REVIEW

of the foreign research advisor for the thesis of doctoral candidate (PhD) Khompysh Ardabek on the theme «Development study of information protection algorithm using the non positional number system (scale of notation)» submitted for the PhD degree of a doctor in the specialty 6D100200 - Information Security Systems

Telecommunication systems are the basis of modern world information systems. Data circulating in such systems may contain valuable information. Therefore, the attacker is trying to steal them, use them illegally or change them. For this reason, in recent years, information security and information security are topical issues.

Of the various ways to protect information, cryptographic methods occupy a special place. New achievements of cryptography allow to solve not only the classic protection against unauthorized use of data, but also many other issues. Therefore, one of the urgent problems is the creation of information security tools that meet modern requirements.

One of the promising areas of data stream encryption is the use of the mathematical apparatus of extended Galois fields $GF(p^v)$. In turn, encryption systems using finite Galois $GF(p^v)$ fields have greater capabilities for implementing various cryptographic functions to ensure the confidentiality and integrity of information. The use of basic additive and multiplicative operations (addition modulo, multiplication modulo, exponentiation modulo) and their various combinations in such systems will increase the level of information security.

However, multiplicative operations associated with exponentiation and its inverse are among the most difficult to implement and require considerable time to reduce the execution time of this procedure, it is advisable to use a polynomial system of classes of deductions. In recent years there has been a trend that is directly related to the use of the mathematical apparatus of a ring of polynomials in cryptographic information security systems. This is largely due to the advantages of non-positional representation and data processing, first of all, the small number of residues allows to create cryptographic data protection systems that can provide high encryption speeds with a sufficiently high level of protection against unauthorized access.

During the preparation of the thesis of A. Hompysh, the complex and topical issues of cryptographic protection of information were considered and the ways of their solution were investigated.

The dissertation developed a symmetric encryption algorithm based on a non-positional polynomial number system. It was shown that the plaintext can be presented in the form of deductions for the modules of the working grounds.

In turn, an increase in the computation speed was achieved due to the independent encryption of the obtained open text deductions for the working

base modules and the resistance to various attacks was investigated taking into account the fact that the composition of the working bases is confidential. A software implementation of this algorithm was developed.

A new block encryption algorithm was also proposed, a method for improving the efficiency of selecting and calculating keys, the EM transformation (raising to a power modulo) and a new method for creating an S-box were described. In addition, it was shown that the algorithm can achieve higher performance, based on the features of primitives in the Galois field $GF(p^v)$. To increase the speed of the encryption algorithm, a nonpositional polynomial number system and an index table of working bases are used. To implement the encryption algorithm, a program was developed in the C ++ programming language. To study the statistical security of the proposed algorithm, statistical and evaluation tests of encrypted texts were conducted. The results obtained were compared with the results of other algorithms.

The thesis work is a complete scientific research and contains valuable scientific results, which have been published in the press.

I believe that the thesis of Khompysh Ardabek «Development study of information protection algorithm using the non positional number system (scale of notation)» meets the requirements for a doctoral dissertation for the degree of Doctor of Philosophy (PhD) in the specialty 6D100200 - Information Security Systems, and has been performed at a high scientific and technical level.

Foreign Research Advisor:

Assoc.Prof.Dr. Muslum Arici

Kocaeli University, Turkey

«21» 12 2019

Doç. Dr. Müslüm ARICI

ПАРАҚТЫҢ АРҒЫ ЖАҒЫНА ҚАРАҢЫЗ
СМ. НА ОБОРОТНОЙ СТОРОНЕ

ОТЗЫВ

зарубежного научного консультанта на диссертационную работу докторанта (PhD) Хомпыш Ардабека на тему «Разработка и исследование алгоритма защиты информации с использованием непозиционных систем счисления», представленную на соискание степени PhD доктора по специальности 6D100200 - Системы информационной безопасности

Телекоммуникационные системы являются основой современных мировых информационных систем. Данные, циркулирующие в таких системах, могут содержать ценную информацию. Поэтому злоумышленник пытается их украсть, несанкционированно использовать или изменить. По этой причине в последние годы обеспечение информационной безопасности и защита информации являются актуальными проблемами.

Из различных способов защиты информации криптографические методы занимают особое место. Новые достижения криптографии позволяют решать не только классическую защиту от несанкционированного использования данных, но и многие другие вопросы. Поэтому одной из актуальных проблем является создание средств защиты информации, отвечающих современным требованиям.

