Scientific Research Publishing

Journal of Information Security, 2024, 15, 299-307
https://www.scirp.org/journal/jis
ISSN Online: 2153-1242
ISSN Print: 2153-1234

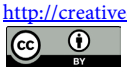
Comparative Study of the Reliability and Complexity of Symmetrical and Asymmetrical Cryptosystems for the Protection of Academic Data in the Democratic Republic of Congo

Mugaruka Buduge Gulain[1,2], Jeremie Ndikumagenge[2], Buhendwa Nyenyezi Justin[3], Bulonza Masumbuko Alexis[4], Katho Seba Jacques[5]

[1]Department of Management Computing for Companies, Section of Commercial and Computing Sciences, Teachers' Training College of Bukavu, Bukavu, The Democratic Republic of the Congo
[2]Center of Research in Infracture, Environment and Technology (CRIET), Doctoral School, University of Burundi, Bujumbura, Burundi
[3]Department of Maths-Physics, Section of Exact Sciences, Teachers' Training College of Bukavu, Bukavu, The Democratic Republic of the Congo
[4]Higher Institute of Medical Techniques of Bukavu, Bukavu, The Democratic Republic of the Congo
[5]Department of Maths-Physics, Section of Exact Sciences, Teachers' Training College of Bunia, Bunia, The Democratic Republic of the Congo
Email: mugarukabuduge@gmail.com, jeremie.ndikumagenge@ub.edu.bi, justinnyenyezi@gmail.com, bulonzaalexis@gmail.com, kathoseba@gmail.com

How to cite this paper: Gulain, M.B., Ndikumagenge, J., Justin, B.N., Alexis, B.M. and Jacques, K.S. (2024) Comparative Study of the Reliability and Complexity of Symmetrical and Asymmetrical Cryptosystems for the Protection of Academic Data in the Democratic Republic of Congo. *Journal of Information Security*, **15**, 299-307.
https://doi.org/10.4236/jis.2024.153017

Received: January 31, 2024
Accepted: May 14, 2024
Published: May 17, 2024



Abstract

In the digital age, the data exchanged within a company is a wealth of knowledge. The survival, growth and influence of a company in the short, medium and long term depend on it. Indeed, it is the lifeblood of any modern company. A company's operational and historical data contains strategic and operational knowledge of ever-increasing added value. The emergence of a new paradigm: big data. Today, the value of the data scattered throughout this mother of knowledge is calculated in billions of dollars, depending on its size, scope and area of intervention. With the rise of computer networks and distributed systems, the threats to these sensitive resources have steadily increased, jeopardizing the existence of the company itself by drying up production and losing the interest of customers and suppliers. These threats range from sabotage to bankruptcy. For several decades now, most companies have been using encryption algorithms to protect and secure their information systems against the threats and dangers posed by the inherent vulnerabilities of their infrastructure and the current economic climate. This vulnerability requires companies to make the right choice of algorithms to imple-

ment in their management systems. For this reason, the present work aims to carry out a comparative study of the reliability and effectiveness of symmetrical and asymmetrical cryptosystems, in order to identify one or more suitable for securing academic data in the DRC. The analysis of the robustness of commonly used symmetric and asymmetric cryptosystems will be the subject of simulations in this article.

