ISSN 0146-4116, Automatic Control and Computer Sciences, 2019, Vol. 53, No. 1, pp. 39–44. © Allerton Press, Inc., 2019.

Security Evaluation of a Brute-force Attack on a Cipher Using a Statistical Criterion for Plaintext[1]

A. V. Babash[a], V. A. Sizov[a, *], and A. A. Mikryukov[a]

[a] *Plekhanov Russian University of Economics, Moscow, 117997 Russia*

**e-mail: sizovva@gmail.com*

Received February 20, 2018; revised July 6, 2018; accepted July 28, 2018

Abstract—The paper presents calculations of the amount of effort and the reliability of the method of brute-force attack on a cipher using a statistical criterion for plaintexts, which has type 1 and type 2 errors. Calculated values of parameters of the discussed cryptanalysis methods for a cipher allows better predictions of its remaining safe operational life taking into account statistical characteristics for recognizing the plaintext and changes in the communication channel parameters.

Keywords: cryptography, cipher, key, decryption, brute force attack

DOI: 10.3103/S0146411619010036

1. INTRODUCTION

It is known that when a cipher is in operational use, it is subjected to cryptographic analysis [1–4] on a regular basis in order to prevent attacks that might pose a danger to it and to predict for how long it will be able to stay in use. To achieve a more precise prediction of the remaining useful life of a cipher [1, 3, 4], it is desirable to have a more precise estimate of the amount of effort it takes to crack it. A more precise estimate of the remaining useful life of a cipher can be obtained using a calculation [1, 3, 4] of the amount of effort required by methods [2] that crack it by automatically finding the plaintext [1, 3, 4]. The plaintext is understood to mean the original text before it was subjected to encryption. Such a text, as a rule, has a certain structure and patterns, which make it possible to use statistical characteristics of the text for its automatic decryption [5]. Thus, for example, a specific original text in any language has its own characteristic frequency of occurrence of specific characters, 2-grams, etc. and its own 'forbidden' k-grams. A universal cipher-cracking method is the brute-force attack [1, 3, 4]. This method is often called a key trial-and-error method or Monte Carlo method, or total method. The paper provides the rationale for calculations of the amount of effort and the reliability of the method of the cipher key trial using a statistical criterion (with Type 1 and 2 errors) for plaintexts. The amount of effort and reliability of the cipher key trial method give a better idea of cryptographic security of a cipher against the key trial method as compared to the universally used parameter – the number of its keys.

One of the main issues in practical cryptography is the issue of the remaining operational life of a cipher. The decision to stop using a cipher and replace it depends on many factors. One of these factors is its cryptographic robustness, which is determined by cryptographers on a regular basis. Therefore, the longevity of a cipher depends on the accuracy of math models that are being used and cipher cracking methods. An analysis of a cipher, as a rule, starts with calculating the parameters of the brute-force method of attack on the cipher, of the total method [6]. Often used as a measure of the amount of effort required by this method is a number of its keys $|K|$ or an average number of keys that need to be tried before the true key is determined $\frac{|K|+1}{2}$ (more often used is $\frac{|K|}{2}$). Many methods of cipher cracking also use, along with solving math problems, partial trials of certain pre-determined, so-called 'weak keys'. In actual practice, all these cases pose the problem of determining plaintext from the data obtained when decrypting the initial ciphertext using the key that is being tried.

[1] The article is published in the original.

It is only natural that solving the latter problem involves using various math models of the plaintext along with a statistical criterion for determining the plaintext. These are the reasons for the importance of the problem of calculating a cipher cracking method using a statistical criterion for plaintext.

Shannon's math model for the cipher is well known [7].

Let A be a cipher with encryption algebra (X, K_e, Y, f), where X is a set of plaintexts, K_e is a set of its keys, Y is a set of cyphertexts, $f: X \times K_e \to Y$ is an encryption function. Let us supplement this model. Let us denote as (Y, K_d, X, F) the deciphering algebra of cipher A, where K_d is a set of deciphering keys for the cipher, $F: Y \times K_d \to X$ is a deciphering function. Let $\chi_e \in K_e$ and $\chi_d \in K_d$ is its corresponding deciphering key. If $x \in X$ and $f(x, \chi_e) = y$, then $F(y, \chi_d) = x$. For symmetric key ciphers one may assume that $K_e = K_d$.

