Оглавление

[**Режимы шифрования** 2](#_Toc53982839)

[Задание 1 5](#_Toc53982840)

[Задание 2 5](#_Toc53982841)

[Задание 3 5](#_Toc53982842)

[Задание 4 5](#_Toc53982843)

[Задание 5 6](#_Toc53982844)

[Задание 6 6](#_Toc53982845)

[Задание 7 6](#_Toc53982846)

[Задание 8 6](#_Toc53982847)

[Задание 9 6](#_Toc53982848)

[Задание 10 7](#_Toc53982849)

[Задание 11 7](#_Toc53982850)

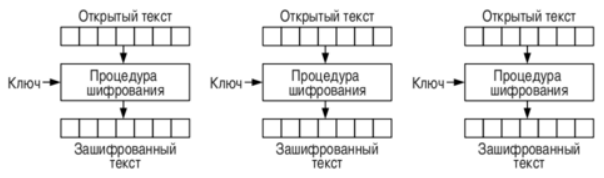
[Задание 12 7](#_Toc53982851)

[Литература 8](#_Toc53982852)

**Режимы шифрования**

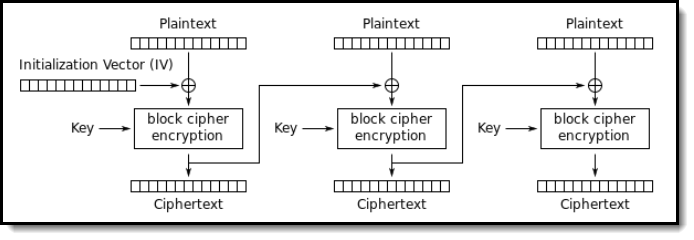
Дополнить нижеприведенные схемы описанием преимуществ и недостатков перечисленных режимов шифрования.

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

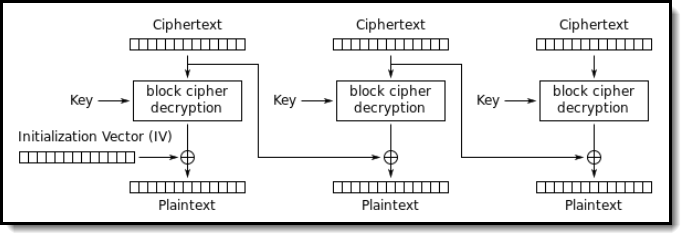


1. – Шифрование в режиме ECB

Режим шифрования CBC (рис.2, 3).

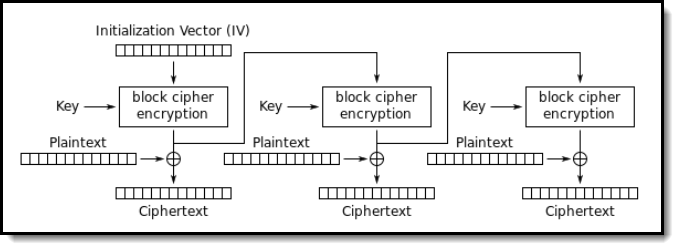


1. – Шифрование в режиме CBC

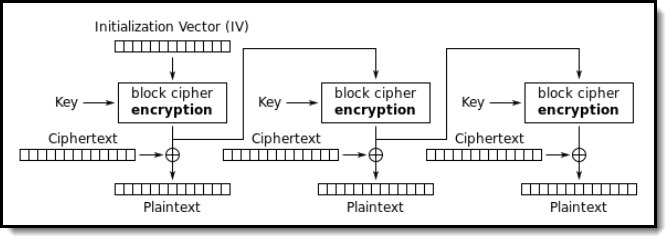


1. – Расшифрование в режиме CBC

Режим шифрования OFB (рис.4, 5).