Keywords

Comparative Study, Cryptosystems, Symmetric Encryption, Asymmetric Encryption

1. Introduction

When it comes to data security and protection, cryptography is today at the heart of the development of new approaches to data and information management. It is in demand by many companies/users wishing to exchange or store information in a safe and secure way. This needs to exchange confidential data between two or more users raises the issue of data security, and requires the availability of reliable and complex security techniques. Encryption remains the only effective means of meeting these requirements. As a result, in recent years, several authors have taken an interest in work on cryptosystems, which we cite here as a non-exhaustive list [1]-[14]. However, the choice of a good encryption algorithm or tool still remains a headache for most users, and this sometimes leads to the vulnerability and inefficiency of information systems. Our study, which compares symmetrical and asymmetrical cryptosystems in order to propose the most appropriate for academic data management in the Democratic Republic of Congo, is therefore justified. Throughout this study, we designed cryptosystems (asymmetric, symmetric) and tested encryption, decryption, random key generation and runtime comparison for each. As long as the private key has remained secret, has not been compromised and only the user for whom it was issued has access to it, data and message encryption provides the following advantages: authentication, non-repudiation, integrity and confidentiality. There are different families of encryption, which we detail as follows: First, secret-key encryption, known as symmetrical encryption, uses a single key to encrypt and decrypt data. Next, public-key encryption, generally referred to as asymmetric encryption, uses two keys (one private, the other public), the first accessible by the public to encrypt the message, and the second (available to the recipient) to decrypt the message. Finally, hybrid encryption combines the two previous techniques. Private and public companies are always faced with the problem of securing secret information, and the only solution to this is to ensure the privacy of users or people who spend the rest of their time on the Internet, because everything is there, and you have to take every possible precaution. Given that privacy is a right, not a favor, we need to work on behalf of those who prefer to use

the Internet as a channel of communication while remaining discreet. Alice communicating with Bob doesn't need or won't feel comfortable and secure if her conversation leaks out. Even if information is stored on servers, PCs or other data storage media, the question remains: how is it stored? If an intruder gains access to your PC or server, can he or she access the data directly? Can he or she read the information contained therein? The answers to these questions will help us decide on the best solution.

2. Materials, Tools, Equipment and Methods

2.1. Material

The comparative study of the reliability and complexity of the two major cryptosystems is based on the analysis of past and present use of the entities that have undergone encryption and decryption operations using the RSA, HILL... algorithms constitutes the working material of this article.

2.2. Tools and Equipment

The Math BIgInteger and matrix libraries in php are the study tools, while number and set theory are the materials.

2.3. Methods

Differential and/or analytic functions and probabilistic laws will be used as a method of study and analysis.

3. Data Protection and Security with Cryptosystems

In recent times, the Internet has become a haven for people from all walks of life, each in search of their own area of interest. This craze is justified by the emergence of attractive technologies in all areas of life. As the number of users increases, so does the need for control: who does what? Who does what? Who does what? How? And this is a real problem for data, which currently represents billions of dollars. The need for this control leads us to think about securing information using appropriate tools [15] [16] [17] [18] [19]. Based on existing techniques, we will describe how to solve the problem of data protection using Asymmetric and Symmetric Algorithms.

3.1. The RSA Algorithm

An RSA encryption system is an easy-to-use, asymmetric encryption method that is very popular in many fields requiring data transfer over the Internet. It consists of two RSA encryption keys, one public and one private. While the public key is used for encryption, the private key is used for decryption. Since **no algorithm** is capable of decoding the private key from the public key, this method is seen as a secure process. In addition to **encryption**, the RSA encryption system can also **generate its own digital signatures**.

Application

An example with small prime numbers (in practice you need very large prime numbers):

1) choose two prime numbers $p = 3$, $q = 11$;

2) their product $n = 3 \times 11 = 33$ is the cipher module;

3) $\varphi(n) = (3 - 1) \times (11 - 1) = 2 \times 10 = 20$;

4) we choose $e = 3$ (first with 20) as the encryption exponent;

5) the decryption exponent is $d = 7$, the inverse of 3 modulo 20 (in fact $ed = 3 \times 7 \equiv 1 \bmod 20$).

Aziel's public key is $(n, e) = (33, 3)$, and his private key is $(n, d) = (33, 7)$. Prisca sends a message to Aziel.

- Encryption of $M = 4$ by Prisca with Aziel's *public key*: $4^3 \equiv 31 \bmod 33$, the cipher is $C = 31$ which Prisca transmits to Aziel;
- Decryption of $C = 31$ by Aziel with his *private key*: $31^7 \equiv 4 \bmod 33$, Aziel finds the original message $M = 4$.

