Электронное пособие по криптографии

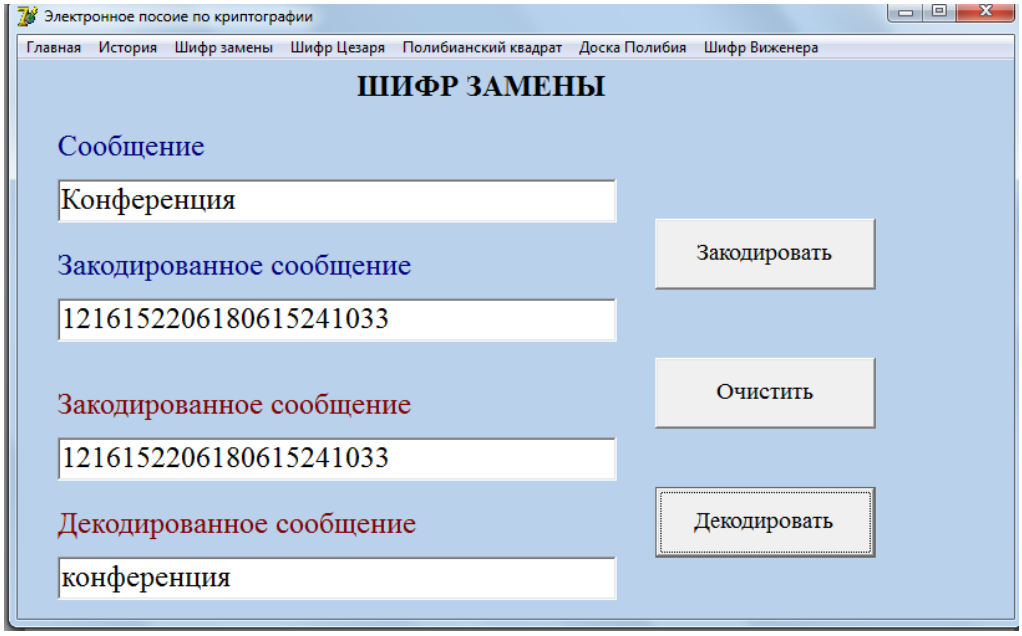
Водальчук Светлана Алексеевна,

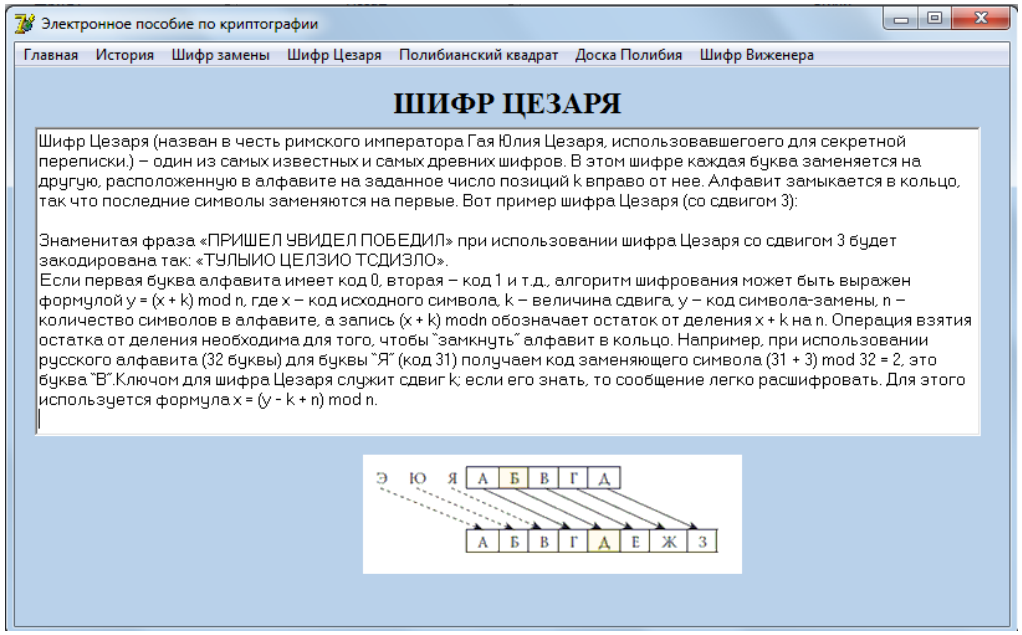
учитель математики, информатики

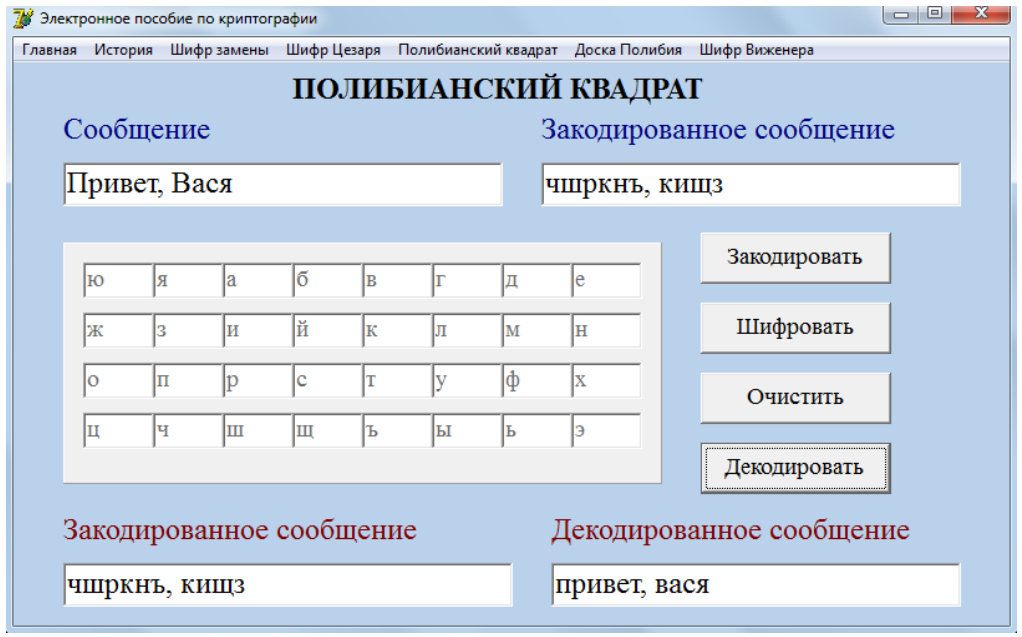
Лицей №36 ОАО «РЖД»

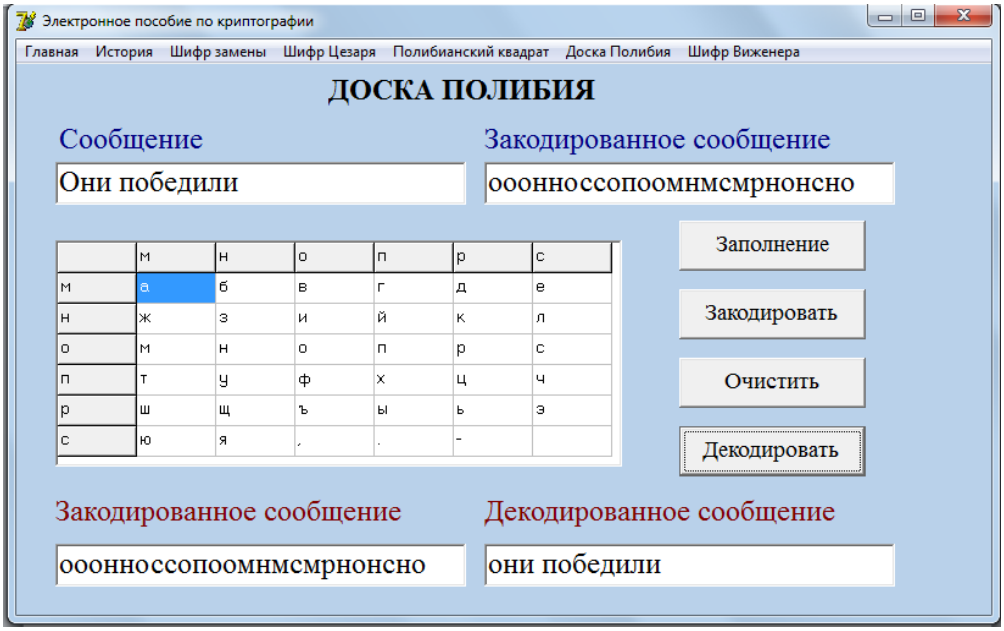
Электронное пособие по криптографии содержит программы, автоматизирующие алгоритмы шифрования – шифр замены, шифр Цезаря, Полибианский квадрат, доска Полибия, шифр Виженера. Электронное пособие разработано в среде программирования Delphi. Практической значимостью работы является привлечение внимания к изучению проблем защиты информации в общеобразовательной школе. Часть вопросов защиты информации может быть изучена в рамках школьной программы по информатике и математике.

