УДК: 004.41

В. А. Колодко, маг.;
Н. Н. Пустовалова, доц., канд. техн. наук (БГТУ, г. Минск)

РЕАЛИЗАЦИЯ КРИПТОГРАФИЧЕСКОГО АЛГОРИТМА ШИФРОВАНИЯ

Основой создания метода шифрования стала легендарная машина Enigma. Ее алгоритм в свое время был уникальным и для взлома документа требовалось немалое количество времени. Однако этот алгоритм можно усовершенствовать и создать более криптостойкий алгоритм шифрования.

При реализации нового алгоритма возникла проблема передачи настроек для шифрования и дешифрования данных. В исходном алгоритме Enigma, настройки были прописаны заранее и в передаче сообщения участвовал только зашифрованный текст.

В разработанном алгоритме был сделан набор настроек на каждый день в году, что позволило избавиться от необходимости в передаче настроек для дешифрования. Получатель и отправитель имеют одинаковый набор настроек, что дает им возможность безошибочно зашифровывать и расшифровывать сообщения.

Особенность алгоритма заключается также в том, что для расшифровки данных не требуется передача открытого ключа. Настройки можно задавать свои, что тоже способствует криптостойкости алгоритма. Для реализации алгоритма шифрования был использован язык программирования C#. Класс TheSecretSettings предназначен для настройки использования метода шифрования и дешифрования на каждый день в году, то есть всего триста шестьдесят шесть настроек.

Основной класс, TheSecret, имеет десять «Роторов», в которых случайным образом записаны буквы латинского и русского алфавита, большого и маленького регистра, цифры. Суть алгоритма заключается в том, что выбирается метод из класса TheSecretSettings, а именно, три «Ротора» из десяти. Сообщение, попавшее в функцию шифрования, посимвольно подвергается кодировке.

Далее по разработанной схеме выбираются символы из «Роторов» и окончательный вариант и будет являться закодированным символом для символа из сообщения, которое необходимо зашифровать.

Дешифрование происходит в обратном порядке.

Алгоритм полезен в любой сфере, например, для конфиденциальности мессенджеров, для аутентификации, для обычного хранения данных в зашифрованном виде, для использования внутри компании, для обеспечения конфиденциальности в случае несанкционированного доступа.