СЕКЦИЯ 4.

ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ

КРИПТОГРАФИЧЕСКИЙ МЕТОД ШИФРОВАНИЯ И РАСШИФРОВКИ ДАННЫХ НА ОСНОВЕ АЛГОРИТМА МАШИНЫ ЭНИГМА

Колодко Вадим Анатольевич

магистрант,
Белорусский государственный технологический университет,
Беларусь, г. Минск

Пустовалова Наталья Николаевна

доц., канд. техн. наук,
Белорусский государственный технологический университет,
Беларусь, г. Минск

CRYPTOGRAPHIC METHOD OF DATA ENCRYPTION AND DECRYPTION BASED ON THE ENIGMA MACHINE ALGORITHM

Vadim Kolodko

Master's degree student,
Belarusian state technological University,
Belarus, Minsk

Natalia Pustovalova

Associate Professor, candidate of technical Sciences,
Belarusian state technological University,
Belarus, Minsk

АННОТАЦИЯ

Целью работы является разработка криптографического алгоритма, который включает в себя методы шифрования и расшифровки данных, а также механизм, который автоматически выбирает настройки для процесса шифрования и расшифровки данных.

В работе использован метод разработки алгоритма шифрования и расшифровки на основе машины Энигма.

В результате был создан новый криптостойкий алгоритм шифрования и расшифровки данных, а также механизм, который автоматически выбирает настройки.

ABSTRACT

The goal of this work is to develop a cryptographic algorithm that includes two methods of data encryption and decryption, as well as a mechanism that automatically selects settings for the data encryption and decryption process.

The paper uses the method of studying and analyzing the encryption and decryption algorithm of the Enigma machine.

As a result, a new cryptographic algorithm for data encryption and decryption was developed. As well as the mechanism that automatically selects settings.

Ключевые слова: Энигма, защита информации, публичный ключ, секретный ключ, механизм, криптостойкий.

Keywords: Enigma, information security, public key, secret key, mechanism, cryptographic.

На сегодняшний день вопрос о защите данных, об информационной безопасности стоит очень остро. Множество компаний, будь это банк, магазин, кинотеатр или фастфуд, пытаются упростить взаимодействие с клиентами, идти в ногу со временем. С этим связанно появление и активное развитие таких продуктов, как мобильные приложения различных банков, множество сайтов для взаимодействия продавцов с клиентами (aliexpress, aviasales, booking и многие другие), личные кабинеты в сервисах, где можно забронировать либо купить билет на сеанс фильма, заказать номер в отеле. В недалеком прошлом популярными стали сервисы аренды велосипедов, электросамоваров, автомобилей и др.

Все эти программные продукты связывает одно – необходимость защиты персональных данных пользователей. Без информационной защиты личных данных клиентов (таких, как личный номер, адрес регистрации, личный номер телефона, личный почтовый адрес, банковские счета, номера банковских карт) данными продуктами никто попросту не пользовался бы.

Защита может и должна применяться на различных уровнях. Будь это защита сервера, либо защита самой информации в базе данных. Безусловно, полную защиту данных гарантировать никто не может. Вне зависимости от уровня защиты, вне зависимости от метода хранения, утечку информации может допустить сам клиент. Может также случиться перепад напряжения, личная информация может подвергнуться атакам злоумышленников при передаче ее по сети. В таких случаях хорошо помогают различные методы шифрования.

Многие методы шифрования хороши по-своему. Возьмем для примера всем известный алгоритм RSA: криптостойкость данного алгоритма хорошая. В алгоритме используются секретный и публичный ключ (для шифрования текста используется секретный ключ, а для его расшифровки – публичный). Таким образом для двух клиентов необходимо иметь две пары секретных ключей и две пары публичных ключей. При передаче данных одна из сторон должна знать публичный ключ противоположной стороны, либо данный ключ должен приходить вместе с шифротекстом, что является недостатком метода.

В данной работе представлен метод, идея которого была позаимствована у алгоритма машины Энигма [1, 2].

Что, если в сети будет передаваться только один шифротекст без всяких намеков на секретный ключ? Был разработан механизм выбора настроек для шифрования и расшифровки данных, что избавляет от необходимости передавать ключ по сети, уменьшает риск взлома при атаке злоумышленников, что является преимуществом перед многими алгоритмами шифрования.

Был создан класс TheSecretSettings, в котором указаны настройки 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. В основном классе присутствуют также функции шифрования и дешифрования. Блок-схема метода шифрования и расшифровки представлена на рисунке 1.

