METHODS FOR CONSTRUCTING HASH FUNCTIONS IN COMPRESSING MAPPINGS OF PRIME NUMBERS

G. Vostrov, *Ph. D., Associate Professor*,
E. Ponomarenko

Odessa National Polytechnic University.

Abstract: In this work we investigate the problem of constructing hash functions which based on the mapping of primes to classes. The problem is considered in the field of financial documentation security. A specific method for hashing information based on compressive mappings of prime numbers was giving.

Key-words: hash-function, cryptosystem, financial document, prime number, prime number class.

In our time, electronic documentation is rapidly replacing paper documents. Often, it is required that a limited number of persons has an access to the information in a financial document has. However, the risk of interception by an intruder of important financial data is significantly increased, when using the Internet to conduct business. Therefore, the task of protecting the document arises in such a way that the persons participating in these processes have an access to the information.

Hash functions can be used to organize the protection of important financial documents. They are a tool for converting an original document into a fixed-length sequence. As part of a particular business process, as a rule, there are many documents, therefore, it is necessary that they have the same hash code for further analysis and data processing.

Hash functions are widely used in cryptosystems. Therefore, a number of specific requirements to cryptographic methods of information protection should be satisfied, such as:

- resistance to the search for the first prototype;
- resistance to the search for the second prototype;
- resistance to collisions.

The hash functions which used in cryptographic applications realize perfect mappings (complete mixing), so changing at least one bit in the original sequence results in an average change in at list half of the convolutional bits [1].

At the moment, the existence of an irreversible hash function remains an unproven fact and is an unsolved problem in computer science. Usually finding an inverse value is just a computationally complex task. Consequently, there is a problem of constructing hash functions in such a way that there does not exist an effective polynomial algorithm for computing the inverse function in a reasonable time.

A possible solution of the problem of protecting financial documents is the construction of hash functions based on the mapping of prime numbers, which is to be investigated.

All prime numbers in class P_{2k} can represent a procedure for compressing data, and the code for this procedure is represented by a prime number $p \in P_{2k}$. In this way $P_{2k} = \{p_1, p_2, \ldots, p_m, \ldots\}$ and $f(p) = 2k$. If a financial document that you want to protect from third-party access is submitted to the input, it can be converted to binary code and then to the decimal number - a. If it is not prime, it is necessary to find the nearest prime number p. By knowing the difference of $(p-a)$, you can restore the value of a.

Further, the problem of protection can be reduced to the problem of decomposition of numbers into simple factors. Let us find a prime number $p*$, such that $p* = pp'+1$,where p is a previously found prime number, p'- a correctly chosen prime number. If numbers p and p' are large enough, then the task is computationally complex.

Consider the map: $x_{n+1} = ax_n(\mathrm{mod}\, p)$. This mapping generates cycles of length $l_a(p)$. In accordance with Euler's theorem: $a^{\varphi(p)} \equiv 1(\mathrm{mod}\, p)$, if a and p - are relatively prime. In particular, for a simple p , $\varphi(p) = p-1$.[2].

If we set $x_0 = 1$, then $x_1 = a(\mathrm{mod}\, p*)$, $x_2 = a^2(\mathrm{mod}\, p*)$, …, $x_{l-1} = a^{l-1}(\mathrm{mod}\, p*)$. If a is the primitive root of the number $p*$, then $l-1 = p*-1$. We obtained a set of degrees a modulo p. Then, by Fermat's small theorem $a^{p-1} \equiv 1(\mathrm{mod}\, p)$. Therefore, the iteration cycle contains all values for which equality $x_{n+1} = 1(\mathrm{mod}\, p*)$ is correct.

In this case, we should use the fact that the length of the iteration cycle $\varphi(p*)$ divides $l_a(p*)$, and their quotient $\frac{\varphi(p*)}{l_a(p*)}$ is the indices of the classes. Then $\frac{p*-1}{l_a(p*)} = k$, where k is an index of the class of membership of the number $p*$.

It is proven that for $a = 4$, prime numbers are mapped to the class P_2.

Inverse calculation is impossible if knowing only the index of the class to which a prime number $p*$ belongs. Since an infinite number of prime numbers can belong to the class, and there is also no knowledge of how the order relations in the class are given.

An important application of such a hash function is to determine the value of a known parameter t to calculate the value of the discrete logarithm $a \equiv t^x(\mathrm{mod}\, p)$. It is important that t must be a primitive root for p, otherwise the problem of discrete logarithm can turn out to be unsolvable.

The question of protection of information security systems using this hashing procedure remains open, with the advent of quantum computers capable of solving the problem of restoring the original data.

References:

1. Fomichev, V.M., Methods discrete mathematics in cryptology [Text], 2010 – 424 p. - ISBN-13: 978-5864042342.
2. Vinogradov, I.M., Fundamentals of the theory of numbers [Text], 2009 – 176 p. - ISBN: 978-5-8114-0535-0.
3. Vostrov, G., Hrinenko, A., Computer modeling of processes of chaos formation in nonlinear dynamic mappings [Text], 2017 - ISSN 2221-3805.
4. Models, methods and means of management of socio-economic objects: monograph / Кол. the authors - Odessa: Bondarenko MO, 2016. - 226 pp.
5. ISBN 978-617-7424-14-6 UDC 303.4 BBK 65.050.9 (4Ukr) 030.1 M 744 (OO Arsiriy, TL Budoratskaya, MG Head, NN Zhuravlyova, O .A.Juran, LM Lingur, EV Malakhov, VP Slobodyanyuk, TP Trufanova, T.V. Filatova, AA Chugunov Models, methods and means of management of socio-economic objects: monograph / O. Ars., TL Budoratska, M.G. Head, N.M. Zhuravlev, O.A. Zhuan, L. M. Lingur, E. V. Malakhov, V. P. Slobodyanyuk, TP Trufanova, T. Filatova, AA Chugunov - Odessa: Bondarenko M.O., 2016.- 226 p.
6. Balan O.S. Reduced time complexity of simulation of 4D symmetric transfer processes: dis. Cand. tech Sciences: 05.13.06 / Balan Alexander Sergeevich. - Odessa, 2003. - 150 pBalan O.S. Underwriting as a tool to improve the efficiency of risk management of the bank [Електронний ресурс] / O.S. Balan, A.V. Levitska, O.O. Sokolovskaya // Економіка: реалії часу. Науковий журнал. – 2015. – № 2 (18). – С. 142-146. – Режим доступу до журн.: http://economics.opu.ua/files/archive/2015/n2.html.
7. Sokolovskaya Z.M. Simulation of business processes of complex economic systems / Z.M. Sokolovsky - Proceedings of Odessa Polytechnic University: Scientific and Scientific-Production Collection. - Odessa 2011. - Vip. 3 (37). - with. 135-141.
8. Sokolovskaya Z.M., Klepikova O.A. Applied models of system dynamics: [monograph] / Z.M. Sokolovsky, OA Klepikova - Odessa: Astroprint, 2015. - 308 p.