ISSN 2414-9500

Молодежь. Общество. Современная наука, техника и инновации

Красноярск 2017

ISSN 2414-9500

Министерство образования и науки Российской Федерации
Сибирский государственный аэрокосмический университет
имени академика М. Ф. Решетнева

при поддержке

Министерства образования и науки Красноярского края

МОЛОДЕЖЬ. ОБЩЕСТВО. СОВРЕМЕННАЯ НАУКА, ТЕХНИКА И ИННОВАЦИИ

Материалы XVI Международной научной конференции бакалавров, магистрантов, аспирантов и молодых ученых (17 мая 2017, г. Красноярск)

Электронный сборник

Красноярск 2017

ISSN 2414-9500

Ministry of Education and Science of Russian Federation
Reshetnev Siberian State Aerospace University

with the support of

Ministry of Education and Science of Krasnoyarsk Territory

YOUTH. SOCIETY. MODERN SCIENCE, TECHNOLOGIES & INNOVATIONS

Collection of papers of the XVI-th International Scientific Conference of bachelor students, master students, post-graduate students and young scientists (May 17, 2017, Krasnoyarsk)

Electronic collection

Krasnoyarsk 2017

УДК 001
ББК 72
М75

Научное издание

М75 **Молодежь. Общество. Современная наука, техника и инновации** [Электронный ресурс] : материалы XVI Междунар. науч. конф. бакалавров, магистрантов, аспирантов и молодых ученых (17 мая 2017, г. Красноярск) : электрон. сб. / под общ. ред. И. В. Ковалёва, М. В. Савельевой, Н. А. Шумаковой ; Сиб. гос. аэрокосмич. ун-т. – Красноярск, 2017. – Электрон. текстовые дан. (1 файл, 5,33 МБ). – Систем. требования: Internet Explorer; Acrobat Reader 7.0 (или аналогичный продукт для чтения файлов формата .pdf). – Режим доступа к сб.: https://flcys.sibsau.ru/page/materials. – Загл. с экрана.

Сборник издается в соответствии с оригиналом, подготовленным редакционной коллегией, при участии редакционно-издательского отдела.

Информация для пользователя: в программе просмотра навигация осуществляется с помощью панели закладок слева; содержание в файле активное.

УДК 001
ББК 72

Подписано к использованию: 05.05.2017. Дата выхода в свет: 05.05.2017
Объем 5,33 МБ. С 139/17.

Макет и компьютерная верстка *Л. В. Звонаревой*

Редакционно-издательский отдел Сиб. гос. аэрокосмич. ун-та.
660037, г. Красноярск, просп. им. газ. «Красноярский рабочий», 31.
E-mail. : rio@sibsau.ru. Тел. (391) 201-50-99.

УДК 004.056.55

PROTOCOL OF SECURE DATA EXCHANGE BASED ON ENCRYPTION ALGORITHM WITH ALTERNATING BLOCK FRAGMENTATION

V. (V.) Mitrashchuk
Scientific Supervisor – V. (V.) Zolotarev
Foreign Language Supervisor – O. (V). Maslova

Reshetnev Siberian State Aerospace University, Krasnoyarsk, Russian Federation

Encryption algorithm with alternating block fragmentation, for which an encryption program with the speed of 120 Kbyte/s has been developed, is shown in this article. Schemes of message authentication and subject authentication for data exchange protocol are suggested. The solution will be implemented for connection with drone aircraft, concealed electronic lock, secure data exchange via "Internet" and in some other spheres.

Keywords: information encryption, transmission protocol, secure data exchange, symmetrical key, alternating block fragmentation.

ПРОТОКОЛ БЕЗОПАСНОГО ОБМЕНА ДАННЫМИ НА ОСНОВЕ АЛГОРИТМА ШИФРОВАНИЯ С ПЕРЕМЕННОЙ ФРАГМЕНТАЦИЕЙ БЛОКА

В. В. Митращук
Научный руководитель – В. В. Золотарёв
Руководитель по иностранному языку – О. В. Маслова

Сибирский государственный аэрокосмический университет
имени академика М. Ф. Решетнева, Российская Федерация, г. Красноярск

Показан алгоритм шифрования с переменной фрагментацией блока, для которого разработана программа-шифратор со скоростью 120 кбайт/с. Предложены схемы имитовставки и аутентификации для протокола передачи данных. Решение будет применено для связи с беспилотным летательным аппаратом, скрытым электронным замком, безопасного обмена данными по сети Интернет и в других направлениях.

