RESEARCH ON THE PROPERTY "AVALANCHE EFFECT" IN IDA CRYPTOGRAPHIC ALGORITHM

Ivan Ivanov, Stella Vetova, Krassimira Ivanova, Neli Maneva

Abstract: *The following paper presents some conducted extensive research on the cryptographic algorithm IDA, concerning one of the basic properties of the block algorithms "avalanche effect". The subject of the research are two different open texts, differing only by one bit and one key, as well as two keys differing only by one bit and one open text.*

Keywords: *cryptography, cryptographic algorithm, avalanche effect, S matrix, IDA algorithm*

ITHEA Classification Keywords: *E.3 Data Encryption – cryptosystems; F. Theory of Computation: F.2 Analysis of Algorithms and Problem Complexity; K. Computing Milieux: K.7 The Computing Profession: K.7.3 Testing, Certification, and Licensing*

Introduction

The purpose of the present paper is the exploration of the IDA algorithm property "avalanche effect" [Ivanov et al., 2014] in the following main tasks: (1) introduction of the property "avalanche effect"; (2) research on the IDA algorithm property "avalanche effect"; (3) results analysis.

The property "avalanche effect"

High result sensibility for initial data alteration is a desirable property for most of the encryption algorithms. According to its essence, any small alteration of the clear text or key should lead to a significant alteration in the ciphertext [Stallings, 2013; Schneier, 2013]. In particular, alteration of any single bit of the clear text or key should lead to the value alteration of great amount of the ciphertext bits [Sokolov & Shangin, 2002]. Even if the alteration in the ciphertext is small, it may cause a significant reduction of the set of keys or the field of the clear text.

Research on the IDA algorithm property "avalanche effect"

To research the IDA algorithm property "avalanche effect", two different clear texts will be encrypted. In this case, both texts differ by only one bit:

P_1 = 00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000000

P_2 = 10000000 00000000 00000000 00000000 00000000 00000000 00000000 00000000

The key is the same:

K = 11101010 11101110 11110000 11100101 11101010 11110010 11101110 11110000 00100000 11101101 11100000 00100000 11110010 11100101 11101011 11100101 11101010 11101110 11101100 11110011 11101101 11101000 11101010 11100000 11110110 11101000 11101110 11101101 11101101 11101000 11110010 11100101

For the clear text encryption, the research is similar:

P = 11110010 11100101 11101011 11100101 11110100 11101110 11101101 11101000, and two keys which differ by one bit:

K_1 = 11101010 11101110 11110000 11100101 11101010 11110010 11101110 11110000 00100000 11101101 11100000 00100000 11110010 11100101 11101011 11100101 11101010 11101110 11101100 11110011 11101101 11101000 11101010 11100000 11110110 11101000 11101110 11101101 11101101 11101000 11110010 11100101

K_2 = 01101010 11101110 11110000 11100101 11101010 11110010 11101110 11110000 00100000 11101101 11100000 00100000 11110010 11100101 11101011 11100101 11101010 11101110 11101100 11110011 11101101 11101000 11101010 11100000 11110110 11101000 11101110 11101101 11101101 11101000 11110010 11100101

The research results are tabled in Table 1.

Table 1. Research the IDA algorithm property "avalanche effect"

Plain text alteration		**Key alteration**	
Loop	**Difference (bits)**	**Loop**	**Difference (bits)**
0	5	0	4
1	14	1	12
2	25	2	18
3	37	3	30
4	39	4	35
5	35	5	31
6	32	6	30
7	31	7	32
8	29	8	32
9	41	9	38

Plain text alteration		Key alteration	
Loop	**Difference (bits)**	**Loop**	**Difference (bits)**
10	39	10	40
11	32	11	33
12	30	12	29
13	30	13	26
14	29	14	30
15	36	15	35

Figure 1 graphically represents the results of the Table 1.

