Chapter 2
GOST Encryption Algorithm and Approaches to its Analysis

Ludmila Babenko
Southern Federal University, Russia

Evgeniya Ishchukova
Southern Federal University, Russia

Ekaterina Maro
Southern Federal University, Russia

ABSTRACT

This chapter considers approaches to analysis of the GOST 28147-89 encryption algorithm (also known as simply GOST), which is the basis of most secure information systems in the Russian Federation. As soon as the GOST algorithm is characterized by a simple structure and uses widely known mathematical operations, approaches to its analysis can be easily propagated to other cryptographic systems. In the conclusion, the authors consider some interesting observations that are related to the structure of GOST encryption and can be useful for further development of cryptanalysis.

INTRODUCTION

The GOST encryption algorithm is a state encryption standard in Russian Federation. The GOST 28147-89 algorithm is recommended by the Federal Security Service of Russia for building cryptographic protection systems for data of limited distribution (commercial secrets, personal data, etc.) Any cryptographic system of data protection certified by the Federal Security Service has to be built using only the following algorithms: GOST R 34.10-2001, GOST R 34.11-94, GOST 28147-89. That is why the majority of information systems for confidential data protection are based on GOST 28147-89. Besides that, this algorithm is used in the hash function described in GOST R34.11-94 and is included into RFC4357 as "id-GostR3411-94-CryptoProParamSet." For example, correspondence of commercial enterprises with pension funds, tax inspection, online auctions cannot be implemented with foreign cryptographic algorithms. GOST 28147-89 is also

DOI: 10.4018/978-1-4666-4030-6.ch002

used in biometric passports of Russian citizens for calculating hash values. Nowadays activities are carried out in Russia on implementing universal e-cards that will also use national cryptographic standards. Many Russian hardware and software data protection tools are based on GOST, such as CryptoPro CSP, VipNet CSP, Lissi CSP, Secret Disk, SafeDisk, Accord trusted boot module, Strazh, etc. Therefore one can conclude that GOST is widely used in many modern information systems.

Originally, the algorithm became known to the international community in 1994 when it was declassified and translated into English. Despite the fact that GOST was designed more than 20 years ago, in 2010 it was among the candidates for codification as an international encryption standard as ISO 18033.

At the session of the 27th ISO committee in 2010, a decision was made to initiate inclusion of GOST into the international standard ISO/IEC 18033.3..The first version was prepared in January, 2011. However, in February 2011 a presentation (Isobe, 2011) was made at Fast Software Encryption (FSE) symposium that contained results of successful application of Reflection – Meet in the Middle Attack (R MITM) against GOST. The attack against full-round GOST encryption demands 232 encryptions, i.e. the complexity of this attack is 2225. Besides that, after when voting on inclusion of GOST into ISO/IEC 18033.3 started, another research (Courtois, 2011) was published that makes strong assumptions about the possibility to break GOST with improved differential cryptanalysis. We should note that this work considers fixed s-boxes, which are different from those offered in ISO/IEC 18033-3.

As of January 27th 2012, the addendum on GOST 28147-89 was deleted from ISO/IEC 18033-3. The Russian party proposes to continue negotiations on considering GOST algorithm as an international standard and to proceed to the second version of proposals. Based on the publications mentioned above, one can make a conclusion that in order to make the decision about inclusion of GOST into ISO/IEC 18033.3, further research on its cryptographic strength should be carries out.

GOST encryption algorithm has four operation modes: simple substitution mode, stream mode, stream mode with feedback and authentication mode. Simple substitution mode is the basic one and all other modes contain it in their structure. We will consider only this mode in the chapter.

GOST algorithm is a symmetric block cipher, which conforms to Feistel scheme. 64-bit blocks of data are submitted to the input and converted into 64-bit blocks of encrypted data by 256-bit key. In each round the right side of plain text messages is processed by function F, which converts data with three cryptographic operations: adding data and subkey modulo 232, substitution of data using S-boxes, and left cyclic shift by 11 positions. Output of F-function is added modulo 2 to the left part of the plaintext, then right and left sides are swapped for next round. The algorithm has 32 rounds. In the last round of encryption right and left parts are not swapped. The overall dataflow diagram of GOST is shown in Figure 1.

GOST uses 8 S-boxes, which convert 4-bit input to 4-bit output. Unlike most encryption algorithms, GOST has no predefined S-boxes and any values can be used for them.

Secret key contains 256 bits and is represented as a sequence of eight 32-bit words: K1, K2, K3, K4, K5, K6, K7 and K8. In each round of encryption one of these 32-bit words is used as a round subkey. When round subkey is calculated, the following principle is used: from round 1 to round 24 the order is straight, (K1, K2, K3, K4, K5, K6, K7, K8, K1, K2, etc.); from round 25 to round 32 reversed order is used (K8, K7, K6, K5, K4, K3, K2, K1).

The more detailed description of GOST and its modes can be found in (Popov, Kurepkin, & Leontiev, 2006). Thus, it appears that the same subkey K1 is used at both the first and the last rounds. As we can see from the description of the algorithm, the round transformation has a rela-