Analysis of cryptographic protection of block cryptographic algorithms on the base of the theoretical digital stability

Ivan Ivanov [1], Rumen Arnaudov [2] and Stella Vetova [3]

Abstract – **the following report presents analysis of cryptographic protection of most used symmetric block cryptographic algorithms nowadays on the base of the theoretical digital stability.**

The theoretical digital stability is assessment reached on condition that the cryptographic algorithm is qualitative and firm to cryptanalysis accelerated attacks but can be attacked only by brute force attack.

Keywords – **cryptanalysis, cryptographic attack, cryptography, cryptographic protection, cryptographic algorithms**

I. Introduction

Cryptanalysis (from Greek κρυπτός — hidden and analysis) — a science for the methods used to reach the original meaning of data after it has been ciphered without the availability of secret information (key) necessary for this purpose. In most cases this concerns the key revealing. In nontechnical sense, cryptanalysis break on the cipher. The term is led by the American cryptographer W. F. Fridmann in 1920.

The results of the cryptanalysis of concrete cipher are called cryptographic attack on this cipher. The successful cryptographic attack fully discrediting the attackable cipher is called.

Cryptanalysis methods [1, 2, 3, 4, 5]

1. Classical cryptanalysis:
- Frequency analysis;
- Kasiski examination;
- Method index matches;
- Method of index mutual matches.
2. Cryptanalysis of symmetric algorithms:
- Differential cryptanalysis;
- Linear cryptanalysis;
- Integral cryptanalysis;
- Statistical cryptanalysis;
3. Cryptanalysis of asymmetric algorithms:
- Decision tasks decomposition numbers of multipliers;
- Solvation of tasks with discrete logarithms;
4. Other methods:
- Attack “Birthday”;
- Attack “Man in the middle“;
- Brute force attack;

As far as the cryptographic protection realizes using block and stream cryptographic algorithms whose concrete realizations are simply defined by the interaction keys, the goal of the cryptanalysis reduces to revealing those interaction keys which are used in the cipher process[6].

Another assessment for the stability of the cryptographic protection exists. It is distinguished for a quantitative expression – theoretical digital stability. This assessment is important mainly for the theoretical estimation of the cryptographic algorithm but can be used by the user too to get information about the quality (grade) of the cryptographic algorithm (cryptographic equipment).

The theoretical digital stability is assessment reached on condition that the cryptographic algorithm is qualitative and firm to cryptanalysis accelerated attacks but can be attacked only by brute force attack [7].

In reality, the opponent does not have information only for the concrete key for interaction which is used in the cipher process. Therefore, the cryptanalysis is brought to search of the used key by the method of brute force that is through all the keys for interaction.

II. Method

Whilst in the cryptanalysis methods of the by brute force there is consecutively testing of the interaction keys from the set {Ki} with size N – key, for the assessment of the stability of the cryptographic algorithms the formula (1) for the mean time for interaction key revealing can be used:

$$\overline{T_{cal}} \approx \frac{Nn_{op} S_{\min}}{6B} 10^{-7}, [years], \qquad (1)$$

where nop is the number of computer operation necessary for 1bit information processing, Smin [bit] – minimum length of the glaring sample, and B [computer operation co/s] is the performance of the processing in the technical base for cryptanalysis.

The interaction key number N is defined by formula (2):

[1] Ivan Ivanov is with the College of Telecommunications and Posts of Sofia, 1 St. Mladenov Blvd, Sofia 1100, Bulgaria, E-mail: ivanivanov@hctp.acad.bg.

[2] Rumen Arnaudov is with the Faculty of Telecommunications at Technical University of Sofia, 8 Kl. Ohridski Blvd, Sofia 1000, Bulgaria, E-mail: ra@tu-sofia.bg.

[3] Stella Vetova is with Bulgarian Academy of Sciences, Acad. G. Bonchev St. Sofia 1113, Bulgaria, E-mail: vetova.bas@gmail.com

$$N = 2k, \text{[number.]}, \qquad (2)$$

Where к is the length of the basic key used by the cryptographic algorithm.