Ключевые слова: шифрование информации, протокол передачи, безопасный обмен данными, симметричный ключ, переменная фрагментация блока.

Necessity in data protection exists almost in every sphere. There are numerous encryption algorithms and data transmission protocols based on them. Thus constant extension of calculating characteristics of electronic devices and appearance of first quantum computers [1] make us think of perfect encryption methods.

Practically, all symmetrical encryption, which exist nowadays, operate on invariable algorithms with the ability key modification and at best S-block and number of encryption rounds. Growth of such codes reliability can be ensured only by encryption block's length extension with simultaneous extension of key size.

At the same time, if there are opportunities for brute-force and at least one pair of the source and encrypted text (defined, for example, by well-known protocol structure), then we can just brute-force all variants of the key, until we get the correct source text. To avoid such situations, encryption algorithm is made secret completely or, for example, only S-block is made secret. Thus, anyone who has this information, even legal users, can get other users keys. In case S-block is unknown,

there is still the possibility of hacking, by brute-force all S-blocks and filtering them according to the known sequence of several blocks consists of source and encrypted text.

To avoid this, at the same time leaving the encrypted algorithm fully opened, it is necessary to change not only sequence of the key, but also all algorithm parameters. All this was realized in encryption algorithm program "Solaris" [2] for OS Windows and Linux, which allows to change randomly such parameters as general key, block and key displacement, two sequential block fragmentations for replacement and addition to key of round, way and type of replacement. Encryption speed is 120 Kbyte/s now. In future, it is possible to increase this figure by using a low-level or hardware software, parallelization and graphic processes.

Block replacement by S-block [3; 4] allows shuffling of consecutive blocks combinations, thereby creating text chains of the same blocks, but in different sequences, and consequently the content. Preliminary block variable fragmentation will provide a significant growth in variability of such chains shuffles combinations, the number of different texts at output (Figure 1). The following block's displacement and variable fragmentation before addition to the key will provide a linear displacement of blocks' combinations relative to each other, which together with variable fragmentation before replacement will provide enough combinations number of consecutive text blocks to ensure there is no possibility to determine which of text is true after the brute-force attack.

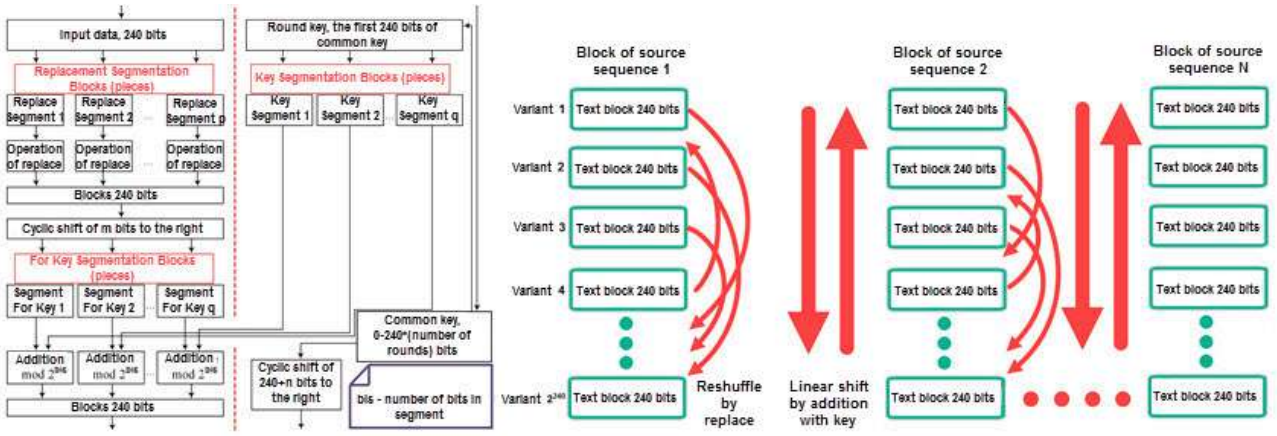

Fig. 1. Scheme of "Solaris" algorithm operation and displacement of sequences chains combinations during encryption

The more sequentially coupled pairs of source and encrypted texts hacker has, the easier is to carry out the cipher text's hacking, but it is difficult to obtain them, and usually the protocol package length is not very long. Moreover, it is possible to increase the database of S-block and the number of rounds. In addition, if this is not enough, it is always possible to increase the block's length or to use computing devices with more dimensions (for example, ternary computers) [5].

Based on the encryption algorithm "Solaris", implementation of secure data transmission protocol "Protocol 125" (Figure 2) becomes possible, which will be used for secure data exchange via Internet, connection to drone aircraft, concealed electronic lock and others.