Одним из перспективных направлений шифрования потока данных является использование математического аппарата расширенных полей Галуа $GF(p^v)$. В свою очередь, системы шифрования, использующие конечные поля Галуа $GF(p^v)$ обладают более широкими возможностями по реализации различных криптографических функций обеспечения конфиденциальности и целостности информации. Применение в таких системах основных аддитивных и мультипликативных операций (сложение по модулю, умножение по модулю, возведение в степень по модулю) и их различных комбинаций позволит повысить уровень защиты информации.

Однако, мультипликативные операции, связанные с возведением в степень и ей обратные относятся к наиболее сложным для реализации и требуют значительных временных затрат для сокращения времени выполнения данной процедуры целесообразно использовать полиномиальную систему классов вычетов. Последние годы наблюдается тенденция, которая напрямую связана с использованием в криптографических системах защиты информации математического аппарата кольца полиномов. Это во многом связано с достоинствами непозиционного представления и обработки данных, прежде всего, малочисленность остатков позволяет создавать системы криптографической защиты данных, способные обеспечивать высокие скорости зашифрования при достаточно высоком уровне обеспечения защиты от НСД(несанкционированный доступ).

В ходе подготовки диссертационной работы А. Хомпыш были рассмотрены сложные и актуальные вопросы криптографической защиты информации и исследованы способы их решения.

В диссертации разработан была алгоритм асимметричного шифрования на основе непозиционной системы счисления.

Было показано, что открытый текст может быть представлен в виде вычетов по модулям рабочих оснований. В свою очередь достигнуто увеличение скорости вычислений за счет независимого шифрования полученных вычетов открытого текста по модулям рабочих оснований и исследована устойчивость к различным атакам с учетом того, что состав рабочих оснований является конфиденциальным. Была разработана программная реализация этого алгоритма.

Также был предложен новый алгоритм блочного шифрования, описан метод повышения эффективности выбора и вычисления ключей, преобразование EM (возведение в степень по модулю) и новый метод создания S-блока. Кроме того, было показано, что в алгоритме можно достичь более высоких показателей, опираясь на особенности примитивов в поле Галуа $GF(p^r)$. Для увеличения скорости алгоритма шифрования используются непозиционная полиномиальная система счисления и индексная таблица рабочих оснований. Для реализации алгоритма шифрования была разработана программа на языке программирования C++. Для исследования статистической безопасности предложенного алгоритма были проведены статистические и оценочные тесты зашифрованных текстов. Полученные результаты сравнивались с результатами других алгоритмов.

Диссертационная работа является законченным научным исследованием и содержит ценные научные результаты, которые опубликованы в печати.

Считаю, что диссертационная работа Хомпыш Ардабека «Разработка и исследование алгоритма защиты информации с использованием непозиционных систем счисления» удовлетворяет требованиям, предъявляемым к докторской диссертации на соискание ученой степени доктора философии (PhD) по специальности 6D100200 - Системы информационной безопасности, и выполнена на высоком научно-техническом уровне.

Зарубежный
Научный руководитель:
Doctor of Sciences,
As. professor. Kocaeli University, Turkey Muslum Arici/ Муслум Ариджи/

21 декабря 2019 год

ПАРАҚТЫҢ АРҒЫ ЖАҒЫНА ҚАРАҢЫЗ
СМ. НА ОБОРОТНОЙ СТОРОНЕ

Республика Казахстан, город Алматы, двадцать восьмое декабря две тысячи двадцатого года. Текст-перевод документа с английского языка на русский язык был выполнен переводчиком Мейрбек Құралай Мейрбекқызы, 18.02.1996 года рождения, ИИН 960218400219.

Подпись _____

Мейрбек Құралай Мейрбекқызы

Республика Казахстан, город Алматы, двадцать восьмое декабря две тысячи двадцатого года. Я, Юсупова Гульвира Киншпековна, нотариус города Алматы, действующий на основании государственной лицензии № 0002419 от 24 марта 2009 года, выданной Комитетом регистрационной службы и оказания правовой помощи Министерства юстиции Республики Казахстан свидетельствую подлинность подписи переводчика Мейрбек Құралай Мейрбекқызы. Личность переводчика установлена, дееспособность и полномочия проверены.

Зарегистрировано в реестре за № 2145
Взыскано 83 тенге

Нотариус _____
Юсупова Гульвира Киншпековна