The experiment is accomplished over the most used symmetric block cryptographic algorithms nowadays such as: DES, K=64 bit, Triple DES, K=112Bit, IDEA, K=128 bit, AES, K=128 bit, AES, K=192 bit, AES, K=256 bit, Blowfish, K=32 bit, Blowfish, K=448 bit, RC5, K=128 bit, RC2, RC5, K=512 bit, RC2, RC5, K=1024 bit.

III. Results

On the base of formula (2), is obtained (table 1, 2 and 3) the dependency of the theoretical digital stability $\overline{T}_{уст}$, the interaction key number N in ncoSmin=10^2, 10^5 and 10^8 and different meanings of the performance of the B = 10^9 co/s; 10^{12} co/s; 10^{15} co/s; 10^{20} co/s; 10^{30} co/s.

Table I. Result in $n_{co}S_{min}=10^8$

N, num.	B, co/s	T_{cal}, years	N, num.	B, co/s	T_{cal}, years
$0,18*10^{20}$	10^9	$3*10^{10}$	$5,19*10^{33}$	10^9	$8,7*10^{24}$
	10^{12}	$3*10^7$		10^{12}	$8,7*10^{21}$
	10^{15}	$3*10^4$		10^{15}	$8,7*10^{18}$
	10^{20}	$3*10^{-1}$		10^{20}	$8,7*10^{13}$
	10^{30}	$3*10^{-11}$		10^{30}	$8,7*10^3$
N, num.	**B, co/s**	**T_{cal}, years**	**N, num.**	**B, co/s**	**T_{cal}, years**
$3,4*10^{38}$	10^9	$5,7*10^{29}$	$6,28*10^{57}$	10^9	$1.02*10^{49}$
	10^{12}	$5,7*10^{26}$		10^{12}	$1.02*10^{46}$
	10^{15}	$5,7*10^{23}$		10^{15}	$1.02*10^{43}$
	10^{20}	$5,7*10^{18}$		10^{20}	$1.02*10^{38}$
	10^{30}	$5,7*10^8$		10^{30}	$1.02*10^{28}$
N, num.	**B, co/s**	**T_{cal}, years**	**N, num.**	**B, co/s**	**T_{cal}, years**
$1,16*10^{77}$	10^9	$1,93*10^{68}$	$7,27*10^{134}$	10^9	$1,21*10^{126}$
	10^{12}	$1,93*10^{65}$		10^{12}	$1,21*10^{123}$
	10^{15}	$1,93*10^{62}$		10^{15}	$1,21*10^{120}$
	10^{20}	$1,93*10^{57}$		10^{20}	$1,21*10^{115}$
	10^{30}	$1,93*10^{47}$		10^{30}	$1,21*10^{105}$
N, num.	**B, co/s**	**T_{cal}, years**	**N, num.**	**B, co/s**	**T_{cal}, years**
$1,34*10^{154}$	10^9	$2.23*10^{145}$	$1,8*10^{308}$	10^9	$3*10^{299}$
	10^{12}	$2.23*10^{142}$		10^{12}	$3*10^{296}$
	10^{15}	$2.23*10^{139}$		10^{15}	$3*10^{293}$
	10^{20}	$2.23*10^{134}$		10^{20}	$3*10^{188}$
	10^{30}	$2.23*10^{124}$		10^{30}	$3*10^{178}$

