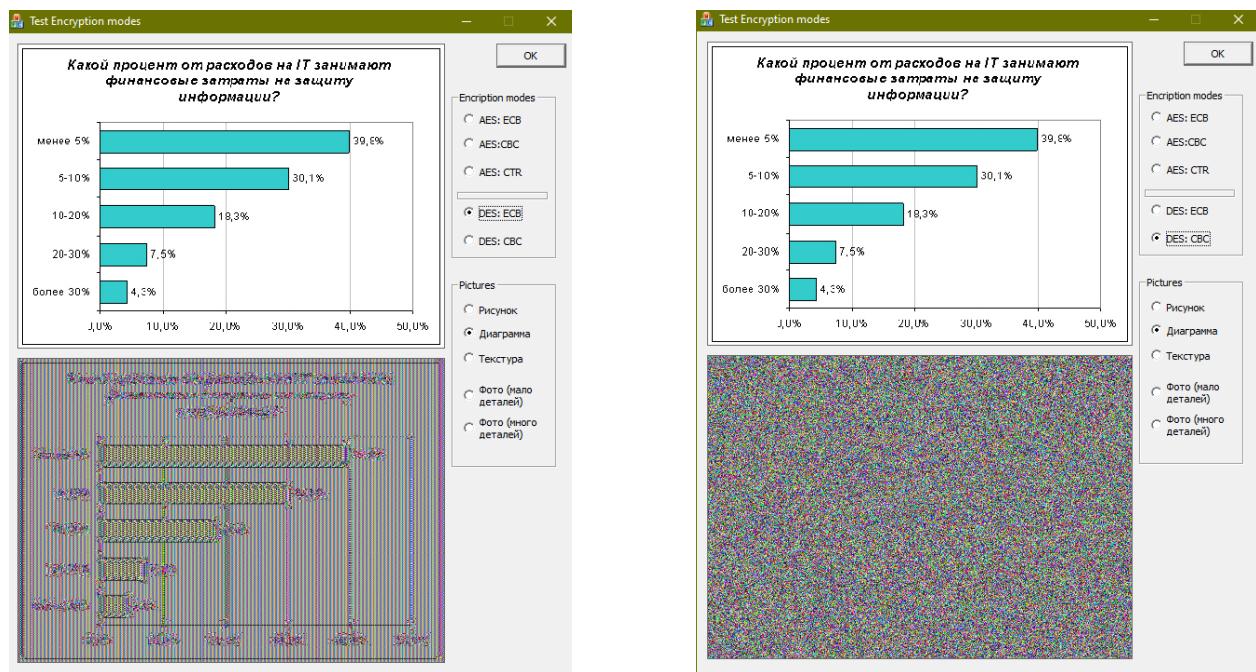


Рисунок 6 – Результат шифрования диаграммы, используя блочный шифр DES в режимах ECB, CBC



