УДК 312.26.004

Р. Г. Абдрахманов (МИФИ),
А. Е. Жуков (МГТУ им. Н.Э. Баумана)

ПОДСТАНОВОЧНО-ПЕРЕСТАНОВОЧНЫЕ ШИФРЫ

Предложен новый метод шифрования данных, основанный на преобразовании и перестановке блоков текста, причем блоки преобразуются и переставляются внутри массива большого размера в зависимости от текущего состояния рабочего ключа и шифруемой информации. Предложенный метод легко реализуется программным способом и обеспечивает рассеивание и перемешивание информации в пределах всего шифруемого массива данных.

Substitution and Permutation Codes / R.G. Abdrakhmanov, A.Ye. Zhukov // Vestnik MGTU. Priborostroenie. 2001. No. 3. P. 22–31.

A new method to code data is suggested on the basis of the transformation and permutation of text blocks inside the larger text block depending on the current state of the cipher key and encoded data. The method is easily implemented by programming means and provides diffusing and mixing data within the entire block of encoded data. Refs.5.

СПИСОК ЛИТЕРАТУРЫ

1. Preneel B., van Leekwijk W., van Linden L., Govaerts R., Vandewalle J. Propagation characteristics of boolean functions // Proc. Eurocrypt-90. Lect. Notes in Comp. Sci. – 1991. – V. 473. – P. 161–173.
2. Месси Дж. Л. Введение в современную криптографию // ТИИЭР. – 1988. – Т. 76. – № 5. – С. 24–42.
3. Menezes A. J., van Oorschot P. C., Vanstone S. A. Handbook of applied cryptography. – CRC Press, 1996.
4. Варфоломеев А. А., Жуков А. Е., Пудовкина М. А. Поточные криптосистемы. Основные свойства и методы анализа стойкости. – М.: Изд-во МИФИ, 2000.
5. Massey J. Shift-register synthesis and BCH decoding // IEEE Trans. Inf. Th. – 1969. – V. IT-15. – № 1. – P. 122–127.
6. Лидл Р., Нидеррайтер Г. Конечные поля. – М.: Мир, 1988.
7. Rueppel R. Analysis and design of stream ciphers. – Springer-Verlag, 1986.

Статья поступила в редакцию 26.03.2001

Руслан Габдрашитович Абдрахманов родился в 1977 г. Студент МИФИ. Специализируется в области защиты информации.

R.G. Abdrakhmanov (b. 1977). Student of Moscow Engineering and Physical Institute. Specializes in the field of data protection.

Алексей Евгеньевич Жуков родился в 1952 г., окончил в 1974 г. МГУ им. М.В. Ломоносова. Канд. физ.-мат. наук, доцент кафедры “Информационная безопасность” МГТУ им. Н.Э. Баумана. Автор более 50 научных работ в области защиты информации.

A.Ye. Zhukov (b. 1952) graduated from the Lomonosov Moscow State University in 1974. Ph.D. (Phys.-Math.), ass. professor of “Data Security” department of the Bauman Moscow State Technical University. Author of over 50 publications in the field of data security.