# Оглавление

Режимы шифрования ..... 2
Задание 1 ..... 5
Задание 2 ..... 5
Задание 3 ..... 5
Задание 4 ..... 5
Задание 5 ..... 6
Литература ..... 7

## Режимы шифрования

Рассмотренные ранее алгоритмы выполнялись в режиме ECB (рис.1).

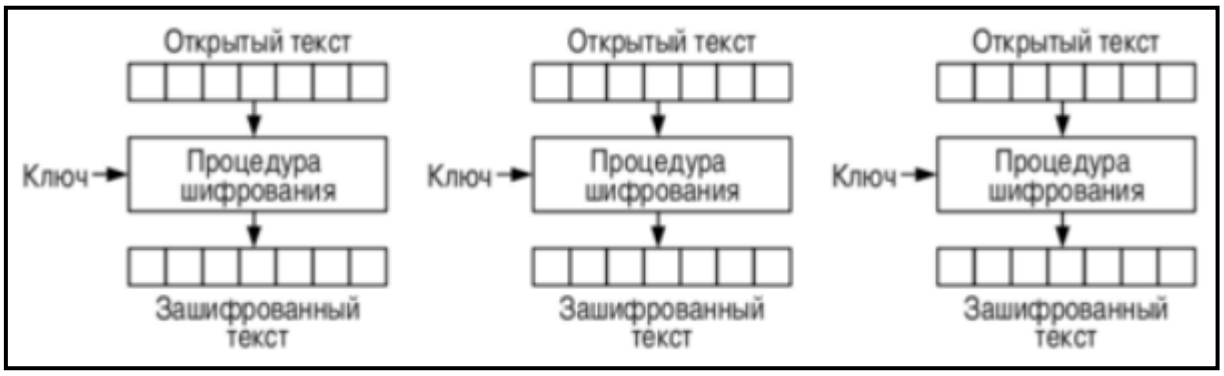


Рисунок 1 – Шифрование в режиме ECB

Режим шифрования CBC (рис.2, 3).

