THESIS SUMMARY

„Cryptographic Algorithms Security”

Author: Eng. Florin Medeleanu

Email: florinmed@yahoo.com, tel: 0723 606 176

Ph.D. supervisor: Professor Ciprian Răcuciu, PhD, Eng.

In **Chapter 1**, introductory elements of the thesis, base notions used in cryptography and general aspects related to cryptographic algorithms, hash functions and message authentication codes are presented. Also, the main purpose of the paper, work and analysis methods used are presented. Details of used work methods and tools are reported throughout the chapters of the thesis.

Chapter 2 presents an analysis of symmetric key cryptographic mechanisms used in the process of providing information security, and also the main cryptanalytic attack methods. In the first part of the chapter, the main criteria of developing and realizing cryptographic systems are presented. The main characteristics of symmetric encryption algorithms, the types of cryptanalytic attacks that can be mounted against these algorithms, and results that can be obtained mounting these cryptanalytic attacks are presented. Linear cryptanalytic attacks, differential cryptanalytic attacks, MITM (meet-in-the-middle) and interpolation attacks are presented, all these being considered fundamental attacks. Also, the resistance of cryptographic encryption schemes obtained by chaining cryptographic algorithms is analyzed.

In **Chapter 3** some block cipher algorithms are analyzed and an in depth analysis of the most important symmetric algorithms, DES and AES, is performed. The design criteria of DES and AES component elements, substitution-permutation network and Feistel network architecture are analyzed. Following the design criteria analysis of the algorithm component elements, having in mind these principles, new component elements were determined and proposed with the purpose of improving the resistance of these algorithms against linear and differential cryptanalysis.

In the second part of the chapter the mathematical notions of asymmetric algorithms are presented and RSA public key cryptographic system is described, because this is the most used asymmetric scheme.

In **Chapter 4** an analysis of block ciphers resistance against cryptanalytic attacks is performed. The resistance of algorithms is analyzed against base attacks (linear, differential, meet-in-the-middle and interpolation attack), brute-force attack, cipher-text matching attack and key-schedule attack. Two types of attacks belonging from differential cryptanalytic attack methods are detailed, which are: differential characteristic method and active and passive element method. These two methods are used in deployment of differential cryptanalytic attack and square attack. The methods are then thoroughly analyzed and completely exemplified, two minimized models of block algorithms are used for this purpose: an SPN simplified algorithm and mini-AES algorithm. Modeling the studied attacks on these algorithms has the role to allow complete understanding of mounting principles of the explained attacks and represents the point of departure for deploying these attacks on real versions of block algorithms, for example AES or DES.

Chapter 5 describes base notions and theory elements of Galois fields, also developing and checking phases of some programs and tools used for Galois field calculus operations. These programs and tools are used subsequently for determining new component elements for the analyzed cryptographic algorithms, DES and AES. The new determined elements, non-linear substitution boxes (S-box), make possible the construction of some personalized cryptographic algorithms, with properties similar to those of standard algorithms (concerning resistance against cryptanalytic attacks) or even better. At the end of this chapter, statistical testing of the proposed algorithms (IAES and IDES) is performed in order to prove the resulting cryptographic properties.

In **Chapter 6** notions and definitions concerning anonymity in the digital environment are presented. Also, theoretical principles and some anonymous signature schemes are presented. Subsequently, the main attack methods against anonymous signature schemes are described.

In the second part of the chapter, an application of anonymous signature schemes is described and two new possible applications of these schemes are proposed: anonymous signature e-lottery and anonymous signature e-voting. These new applications were designed by author and he realized simulation and implementation of some parts of these applications, proving the viability and efficiency of the proposed solutions. Based on the results obtained through these simulations, the proposed anonymous signature e-lottery system could be experimentally implemented, as an intermediate phase toward carrying out a complete functional e-lottery system.

Chapter 7 is represented by the main conclusions of the paper, the synthesis of the main original contributions of the author both theoretical and practical made during the research conducted within the doctoral studies program and future research directions.