INTERNATIONAL JOURNAL OF MATHEMATICS AND COMPUTERS IN SIMULATION
DOI: 10.46300/9102.2022.16.14 Volume 16, 2022

Heru Technologies encryption method: Unique in the world that uses unpublished mathematical formulas and encrypts with binary disturbances.

Carlos Roberto França
Department: Academic Coordination
Federal University of Fronteira Sul
Chapecó/SC, Brazil

Abstract — **Several mathematical concepts remain unchanged for centuries, many were never even considered to be expanded upon. Typical cases, such as the ratios of geometric and arithmetic progressions, for example, which until now humanity uses with a singular, unique and fixed value. The search for new elements, new formulas, expansion of concepts such as accelerations and other magnitudes belonging to the field of kinematics, were motivating factors for the Brazilian researcher who created the Infinite Series with Multiple Ratios (SRMs), with whom the author of this article had the honor to work and help in the creation of these new magnitudes of the exact sciences with countless applications. SRMs remain unknown to humanity to this day, even though more than 23 years have passed since the first presentations and publication in a Brazilian technical magazine. The passion for low-level computing made the author of this article see that SRMs have infinite applicability in machine language, data compression, data lookup and cryptography. This article presents a cryptographic method made with these mathematical elements totally unknown to humanity and with surprising results that will be reported here**.

Keywords— Infinite Series with Multiple Ratios, cryptography, interoperability, computational mathematics, binary perturbations

I. Introduction

The Heru Technologies Cryptographic Method generated software with great applicability in the field of information security, more specifically in the protection of sensitive information from government companies or private companies and even digital data of individuals. It works from binary perturbations caused by using specific mathematical formulas. These formulas come from a mathematical research that has never been made available in printed or digital book in Brazil or any other country, but which are the domain of the author of the Cryptographic Method presented here, because he participated in the research that originated the formulas. Unpublished, including being responsible for forwarding them, named as Infinite Series with Multiple Ratios (SRMs), to Universities in Brazil and abroad, having been published in a technical journal of one of these institutions. The Heru Cryptographic Method is one of the applicability of SRMs, providing a totally unprecedented encryption, by the mathematical principles used and the only 100% Brazilian. Heru Crypto does not use any specific hardware and works independently of computing platforms. The Method originated the ZK Encryption Software or Heru Technologies, which, in addition to the aforementioned properties, is fully customizable due to its high degree of interoperability. In addition to compatibility with any operating system, it is possible to encrypt any type of file, including those that have already been encrypted by other software and methods. For a better understanding of the state of the art of this 100% Brazilian encryption, since the methods used in Brazil and in most countries are hybrid (solutions based on methods such as AES, an American standard, customized to meet the needs and demands of the public and private), it is important that we know at least the contexts of the emergence and foundation of the unprecedented formulas that gave rise to ZK or Heru Technologies cryptography. Let's get to the facts:

Research involving Infinite Series with Multiple Ratios (SRMs), was initiated by Sir Isaac Newton, but he did not complete or publish it. Some citations in documentaries about the incomplete work of the brilliant physicist were the source of inspiration for two Brazilian researchers, and what served as an aid at the time, in the early 1990s, accompanied the search for practical applications for the set of 16 (sixteen) formulas. By insisting and dedicating himself to SRMs for more than 23 years, success has been achieved with a strong cryptography that has attracted the interest of several universities, research centers, governments and large companies in Brazil and abroad. Presentations were made in Israel, some to Brazilian government entities, including approvals and recommendations.

SRMs complement and extend centuries-old physical and mathematical concepts, such as those involving arithmetic and geometric progressions, Newtonian kinematics, Torricelli's equation, and others. They are all formulas based on singular events with a single ratio, or a speed or acceleration stipulated as a starting point for solving problems in the universes of physics and mathematics. The Infinite Series with Multiple Ratios work with a finite set of size ratios (n), where n is any number belonging to the set Z + (positive integers).

