

It is necessary to underline, that given results should be considered only as dynamic reflection of complex realization variants effectiveness depending on initial keys length and should not be considered as univalent acknowledgement of small value of this length advantages. Generally, initial keys length will be commensurable with initial keys length in the modern ciphers. It is why initial key structure should contain bits assigning virtual sample space discrete form aspect, and also discrete sampling, quantization and scaling parameters.

As a whole, from complex probing follows that its realization in random sequences generator mode is potentially capable to provide indexes that considerable exceed known analogs. Taking into account, that development of a casual (pseudorandom) sequence makes unrolled key forming basis which performances finally determine encryption quality. Obtained lead-out may be generalized on all developed software complex modes.

Given results are obtained at Russian Federation Education Ministry grant (T02-03.1-816) support.

NEW APPROACH TO INFORMATION TECHNOLOGIES QUANTATIVE QUALITY ESTIMATION

Kotenko V.V., Rumjantsev K.E., Polikarpov S.V., Levendyan I.B.

Taganrog State University of Radioengineering,
Taganrog

Progressing growth of information technologies value in the modern world demands perfecting theoretical and practical basis of their protection. It generates problems which solution is rather inconvenient from positions of public approaches to a privacy. The major problem is protection quality estimation. First of all this problem appears in ciphers quality rating vagueness. The reference direction of it was definition of the so-called standard of encryption of XXI century which was carried out within the framework of National Standards institute of Standards and Technologies (NIST) USA conferences series

in 1997-2000 The fact is that the best cipher was chosen only by participants of the Third Conference (April 2000) votes. Results of this voting (RIJNDAEL-86, SERPENT 59, TWOFISH-31, RC6-23, MARS-13) determined the best XXI century algorithm RIJNDAEL, obtained during implementation of AES project.

The researches which have been carried out by authors shows that the marked problem may be solved from positions of the approach offering virtual conception of the encryption process. Using of this approach allowed authors to receive analytical expressions for efficiency $D(\Phi, u)$ of encryption Φ and to create software complex, which distinctive features are: 1) possibility of encryption efficiency quantitative estimation, including real-time processing; 2) registration of messages, keys and cryptograms bands statistical performances during encryption; 3) registration of messages radiants information performances influences (first of all redundancies).

Using of the created complex for quality estimation of the ciphers listed above has suggested competency of NIST guidelines. So, efficiency of algorithm RIJNDAEL (fig. 1) for radiants u_A of the English language is $D(\Phi, u_A) = -7.4604 * 10^{-3}$, That corresponds higher protection quality comparison with algorithm SERPENT, for which $D(\Phi, u_A) = -8.0781 * 10^{-3}$. The negative values $D(\Phi, u_A)$ mean, that these algorithms do not meet requirements for theoretical undecoding capability which is showed at $D(\Phi, u) \geq 0$. In this case higher protection quality of encryption means values $D(\Phi, u)$ tented to zero in the negative axis.

Using of the offered approach and the program complex created on its basis opens fundamentally new area of researches in the field of information technologies protection quality estimations. Given results are obtained at Russian Federation Education Ministry grant (T02-03.1-816) support.

