# A methodology for symmetric encryption algorithms evaluation

*M. Stanek, D. Olejar*
*Comenius University Bratislava*

*Department of Computer Science, Faculty of Mathematics and Physics of Comenius University,*
*Mlynska dolina, 842 15 Bratislava, Slovakia*
*e-mail: {stanek, olejar}@dcs.fmph.uniba.sk*

**Abstract**
Encryption algorithms are often used in various applications to protect sensitive data. The lack of analysis in many systems has drawn our attention to the need for a methodology for symmetric encryption algorithms evaluation. The methodology should serve as a guide for designers of algorithms and also for customers, nonspecialists. Our paper provides the first step towards developing such methodology.

**Keywords**
**Symmetric cryptosystem, evaluation**

## 1 INTRODUCTION

Cryptographic algorithms and protocols protect valuable or sensitive data processed in various information systems. They are able to provide confidentiality, integrity and authenticity of data. One of the most important methods of data protection is encryption. It is used to protect password files, sensitive information stored in databases and archives, e-mail, etc. Encryption and other cryptographic services enable electronic commerce on the Net (Wayner, 1997). Encryption has also become an important part of various standards: Secure Socket Layer – SSL

(Freier, Karlton and Kocher, 1996), Secure Hypertext Transfer Protocol – SHTTP, Secure Electronic Transaction – SET (SET, 1997).

Insufficient knowledge of cryptology and/or the attempts to avoid licence problems bring on the creation of many "home-made" cryptographic algorithms/products of very questionable quality. Most of them are symmetric encryption algorithms, since the design of asymmetric cryptosystems or of more advanced cryptographic protocols is out of scope of cryptographic laymen. To enable the users (and maybe the designers, too) to evaluate and compare symmetric encryption algorithms, a methodology providing evaluation criteria is needed. This paper should serve as the first step towards such methodology. We suppose the reader is familiar with basic notions of cryptology. If some problems appear, we recommend him/her to consult Meyer and Matyas (1982) or Konheim (1981).

## 2 GOALS AND SCOPE OF METHODOLOGY

The goals of our methodology are:

- to provide a unified approach to the initial description and evaluation of encryption algorithms;
- to provide a systematic view of the most important cryptographic parameters of encryption algorithms;
- to detect poorly designed encryption algorithms with serious flaws;
- to provide results in the form intelligible for nonspecialists.

The methodology is restricted to symmetric encryption algorithms and is organised in the following way:

- general classification and basic properties of algorithm;
- parameters and scheduling of keys;
- properties of cryptographic transformation;
- functional characteristics.

## 3 STRUCTURE OF METHODOLOGY

### 3.1 General classification and basic properties of symmetric cryptosystems

These facts describe fundamental properties of the algorithms:

1. Type of algorithm – whether the algorithm is block cipher or stream cipher.
2. Correctness – an encryption algorithm is correct if and only if for all keys and all plaintexts the decryption of ciphertext yields again the original plaintext.
3. Length of the input/output block (block ciphers).
4. Length of the plaintext/running key block (stream ciphers).
5. Algebraic type of transformations (block ciphers) – the basis of transformation, e.g. substitution-permutation network, Feistel cipher, cellular automata, etc.

6. Algebraic structure of a set of transformations (block ciphers) – whether the set of all transformations forms a group, …
7. The way the cipher treats the last incomplete (plaintext) block (block ciphers).
8. Length of the period (stream ciphers).
9. Cryptographic modes – all of them have to be listed and analysed in detail for their cryptographic strength and error propagation.

### 3.2 Parameters and scheduling of keys

The properties of a key and its influence on cryptographic transformation are also very important for evaluation. Some aspects should be considered:

1. Length of key, equivalent keys – the key should be long enough to avoid brute-force attacks. Two keys are equivalent if they lead to the same transformation. Large number of equivalent keys reduces the complexity of exhaustive key search.
2. Weak and suspicious keys – keys which reduce the strength of transformation. They should be enlisted and their influence upon algorithm analysed.
3. Key scheduling – length of subkeys, weak subkeys, equivalent subkeys, …

### 3.3 The properties of cryptographic transformations

Although the transformations of various symmetric encryption algorithms may be very different, there are some properties which every transformation used in cryptographic applications ought to have.

In stream ciphers the following parameters of the running key (besides the length of the period) belong to the most important (see Golomb (1967) or Rueppel (1986)):

1. Statistical parameters of the running key – probability of *n*-tuples of running key digits, autocorrelation, …
2. Cryptographic robustness of the running key sequence – unpredictability of the running key sequence.
3. Linear complexity profile of the running key sequence – good linear complexity profile (Rueppel, 1986).