Table II. Result in $n_{co}S_{min}=10^5$

N, num.	B, co/s	T_{cal}, years	N, num.	B, co/s	T_{cal}, years
$0,18*10^{20}$	10^9	$0,3*10^8$	$5,19*10^{33}$	10^9	$8,7*10^{21}$
	10^{12}	$0,3*10^5$		10^{12}	$8,7*10^{18}$
	10^{15}	$0,3*10^2$		10^{15}	$8,7*10^{15}$
	10^{20}	$0,3*10^{-3}$		10^{20}	$8,7*10^{10}$
	10^{30}	$0,3*10^{-13}$		10^{30}	$8,7*10$
N, num.	**B, co/s**	**T_{cal}, years**	**N, num.**	**B, co/s**	**T_{cal}, years**
$3,4*10^{38}$	10^9	$0,57*10^{27}$	$6,28*10^{57}$	10^9	$1.02*10^{46}$
	10^{12}	$0,57*10^{24}$		10^{12}	$1.02*10^{43}$
	10^{15}	$0,57*10^{21}$		10^{15}	$1.02*10^{40}$
	10^{20}	$0,57*10^{16}$		10^{20}	$1.02*10^{35}$
	10^{30}	$0,57*10^6$		10^{30}	$1.02*10^{25}$
N, num.	**B, co/s**	**T_{cal}, years**	**N, num.**	**B, co/s**	**T_{cal}, years**
$1,16*10^{77}$	10^9	$1,93*10^{65}$	$7,27*10^{134}$	10^9	$1,21*10^{123}$
	10^{12}	$1,93*10^{62}$		10^{12}	$1,21*10^{120}$
	10^{15}	$1,93*10^{59}$		10^{15}	$1,21*10^{117}$
	10^{20}	$1,93*10^{54}$		10^{20}	$1,21*10^{112}$
	10^{30}	$1,93*10^{44}$		10^{30}	$1,21*10^{102}$
N, num.	**B, co/s**	**T_{cal}, years**	**N, num.**	**B, co/s**	**T_{cal}, years**
$1,34*10^{154}$	10^9	$2.23*10^{142}$	$1,8*10^{308}$	10^9	$3*10^{296}$
	10^{12}	$2.23*10^{139}$		10^{12}	$3*10^{293}$
	10^{15}	$2.23*10^{136}$		10^{15}	$3*10^{290}$
	10^{20}	$2.23*10^{131}$		10^{20}	$3*10^{185}$
	10^{30}	$2.23*10^{121}$		10^{30}	$3*10^{175}$

Table III. Result in $n_{op}S_{min}=10^2$

N, num.	B, co/s	T_{cal}, years	N, num.	B, co/s	T_{cal}, years
$0,18*10^{20}$	10^9	$0,3*10^5$	$5,19*10^{33}$	10^9	$8,7*10^{18}$
	10^{12}	$0,3*10^2$		10^{12}	$8,7*10^{15}$
	10^{15}	$0,3*10^{-1}$		10^{15}	$8,7*10^{12}$
	10^{20}	$0,3*10^{-6}$		10^{20}	$8,7*10^7$
	10^{30}	$0,3*10^{-16}$		10^{30}	$8,7*10^{-3}$
N, num.	**B, co/s**	**T_{cal}, years**	**N, num.**	**B, co/s**	**T_{cal}, years**
$3,4*10^{38}$	10^9	$0,57*10^{24}$	$6,28*10^{57}$	10^9	$1.02*10^{43}$
	10^{12}	$0,57*10^{21}$		10^{12}	$1.02*10^{40}$
	10^{15}	$0,57*10^{18}$		10^{15}	$1.02*10^{37}$
	10^{20}	$0,57*10^{13}$		10^{20}	$1.02*10^{32}$
	10^{30}	$0,57*10^3$		10^{30}	$1.02*10^{22}$
N, num.	**B, co/s**	**T_{cal}, years**	**N, num.**	**B, co/s**	**T_{cal}, years**
$1,16*10^{77}$	10^9	$1,93*10^{62}$	$7,27*10^{134}$	10^9	$1,21*10^{120}$
	10^{12}	$1,93*10^{59}$		10^{12}	$1,21*10^{117}$
	10^{15}	$1,93*10^{56}$		10^{15}	$1,21*10^{114}$
	10^{20}	$1,93*10^{51}$		10^{20}	$1,21*10^{109}$
	10^{30}	$1,93*10^{41}$		10^{30}	$1,21*10^{99}$
N, num.	**B, co/s**	**T_{cal}, years**	**N, num.**	**B, co/s**	**T_{cal}, years**
$1,34*10^{154}$	10^9	$2.23*10^{139}$	$1,8*10^{308}$	10^9	$3*10^{296}$
	10^{12}	$2.23*10^{136}$		10^{12}	$3*10^{293}$
	10^{15}	$2.23*10^{133}$		10^{15}	$3*10^{290}$
	10^{20}	$2.23*10^{128}$		10^{20}	$3*10^{185}$
	10^{30}	$2.23*10^{118}$		10^{30}	$3*10^{175}$

On the base of formula (2), we reach the dependency between the basic cryptographic keys length K and the possible number of combinations for the same N.