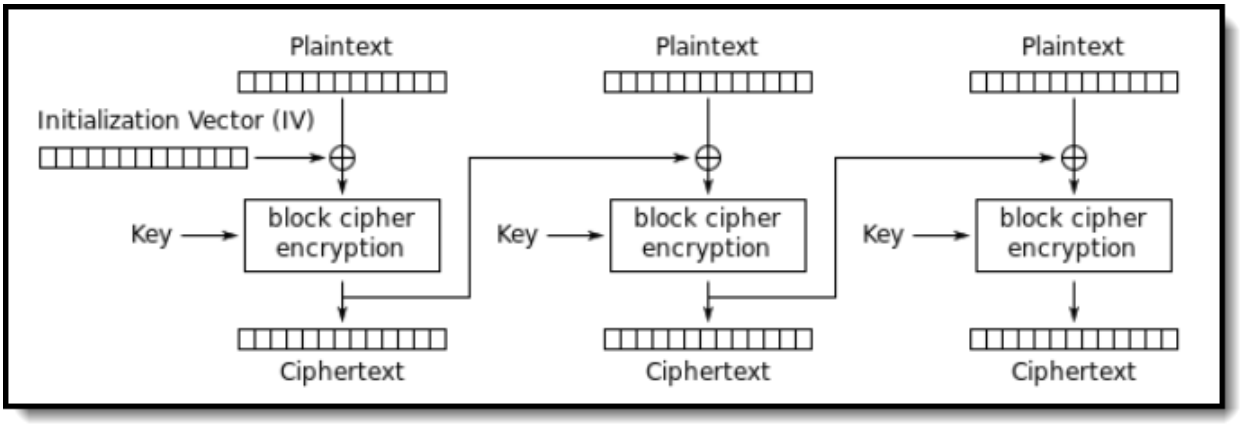


Рисунок 2 – Шифрование в режиме CBC

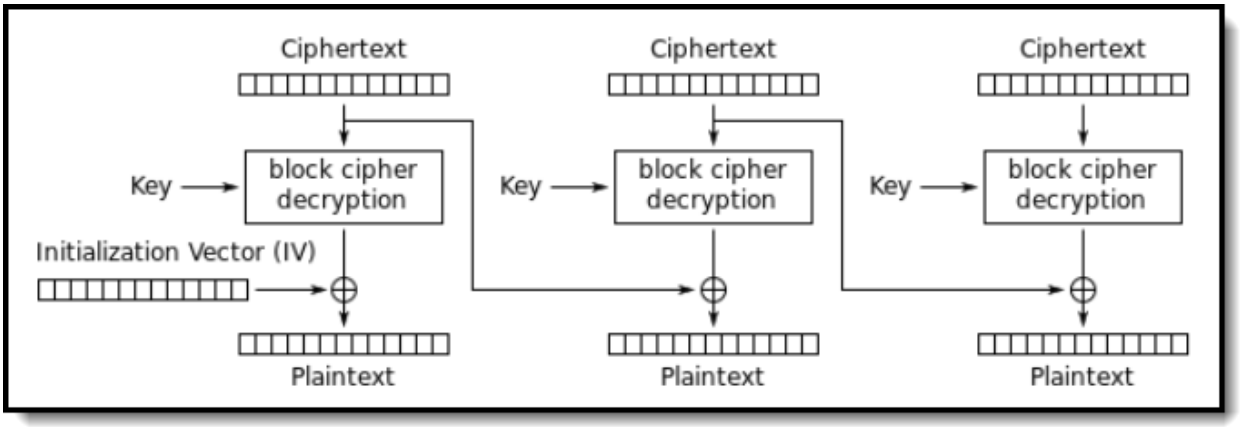


Рисунок 3 – Расшифрование в режиме CBC

Режим шифрования OFB (рис.4, 5).

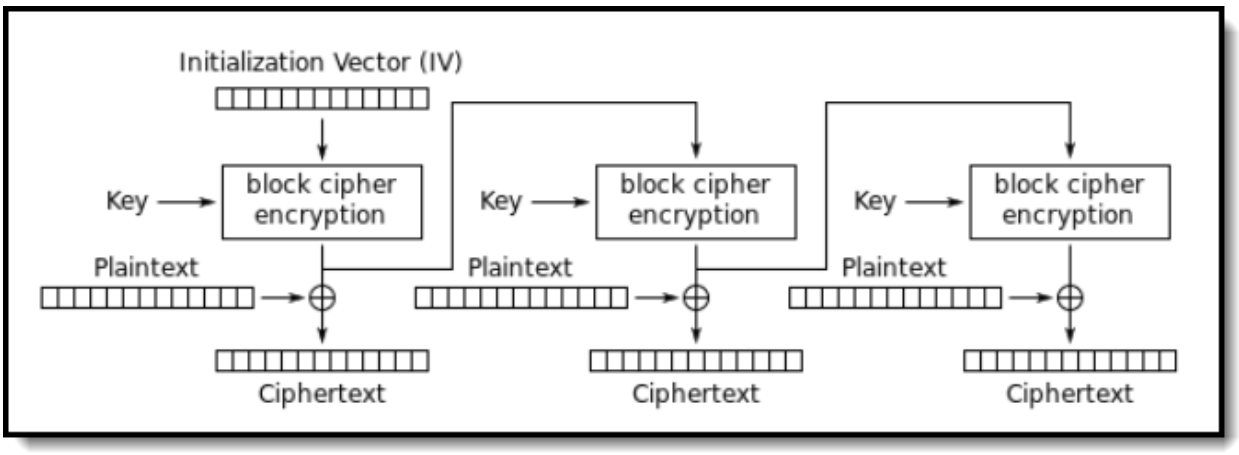


Рисунок 4 – Шифрование в режиме OFB

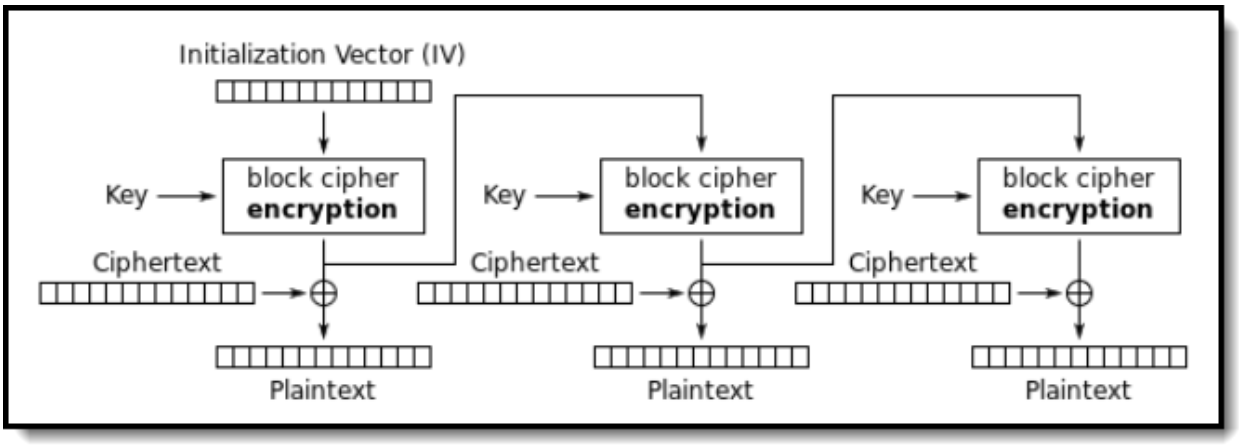


Рисунок 5 – Расшифрование в режиме OFB

Режим шифрования CFB (рис.6, 7).