The problem is to solve the equation $f(x,\chi_e) = y$ for x with known y for a known cipher A.

One of the methods for solving this equation is to try pairs of elements (x', χ') from $X \times K_e$. Calculated for each pair (x', χ') is the value of $f(x', \chi') = y'$ and y is compared with y'. For asymmetric key cipher (a cipher with public key χ_e) one more method can be used. For each tried sample of $x' \in X$ the value of $f(x', \chi_e) = y'$ is compared with y. The plaintext x, for which $y = y'$, is considered to be the solution of the problem.

The total method of brute-force attack on the cipher consists in random trials of keys χ^* from K_d. For each tried key χ^* the ciphertext is deciphered and the obtained text $F(y, \chi^*)$ is checked to see if it belongs to the set of meaningful texts.

It is assumed that the check to see if the decrypted text belongs to the set of meaningful texts is performed using a certain 'hypothetical statistical criterion for meaningful texts' which has Type 1 and 2 errors (for example Neyman-Pearson criterion [8], forbidden bigrams criterion [9] etc.): α is a probability of rejecting a meaningful text (in terms of statistical criterion – rejection of hypothesis $H(0)$ corresponding to probability distribution $P(0)$); β is the probability of mistaking a meaningless text for a meaningful text (accepting hypothesis $H(0)$, while hypothesis $H(1)$ is true – sampling from distribution $P(1)$ corresponding to unreadable texts). From here on $\beta \neq 1$.

It is also assumed that the key trials consist in consecutively randomly and equiprobably trying without repeats r keys out of K_d. The trial process ends after ξ keys have been tried; $\xi = j$ is a number of the first key $(1 \le j \le r)$ for which the corresponding decrypted text will be recognized by the criterion as a meaningful text, or $\xi = r$, if such an event does not happen for any $j \le r$.

The main characteristics of the cryptographic security of a cipher against the total method of solving the problem are the amount of effort $E^{\alpha,\beta}(r)$ required by the method – an average number of tried keys (a mean value of random variable ξ).

Reliability $\pi^{\alpha\beta}(r)$ of the method – the probability of determining the true meaningful text.

The calculation of these characteristics of the total method will be done under the following assumptions: when ciphertext y is deciphered with all the keys χ^* from K_d, among the deciphered texts $\{F(y, \chi^*): \chi^* \in K_d\}$ there exists a single meaningful text, which is the true text x_Y; in the set K_d there exists a single key χ^*_Y, for which $F(y, \chi^*_Y) = x_Y$. These assumptions allow interpreting the use of the hypothetical statistical criterion for the meaningful text, as the criterion for checking a tried key χ^* to see if it matches the unknown true key χ^*_Y. There is a probability α that the true key will be identified as false (while hypothesis $H(0)$ is fulfilled, the criterion will accept $H(1)$), and there is a probability β that a false key will be identified as true (while hypothesis $H(1)$ is fulfilled, $H(0)$ will be accepted). The process of trying the keys will end after ξ keys have been tried; $\xi = j$ is the number of the first key $(1 \le j \le r)$, which will be identified by the statistical criterion as the true key, or $\xi = r$, if such an event does not occur at any $j \le r$.

This paper is structured as follows: Section 1 provides the rationale for the need to state the problem. A brief summary of the results of this work is given. This section also provides known results on the subject.

The main results are contained in Section 2, which present the calculations of the amount of effort and the reliability of the cypher key trial without return taking into account the determination of plaintext by a statistical criterion having Type 1 and 2 errors.

The Section 3 contains references to the sources of the subject domain. The conclusions and open issues are stated in the Conclusion.

2. CALCULATION OF THE AMOUNT OF EFFORT REQUIRED FOR A BRUTE-FORCE ATTACK AND CALCULATION OF RELIABILITY OF A BRUTE-FORCE ATTACK

Let us first calculate the amount of effort $E^{\alpha,\beta}(r)$ required for a brute-force attack. For brevity sake, from here on $K_e = K$.