Speed of execution does not depend on n, but rather on d. The higher the latter, the longer the calculation will take. This is due to the algorithm used, which will take longer the larger d is. The algorithm we've just explained using an example is easy to understand, but requires a great deal of attention during implementation. The numbers used are coded on 512 bits, which are better recognized as integers. Some libraries call them Biginteger. Based on a number of tests we've carried out, we've found that the robustness of this algorithm increases as the number of bits increases. Although this solution is effective, would it be necessary to weigh down an entire system while ensuring its security? We propose to use this tool for password encryption and nothing else. The only problem with the RSA algorithm is its vulnerability to integer factorization if the number of bits is often less than 512.

3.2. C. Hill's Algorithm

In 1929, mathematician-cryptographer Lester Hill (18911961) published an article in the American Mathematical Monthly entitled *Cryptography in an algebraic alphabet*, in which he detailed a new type of encryption algorithm. His idea was no longer to code letter by letter, but to code groups of m letters simultaneously! Of course, the larger m is, the more difficult statistical analysis becomes! Hill's cipher is an encryption method that uses square matrices. The cipher obtained by coding the letters in blocks of two is called 2-Hill's cipher, the cipher obtained by coding the letters in blocks of three is called 3-Hill's cipher, and so on [20] [21] [22] [23] [24].

3.2.1. Encryption

In the first phase, each letter of the text to be encrypted is replaced by a numerical value, that of its rank in the alphabet, *i.e.* we replace each letter by its order in the alphabet: A becomes 1, B becomes 2..., Z becomes 26. The resulting numbers are grouped by m (for example, $m = 2$). The letters P_k and P_{k+1} in the plain text will be enciphered C_k and C_{k+1} using the formula below:

$$\begin{pmatrix} C_k \\ C_{k+1} \end{pmatrix} = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \cdot \begin{pmatrix} P_k \\ P_{k+1} \end{pmatrix} (\mathrm{mod}\, 26)$$

This means, for the sake of clarity, that the first two letters of the clear message (P_1 and P_2) will be encrypted (C_1 and C_2) according to the following two equations:

$$C_1 = aP_1 + bP_2 (\mathrm{mod}\, 26)$$

$$C_2 = cP_1 + dP_2 (\mathrm{mod}\, 26).$$

a, b, c, d are integers, C_1 and C_2 will also be integers. The choice of key here corresponds to the choice of a number m, and the choice of linear combinations to be performed (these are always the same from block to block).

Examples of encryption

All using the character table where A is equivalent to 1 and Z to 0:

1) We want to code the message "I love you" in taking as encryption key the matrix $P_1 = \begin{pmatrix} 9 & 4 \\ 5 & 7 \end{pmatrix}$. After replacing the letters by their rank in the alphabet (a = 1, b = 2, etc.), we obtain:

$$C_1 = 9.10 + 4.5 (\mathrm{mod}\, 26) = 110 (\mathrm{mod}\, 26) = 6$$

$$C_2 = 5.10 + 7.5 (\mathrm{mod}\, 26) = 85 (\mathrm{mod}\, 26) = 7.$$

She'll do the same with the 3rd and 4th letters, 5th and 6th, and so on. In the end, she gets (Table 1):

2) Let the matrix $P_2 = \begin{pmatrix} 3 & 2 \\ 1 & 3 \end{pmatrix}$. If we want to encrypt the message "Rendezvous tonight", we obtain the cryptogram: "UDZBI WLOSR VSSAY STAIE AM".

3.2.2. Decryption

To decrypt, the principle is the same as for encryption: we take the letters in pairs, then multiply them by a matrix.

$$\begin{pmatrix} P_1 \\ P_2 \end{pmatrix} = \begin{pmatrix} a & b \\ c & d \end{pmatrix}^{-1} (\mathrm{mod}\, 26).$$

This matrix must be the inverse of the encryption matrix (modulo 26). Ordinary.