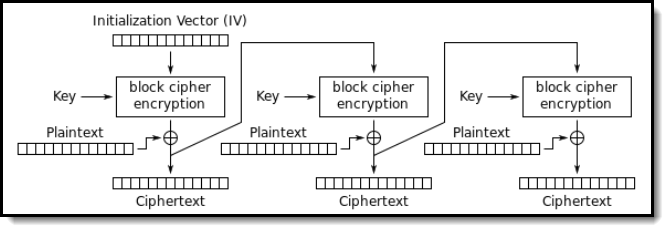


1. – Шифрование в режиме OFB

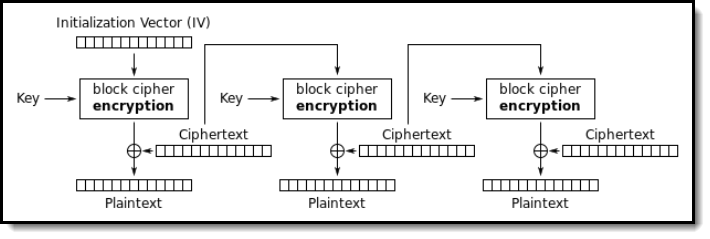


1. – Расшифрование в режиме OFB

Режим шифрования CFB (рис.6, 7).

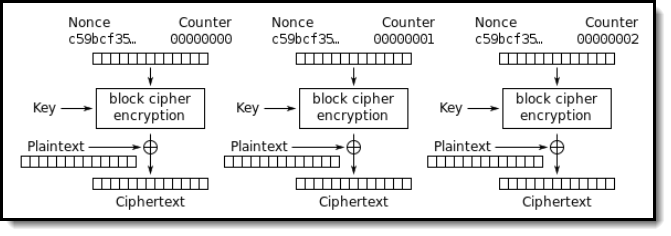


1. – Шифрование в режиме CFB

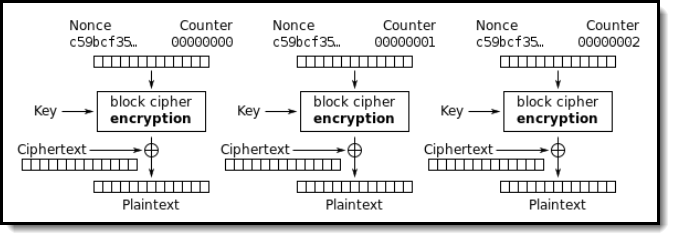


1. – Расшифрование в режиме CFB

Режим шифрования CTR (рис.8, 9).



1. – Шифрование в режиме CTR



1. – 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, ). 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, ). 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. , ). Ключ равен 174. Вектор инициализации равен 9. Зашифровать в режиме ECB и в режиме СFB, 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. , ). 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

Расшифровать файл z5\_vigener\_cbc\_c\_all.bmp. Шифр Виженера. Режим CBC. Ключ: MODELING, вектор инициализации: 67. Зашифровать, оставив первые 50 байт без изменения.

## Задание 6

Расшифровать файл im4\_vigener\_ofb\_c\_all.bmp. Шифр Виженера. Режим OFB. Ключ: MODULATOR, вектор инициализации: 217. Зашифровать, оставив первые 50 байт без изменения.

## Задание 7

Расшифровать файл im5\_vigener\_cfb\_c\_all.bmp. Шифр Виженера. Режим CFB. Ключ: MONARCH, вектор инициализации: 172. Зашифровать, оставив первые 50 байт без изменения.

## Задание 8

Расшифровать файл z6\_vigener\_ctr\_c\_all.bmp. Шифр Виженера. Режим CTR. Ключ: MONOLITH, вектор инициализации: 167. Зашифровать, оставив первые 50 байт без изменения.

## Задание 9

Расшифровать файл im15\_affine\_cbc\_c\_all.bmp. Шифр аффинный. Режим CBC. a= 129 b= 107 iv = 243. Зашифровать, оставив первые 50 байт без изменения.

## Задание 10

Расшифровать файл im16\_affine\_ofb\_c\_all.bmp. Шифр аффинный. Режим OFB. a= 233 b= 216 iv = 141. Зашифровать, оставив первые 50 байт без изменения.

## Задание 11

Расшифровать файл im17\_affine\_сfb\_c\_all.bmp. Шифр аффинный. Режим CFB. a= 117 b= 239 iv = 19. Зашифровать, оставив первые 50 байт без изменения.

## Задание 12

Расшифровать файл z4\_affine\_сtr\_c\_all.bmp. Шифр аффинный. Режим CTR. a= 61, b= 18, iv = 92. Зашифровать, оставив первые 50 байт без изменения.

# Литература

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