Let B_t be an event consisting in t-th key being true in the scheme of consecutive key trials without return, $t \in \{1,...,|K|\}$;

– $E^{\alpha,\beta}(r, t)$ is a mean value of ξ in the event of B_t;

– $E^{\alpha\beta}(t \le r)$ is a mean value of ξ in the event of the true key being among the first r of the tried keys;

– $E^{\alpha\beta}(t \ge r+1)$ is a mean value of ξ in the event of the true key being absent from the first r of the tried keys.

From the formula of conditional mathematical expectation we obtain

$$E^{\alpha,\beta}(r) = \frac{r}{|K|}E^{\alpha,\beta}(t \le r) + \frac{|K|-r}{|K|}E^{\alpha,\beta}(t \ge r+1).$$

To calculate the value of $E^{\alpha,\beta}(t \le r)$, let us first calculate $E^{\alpha,\beta}(r, t)$ at $t \le r$:

$$E^{\alpha,\beta}(r,t) = \sum_{m=1}^{t-1} m(1-\beta)^{m-1}\beta + t(1-\beta)^{t-1}(1-\alpha) + \sum_{m=t+1}^{r} m\alpha(1-\beta)^{m-2}\beta + r\alpha(1-\beta)^{r-1}.$$

The first term corresponds to completion of trials at some k-th key, where $k \le t-1$ (recall that the true key is tried during the t-th trial). The second term corresponds to identifying the true key during the t-th trial. The third term corresponds to a situation similar to the first one for $k \ge t+1$. The fourth term corresponds to a situation where in each of the first r trials the criterion accepted hypothesis $H(1)$.

If the true key is among the first r of the tried keys, it may, with the probability of $\frac{1}{r}$, appear during any t-th trial, $t \in \{1, ..., r\}$. Therefore

$$E^{\alpha,\beta}(t \le r) = \sum_{t=1}^{r} E^{\alpha,\beta}(r,t)p(B_t),$$

$$E^{\alpha,\beta}(t \le r) = \frac{1}{r}\sum_{t=1}^{r}\left(\sum_{m=1}^{t-1} m(1-\beta)^{m-1}\beta + t(1-\beta)^{t-1}(1-\alpha) + \sum_{b=e+1}^{r} m\alpha(1-\beta)^{m-2}\beta + r\alpha(1-\beta)^{r-1}\right)$$

$$= \frac{\beta}{r}\sum_{t=1}^{r}\sum_{i=1}^{t-1} i(1-\beta)^{i-1} + \frac{1-\alpha}{r}\sum_{t-1}^{r} t(1-\beta)^{t-1} + \frac{\alpha\beta}{r(1-\beta)}\sum_{t=1}^{r}\sum_{i=t+1}^{r} i(1-\beta)^{i-1} + r\alpha(1-\beta)^{r-1}.$$

By changing the order of summation in double sums we obtain

$$E^{\alpha,\beta}(t \le r) = \frac{\beta}{r}\sum_{j=1}^{r-1} j(1-\beta)^{j-1}(r-j) + \frac{\alpha\beta}{r(1-\beta)}\sum_{i-2}^{r} i(1-\beta)^{i-1}(i-1) + \frac{1-\alpha}{r}\sum_{t=1}^{r} t(1-\beta)^{t-1} + r\alpha(1-\beta)^{r-1}.$$

Adding to the first sum the term at $j = r$, and to the second sum the term at $i = 1$ (which are equal to zero) and, and changing everywhere the summation index to "k", combining the first three terms into one term, we obtain

$$E^{\alpha,\beta}(t \le r) = \frac{1}{r}\sum_{k=1}^{r} k(1-\beta)^{k-1}\left[\beta(r-k) + \frac{\alpha\beta}{1-\beta}(k-1) + (1-\alpha)\right] + r\alpha(1-\beta)^{r-1}.$$

In the case where the true key is not among the first r tried keys, the mean number of the tried keys is

$$E^{\alpha,\beta}(t \le r+1) = \sum_{k=1}^{r} k(1-\beta)^{k-1}\beta + r(1-\beta)^{r}.$$