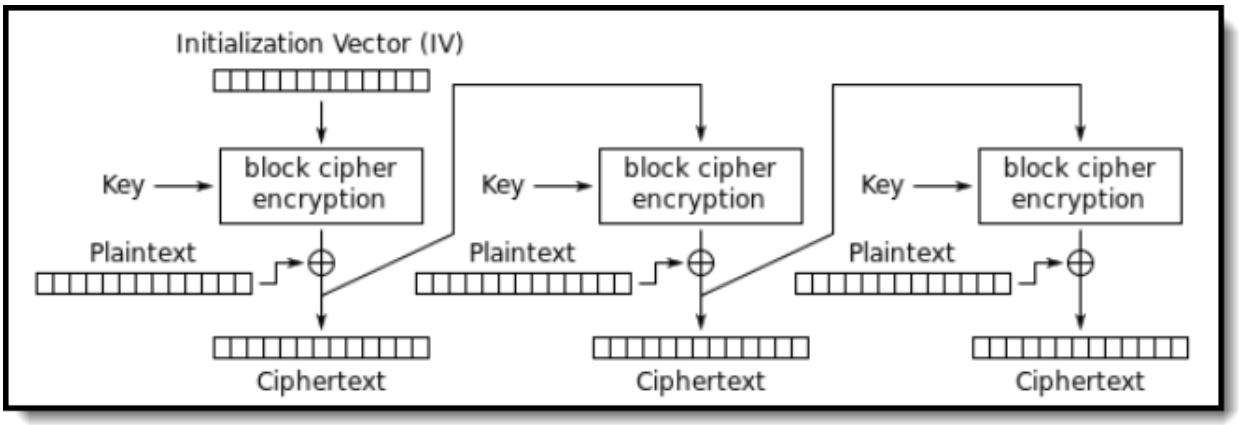


Рисунок 6 – Шифрование в режиме CFB

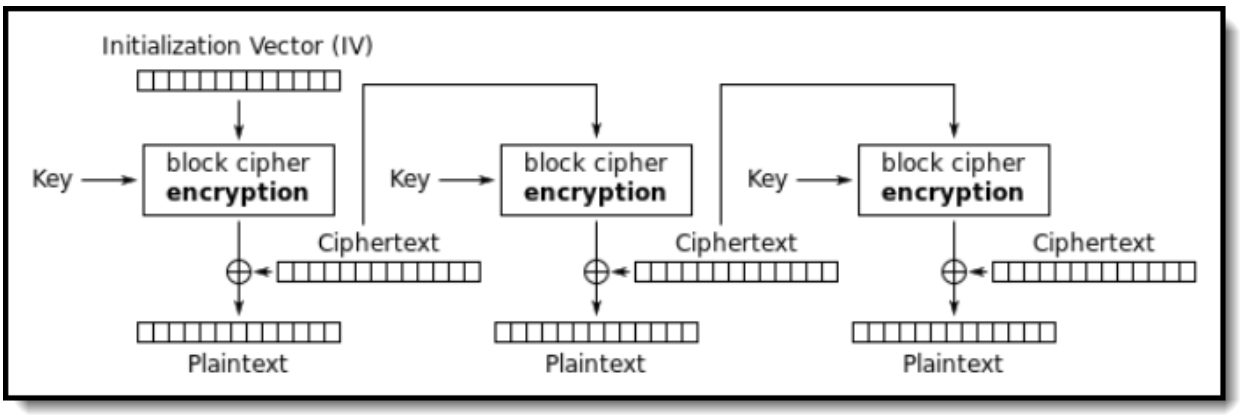


Рисунок 7 – Расшифрование в режиме CFB

Режим шифрования CTR (рис.8, 9).