Рисунок 7 – Текстура

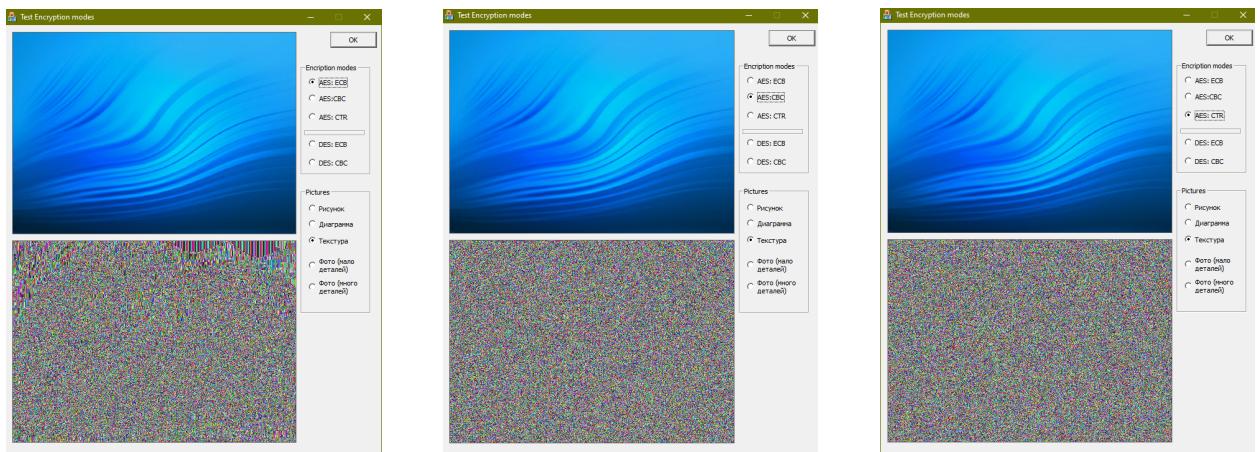


Рисунок 8 – Результат шифрования текстуры, используя блочный шифр AES в режимах ECB, CBC, CTR

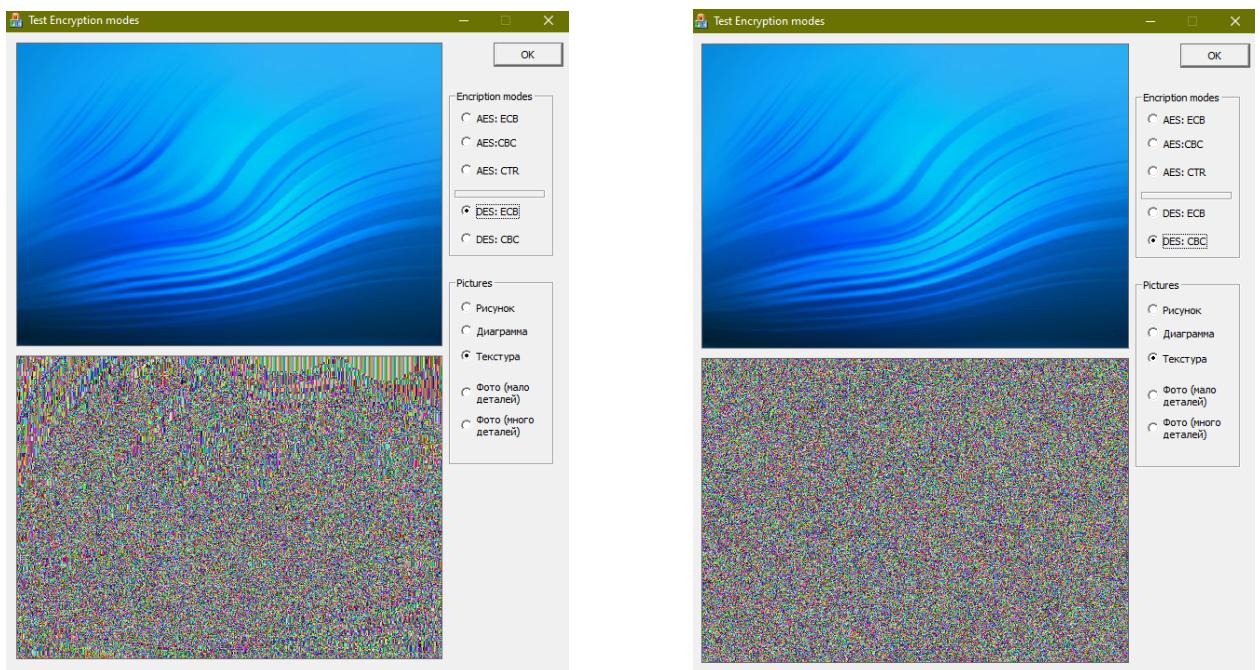


Рисунок 9 – Результат шифрования текстуры, используя блочный шифр DES в режимах ECB, CBC