Below are some concepts of SRMs formulas:

According to the creator of the Infinite Series with Multiple Ratios, Professor Edgar Oliveira Rodrigues [RODRIGUES,1995] the following basic concepts are essential for understanding these new mathematical elements.

A) ARITHMETIC SERIES - GENERAL TERM

x=0 → $a_n = a_k + (y-1)R$ (1)

x is the remainder of the division made by the number of terms in the series (n), and the amplitude of the interval (K). For better understanding, it is necessary to understand some concepts:

a) Homologous Term (TH) is defined by the module between the terms. If it is a multiple of K, they are homologous;

Ex. We will take K=5, arbitrarily, to facilitate the proofs

a7 TH a22, since | 7 - 22|= 15 which is a multiple of 5, arbitrated value for k

b) Another important concept concerns the periods.

Let's imagine a series with 23 terms (a23) e K= 5

23/5 = 4 and with remainder 3

4 is the integer quotient of the division (n/k) and represents the number of periods (y)

y = 4 periods [a2, a6], [a7, a11], [a12, a16],[a17,a21]

The remainder of the division (n/k), represented by (x), locates the term in the series.

Examples:

If x=1 we have the following relations in the 4 periods above, dividing the last term by k (1st period the last term is a6), in the second period it is a11, in the third period it is a16, and in the fourth period it is a21.

So for x=1 we have: 6/5 = 1 remainder 1, 11/5=2 remainder 1, 16/5= 3 remainder 1 and 21/5= 4 remainder 1

This fact indicates that the homologous term is always the last of each period and homologous to (a1). So, a1 th a6, a1 th a11, a1 th a16 and a1 th a21

If x = 0, we will have the following relationships in the 4 periods above.

5/5=1 remainder 0, 10/5=2 remainder 0, 15/5=3 remainder 0, and 20/5=4 remainder 0

We can observe that all homologous terms to the 1st are the penultimate terms of each period. As there is no (a_0) in the series, the 1st th is the penultimate of the period, causing the number of periods to be subtracted from one unit:

(y -1).

Let's look at one more important observation.

a5 th a20, because 20/5 = 4 remainder 0

Note that between a5 and a20 there are only three complete periods, which are:

[a20,a16], [a15,a11],[a10,a6]

So if x=0 there will be (y-1) periods

(ax th an) for x>= 1, for example 23/5 = 4 remainder 3, so x=3 which is the remainder and a3 th a23 since | 3 - 23|= 20 which is a multiple of 5

If x>= 2, the term will be found in the incomplete period (x-1) positions above the full period. Example: a23 23/5 = 4 remainder 3, as x is the remainder of the n/k division we have (3 -1) = 2 and actually a23 is two positions above the last period.

Generalizing: a_x th a_n for x>= 1

So for the first formula having x = 0, comes → $a_n = a_k + (y-1)R$

X=0 → $a_n = a_k + (y-1)R$

R=$\sum_1^k r$ that is, R is the sum of the multiple ratios of the set r that will have an amplitude (number of elements) represented by K.

From the explanations arising from the 1st formula, it is possible to deduce and use the others that make up the scope of the Arithmetic series.

x >=1 → $a_n = a_x + y_R$ (2)

SUM

X=0 → $S_n = y$ (3)

x=1→ $S_n = a_1 + y\sum p1 + \frac{KRy(y-1)}{2}$ (4)

x>=2→ $S_n = \sum_1^x a + y[\sum p1 + (x-1)R] + \frac{KRy(y-1)}{2}$ (5)

B) GEOMETRIC SERIES - GENERAL TERM

The same concepts are adopted, with Q as the symbol of the product of the ratios.