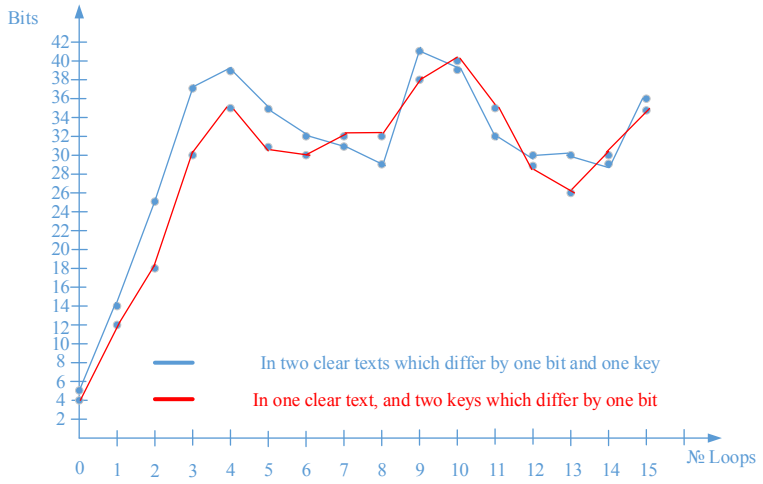

Figure 1. Research results on the IDA algorithm property "avalanche effect"

As can be seen from Figure 1 and Table 1, IDA algorithm has strong avalanche effect. Yet, it is seen that after the third encryption loop there is a difference of 37 bits. At the end of the encryption process, there is a difference of 36 bits.

On the analogy of the first case, in the clear data encryption using keys which differ by one bit (Figure 1 and Table 1), the avalanche effect is strong too. It is seen that after the third encryption loop, there is a difference of 30 bits. At the end of the encryption process, there is a difference of 35 bits.

To compare the results, the DES algorithm is put to test in the conditions described earlier. Table 2 and Figure 2 depict the obtained results.

As Figure 2 and Table 2 show, the DES algorithm demonstrates strong avalanche effect too. It is also seen that after the third loop of the encryption process, a difference of 35 bits occurs. At its end, there is a difference of 34 bits.

Similar to the first case, in the clear data encryption using two bits which differ by one bit (Figure 2 and Table 2) the avalanche effect is strong too. It is clearly seen that after the third encryption loop, there is a difference of 28 bits. At the end of the encryption process, the difference reaches 35 bits.

Table 2. Research the DES algorithm property "avalanche effect"

Plain text alteration		**Key alteration**	
Loop	**Difference (bits)**	**Loop**	**Difference (bits)**
0	1	0	0
1	6	1	2
2	21	2	14
3	35	3	28
4	39	4	32
5	34	5	30
6	32	6	32
7	31	7	35
8	29	8	34
9	42	9	40
10	44	10	38
11	32	11	31
12	30	12	33
13	30	13	28
14	26	14	26
15	34	15	35