Рисунок 10 – Фотография с небольшим количеством деталей

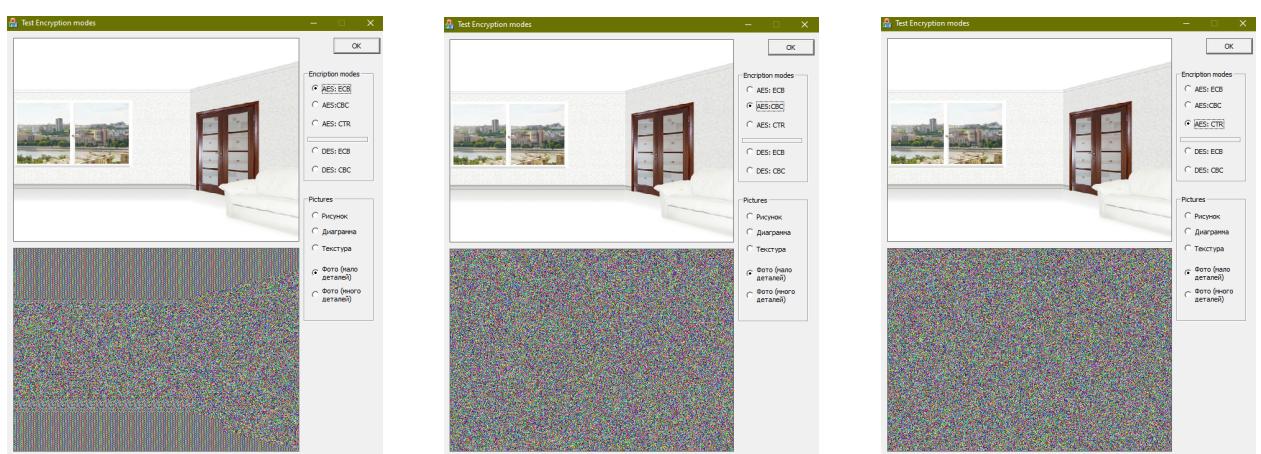


Рисунок 11 – Результат шифрования фотографии с небольшим количеством деталей, используя блочный шифр AES в режимах ECB, CBC, CTR

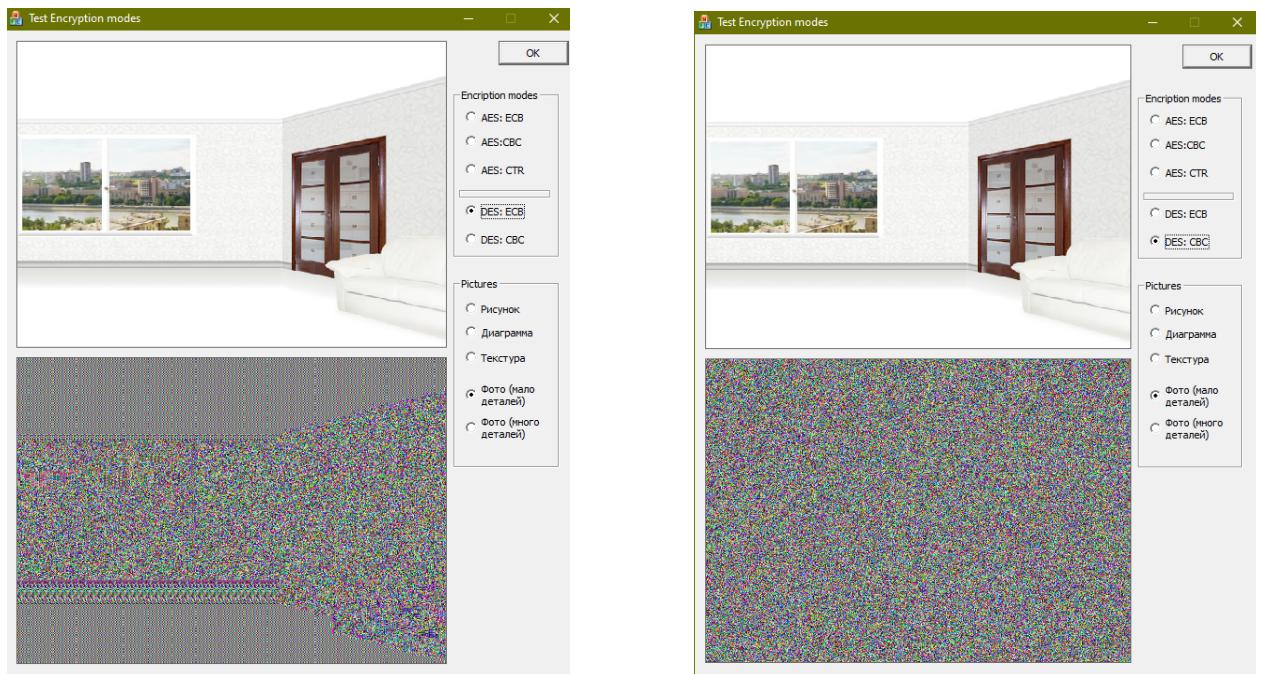


Рисунок 12 – Результат шифрования фотографии с небольшим количеством деталей, используя блочный шифр DES в режимах ECB, CBC



