Mykhailo Lutsenko
I. V. Oleshko, research supervisor
K. T. Umyarov, language adviser
Kharkiv National University of Radioelectronics, Kharkov

Analysis of NESSIE Project Block Ciphers

Nowadays cryptography is an essential part of life, economics and business. Cryptographic algorithms are used in almost every electronic system in order to protect personal data, to maintain secure connections in computer networks and to restrict access to secret data for those who must not have such a privilege.

Block ciphers are one of the easiest, yet powerful kind of cryptographic algorithms. Their security goals are confidentiality and authenticity. They operate with fixed-length groups of bits, called blocks and belong to symmetric algorithms, i.e., they use a single key for both encryption and decryption of data.

The area of use for block ciphers spreads from small cash registers to major banking systems, from cellphones to enormous computer networks. Their simplicity, efficiency and reliability have made them an obvious choice for using in all these electronic systems.

NESSIE (New European Schemes for Signatures, Integrity and Encryption) was a European research project funded from 2000 to 2003 to identify secure cryptographic primitives. The NESSIE participants include some of the foremost active cryptographers in the world. Among forty-two submitted algorithms, twelve were selected as the most secure, reliable and recommended to use in five categories, which are block ciphers, public-key encryptions, MAC algorithms and hash functions, digital signature algorithms and identification schemes. Among twelve selected algorithms, four were block ciphers. The selected algorithms were MISTY1, Camellia, SHACAL-2 and well-known AES. These algorithms are still widely used as they are, or as basis for more difficult algorithms and cryptographic protocols.

As an example, this research introduces AES algorithm, which was firstly known as Rijndael and was the winner of Advanced Encryption Standard process. The algorithm is a prominent representative of block ciphers, based on substitution-permutation networks. It uses four complex operations to transform a block of plaintext into a cryptographic text or a cryptogram. This algorithm is widely used in computer networks for public key encryptions in cryptographic protocols to provide confidentiality, authenticity and integrity, which are the main goals for cryptography as a whole.

Block ciphers have been a major tool for information security for many years and they are still developing into more complex and secure cryptographic systems. Obviously, electronic system will stick to block ciphers for many years ahead due to their simplicity both for developers to realize and for electronic systems to implement.