Оглавление

[Варианты заданий (алгоритм S-DES) 2](#_Toc56375638)

[**Вариант 1** 2](#_Toc56375639)

[**Вариант 2** 2](#_Toc56375640)

[**Вариант 3** 2](#_Toc56375641)

[**Вариант 4** 2](#_Toc56375642)

[**Вариант 5** 2](#_Toc56375643)

[**Вариант 6** 3](#_Toc56375644)

[**Вариант 7** 3](#_Toc56375645)

[**Вариант 8** 3](#_Toc56375646)

[**Вариант 9** 3](#_Toc56375647)

[**Вариант 10** 3](#_Toc56375648)

[**Вариант 11** 3](#_Toc56375649)

[**Вариант 12** 3](#_Toc56375650)

[**Вариант 13** 3](#_Toc56375651)

[**Вариант 14** 4](#_Toc56375652)

[**Вариант 15** 4](#_Toc56375653)

[**Вариант 16** 4](#_Toc56375654)

[Литература 5](#_Toc56375655)

# Варианты заданий (алгоритм S-DES)

**Вариант 1**

Расшифровать файл aa2\_sdes\_c\_cbc\_all.bmp – зашифрованное шифром S\_DES изображение в формате bmp. Режим шифрования CBC. Ключ равен 845. Вектор инициализации равен 56. Зашифровать в режиме ECB и в режиме CBC, оставив первые 50 байт без изменения. Сравнить полученные изображения.

**Вариант 2**

Расшифровать файл aa3\_sdes\_c\_ofb\_all.bmp – зашифрованное шифром S\_DES изображение в формате bmp. Режим шифрования OFB. Ключ равен 932. Вектор инициализации равен 234. Зашифровать в режиме ECB и в режиме OFB, оставив первые 50 байт без изменения. Сравнить полученные изображения.

**Вариант 3**

Расшифровать файл aa4\_sdes\_c\_cfb\_all.bmp – зашифрованное шифром S\_DES изображение в формате bmp. Режим шифрования CFB. Ключ равен 455. Вектор инициализации равен 162. Зашифровать в режиме ECB и в режиме CFB, оставив первые 50 байт без изменения. Сравнить полученные изображения.

**Вариант 4**

Расшифровать файл im38\_sdes\_c\_ctr\_all.bmp – зашифрованное шифром S\_DES изображение в формате bmp. Режим шифрования CTR. Ключ равен 572. Вектор инициализации равен 157. Зашифровать в режиме ECB и в режиме CTR, оставив первые 50 байт без изменения. Сравнить полученные изображения.

**Вариант 5**

Дешифровать файл im39\_sdes\_c\_cbc\_all.bmp. Шифр SDES. Режим CBC. iv= 132. Зашифровать, оставив первые 50 байт без изменения.

**Вариант 6**

Дешифровать файл im40\_sdes\_c\_ofb\_all.png. Шифр SDES. Режим OFB. iv= 179.

**Вариант 7**

Дешифровать файл im41\_sdes\_c\_cfb\_all.jpg. Шифр SDES. Режим CFB. iv= 121. Зашифровать, оставив первые 50 байт без изменения.

**Вариант 8**

Дешифровать файл im42\_sdes\_c\_ctr\_all.tif. Шифр SDES. Режим CTR. iv= 189. Зашифровать, оставив первые 50 байт без изменения.

**Вариант 9**

Дешифровать файл t15\_sdes\_c\_cbc\_all.txt. Шифр SDES. Режим CBC. iv= 202.

**Вариант 10**

Дешифровать файл t16\_sdes\_c\_ofb\_all.txt. Шифр SDES. Режим OFB. iv= 212.

**Вариант 11**

Дешифровать файл t17\_sdes\_c\_cfb\_all.txt. Шифр SDES. Режим CFB. iv= 232.

**Вариант 12**

Дешифровать файл t18\_sdes\_c\_ctr\_all.txt. Шифр SDES. Режим CTR. iv= 261.

**Вариант 13**

Расшифровать файл im35\_sdes\_c\_cbc\_all.bmp. Шифр SDES. Режим CBC. Key = 904, iv= 46. Зашифровать, оставив первые 50 байт без изменения.

**Вариант 14**

Расшифровать файл im36\_sdes\_c\_ofb\_all.bmp. Шифр SDES. Режим OFB. Key = 952, iv= 201. Зашифровать, оставив первые 50 байт без изменения.

**Вариант 15**

Расшифровать файл im37\_sdes\_c\_cfb\_all.bmp. Шифр SDES. Режим CFB. Key = 862, iv= 221. Зашифровать, оставив первые 50 байт без изменения.

**Вариант 16**

Расшифровать файл m26\_sdes\_c\_ctr\_all.bmp. Шифр SDES. Режим CTR. key=87, iv=69. Зашифровать, оставив первые 50 байт без изменения.

# Литература

[1] Schaefer E, “A Simplified Data Encryption Standard Algorithm”, Cryptologia, Vol .20, No.1, pp. 77-84, 1996.

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