Рисунок 13 – Фотография с большим количеством деталей

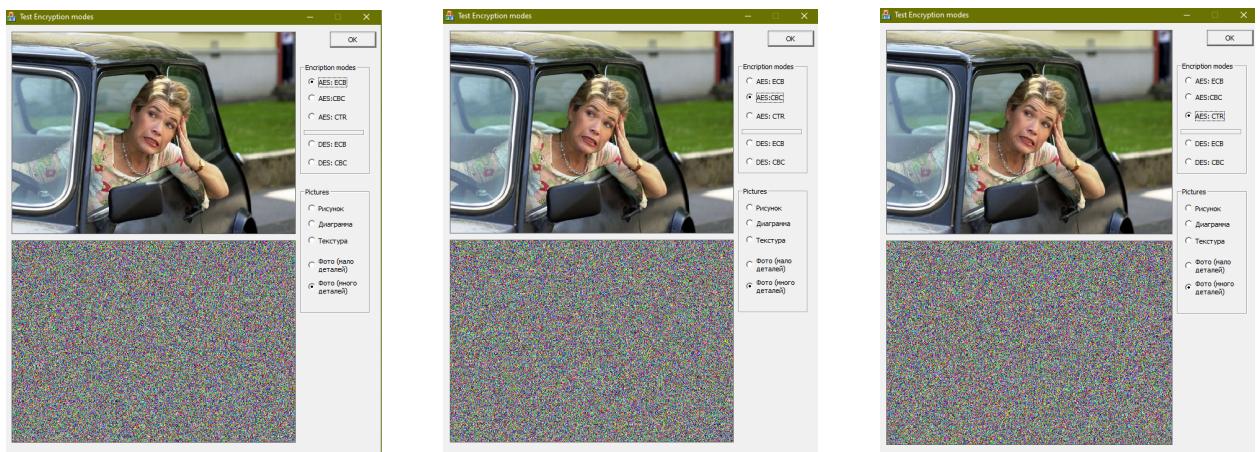


Рисунок 14 – Результат шифрования фотографии с большим количеством деталей, используя блочный шифр AES в режимах ECB, CBC, CTR

