Компьютерный практикум 3

***Задание:*** сформировать систему шифрования с помощью замены, с использованием случайного смещения протестировать ее.

1. Реализовать проект на Delphi.
	1. С помощью средств визуализации спроектировать форму.
		1. Элементы текстовых сообщений являются элементами типа Label.
		2. Для реализации ввода сообщения берется элемент Edit, который позволяет вводить данные по умолчанию, так и непосредственно пользователем при работе с системой.
		3. Для вывода результата шифрования и дешифрования используется так же элемент Edit, который модифицируется во время выполнения программы.
		4. Кнопка «Сброс» позволяет сбрасывать введенное сообщение при ошибке или при формировании нового сообщения.
	2. Алгоритм шифрования заменой начинает работать при нажатии кнопки «шифровать».
		1. Для реализации алгоритма необходимо щелкнуть 2 раза по кнопке, перейти в режим кодирования.
		2. В режиме кодирования написать программу кодирования путем замены, для замены использовать функцию Random от случайного числа. Выбранное случайное число будет являться паролем для шифрования сообщения и его дешифровки.
		3. Шифрование производится путем использования функции XOR и пароля. Пример замены в программе:

m(i) = Int(Random(pass) \* 32) Xor m(i), где

m(i) – код символа сообщения;

Random(pass) – случайная величина, где в качестве аргумента взят пароль

* + 1. Запустить проект, ввести сообщение и посмотреть результат шифрования.
	1. Алгоритм дешифрования заменой начинает работать при нажатии кнопки «дешифровать».
		1. Для реализации алгоритма необходимо щелкнуть 2 раза по кнопке, перейти в режим кодирования.
		2. В режиме кодирования написать программу раскодирования путем замены, для замены использовать симметричную функцию дешифрования.

m(i) = Int(Random(pass) \* 32) Xor m(i), где

m(i) – код символа сообщения;

Random(pass) – случайная величина, где в качестве аргумента взят пароль.

Получается симметричное преобразование сообщения.

* + 1. Запустить проект, ввести сообщение и посмотреть результат шифрования и дешифрования.

Введенное сообщение и расшифрованное должны быть идентичны!!!

* 1. Протестировать полученную систему.
		1. Вводить различные сообщения и сравнивать с результатом дешифровки.
		2. Определить диапазон значений, где система работает безошибочно.