The inverse of the matrix $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$ is: $\begin{pmatrix} a & b \\ c & d \end{pmatrix}^{-1} = \frac{1}{ad - bc} \begin{pmatrix} d & -b \\ -c & a \end{pmatrix}$.

But what does this mean in the Z26 context? Let's go back to our example.

Decryption example

Table 1. Plain text encrypted with C.HILL.

Letters	j	e	v	o	u	s	a	i	m	e
Ranks (P_k)	10	5	22	15	21	19	1	9	13	5
Encrypted ranks (C_k)	6	7	24	7	5	4	19	16	7	22
Numerical letters	F	G	X	G	E	D	S	P	G	V

To decrypt the message sent by key P_1, we must calculate:

$$\begin{pmatrix} 9 & 4 \\ 5 & 7 \end{pmatrix}^{-1} = \frac{1}{43}\begin{pmatrix} 7 & -4 \\ -5 & 9 \end{pmatrix} (\text{mod } 26) = 43^{-1}\begin{pmatrix} 7 & -4 \\ -5 & 9 \end{pmatrix} (\text{mod } 26)$$

As pgdc(43,26) = 1, (43) -1 exists in Z26 and (43) -1 equals 23. The receiver now has the decryption matrix:

$$\begin{pmatrix} 9 & 4 \\ 5 & 7 \end{pmatrix}^{-1} = 23\begin{pmatrix} 7 & -4 \\ -5 & 9 \end{pmatrix} (\text{mod } 26) = \begin{pmatrix} 161 & -92 \\ -115 & 207 \end{pmatrix} (\text{mod } 26) = \begin{pmatrix} 5 & 12 \\ 15 & 25 \end{pmatrix} (\text{mod } 26)$$

so he takes the matrix $\begin{pmatrix} 5 & 12 \\ 15 & 25 \end{pmatrix}$ to decipher the message "FGXGE DSPGV" after replacing the letters by their rank in the alphabet ($A = 1$, $B = 2$, etc.), he will obtain:

$$P_1 = 5.6 + 12.7 (\text{mod } 26) = 114 (\text{mod } 26) = 10$$

$$P_2 = 15.6 + 25.7 (\text{mod } 26) = 265 (\text{mod } 26) = 5.$$

He'll do the same with the 3rd and 4th letters, 5th and 6th, and so on. In the end, he gets (Table 2):

4. The Strengths and Weaknesses of Each Algorithm

Security algorithms are designed to prevent potential attacks. They are implemented in computer systems to guard against malicious control. Although these systems are equipped with sophisticated algorithms, they are not immune to everyday threats. Algorithms that guarantee the best security (with a really low probability of unbreakability) compared to others are often referred to as strong. Below we have attempted to detail the strengths and weaknesses of the algorithms we have studied. We have found that the only weakness common to all asymmetric encryption algorithms is related to the time it takes to execute or process the information: as security becomes increasingly high, the execution

Table 2. Decrypting ciphertext in clear text.

Numerical letters	F	G	X	G	E	D	S	P	G	V
Ranks encrypted (C_k)	6	7	24	7	5	4	19	16	7	22
Ranks (P_k)	10	5	22	15	21	19	1	9	13	5
Letters	j	e	v	o	u	s	a	i	m	e

Étiquettes de lignes	Somme de RSA	Somme de C.HILL
64	0.006	0
128	0.006	0
256	0.01	0
512	0.119	0
1024	0.119	0
2048	0.2	0
Total général	0.46	0

Figure 1. Execution time of C.HILL and RSA algorithms.

