ISSN: 2277-3754
ISO 9001:2008 Certified
International Journal of Engineering and Innovative Technology (IJEIT)
Volume 4, Issue 12, June 2015

Cryptographic Algorithm IDA for Security and Data Storage Increase in the Integrated Application of the European System "Ecall" For Automatic Emergency Calls in Car Accidents

Ivan Ivanov, Stella Vetova, Georgi Stanchev

***Abstract*— the following paper presents a new cryptographic algorithm designed for wide area application in the integration of the European system "eCall" with other information systems such as GPS tracking, telemetry systems, fleet management and more. It provides automatic phone call to the emergency number 112 as a priority, but simultaneously many other functions are performed whereat necessity for data protection and secure data storing arises. The algorithm is designed on the base of DES algorithm and in accordance with "Feistel" scheme. It is a 64-bit symmetric block cryptographic algorithm, using 256-bit cryptographic key.**

***Index Terms*—cryptography, Feistel scheme, cryptographic algorithm, security enhancement, data storage, telemetry systems, data protection.**

I. INTRODUCTION

The System “eCall” is developed by a consortium of groups and institutions in the country members of the EU aiming to create a single standard for these calls, with a view to the operation of the system for the entire EU territory. This is accomplished through projects HeERO1 and HeERO2 [1]. Project implementation is led by ERTICO (European Road Transport Telematics Implementation Coordination’s crl). The documentation states that it can be integrated along with the performance of other functions associated with the use of the car so that more efficient usage of resources in the system “eCall” to be achieved. The authors of this work are a part of a team from Technical University of Sofia and HSTP (Higher School of Telecommunications and Post). They participated in the project HeERO 2 and in the development of Enterprays Communications Group Ltd. which integrates with the system „eCall”.

II. ALGORITHM

The algorithm IDA (Ivanov, Dikov, Arnaudov) [2÷6] is designed on the base of DES algorithm and in accordance with Feistel scheme. It is a 64-bit symmetric block cryptographic algorithm using a 256-bit cryptographic key. It consists of sixteen internal cycles containing transpositions, substitutions and nonlinear procedures.

A. *Algorithm description*

The algorithm works on 64-bit data blocks, using a 256-bit key for encryption and decryption. In the process of the data manipulation, bitwise and logical operations are involved as well as table permutations. The simplicity of the operation allows the implementation of the algorithm in a very wide range of computing systems - embedded microcontrollers, general purpose processors and programmable logic devices. Any details of the algorithm itself can be found in its specification document. The information flow is divided into blocks of clear information with length of 64 bits (Fig. 1). In the initial phase and final displacement, 64-bit blocks are submitted and blocks with the same length are generated. Displacement is a process of replacing the positions of bits without changing values, which is 1-1 shift, i.e. the number of bits is retained. The shifting is based on Table I and Table II.

Table I. Initial transposition

58	50	42	34	26	18	10	2
60	52	44	36	28	20	12	4
62	54	46	38	30	22	14	6
64	56	48	40	32	24	16	8
57	49	41	33	25	17	9	1
59	51	43	35	27	19	11	3
61	53	45	37	29	21	13	5
63	55	47	39	31	23	15	7

Table II. Final transposition

40	8	48	16	56	24	64	32
39	7	47	15	55	23	63	31
38	6	46	14	54	22	62	30
37	5	45	13	53	21	61	29
36	4	44	12	52	20	60	28
35	3	43	11	51	19	59	27
34	2	42	10	50	18	58	26
33	1	41	9	49	17	57	25

The obtained bit sequence is divided into two sequences - left L (0) and right R (0), each of which containing 32 bits. Then, the process performs encryption, using the function F (.). This feature is performed in two parts. First, the 32-bit output sequences of both F (.) functions are submitted to the first inputs of the two XOR adders. Then, the second inputs of these adders are fed with two 32-bit sub keys. The 32-bit output sequences of both XOR adders, change places, i.e. the left one becomes the right one and vice versa. This forms the input sequence for the next cycle. These procedures are

ISSN: 2277-3754
ISO 9001:2008 Certified
International Journal of Engineering and Innovative Technology (IJEIT)
Volume 4, Issue 12, June 2015

carried out up to sixteen times on the base of internal cycles.