X=0→ $a_n = a_k Q^{(y-1)}$ (6)

x >=1→ $a_n = a_x Q^y$ (7)

x=0→ $S_n = a_1(1-Q^y) + \frac{\sum p1(Q^y-1)}{Q-1}$ (8)

x=1→ $S_n = a_1 + \frac{\sum p1(Q^y-1)}{Q-1}$ (9)

x>=2→ $S_n = a_1 + Q^y \sum_2^x a + \frac{\sum p1(Q^y-1)}{Q-1}$ (10)

SUM OF INFINITE TERMS

0 < Q <1 n→ ∞ ∴ $y \to \infty$

$S_n = a_1 + \frac{\sum p1}{1-Q}$ $n \to \infty$ (11)

Application of Multiple Ratios to Movement Instantaneous speed - application of the 1st and 2nd solving formulas.

Space traveled

X=0→ $S_n = y$ (12)

X=1→ $S_n = a_1 + y\sum p1 + \frac{KRy(y-1)-(v_0+v_f)}{2}$ (13)

x>=2→ $\boldsymbol{S_n} = \sum_1^x a + y$ (14)

It is worth mentioning again that the SRMs were never published in books, but were presented at meetings of the Brazilian Society for the Progress of Science - SBPC

[SBPC,1997, p715], [SBPC,1998, p 404-405], [SBPC,1998, p 1044] and validated by renowned Brazilian editors and Brazilian and Canadian mathematicians. This work does not intend to discuss SRMs, but rather to present the first computational application originated by them, which is the ZK Cryptographer, here also called Heru Technologies Cryptographic Method.

II. STATUS OF THE TECHNIQUE

The Heru Cryptographic Method was implemented in C Language, having been tested on Windows and MAC OS platforms and without any restrictions regarding its use in other computing environments, including cell phones, tablets and other equipment that allow embedded technologies. Encryption is closed or state and in this case, the method itself generates the key, with no compilation of public and private keys, which are usual in most cryptographic methods. The exceptions are the algorithms used by governments and some private companies such as blackberry that adopts this type of encryption used by our method. The main purpose of the Heru Technologies Cryptographic Method is to serve as an embryo for closed encryptions of the federal government and even to foster discussions about the need for Brazil and other countries to have their cryptographic methods 100% copyright and without the need to pay royalties to use foreign technologies, but this subject will be taken up in more detail in the final remarks.

III. DESCRIPTION OF TECHNICAL FUNCTIONALITIES

Encryption takes place with the following steps:
Step 1: Submit a file of any size and type, apply SRMs mathematical formulas to hegemonize the bytes of the input file, size N, going from B1 (first byte of the file) to Bn (last byte of the file). This treatment is done from the numerical values of each byte, recognized and manipulated by any operating system.
The main objective of the hegemonization process is to eliminate the dispersiveness between the bytes, making the sets more homogeneous in terms of distance, points of convergence and other mathematical characteristics that will make it possible to organize the original file into sub-files, when it is not possible to hegemonize in a single step;

Step 2: After processing the information from step 1, the distance between the bytes is determined (by applying formulas) and the least dispersive groups are found. After the creation/separation of minimally cohesive groups, the relevant differentiations for each group are taken and a numerical set derived from this information is stipulated. These sets will be written to memory at runtime and used for decryption;

Step 3: The elements that cannot fit into the cohesive groups form the waiting groups and the process is repeated until there are no more waiting groups;

Step 4: Register the numbers of groups and information on the characteristics of each one, such as: first element, distances, amounts of data from each group and mathematical information extracted from each group and any and all information peculiar to the hegemonization processes mentioned in the step 1. This information is recorded at runtime and the elements that passed through the previous steps are discarded, as the extracted and recorded features are enough to decrypt and recover the input file without any loss of information or distortion of the original data, regardless of whether it is images, videos, documents, etc.;

Step 5: The bytes that were not allocated after going through the previous steps form a subfile with identification of B1 (first byte, which is the first element that was not allocated) and Bn (last unallocated element). Having B1 and Bn, the process is repeated until there are no deallocated elements left. The sub-files receive the same mathematical treatment given to the input file of size N, and likewise the extracted data is stored in memory and used in the decryption process.

