Учреждение образования

«БЕЛОРУССКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ

ИНФОРМАТИКИ И РАДИОЭЛЕКТРОНИКИ»

Кафедра интеллектуальных информационных технологий

**Отчет по лабораторной работе №3**

**по курсу «СиМОИБ»**

**на тему: «Блочные шифры. Режимы шифрования»**

|  |  |
| --- | --- |
| Выполнил студент группы 821703: | Веренич К.О. |
| Проверил: | Захаров В. В. |

**МИНСК**

**2020**

Задание 1: Зашифровать предложенные изображения всеми возможными алгоритмами, во всех возможных режимах. Результаты шифрования отразить в отчете в виде скриншотов.

|  |  |
| --- | --- |
| **Тип шифрования** | **Изображение** |
| До шифрования |  |
| AES:ECB |  |
| AES:CBS |  |
| AES:CTR |  |
| DES:ECB |  |
| DES:CBC |  |

Задание 2:Оценить полученные результаты и объяснить их причины.

Сделать какой-либо вывод об исходном изображении по зашифрованному можно, используя алгоритм шифрования AES в режим ECB (режим простой замены) . В этом режиме каждый блок открытого текста заменяется блоком шифртекста. Недостатком данного режима является то, что в результате зашифрования получаются одинаковые блоки шифртекста, и поэтому, имея зашифрованную картинку, можно получить некоторое представление о ней. Используя алгоритм шифрования **DES** мы получим примерно такую же картину, но так как размер блока в нем в два раза меньше, то и зашифрованное изображение получается более детальное,

|  |  |
| --- | --- |
| AES:ECB | DES:ECB |
|  |  |

Задание 3: Дать рекомендации по применению алгоритмов шифрования и их режимов в зависимости от типов изображения, шифрования и особенностей применения.

Для изображений типа текстура или из ображений, в которых много деталей, можно использовать режим **ECB** с алгоритмом шифрования **AES** и **DES**. Лучше использовать алгоритм **AES**, так как размер блока у него в 2 раза больше, чем **DES**, значит количество блоков будет меньше, и зашифрование(расшифрование) будет проходить быстрее, нежели в алгоритме **DES**.

|  |  |
| --- | --- |
| AES:ECB | DES:ECB |
|  |  |

Для зашифрования изображений в которых присутствуют повторяющиеся элементы или на фотографии малое количество деталей можно использовать режимы **CBC** и **CTR** алгоритма шифрования **AES** и **CBC** алгоритма **DES**. Если сравнивать **CBC(AES**) и **CBC(DES)**, то лучшим режимом будет **CBC(AES)**, так как у обоих шифрование текущего блока зависит от шифрования всех предыдущих, но так как **CBC(AES)** имеет меньшее количество блоков, зашифрование с использование данного режима будет проходить быстрее. Если же сравнивать режимы **CBC** и **CTR**, то лучшим из них будет **CTR**, так как режим **CTR** зашифровывает текущий блок в зависимости от значения счетчика и это предоставляет возможность распаралеливать выполнение операций зашифрования и расшифрования, что дает преимущество перед **CBC**. Поэтому рекомендуется режим **CTR**.

Задание 4: Влияет ли длина блока на визуальный результат шифрования

При использовании режимов **CBC** и **CTR** длина блока особо не влияет на режим шифрования.

При использовании режима **ECB** длина блока значительно влияет на режим шифрования. При зашифровании с помощью алгоритма **DES** (длина блока 64 бит) на картинке можно рассмотреть намного больше деталей, чем при использовании **AES**(длина блока 128 бит).