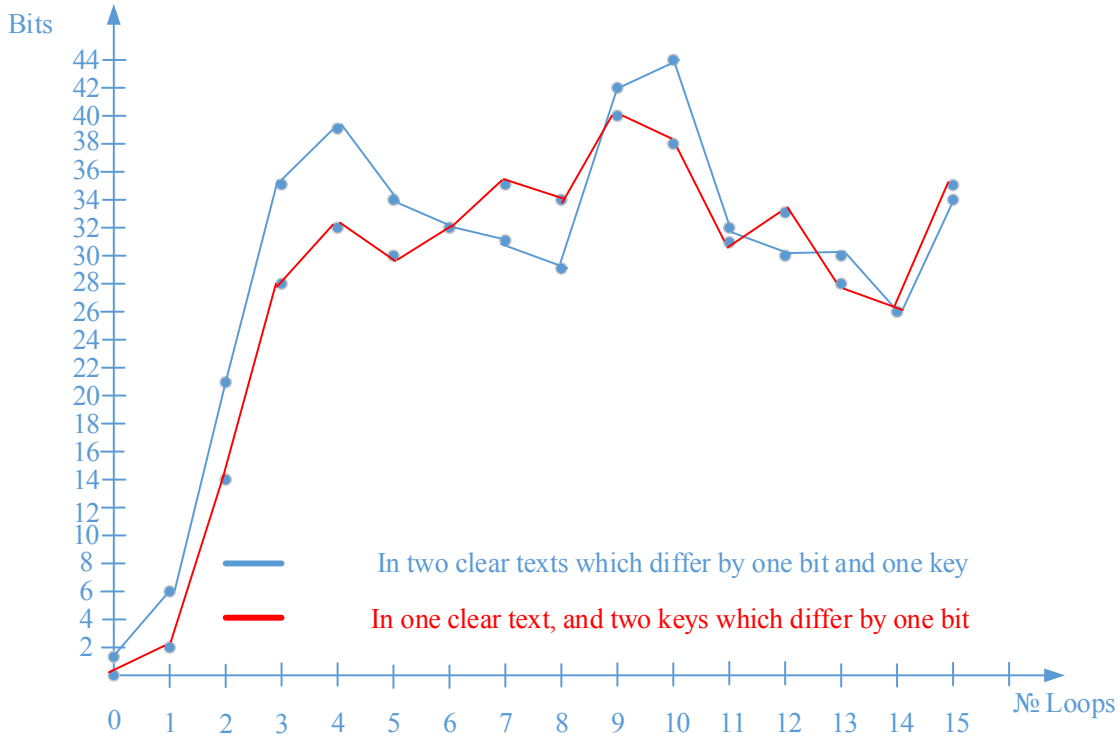

Figure 2. Research results on the DES algorithm property "avalanche effect"

Conclusion

As a result of the performed research work, there are three obtained results:

1. In the IDA algorithm in two clear texts which differ by one bit and one key, after the third encryption loop there is a mean difference of 35 bits from the total 64 bits for the rest twelve loops;
2. In the IDA algorithm in one clear text, and two keys which differ by one bit after the third loop of the encryption process, there is a mean difference of 33 bits from the total 64 bits for the rest twelve loops;
3. The IDA algorithm possesses a better avalanche effect compared to the DES algorithm (mean difference of three bits).

Acknowledgements

The paper is published with partial financial support from the "Scientific Research Fund" of University of Telecommunications and Posts, Sofia, Bulgaria, by the research project "Methods for development and estimation of cipher functions in block encryption algorithms".

Bibliography

[Ivanov et al., 2014] Ivanov I, Arnaudov R, Dikov D, Stanchev G, Patent application 111513: Method for increasing data security in storage and during information transmission in special purpose telemetry systems, Bulgarian patent office, Official Bulletin, Issue 12, pp.14, Dec 2014.

[Katz & Lindell, 2014] Katz J., Lindell Y. Introduction to Modern Cryptography, Second Edition (Chapman & Hall/CRC Cryptography and Network Security Series), CRC Press, 2014.

[Schneier, 2013] Schneier B., Appliet Cryptography Protocols, Algorithms, and Source Code in C, Wiley, 2013.

[Sokolov & Shangin, 2002] Sokolov V., Shangin F. Information protection distribured corporate networks and systems. DMK Press, Moskva, 2002.

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

Authors' Information

Ivan Ivanov *– Assist. Prof. PhD; University of Telecommunications and Posts, Sofia, Bulgaria; e-mail: i.ivanov@utp.bg;*

Major Fields of Scientific Research: Information and Network Security, Cryptographic Methods and Algorithms, Cyber security.

Stella Vetova *– Scientific Researcher, e-mail: vetova.bas@gmail.com*

Major Fields of Scientific Research: Databases and security, Artificial Intelligence, Computer networks.

Krassimira Ivanova *- Assoc. prof. Dr.; University of Telecommunications and Posts, Sofia, Bulgaria; Institute of Mathematics and Informatics, BAS, Bulgaria; e-mail: krasy78@mail.bg;*

Major Fields of Scientific Research: Software Engineering, Business Informatics, Data Mining, Multidimensional multi-layer data structures in self-structured systems

Neli Maneva *– student; University of Telecommunications and Posts, Sofia, Bulgaria; e-mail: i.ivanov@utp.bg;*

Major Fields of Scientific Research: Information and Network Security, Computer networks and protocols.