Firstly, the protocol is expected to implement two modes of encrypted data transmission: not guaranteed delivery by UDP, guaranteed delivery by TCP. In addition, for practical usage, algorithms of message authentication and subject authentication with the use of a session key were developed.

Algorithm of message authentication by UDP (Figure 2), after generating the configuration and the initial key, encryption algorithm is as follows: the generation of the session key for the next cycle of reception and transmission; session key encryption by the primary key using Solaris algorithm with a predetermined configuration; transmission of encrypted session key; message encryption by the session key with the use of Solaris algorithm with a predetermined configuration; transmission of encrypted message. In case of message authentication by TCP, a new session key is sent

together with the message (Figure 2). If delivery confirmation did not come, it is sent as a separate message together with the session key identifier until it is delivered.

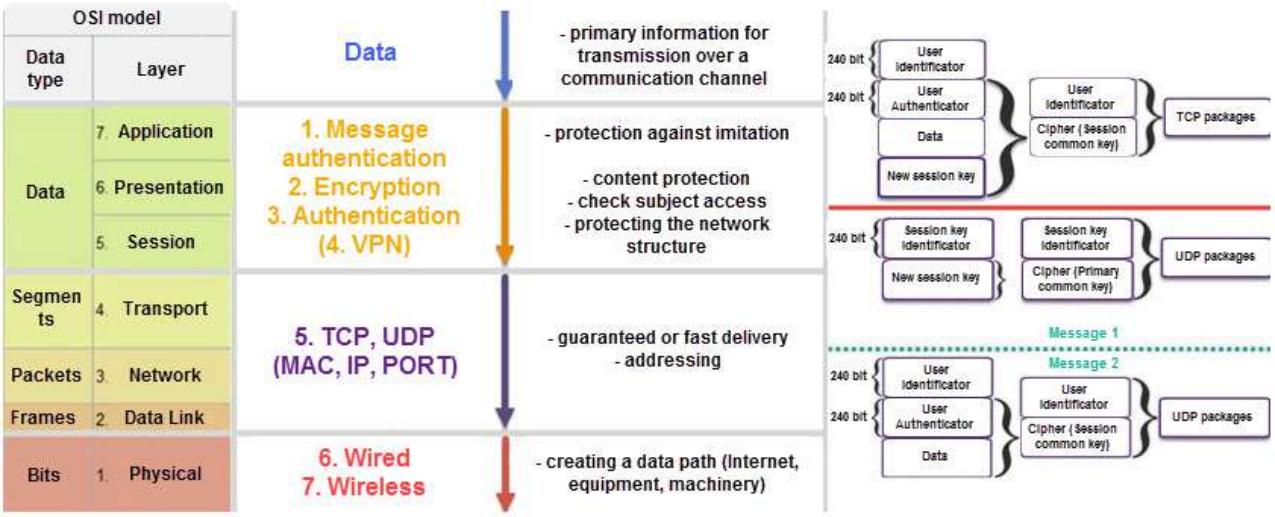

Fig. 2. Protocol key functions and schemes

Authentication mechanism is based on: providing each user a unique configuration and primary key of “Solaris” algorithm that remain unchanged until a new key issue; adding of index, which identifies user, who owns the key, to the encrypted message; placing the unique user data inside the encrypted message, by which authentication is performed after message decryption.

References

1. Sadovnichiy V. A. Kvantovyy komp'yuter i kvantovye vychisleniya (Quantum computers and quantum computing), Izhevsk. Izhevskaya respublikanskaya tipografiya. 1999. 288 p. (In Russ.)

2. Zhdanov O. N., Sokolov A. V. Algoritm shifrovaniya s peremennoy fragmentatsiey bloka (The encryption algorithm with variable block fragmentation): problemy i dostizheniya v nauke i tekhnike, vyp. 2). Omsk. Innovatsionnyy Tsentr Razvitiya Obrazovaniya i Nauki. 2015. Pp. 153–159. (In Russ.)

3. Lidl R., Niederreiter H. Introduction to finite fields and their applications. New York. Cambridge University Press. 1986. 416 p.

4. Gadiel S. Table of Low-Weight Binary Irreducible Polynomials, Hewlett. Computer Systems Laboratory HPL-98-135. 1998. 16 p.

5. Zhdanov O. N., Sokolov A. V. Block symmetric cryptographic algorithm based onprinciples: Far East Journal of Electronics and Communications Vol. 16, № 3. India. Pushpa Publishing House. 2016. Pp. 573–589.