The most important properties of block ciphers are:

1. Regularity – output values (keys, ciphertext blocks) should be equally probable.
2. Interdependence between bits of the key or plaintext and the ciphertext - the avalanche characteristics, e.g. every change of input (key, plaintext) should result in change of every ciphertext bit with 50% probability.
3. Dependence of the ciphertext bits – every ciphertext bit ought to be statistically independent of every subset of the remaining bits of the ciphertext block.
4. Correlation immunity – the transformation must not leak any information on the plaintext.

### 3.4 Statistical testing of symmetric encryption algorithms

If a cryptosystem is described formally (mathematically), some of its properties can be determined exactly (e.g. regularity, algebraic type of transformations, etc.). Nevertheless, since most of cryptosystems are too cumbersome to be analysable mathematically in detail, statistical tests are used.

1. Which properties are to be tested? – In the case of stream cipher: the „randomness“ of the running key sequence, the properties of cryptographic transformations, the relations between related keys and corresponding running key sequences. In case the of block cipher: the avalanche characteristics, correlation, dependence of ciphertext on plaintext bits and bits of keys.
2. The way of testing the properties of symmetric encryption algorithms – there are many statistical tests; see Knuth (1969), Bhattacharyya and Johnson (1977) and others. Here, the required measure of confidence, size of tested samples, etc. ought to be specified.

## 4 FUNCTIONAL CHARACTERISTICS

Functional characteristics describe qualitative parameters of algorithm and its particular implementation. It is often difficult to specify them by quantitative measures. They often create a profile for customers' decision. We mention six of them:

1. Encryption vs. decryption algorithm – differences (where, how).
2. Simplicity of software/hardware implementation.
3. Speed of encryption/decryption (in KB/sec or MB/sec).
4. Memory requirements – for encryption, decryption, keys (subkeys).
5. Modes of operation – which modes are supported.
6. Modularity – the ability to change the size of key, block length, number of rounds or other parameters, respectively.

## 5 PRACTICAL ASPECTS

Many practical aspects, influencing the security of used encryption algorithms are independent of particular symmetric encryption algorithm and, therefore, cannot be part of its evaluation. On the other hand, they are very important in real-life environments.

1. Assurance (the quality of implementation) – in both, SW and HW (for HW implementation, see for example National Institute of Standards and Technology (1994)).
2. Key management – generation, distribution, using, storing and destroying the keys.
3. Security policy – security procedures related to encryption mechanisms.

There are some other aspects of safe and secure use of encryption algorithm related to risk analysis, computer system security evaluation, etc.

## 6 CONCLUSION

The methodology presented in this paper tried to collect, order and describe parameters and properties of symmetric ciphers which have to be taken into account when the cryptographic strength of a cipher is to be evaluated. The cryptographic strength of every cryptosystem depends on its implementation and on the way in which it is used (applications and protocols). Therefore, it cannot be estimated absolutely and it is the designer/user who has to determine the most important parameters, and the criteria, which the chosen parameters must satisfy.

## 7 REFERENCES


Bhattacharyya, G.K. and Johnson, R.A. (1977) Statistical Concepts and Methods, John Wiley & Sons, New York.

Freier, A.O., Karlton, P. and Kocher P.C. (1996) SSL 3.0 SPECIFICATION, Internet Draft, Transport Layer Security Working Group, http://search.netscape.com/eng/ssl3/.

Golomb, S.W. (1967) Shift register sequences, Holden-Day, San Francisco.

Konheim, A.G. (1981) Cryptography: A Primer, John Wiley, New York.

Knuth, D.E. (1969) The art of computer programming, Vol. 2 (Seminumerical Algorithms), Addison-Wesley.

Meyer, C.H. and Matyas, S.M. (1982) Cryptography: A New Dimension in Computer Data Security, John Wiley & Sons, New York.

Rueppel, R.A. (1986) Analysis and design of stream ciphers, Springer-Verlag, Berlin.

SET (1997) Secure Electronic Transaction Specification, http://www.visa.com/cgi-bin/vee/nt/ecomm/set/intro.html, http://www.mastercard.com/set/.

National Institute of Standards and Technology (1994) Security Requirements for Cryptographic Modules, FIPS PUB 140-1.

Wayner, P. (1997) Digital Cash: Commerce on the Net, 2nd Edition, Ap Professional.


## 8 BIOGRAPHY

**Martin Stanek** (born in 1973) is a PhD student of computer science at Comenius University in Bratislava.

**Daniel Olejar** (born in 1957) is an associate professor of computer science at Comenius University in Bratislava. His primary research interests are cryptography and data security.