B. Realization of the function F (.)

The realization of the function F (.) is designed in the following manner. Initially, the right side of Ri-1 of the data block is expanded with 32 to 48 bits by repeating the bits with number 1, 4, 5, 8, 9, 12, ..., 24, 28, 32 (the border bits of the groups, consisting of four consecutive bits). The new bits of the extension join in a cyclic order the eight adjoining structures containing 4 bits each by the following scheme:

r32 r1 r2 r3 r4 r5, r4 r5 r6 r7 r8 r9, …….., r28 r29 r30 r31 r32 r1 (1)

Then, the part Ri-1 with length of 48 bits is multiplied by mod 2 48-bit key Ki element by element and divided into eight successive structures with length of 6 bits. These structures are submitted to the S - boxes, performing nonlinear procedure - a choice of 4 outputs (bits) from 6 inputs (bits). Then, the transposition P accomplishes in a specific scheme and produces the final result of the cryptographic processing F (.) with length of 32 bits.

C. Generation of the 64 bit keys {Kj}

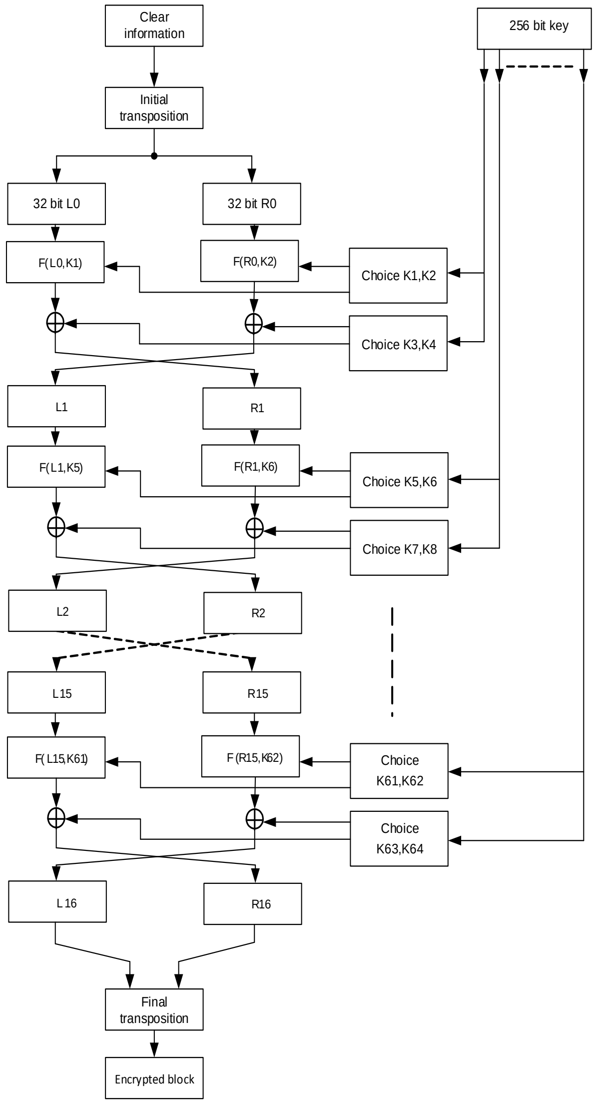

Fig. 1. Overall block diagram of the encryption algorithm

The generation of the 64 bit keys {Kj} with length of 48 bits and 32 bits is performed according to the standard algorithm shown in the right part of Fig.1. The key {Kj} is introduced in the cryptographic scheme with length of 256 bits. The keys involved in each cycle are generated from the basic key in the following manner. The process requires work with a certain number of bits for the sub keys, as follows: the first 48 bits of the basic key are planned to be the key K1 and are fed at the input of the function F (L0, K1), the next 48 bits are designed to be the key K2 and are fed at the input of F (R0, K2), the following 32 bits are designed to be K3 and fed at the input of the first XOR adder of the first cycle, the next 32 bits are planned to be the key K4 and fed at the input of the second XOR adder of the first cycle. Then, the quadruple keys for the second cycle are generated according to the same algorithm. The process continues up to the sixteenth cycle. After reaching the last byte of the basic key, a 25 bit linear shift is performed to the left in the 256-bit sequence as many times as necessary to obtain the required number of sub keys. Based on the proposed scheme in Figure 1, the cryptographic resistance of the encrypted data is significantly enhanced, using the 256-bit master key, the implementation of function F (.) over the left and right part of the data and the use of 64 sub keys for the sixteenth internal cycles.