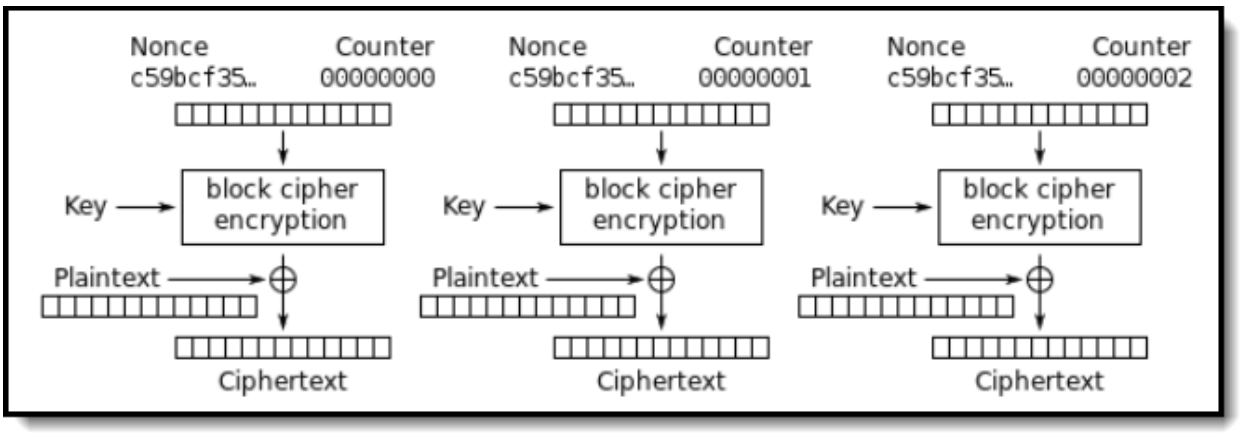


Рисунок 8 – Шифрование в режиме CTR

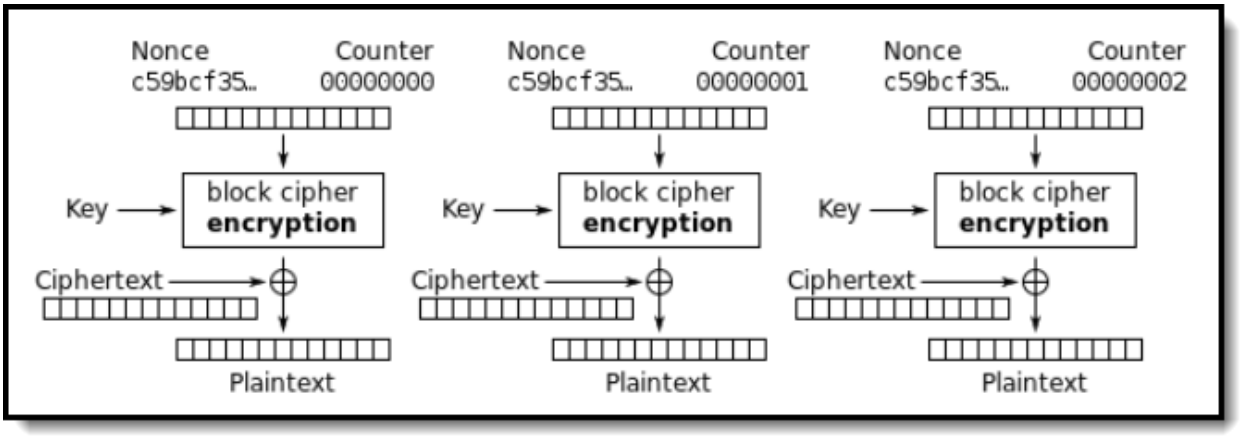


Рисунок 9 – Расшифрование в режиме CTR

### Задание 1

Расшифровать файл z1_caesar_cbc_c_all.bmp – зашифрованное шифром Цезаря изображение в формате bmp. Режим шифрования CBC (рис. 2, 3). Ключ равен 223. Вектор инициализации равен 59. Зашифровать в режиме ECB и в режиме CBC, оставив первые 50 байт без изменения. Сравнить полученные изображения.

### Задание 2

Расшифровать файл im8_caesar_ofb_c_all.bmp – зашифрованное шифром Цезаря изображение в формате bmp. Режим шифрования OFB (рис. 4, 5). Ключ равен 56. Вектор инициализации равен 9. Зашифровать в режиме ECB и в режиме OFB, оставив первые 50 байт без изменения. Сравнить полученные изображения.

### Задание 3

Расшифровать файл z2_caesar_cfb_c_all.bmp – зашифрованное шифром Цезаря изображение в формате bmp. Режим шифрования CFB (рис. 6, 7). Ключ равен 174. Вектор инициализации равен 9. Зашифровать в режиме ECB и в режиме CFB, оставив первые 50 байт без изменения. Сравнить полученные изображения.

### Задание 4

Расшифровать файл z3_caesar_ctr_c_all.bmp – зашифрованное шифром Цезаря изображение в формате bmp. Режим шифрования CTR (рис. 8, 9). Ключ равен 223. Вектор инициализации равен 78. Зашифровать в режиме ECB и в режиме CTR, оставив первые 50 байт без изменения. Сравнить полученные изображения.

## Задание 5

Для одного из расшифрованных изображений выполнить следующее: на одном и том же ключе и векторе инициализации зашифровать во всех рассмотренных режимах, включая ECB, оставив первые 50 байт без изменения. Сравнить полученные изображения.

## Литература

[1] Stallings W, “Cryptography And Network Security. Principles And Practice”, 5th Edition, 2011.