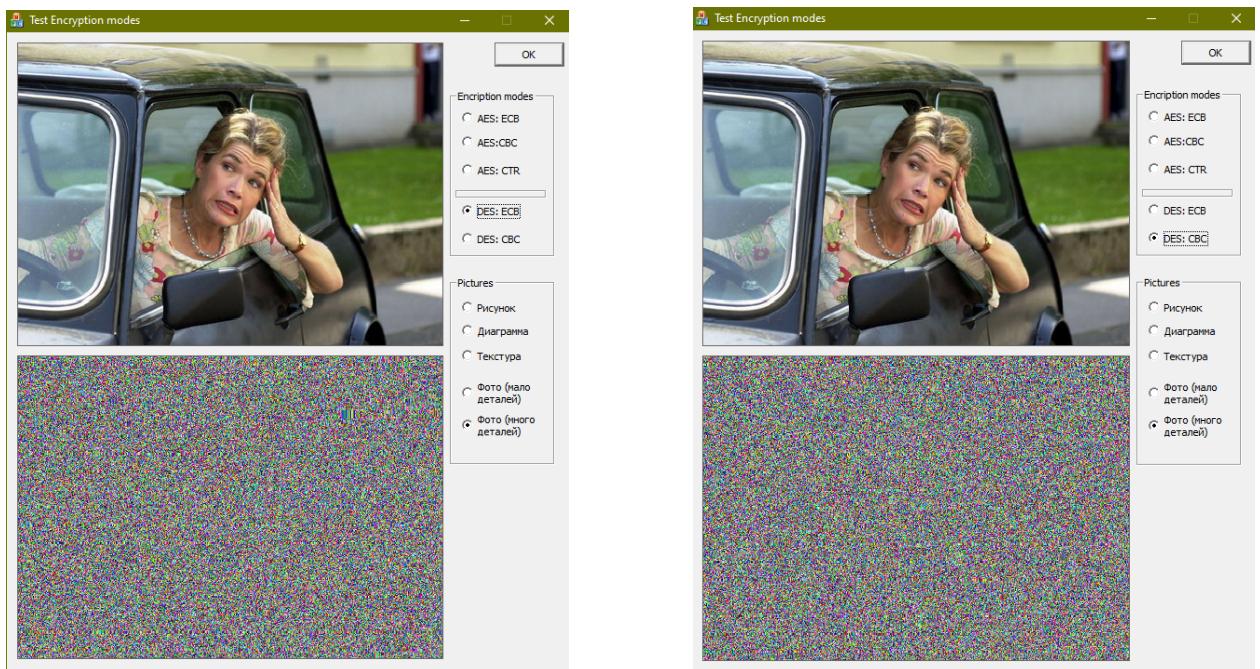


Рисунок 15 – Результат шифрования фотографии с большим количеством деталей, используя блочный шифр DES в режимах ECB, CBC

В режиме ECB (Electronic Code Book) на всех типах изображений — будь то компьютерный рисунок, диаграмма, текстура или фотография — сохраняются контуры и структурные элементы. Особенно ярко это проявляется на изображениях с большими однородными областями: сетка, образованная границами блоков шифра, остаётся чётко различимой. Это происходит потому, что в ECB каждый блок исходных данных шифруется независимо, и одинаковые блоки открытого текста всегда преобразуются в одинаковые блоки шифротекста. Отсюда, режим ECB не обеспечивает конфиденциальность

структуры данных и категорически не рекомендуется для шифрования изображений или любых структурированных данных.

В отличие от ECB, режимы CBC (Cipher Block Chaining) и CTR (Counter Mode) полностью разрушают визуальные паттерны. Зашифрованные изображения в этих режимах выглядят как случайный шум, без каких-либо различимых форм или контуров. В режиме CBC это достигается за счёт того, что каждый блок открытого текста перед шифрованием складывается по модулю 2 с предыдущим блоком шифротекста, что создаёт сильную зависимость между блоками. В режиме CTR блочный шифр преобразуется в поточный: генерируется псевдослучайная гамма путём шифрования последовательных значений счётчика, которая затем накладывается на открытый текст. Оба режима эффективно скрывают структуру данных, но CTR имеет преимущество — он позволяет параллельную обработку и предварительную генерацию ключевого потока, что делает его более производительным.

При сравнении алгоритмов AES и DES было замечено, что размер блока шифра (128 бит у AES против 64 бит у DES) оказывает значительное влияние на результат только в режиме ECB. На изображениях, зашифрованных DES в режиме ECB, “квадратная” структура (сетка 8×8 пикселей) более выражена и детализирована, чем у AES (сетка 16×16 пикселей). Это связано с тем, что меньший размер блока приводит к более частому повторению одинаковых блоков на однородных участках изображения, что усиливает визуальный артефакт. В режимах CBC и CTR размер блока не влияет на визуальный результат, поскольку зависимость между блоками полностью устраняет повторяемость, и изображения в обоих случаях выглядят как однородный шум.

ВЫВОД

В ходе лабораторной работы было экспериментально подтверждено, что режим ECB непригоден для шифрования структурированных данных, таких как изображения, поскольку он не скрывает повторяющиеся паттерны. Режимы CBC и CTR эффективно разрушают структуру и обеспечивают высокую степень конфиденциальности. Также было показано, что размер блока влияет на визуальную “зернистость” артефактов в ECB, но не на безопасность в других режимах. Для современных приложений рекомендуется использовать AES в режиме CTR или CBC, избегая ECB во всех случаях, где важна конфиденциальность содержания.