Crimson Publishers
Wings to the Research

Opinion

Cryptography And Its Implications on Electronics and Devices: A Time-Complexity Algorithmical Analysis

Fausto Abraham Jacques-García*

Information Science School, Queretaro State University, México

ISSN: 2640-9739

***[1]Corresponding author:** Fausto Abraham Jacques-García, Information Science School, Queretaro State University, México

Submission: July 11, 2022

Published: July 27, 2022

Volume 2 - Issue 3

How to cite this article: Fausto Abraham Jacques-García. Cryptography And Its Implications on Electronics and Devices: A Time-Complexity Algorithmical Analysis. COJ Elec Communicat. 2(3). COJEC.000538.2022.
DOI: 10.31031/COJEC.2022.02.000538

Introduction

Information is the third pillar of the natural world, along with matter and energy [1]. The Natural World is founded on Matter, Energy and Information. We can classify these three pillars in the Real-World (R-W), which is formed by Matter and Energy, and the Abstract-World (A-W), formed by Information. Information connects the real-world with the Abstract-World.

Now, Matter and Energy have been developed through centuries of exhaustive research. While Information Science just through 74 years, so far; formally speaking. The abstract-world needs to be study more than ever before, as well as research and technology development for direct appliance in the issues we face nowadays; same as the real-world back then. But how can information be defined?

Well, there are the Classical and the Contemporary approaches. In the Classical one, given by Claude Shannon in 1948, information is a probabilistic measure of the variability or uncertainty of messages that can be received from a source. Thus, information is the message that one does not expect and know (Entropy). On the other hand, Information is organized data that represents the messages, knowledge and/or abstracted real-world entities. Thus, Information is a property or attribute of the natural world that can be generally abstracted.

Observe that the word 'data' is inside the definition above. It is also necessary to define data. Data are random fragments of information or bits, which follow an entropic behavior. Data is the atomic unit of information (bit) as a classical axiom. A chain of eight bits (byte) is to be processed using Boolean algebra. Now, as a contemporary axiom, data are isolated and raw facts, which are in a significant context, and through one or more processing operations, it can be inferred if they are entities, objects, people or events. Those isolated and raw facts are to be processed using Computer Science.

Information shapes the universe. Information is what makes matter and energy to be. In the same way, Matter and Energy allows us to work with Information. A Laboratory Analogy: A lab is formed by Instruments and Artifacts according to Rabardel [2]. In an Information Lab, instruments equal Mathematics and Artifacts equals Computers. A digital computer runs on matter and energy, and it is a synchronic temporized finite state machine. Mathematics allows us to model, represent and work with the relations of the information entities around us, to know and understand our universe. While with Computers we can automatize this process, making it more efficient. Optimization.

Once again, we can observe a bidirectional dependence relation in these abstract concepts.

Information & Computer Science seeks to make a better appliance of a process or a method. This to optimize resources such as *space*, *time*, *energy* and *matter*. Its implications have a positive impact on *Society*, *Environment* and *Economics*.

"The science of Cryptography has matured and leads to the development of software applications to strengthen data security to maintain the integrity of stored data or data that is being sent to a specific destination", García & Canchola [3]. Cryptography is now a Cornerstone in Computer Science!

Now, According to Alarcón-Narváez & Jacques-García [4], Symmetric Encryption is a form of cryptosystem in which encryption and decryption are performed using the same Key. Techniques such as Substitution and Transposition are used in this kind of Crypto Algorithms, such as the Hill n-Cipher and AES (Advanced Encryption Standard). Focusing in Hill Cipher, it works with square-matrices. A random square matrix $\langle k \rangle$ for the encryption, and the modular inverse of that matrix $\langle k_m^{-1} \rangle$ for the decryption. The bigger the matrix, the better the security of the data. Moreover, If the matrix-size is equals the message-size then the Shannon's Principle of Perfect Secrecy is accomplished. That is why it is vital to study and analyze some of the most used matrix numerical methods for Symmetric Cryptography [5].