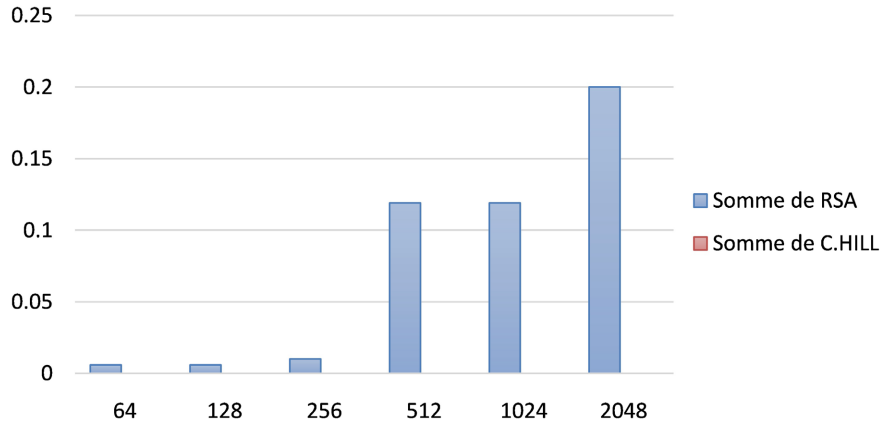


Figure 2. Graph of execution times for C.HILL and RSA algorithms.

time also becomes enormous. And this in turn leads to wasted time if we don't think about how to optimize the system in the most rational way possible. Hill's symmetrical encryption algorithms, on the other hand, are vulnerable to attack, as the key often used is not trusted and does not guarantee better data protection. No system can guarantee total data security; they are all vulnerable to network barbarism. Even if computer systems don't have a perfect guarantee of data security, we can't reassure you that algorithms using asymmetric encryption, such as RSA in our case study, represent fewer risks than those using symmetric encryption. However, we carried out encryption tests using 15-byte text, an HP i5 computer (speed 4GHZ) with 8GB RAM, and obtained the following result in terms of execution time (expressed in seconds): (**Figure 1**, **Figure 2**).

After various tests, Hill's encryption is suitable for all data on an information system except images, but its vulnerability does not guarantee acceptable comfort. The two figures below show that even if the length of the key and that of the text to be encrypted increase, the execution time remains almost the same, a fact that does not apply to RSA encryption. Execution time is a function of key length and text length.

5. Conclusions

The use of IT systems has become indispensable in all organizations, and none can claim to be exempt from this requirement. Communication with the outside world is just as vital. To sell their products, companies need customers and exchanges with the outside world.

The advent of the Internet has made available to the general public all the information available on corporate IT systems, and this has led to the covetousness of dangerous people called malicious or hackers who want to jeopardize the lives of organizations at any time. The question is whether to distance oneself from the Internet and lose communication with the outside world (customers, etc.), or to take the risk and allow the company to move forward. The second alternative is conceivable, while looking for protection mechanisms. This stage consists of choosing algorithms dedicated to protecting information according to the com-

plexity of the data to be processed. That's why, throughout our study, we've given details of the two types of encryption, so that researchers can choose the one that's right for them, based on the relevance of the data to be stored. This is the subject of this work.

Conflicts of Interest

The authors declare no conflicts of interest regarding the publication of this paper.

References

[1] National Bureau of Standards, U.S. Department of Commerce (2001) Advanced Encryption Standard (AES), Federal Information Processing Standard (FIPS), Publication 197. Washington DC. https://csrc.nist.rip/publications/detail/fips/197/final

[2] Medien, Z., Mohsen, M., Lazhar, K., Adel, B. and Rached, T. (2007) A Modified AES Based Algorithm for Image Encryption. *International Journal of Computer, Electrical, Automation, Control and Information Engineering*, **1**, 745-750.

[3] Deamen, J. and Rijimen, V. (2002) The Design of Rijindal: AES-Advanced Encyption Standard (Information Security and Cryptography). Springer-Verlag, Berlin.