The last term corresponds to a situation where for each of the tried keys the criterion accepted hypothesis $H(1)$. To obtain the final formula for the amount of effort $E^{\alpha,\beta}(r)$ required by the total method we shall insert the obtained expressions for $E^{\alpha,\beta}(t \le r)$, $E^{\alpha,\beta}(t \ge r+1)$ into the initial formula:

$$E^{\alpha,\beta}(r) = \frac{r}{|K|}E^{\alpha,\beta}(t \le r) + \frac{|K|-r}{|K|}E^{\alpha,\beta}(t \ge r+1),$$

$$E^{\alpha,\beta}(r) = \frac{1}{|K|}\sum_{k=1}^{r} k(1-\beta)^{k-1}\left[\beta(r-k) + \frac{\alpha\beta}{1-\beta}(k-1) + (1-\alpha)\right]$$

$$+ \frac{r}{|K|}r\alpha(1-\beta)^{r-1} + \frac{|K|-r}{|K|}\left(\sum_{k=1}^{r} k(1-\beta)^{k-1}\beta + r(1-\beta)^{r}\right).$$

If we set $r = |K|$, we shall obtain the formula for the mean number of trials in the total method, provided that all the keys are tried.

$$E^{\alpha,\beta}(|K|) = \frac{1}{|K|}\sum_{k=1}^{|K|} k(1-\beta)^{k-1}\left[\beta(|K|-k) + \frac{\alpha\beta}{1-\beta}(k-1) + (1-\alpha)\right] + |K|\alpha(1-\beta)^{r-1}.$$

Let us assume that $r = |K|$ and $\alpha = \beta = 0$, in other words, let us consider the case where the total method tries all the keys and the text rejection criterion works without errors. Then

$$E^{0,0}(|K|) = \frac{1}{|K|}\sum_{k=1}^{|K|} k = \frac{|K|+1}{2}.$$

In the case where $r = |K|$, $\alpha \neq 0$, $\beta = 0$, that is, where a procedure is used which precludes identifying a false key as the true one, but allows the failure to identify the true key, we have

$$E^{0,0}(|K|) = \frac{1}{|K|}\sum_{k=1}^{|K|} k[1-\alpha] + |K|\alpha = \frac{(1-\alpha)(|K|+1)|K|}{2|K|} + |K|\alpha = \frac{|K|+1}{2}(1-\alpha) + |K|\alpha.$$

If we assume that $r = |K|$, $\alpha = 0$, $\beta \neq 0$, that is, if we consider decision-making procedures which make losing the true key impossible, then

$$E^{0,\beta}(|K|) = \frac{1}{|K|}\sum_{k=1}^{|K|} k(1-\beta)^{k-1}(\beta(|K|-k)+1) = \frac{1}{|K|}\sum_{k=0}^{|K|} k(1-\beta)^{k-1}(\beta(|K|-k)+1)$$
$$= \frac{\beta|K|+1}{|K|}\sum_{k=1}^{|K|} k(1-\beta)^{k-1} - \frac{\beta}{|K|}\sum_{k=0}^{|K|} k^2(1-\beta)^{k-1}.$$

To calculate the sums included in the latter expression, let us consider the function

$$\Phi(x) = \sum_{k=0}^{|K|} x^k = \frac{1-x^{k+1}}{1-x},$$

$$\sum_{k=0}^{|K|} kx^{k-1} = \Phi'(x) = \frac{-(|K|+1)x^{|K|}(1-x) + 1 - x^{|K|+1}}{(1-x)^2},$$

$$\sum_{k=0}^{|K|} k^2x^{k-1} = \sum_{k=0}^{|K|} k(k-1)x^{k-1} + \sum_{k=0}^{|K|} kx^{k-1} = x\Phi''(x) + \Phi'(x).$$

At the same time

$$\Phi''(x) = \frac{-(|K|+1)|K|x^{|K|-1}}{1-x} + \frac{2\Phi'(x)}{1-x}.$$

It follows from here that

$$\sum_{k=0}^{|K|} k^2x^{k-1} = \frac{-(|K|+1)|K|x^{|K|}}{1-x} + \frac{1+x}{1-x}\Phi'(x).$$