In K=64 bit, N = 2^{64} = $0,18*10^{20}$;
In K=112 bit, N = 2^{112} = $5,19*10^{33}$;
In K=128 bit, N = 2^{128} = $3,4*10^{38}$;
In K=192 bit, N = 2^{192} = $6,28*10^{57}$;
In K=256 bit, N = 2^{256} = $1,16*10^{77}$;
In K=448 bit, N = 2^{448} = $7,27*10^{134}$;
In K=512 bit, N = 2^{512} = $1,34*10^{154}$;
In K=1024 bit, N = 2^{1024} = $1,8*10^{308}$;

Fig. 1, 2, and 3 illustrate the dependency of the theoretical digital stability $\overline{\boldsymbol{T}}_{\boldsymbol{ycm}}$, the interaction key number N in ncoSmin=10^2, 10^5 and 10^8 and different meanings of the performance of the B = 10^9 co/s; 10^{12} co/s; 10^{15} co/s; 10^{20} co/s; 10^{30} co/s.

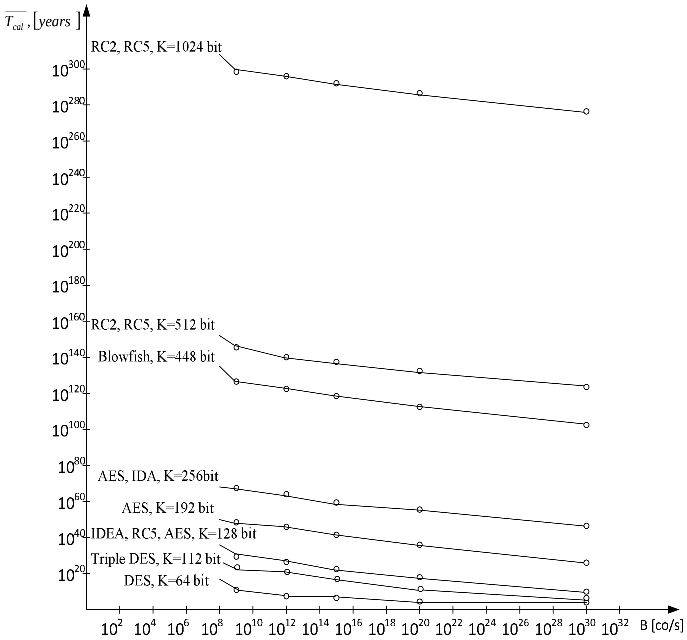

Fig. 1. Graphics of the dependency for the different algorithms and $n_{co}S_{min}=10^8$.

The graphics (fig.1) shows that the theoretical digital stability goes down increasing the performance of the process in the technical base for cryptoanalysis.

For DES algorithm, in K = 64 bit, and processing capacity of the modern computers (4÷5 GHz processors) the theoretical digital stability is low as for values B = 10^{20} op/s and B = 10^{30} op/s, it is respectively : $\overline{T}_{cal}$ = $0,3*10^{-11}$ = 95 µs; $\overline{T}_{cal}$ = $0,3*10^{-1}$ = 946080 s. = 11 days, it is insignificant.

For the cryptographic algorithms where K≥128 bits, guaranteed cryptographic protection is applied.

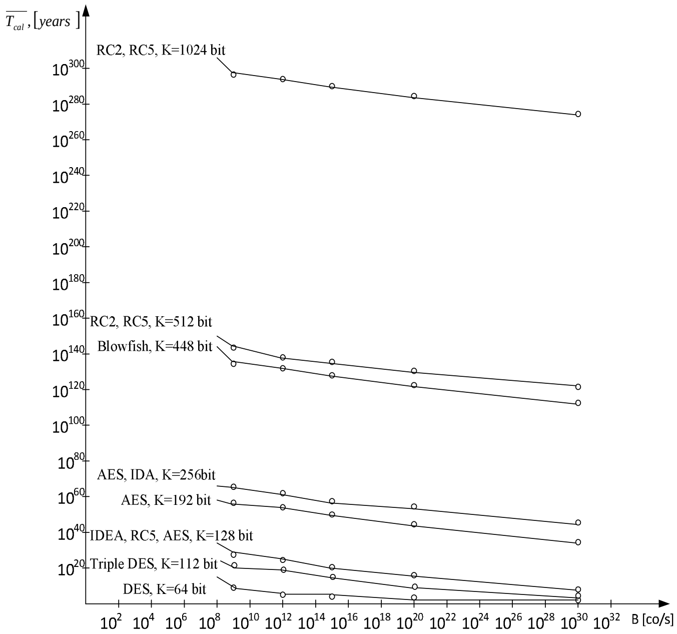

Fig. 2. Graphics of the dependency for the different algorithms and $n_{co}S_{min}=10^5$.