Technical Information - DESCRIPTOGRAPHY

The original file is recovered from the characteristics stored in the steps described in the Encryption process. This information is unique and exclusive to each file, and only reassembles the files with the reapplications of the specific mathematical formulas used in the processes.
Decryption uses the information stored from the first to the last moment of the cryptographic process. No information is lost from the original file and with that the chances of distortion or loss of information are totally discarded.
The following figures represent some screens recorded during the encryption and decryption processes of an image file with a jpg extension. The demo can be accessed in full at the following address:

https://youtu.be/dD4kmPqGmdw

Heru Technologies Cryptographic Method Strength Test.

Encryption algorithms usually pass the process robustness test. Normally, an image file is used to verify the treatment given to the pixels and, in this way, an attempt is made to discover information or weaken the algorithm, or a file composed of the same digit repeated several times is adopted. In the case of the ZK Cryptograph, the option of strength or encryption test for specialists was performed with a 1kb *.txt file formed exclusively by digits 1 (one). The commented test is available at the following link:

https://youtu.be/dTxWhDWlje0

The above test was requested after being screened by Brazilian experts who work in military institutions and/or with the GSI (Institutional Security Office), a body directly linked to the Presidency of the Republic and whose function is to regulate cryptography in our country. This quote is certainly superficial, as I will not open a space for discussion about the procedures of Brazilian Institutional Security, but I note that the Heru Technologies Cryptographic Method or Zk

Cryptography has already been presented to ABIN (Brazilian Intelligence Agency), Brazilian Navy, SERPRO and other government agencies. The search for space and peer recognition is one of the winning brands of Cryptograph ZK, which has been gaining credibility since when it became a reality with the achievement of "SINAPSE DA INOVAÇÃO" in 2013/2014. The investment and trust of the Government of Santa Catarina through the Department of Development, the CERTI Foundation and the Foundation for Support of Research and Innovation of the State of Santa Catarina (FAPESC), were major milestones and made it possible to materialize what could be the First Latin American Encryption Standard.

IV. CONSIDERATIONS

The Cryptographic Method presented here has numerous applicability, being able to encrypt any data set and with strong potential for cloud computing and mobile technologies. In addition to the innovative and unprecedented mathematics, the generated cryptograph stands out for its interoperability and versatility of use, totally different from the tools available on the world market.

Another fundamental aspect is the inexistence in Brazil and in Latin American countries of closed or state algorithms. This fact has already brought us some problems with international espionage, files and sensitive information from the federal government being searched and snooped by intelligence agencies from other countries, putting national security at risk and hybrid solutions contribute a lot to this happening. I believe you can't use closed or state encryption on a large scale, but at least sensitive government information should have its own protection and no algorithms with the backbone coming from US AES or any other foreign cryptographic standard. No matter how much customization is done, the author percentage will always have a considerable margin of intelligence from outside and this weakens and promotes episodes such as the Edward Snowden case. What is sought with the Heru Technologies Encryption Method, which results in the Zk cryptographer, is the adoption of 100% Brazilian cryptographic solutions and our autonomy in the areas of Information Security.

REFERENCES

[1] Rodrigues, Edgar - Infinite Series with Multiple Reasons, Journal of scientific dissemination, Logos Informática - issue 02 - Luterana University of Brazil, October 1995.

[2] Minutes of the Brazilian Society for the Progress of Science (SBPC) - 49th Annual Meeting of the Federal University of Minas Gerais, p. 715. Belo Horizonte-MG July 13, 1997.

[3]. Minutes of the Brazilian Society for the Progress of Science (SBPC), 6th Extraordinary Meeting, October 28 to 31, 1998 - Maringá - PR. pg. 404-405.

[4]. Minutes of the Brazilian Society for the Progress of Science (SBPC), 50th Annual Meeting from July 12 to 17, 1998. Federal University of Rio Grande do Norte, Natal-RN. pg. 1044).