Оглавление

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.