Fig. 2 depicts the dependency for the different algorithms and $n_{co}S_{min}=10^5$. It shows that for the DES algorithm in K = 64 bits, the theoretical digital stability is low as for values of B = 10^{20} op/s and B = 10^{30} op/s, it is respectively: $\overline{T}_{cal}$ = $0,3*10^{-13}$ = 0,95 µs; $\overline{T}_{cal}$ = $0,3*10^{-3}$ = 9460,8 s.= 2,63 hours, it is insignificant.

For the cryptographic algorithms where K≥128 bits, guaranteed cryptographic protection is applied.

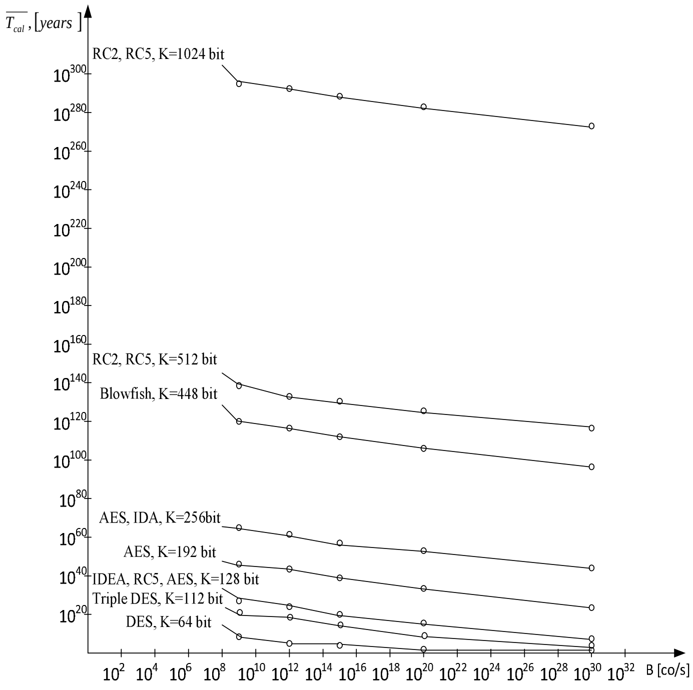

Fig. 3. Graphics of the dependency for the different algorithms and $n_{co}S_{min}=10^2$.

From Fig. 3 it is seen that for the DES algorithm in К = 64 bits, the theoretical digital stability is low as for values of B = 10^{15} op/s, B = 10^{20} op/s and B = 10^{30} op/s, it is respectively: $\overline{T_{cal}}$ = 0,3*10^{-16} = 0,95 ns; $\overline{T_{cal}}$ =0,3*10^{-6} = 9,46 s, $\overline{T_{cal}}$ = 0,3*10^{-1} = 946080 s. = 11 days, it is insignificant.

For the cryptographic algorithms where К≥128 bits, guaranteed cryptographic protection is applied.

IV. Conclusion

The accomplished analysis is based on three different Smin [bit] – minimal lengths of the glaring sample: 10^2 bit, 10^5 bit и 10^8 bit.

On the base of the presented analysis and graphics, it is clearly seen that the theoretical digital stability of the tested cryptographic algorithms including the mean time of key revealing goes down increasing the performance of the processing in the technical base for cryptanalysis.

For the cryptographic algorithms using key length shorter than 128 bits (DES, Triple DES), the mean time for key revealing is very short whilst those algorithms using key length with or more than 128bits are noticeable for good and high guaranteed stability of cryptographic protection..

References

[1] Bauer F. Decrypted secrets methods and maxims of cryptology, Springer, 2007.

[2] Joye M., Tunstall M. Fault analysis in cryptography, Springer, 2012.

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

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

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

[6] Sokolov A. Shangin B. Information protection rzpredelenyh corporate networks and systems, DMK Press", M., 2002.

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