Government Standard of the U.S.S.R. 28147—89
Cryptographic Protection for Data Processing Systems

Translated from the Russian by

Aleksandr Malchik

Sun Microsystems Laboratories
Mountain View, California

with editorial and typographic assistance from

Whitfield Diffie

Sun Microsystems
Mountain View, California.

Preface to the English Translation

The Government Standard of the U.S.S.R. 28147—89, Cryptographic Protection for Data Processing Systems, appears to have played a role in the Soviet Union similar to that played by the U.S. Data Encryption Standard (FIPS 46). When issued, it bore the minimal classification 'For Official Use,' but is now said to be widely available in software both in the Former Soviet Union and elsewhere. In apparent contrast to DES's explicit limitation to unclassified information, the introduction to GOST 28147—89 contains the intriguing remark that the cryptographic transformation algorithm "does not place any limitations on the secrecy level of the protected information."

The algorithms are similar in that both operate on 64-bit blocks by successively modifying half of the bits with a function of the other half. Beyond that, the similarity declines and several differences are visible.

- The Soviet system has 32 rounds rather than the 16 of DES.
- Each round is somewhat simpler than a round of DES. In the 'f' function, 32 bits of text are added modulo 32 to 32 bits of key, transformed by a block of eight, 4-bit to 4-bit S-boxes and rotated 11 bits to the left.
- In contrast to DES's meager 56 bits of key, GOST 28147—89 has 256 bits of primary key and 512 bits of secondary key. The secondary key is

the block of eight S-boxes, which are specific to individual networks and are not included in the standard.

- In place of the complex key schedule of DES, the primary key is divided into eight 32-bit words. For the first twenty-four rounds, these are used cyclically in ascending order. For the last eight, they are used in descending order.

The standard is also somewhat broader that FIPS46. It includes output feedback and cipher feedback modes of operation, both limited to 64-bit blocks, and a mode for producing message authentication codes.

The translation is intentionally colloquial, preferring standard English terms to charmingly quaint cognates of the Russian. The objective is to make it easy for English speaking cryptographers to identify what is novel with minimal effort. In some places, particularly the glossary, this has changed the wording considerably and a few remarks on some of the freeer choices, seems in order.

In Russian, the expression 'the GAMMA of a cipher' means the keystream and the term for an additive keystream cipher is 'GAMMIROVANIA.' This has been translated as 'output feedback,' because that is the way in which their keystream is generated and is the name of the corresponding mode in FIPS81.

The Russian term that literally translates 'keystream mode with feedback' corresponds to 'cipher feedback mode' and that term has been used throughout.

The Russian term for authentication translates, not unreasonably, as 'imitation insertion protection.' The term for authenticator, however, is literally the 'imitation insertion.' This has been rendered as 'message authentication code.'

Because of the substantial amount of mathematical notation, the translation has been typeset in TEX. The numbers in boxes in the margins show the approximate page boudaries in the original document.

Aside from the elimination of errors, which are undoubtedly still numerous, the translation is complete except for the diagrams, which will be added when a flowchart program with TEX compatible Postscript output is located. Please send comments and corrections by email to:

whitfield.diffie@Eng.Sun.Com or on paper to me at:

Sun Microsystems, MTV14-203
2550 Garcia Avenue
Mountain View, CA 94043

Whitfield Diffie
Distinguished Engineer
October 1993

References

Data Encryption Standard, National Bureau of Standards, Federal Information Processing Standard Publication No. 46, January 1977.

DES Modes of Operation, , National Bureau of Standards, Federal Information Processing Standards Publication No. 81, September 1980.