There are many numerical methods oriented to matrices. But just a few oriented to modular inverse matrices computation. To mention some, Leibniz (determinats and adjoint matrices), Eisenberg (Gauss-Jordan with implicit modularization), Gauss-Jordan with explicit modularization, Montante with Euclidean Explicit modularization and Gauss-Jacques (Row Echelon Form -REF- with Euclidean-Implicit Modularization); methods.

All of the above allow matrix-based crypo-algorithms sucha as Diffie-Hellman´s to result Scalar Fields (SF) Z_n as required by the message codification. Where each codified/de-codified subset (vector) belongs to a Linear Arithmetic Space Z_n^m. Where $[n]$ stands for the natural numeric set (NNS) $\{N\}$ limited by the system codification required, and $[m]$ stands for the dimension of the resulting vectors or each linear operation performed. The key in this context is the amount of resources [Time, Energy, Hardware Specs, Mony Costs, etc.] needed to compute $\langle k_m^{-1} \rangle$.

We can use algebra, calculus and Computer Science big 'O' notation to make a comparison out of this. To be briefly, I start with the classical by the axiom that a determinant or a cofactor matrix such as the adjoint possesses a Computer Complexity of $|O(n!)|$, that's the Leibniz's. That is factorial, the worst case. Eisenberg [6] as Alan Konheim some years before, considered a Computer Complexity of $|O(n^2m^2)|$ a fourth-degree polynomial. It is good, a very good approach. To go on with the contemporary by the Gauss-Jordan resolution and then, Modular Arithmetic with a Computer Complexity of $|O(n^2m^2)|$, which is better in velocity, but it works out of the SF with memory issues. Bareiss-Montante with Eulidean Modularization helps even better having $|O(n \log m)|$, however the variable which will save the product value to obtain the reciprocal in the latter, also resides outside the SF makes this option not good computationally economy speaking. But according to Jacques-García et al. [7] using the REF operations with Euclidean-Implicit Modularization (the Gauss-Jacques) makes it an instrument itself by nature *per se* [2], and the best choice of all resulting in $|O(n^3 \log m)|$ with excellent use of computer memory as working in the limits of the Scalar Field Z_n, no less, no more. To finish, the notation of this time-complexity algorithmic analysis, $[n]$ represents dimensional matrix-size, and $[m]$, for modular arithmetic value.

So, when working with Square-Matrix-Based-Symmetric Encryption and its Optimal Implications on Electronic and Devices now and in the future; digital and/or quantum; Gauss-Jacques method is the abstract-world existing algorithm to apply and implement directly in the real-world technology best alternative. Moreover, Eisenberg's approach to *Modular Linear Algebra* can now be more formally developed with the existing state-of-the-art matrix numerical methods discovered, published and disseminated.

References

1. Wang, Yingxu (2003) On cognitive informatics. Brain and Mind. 4. pp. 151-167
2. Rabardel Pierre (1995) Les hommes et les technologies: une approche cognitive des instruments contemporains. Editeur Armand Colin.
3. García FAJ, Luz Canchola Magdaleno S (2015) Vector cryptography system: An approach for the analysis of linear arithmetic spaces. 12th International Conference on Information Technology-New Generations, pp. 522-527.
4. Alarcón-Narváez D, Jacques-García FA (2021) Towards a symmetric crypto algorithm: The HAJ. In: Latifi S (Ed.), ITNG 2021 18th International Conference on Information Technology-New Generations. Advances in Intelligent Systems and Computing, Springer, Cham, 1346: 121-126.
5. Martínez-Martínez AN, García FAJ (2021) A comparative study between two numerical methods for symmetric cryptography uses and applications. In: Latifi S (Ed). ITNG 202118th International Conference on Information Technology-New Generations. Advances in Intelligent Systems and Computing, Springer, Cham, 1346: 127-130.
6. Eisenberg, Murray (1999) Hill ciphers and Modular Linear Algebra. Copyrights (1998). University of Massachusetts, Amherst, Massachusetts, USA, pp. 1-19.
7. Jacques-García FA, Uribe-Mejía D, Macías-Bobadilla G, Chaparro-Sánchez R (2022) On modular inverse matrices a computation approach. South Florida Journal of Development, Miami, Florida, USA, 3(3): 3100-3111.