By using the obtained expressions at $x = 1-\beta$ for $E^{0,\beta}(|K|)$ we shall have

$$E^{0,\beta}(|K|) = \frac{\beta|K|+1}{|K|}\Phi'(1-\beta) + (|K|+1)(1-\beta)^{|K|} - \frac{2-\beta}{|K|}\Phi'(1-\beta),$$

where

$$\Phi'(1-\beta) = \frac{-(|K|+1)(1-\beta)^{|K|}\beta + 1 - (1-\beta)^{|K|+1}}{\beta^2}.$$

Inserting the latter expression in the formula for $E^{0,\beta}(|K|)$ after elementary manipulations we shall obtain

$$E^{0,\beta}(|K|) = \frac{\left[1-(1-\beta)^{|K|+1} - (|K|+1)(1-\beta)^{|K|}\beta\right][\beta(|K|+1)-1]}{|K|\beta^2}.$$

A simple analysis shows that when $|K| \to \infty$

$$E^{0,\beta}(|K|) \to \frac{1}{\beta}.$$

Therefore, for large values of $|K|$ one could use an approximate equation $E^{0,\beta}(|K|) \cong \frac{1}{\beta}$.

Let us now proceed with the calculation of the reliability for the method of total key trials, that is, the probability $P(r, \alpha, \beta)$ of identifying the true key using this method.

Let C be an event consisting in identifying the true key while r keys are tried. Let us use events B_t, $t \in \{1, ..., |K|\}$ that were introduced earlier. Events B_t are incompatible, for which reason the event C is representable in the form $C = \bigcup_{t=1}^{r}(C \cap B_t)$. It follows from here that

$$P(r, \alpha, \beta) = P(C) = \sum_{t=1}^{r} P(C \cap B_t) = \sum_{t-1}^{r} P(B_t)P(C/B_t) = \frac{1}{|K|}\sum_{t=1}^{r} P(C/B_t),$$

by virtue of the fact that $P(B_t) = \frac{1}{|K|}$. On the other hand, $P(C/B_t) = (1-\beta)^{t-1}(1-\alpha)$. Therefore

$$P(r, \alpha, \beta) = \frac{1-\alpha}{|K|}\sum_{t=1}^{r}(1-\beta)^{t-1} = \frac{(1-\alpha)(1-(1-\beta)^r)}{|K|\beta}.$$

The latter equation is true for $\beta \neq 0$.

3. RELATED WORKS

A specific original text in any language to which block or stream encryption is applied has its own characteristic. Block ciphers are used as building blocks for many symmetric cryptographic primitives for encryption, authentication, pseudo-random number generation, and hash functions. Security of these primitives is evaluated in regard to known attacks against block ciphers. Among the different types of attacks, the statistical ones exploit non-uniform behavior of the data extracted from the cipher to distinguish the block cipher from random permutations. Differential cryptanalysis [10–13] and linear cryptanalysis [10, 13] are the most prominent statistical attacks against block ciphers.

As a result of each of these attacks, there are a number of possible block cipher keys that are subsequently tested by decoding the specified sequence of encrypted blocks to find the true key.

A typical attack for stream ciphers, for example, gaming cipher [14], is an attack on the key according to the specified open and corresponding encrypted text.

Widely known attacks on such generators are Weak key attacks and Related-key attacks) [15, 16].

The keys from the set of weak (or cohesive) keys are tested by decoding the specified encrypted text to find the true key.

In these problems, to clarify the time complexity of attacks when testing keys, one can use statistical criteria in the acceptance of hypotheses: $H(0)$ – when the key is tried, the decrypted text is plaintext and, therefore, the test key is true; $H(1)$ – decrypted text (possibly decoded text) is not a clear text, the key to be tested is false.

Known attacks on block and stream ciphers are attacks of the type meet-in-the-middle attack, for example, [17–19]. At the final stage of such attacks, you can also use statistical criteria to determine the plaintext.

4. CONCLUSIONS

Exact values have been obtained for the amount of effort and the reliability of a brute-force attack aiming to determine the plaintext from a ciphertext using a statistical criterion for determining the plaintext. Intermediate calculation formulas for these values and formulas for the amount of effort and reliability of the brute-force attack in particular cases can be used for updating the values of the amount of effort and reliability for other deciphering methods, including trials of a portion of the keys. One could take as an example the method of equivalent keys. If a cipher has L classes of equivalent keys, then the mean number of key trials without return until a key equivalent to the true key appears will be no more than L trials [20]. Therefore, the upper estimate of the amount of effort and the reliability of the brute-force attack for such

a cipher can be made from formulas that were obtained for them by replacing the value of $|K|$ with L in these formulas.