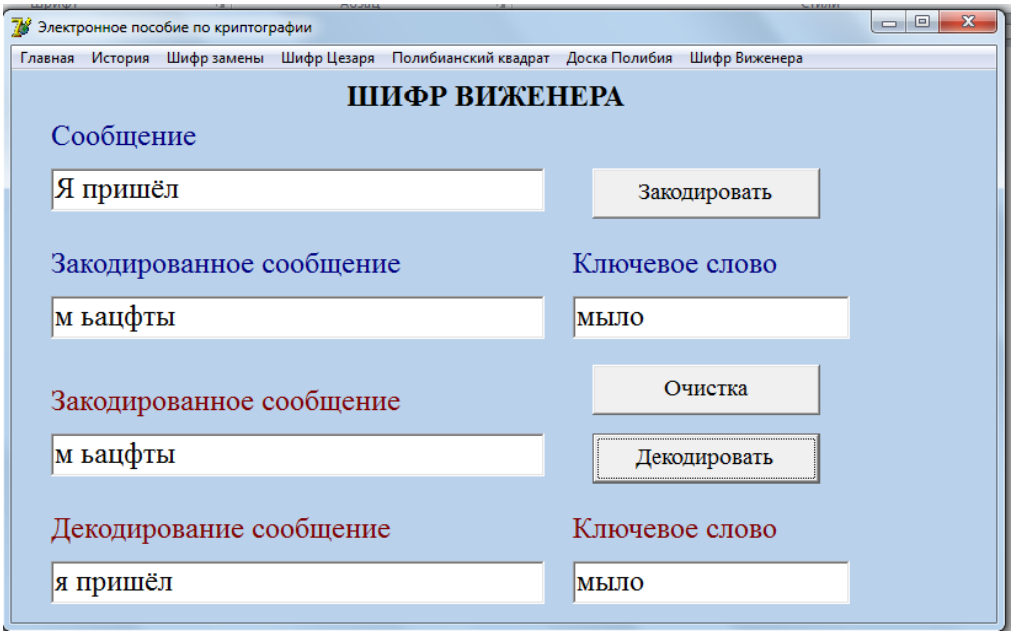
Главная форма электронного пособия


Электронное посоие по криптографии
Главная
История
Шифр замены
Шифр Цезаря
Полибианский квадрат
Доска Полибия
Шифр Виженера
ШИФР ЗАМЕНЫ
Сообщение
Конференция
Закодировать
Закодированное сообщение
121615220618061524 1033
Очистить
Закодированное сообщение
121615220618061524 1033
Декодировать
Декодированное сообщение
конференция


Электронное пособие по криптографии
Главная
История
Шифр замены
Шифр Цезаря
Полибианский квадрат
Доска Полибия
Шифр Виженера
ШИФР ЦЕЗАРЯ
Шифр Цезаря (назван в честь римского императора Гая Юлия Цезаря, использовавшегоего для секретной переписки.) – один из самых известных и самых древних шифров. В этом шифре каждая буква заменяется на другую, расположенную в алфавите на заданное число позиций k вправо от нее. Алфавит замыкается в кольцо, так что последние символы заменяются на первые. Вот пример шифра Цезаря (со сдвигом 3):
Знаменитая фраза «ПРИШЕЛ УВИДЕЛ ПОБЕДИЛ» при использовании шифра Цезаря со сдвигом 3 будет закодирована так: «ТУЛЫИО ЦЕЛЗИО ТСДИЗЛО».
Если первая буква алфавита имеет код 0, вторая – код 1 и т.д., алгоритм шифрования может быть выражен формулой y = (x + k) mod n, где x – код исходного символа, k – величина сдвига, y – код символа-замены, n – количество символов в алфавите, а запись (x + k) modn обозначает остаток от деления x + k на n. Операция взятия остатка от деления необходима для того, чтобы "замкнуть" алфавит в кольцо. Например, при использовании русского алфавита (32 буквы) для буквы "Я" (код 31) получаем код заменяющего символа (31 + 3) mod 32 = 2, это буква "В".Ключом для шифра Цезаря служит сдвиг k; если его знать, то сообщение легко расшифровать. Для этого используется формула x = (y - k + n) mod n.
Э Ю Я А Б В Г Д
А Б В Г Д Е Ж З


Электронное пособие по криптографии
Главная
История
Шифр замены
Шифр Цезаря
Полибианский квадрат
Доска Полибия
Шифр Виженера
ПОЛИБИАНСКИЙ КВАДРАТ
Сообщение
Привет, Вася
Закодированное сообщение
чшркнъ, кищз
ю я а б в г д е
ж з и й к л м н
о п р с т у ф х
ц ч ш щ ъ ы ь э
Закодировать
Шифровать
Очистить
Декодировать
Закодированное сообщение
чшркнъ, кищз
Декодированное сообщение
привет, вася


Электронное пособие по криптографии
Главная
История
Шифр замены
Шифр Цезаря
Полибианский квадрат
Доска Полибия
Шифр Виженера
ДОСКА ПОЛИБИЯ
Сообщение
Они победили
Закодированное сообщение
ооонноссопоомнмсмрнонсно
м н о п р с
м а б в г д е
н ж з и й к л
о м н о п р с
п т у ф х ц ч
р ш щ ъ ы ь э
с ю я , . -
Заполнение
Закодировать
Очистить
Декодировать
Закодированное сообщение
ооонноссопоомнмсмрнонсно
Декодированное сообщение
они победили


Электронное пособие по криптографии
Главная
История
Шифр замены
Шифр Цезаря
Полибианский квадрат
Доска Полибия
Шифр Виженера
ШИФР ВИЖЕНЕРА
Сообщение
Я пришёл
Закодировать
Закодированное сообщение
м ьацфты
Ключевое слово
мыло
Очистка
Закодированное сообщение
м ьацфты
Декодировать
Декодирование сообщение
я пришёл
Ключевое слово
мыло