III. APPLICATION DESCRIPTION

The algorithm is implemented through the standard C – programming language along with Visual Studio Express 2010 and Windows 7 OS used as environment. Various successive phases of the algorithm are divided into functions implemented in simple console application. No exotic or non-standard library functions are used in order to achieve better compatibility with different versions of C language. To confirm the compatibility, a test application is successfully compiled with GCC for Linux too. The console application works as the direction (encryption or decryption), the source and the result of the operation as well as the key are set as parameters of the command line. The initial data, the result of encryption / decryption and key are binary files whose names are the parameters described above.

IV. APPLICATION GOALS

The first goal of the application is to demonstrate the correct (according to the specification) operation of the algorithm, as well as to allow testing with variations in successive phases. The tests are conducted (1000 totally) with random data, which is encrypted, decrypted and the obtained result is compared for matching the original data. The internal iterations increase or reduce; the individual successive phases are added or removed. The results from the coherent encryption and decryption are always successful and coincide. Another object of the application is the assessment of the complexity, performance, load of the computing device during encryption and decryption. The measurements and assessments prove that the algorithm is applicable not only for

64-bit general purpose processors, but for 32-bit embedded microcontrollers too. The necessary memory for data and instructions (RAM, ROM), and CPU load (MIPS) are fully achievable for widely spread in the industrial and communications applications such as ARM Cortex-M3 microcontrollers. IDA algorithm is implemented in a system based on the system "eCall" and integrated with a system with additional functions – fleet management, in service of the car owner or driver, of the insurers and in aid to the police service as follows [7, 8, 9]:

- **the software for the service of the car owner or the driver, through the following functions:**
  - Reading the encrypted information related to administrative duties of the owner of the motor vehicle from the database;
  - Decryption of the information;
  - Preview of the decrypted information.
- **In the software for use by the authorized services and insurers (Figure 2) (The text in the figures is a Bulgarian, because the application is intended for use in Bulgaria):**
  - Reading the encrypted information related to the administrative duties of the owner of the motor vehicle from the database;
  - Decryption of the information;
  - Preview of the decrypted information;
  - Changing the decrypted information;
  - Encryption of the modified information;
  - Recording of the encrypted information.
- **In the software serving the police service (Figure 3)(The text in the figures is a Bulgarian, because the application is intended for use in Bulgaria).**
  - Reading the encrypted information related to the administrative duties of the owner of the motor vehicle from the database;
  - Decryption of the information;
  - Preview of the decrypted information;
  - Reading the encrypted information related to the measurements from the inertial sensors of the In-Vehicle System (IVS) device.

V. PRACTICAL APPLICATIONS

The main application of the algorithm executed in C # is used for the encrypted transfer and storage of the information from the communication server to the data server. The autonomous mobile devices that transmit telemetry information such as coordinates, speed, course, data from various sensors, events and receiving commands and settings are connected to the communication server. Another application of the algorithm can be both: to protect the data stored in the mobile devices and to exchange the information between each device and the communication server. The relatively high reliability and good protection of the algorithm against unwanted external decoding makes it an excellent choice for sharing encrypted data in virtually all transmission media. Particular attention should be paid to the exchange discipline, storage and periodic removal of the encryption keys of the separate countries, using the proposed algorithm.