Thus, the paper reviews an actual task of reliability estimation for a cryptographic cipher using a statistical criterion for cipher lifetime. Method allows a formal prediction of the cipher's effective time of usage regarding the statistical characteristics for recognizing the plaintext and changes in the channel parameters.

REFERENCES

1. Banks, M.J., *A Search-Based Tool for the Automated Cryptanalysis of Classical Ciphers,* 2008.
2. *Encyclopedia of Cryptography and Security,* van Tilborg, H.C.A., Ed., Springer Science+Business Media, Inc., 2005.
3. Schneier, B., *Applied Cryptography: Protocols, Algorithms, and Source Code in C,* 1993.
4. Katz, J. and Lindell, Y., *Introduction to Modern Cryptography,* CRC Press, 2015, 2nd ed.
5. Lukanin, A.V., *Automatic Processing of Natural Language,* Chelyabinsk: SUSU, 2011.
6. Graham, R.D., *Password Cracking, Mining, and GPUs,* 2011.
7. Shannon, C., *Works on Information Theory and Cybernetics,* Moscow: Inostr. Liter., 1963.
8. Neyman, J. and Pearson, E.S., On the problem of the most efficient tests of statistical hypotheses, *Philos. Trans. R. Soc., A,* 1933, vol. 231, pp. 289–337.
9. Menezes, A.J., Van Oorschot, P., and Vanstone, S., *Handbook of Applied Cryptography,* New York: CRC Press, 1996.
10. Rasoolzadeh, S., Ahmadian, Z., Salmasizadeh, M., and Aref, M.R., Total break of Zorro using linear and differential attacks, *IACR Cryptol. ePrint Arch.,* 2014, vol. 220. http://eprint.iacr.org/2014/220.
11. Van Lint, J.H. and Wilson, R.M., *A Course in Combinatorics,* Cambridge University Press, 2001.
12. Hongjun Wu and Bart Preneel, *Differential cryptanalysis of the stream ciphers Py, Py6 and Pypy cryptology*, *EUROCRYPT,* 2007, pp. 276–290.
13. Differential cryptanalysis and linear distinguisher of full-round Zorro, *Applied Cryptography and Network Security—ACNS 2014*; *Lect. Notes Comput. Sci.,* 2014, vol. 8479, pp. 308–323.
14. Biham, E., New type of cryptanalytic attacks using related key, *EUROCRYPT'93*; *Lect. Notes Comput. Sci.,* 1994, vol. 765, pp. 229–246.
15. NIST, Recommendation for the Triple Data Encryption Algorithm (TDEA) Block Cipher, (Archive 23.01.2012) Special Publication 800-67, p. 14.
16. Fluhrer, S., Mantin, I., and Shamir, A., Weaknesses in the key scheduling algorithm of RC4, *Eighth Annual Workshop on Selected Areas in Cryptography (August 2001)*. http://citeseer.ist.psu.edu/fluhrer01weaknesses.html. Accessed September 17, 2001.
17. Zheng, Y. and Wu, W., Biclique Attack of Block Cipher SKINNY, *Information Security and Cryptology. Inscrypt 2016*; *Lect. Notes Comput. Sci.,* 2017, vol. 10143.
18. Çoban, M., Karakoç, F., and Boztas, Ö., Biclique Cryptanalysis of TWINE, *Cryptology and Network Security. CANS 2012*; *Lect. Notes Comput. Sci.,* 2012, vol. 7712.
19. Rechberger, C., On bruteforce-like cryptanalysis: New meet-in-the-middle attacks in symmetric cryptanalysis, *Information Security and Cryptology—ICISC 2012*; *Lect. Notes Comput. Sci.,* 2013, vol. 7839.
20. Babash, A.V., *Cryptographic and Theoretical Automaton Aspects of Modern Information Protection,* Moscow: International Consortium "Electronic University," Eurasian Open Institute, MESI, 2008, vol. 1.