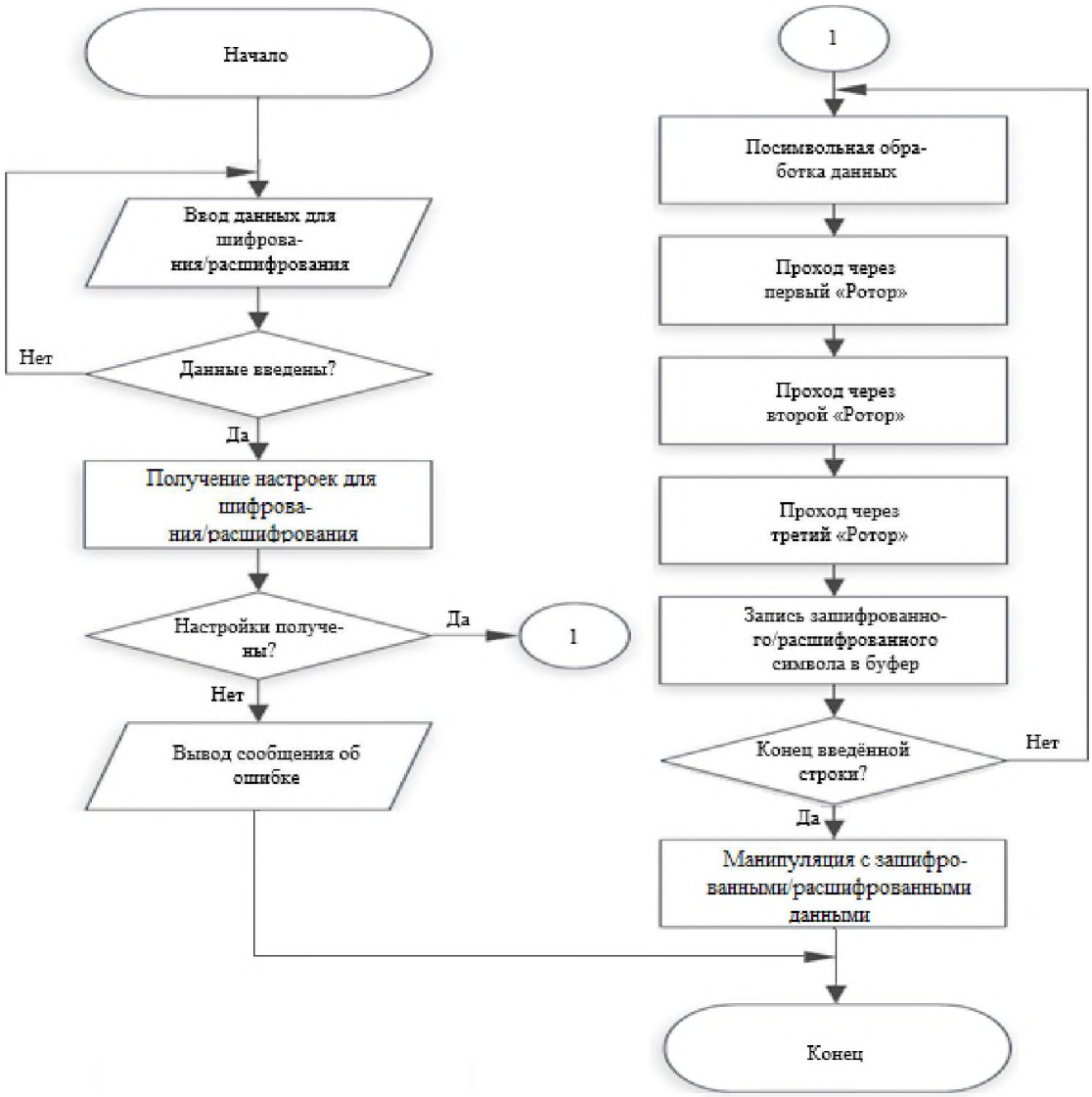

Рисунок 1. Блок-схема метода шифрования и расшифрования

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.

С первого «Ротора» выбирается символ, соответствующий выбранному символу из сообщения, которое необходимо зашифровать. В первом «Роторе» запоминается позиция данного символа и из стандартного «Ротора» записывается символ, соответствующий этой позиции.

Со второго «Ротора» выбирается символ, который соответствует выбранному символу из стандартного «Ротора». Во втором «Роторе» запоминается позиция данного символа и из стандартного «Ротора» записывается символ, соответствующий этой позиции.

С третьего «Ротора» выбирается символ, который соответствует выбранному символу из стандартного «Ротора». В третьем «Роторе»

запоминается позиция данного символа и из стандартного «Ротора» записывается символ в буфер. Именно этот символ и будет являться закодированным символом для символа из сообщения, которое необходимо зашифровать.

Дешифрование происходит наоборот: из стандартного ротора выбирается символ, соответствующий выбранному символу сообщения, которое необходимо зашифровать. В стандартном «Роторе» запоминается позиция символа и из третьего «Ротора» записывается символ, соответствующий позиции. Далее происходит поиск записанного символа в стандартном «Роторе», запоминается позиция символа, и из второго «Ротора» записывается символ, соответствующий позиции. Затем записанный символ ищется в стандартном «Роторе», запоминается позиция символа, и из первого «Ротора» записывается символ в буфер. Именно этот символ и будет являться раскодированным символом для символа из сообщения, которое необходимо расшифровать.

Особенность разработанного алгоритма заключается в том, что для расшифровки данных не требуется передача открытого ключа. Настройки можно задавать свои, что тоже способствует криптостойкости алгоритма.

Для реализации метода шифрования и расшифровки был использован язык программирования C#.

Список литературы:

1. Рижменантс, Дирк. Технические детали Энигмы. Шифровальные машины и криптология.
2. Kruh L., Deavours C. The commercial Enigma: beginnings of machine cryptography.