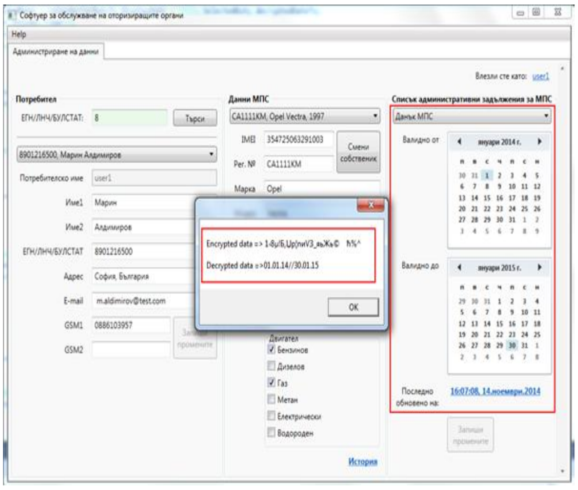

Fig 2. Encrypted and decrypted data displayed through the software designated for the authorizations services

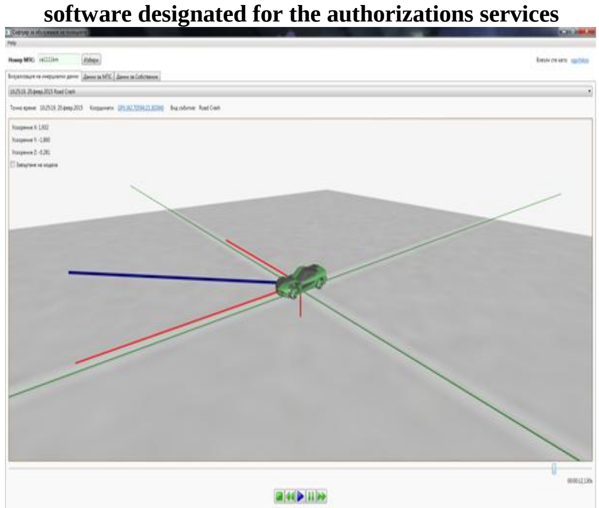

Fig 3. Preview of the decrypted inertial data, using the software, serving the police service

VI. CONCLUSION

The suggested algorithm concerns data encryption for telemetry systems and databases with special purpose and high level of protection. It is a 64-bit symmetric block cryptographic algorithm, using a 256-bit cryptographic key. It consists of 16 insides cycles, containing transpositions, substitutions and nonlinear procedures. When using encryption in telemetry systems, special-purpose data can be sent in real time and securely stored in an appropriate buffer (memory) and delivered only to the recipient as intended: insurance, road assistance, fire, ambulance etc., with guaranteed cryptographic resistance.

REFERENCES

[1] Stallings W. Cryptography and Network Security: Principles and Practice (6th Edition), Hardcover, 2013.

[2] ERTICO ITS Europe, HeERO1&HeERO2 projects description http://ertico.com/projects/heero.

[3] National Institute of Standards and Technology (NIST), Federal Information Processing Standard 46 (FIPS PUB 46).

[4] Ivanov I. Laboratory experiments on security and protection of information and administration and protection of communication and computer networks. HS CTP, Sofia 2013.

[5] Ferguson, N., Schneier, B., Kohno, T. Cryptography Engineering: Design Principles and Practical Applications, Wiley, 2010.

[6] Sokolov V., Shangin F. Information protection razpredelenyh corporate networks and systems. DMK Press, Moscow, 2002.

[7] Aldimirov M., Stanchev G., Arnaudov R. Testing of an IVS prototype for the eCall system under the European HeERO2 project and analysis of the results from the jointly tests with 112 emergency call center. IJEIT, 2015.

[8] Aldimirov M., Stanchev G., Arnaudov R. Integrated System for Car Park Management and Ecall Road Accident Signalization. IJEIT, 2015.

[9] Zahariev P., Hristov G., Tsvetkova I. An Approach towards Balanced Energy Consumption in Hierarchical Cluster-based Wireless Sensor Networks, Journal of Computing and Information Technology Vol.20, 2012, No 3, pp. 159-165, ISSN 1330-1136.

AUTHOR PROFILES

Ivan Ivanov is an assistant professor at the High School of Telecommunications and Post. He has graduated the Technical University of Sofia. He has been working in the field of information and network security, and cryptographic methods and algorithms.

Stella Vetova has graduated the Technical University of Sofia in 2001. She has been working in the field of information technology and the protection of databases.

Georgi Stanchev is an assistant professor from the Department “Fundamentals and technical means of design” at the Technical university of Sofia and a member of the Bulgarian Standardization Union. His areas of expertise include standardization, conformity assessment, design of mechanical and electronic devices, etc.