[4] Han, F.L., Hu, J.K., Yu, X.H. and Wang, Y. (2007) Fingerprint Images Encryption *via* Multi-Scrollchaotic Attractors. *Applied Mathematics and Computation*, **185**, 931-939. https://doi.org/10.1016/j.amc.2006.07.030

[5] Wang, Y., Wong, K.W., Liao, X.F. and Chen, G.R. (2011) A New Chaos-Based Fast Image Encryption Algorithm. *Applied Soft Computing*, **11**, 514-522. https://doi.org/10.1016/j.asoc.2009.12.011

[6] Pareek, N.K., Patidar, V. and Sud, K.K. (2006) Image Encryption Using Chaotic Logistic Map. *Image and Vision Computing*, **24**, 926-934. https://doi.org/10.1016/j.imavis.2006.02.021

[7] Yong, Z. (2011) Image Encryption with Logistic Map and Cheat Image. 2011 3*rd International Conference on Computer Research and Development*, Shanghai, 11-13 March 2011, 97-101.

[8] Liu, L.L., Zhang, Q. and Wei, X.P. (2012) A RGB Image Encryption Algorithm Based on DNA Encoding and Chaos Map. *Computers and Electrical Engineering*, **38**, 1240-1248. https://doi.org/10.1016/j.compeleceng.2012.02.007

[9] Ariffin, M. and Noorani, M. (2008) Modified Baptista Type Chaotic Cryptosystem *via* Matrix Secret Key. *Physics Letters A*, **372**, 5427-5430. https://doi.org/10.1016/j.physleta.2008.06.077

[10] Lenstra, A.K. and Lenstra Jr., H.W. (1993) The Development of the Number Field Sieve. Springer, Berlin. https://doi.org/10.1007/BFb0091534

[11] Lenstra, A.K., Lenstra Jr., H.W. and Lov'asz, L. (1982) Factoring Polynomials with Rational Coefficients. *Mathematische Annale*, **261**, 513-534. https://doi.org/10.1007/BF01457454

[12] Krikor, L., Baba, S., Arif, T. and Shaaban, Z. (2009) Image Encryption Using DCT and Stream Cipher. *European Journal of Scientific Research*, **32**, 48-58.

[13] Gutmann, P. (2011) Engineering Security. University of Auckland, Auckland.

[14] ISO 27001 Information Security Management Systems. https://www.intertek.com/assurance/iso-27001/?gad_source=1&gclid=EAIaIQobCh

MInIjsjp78hQMV3kFBAh2a0QjYEAAYAiAAEgK3gPD_BwE

[15] ISO/IEC (2005) Information Security Management Systems—Requirements. 27001. https://info.compliancepoint.com/iso-27001-certification?utm_term=iso%27001%20certification&utm_campaign=ISO+27001&utm_source=adwords&utm_medium=ppc&hsa_acc=8022846127&hsa_cam=14298165258&hsa_grp=128815088111&hsa_ad=589060653560&hsa_src=g&hsa_tgt=kwd-3912594368&hsa_kw=iso%2027001%20certification&hsa_mt=p&hsa_net=adwords&hsa_ver=3&gad_source=1&gclid=EAIaIQobChMI-5rK3p78hQMVyz8GAB3-Gw7iEAAYAiAAEgLKFPD_BwE

[16] ISO/IEC (2005) Information Technology. Code of Practice for Information Security Management. 17799. https://webstore.ansi.org/standards/iso/isoiec177992005?gad_source=1&gclid=EAIaIQobChMIrpbJxp_8hQMVlz4GAB1iAAUjEAAYAyAAEgIsDvD_BwE

[17] Llorens, C., Levier, L. and Valois, D. (2006) Tableaux de bordaux de la sécurité réseau. Eyrolles, Paris.

[18] Longeon, R. and Archimbaud, J.L. (1999) Guide de la sécurité des systèmes Information—For Managers. Center National de la Recherche Scientifique (CNRS), Paris.

[19] Lucas, M.W. (2006) PGP & GPG—Assurer la confidentialité de ses e-mails et de ses fichiers. Eyrolles, Paris.

[20] Mattatia, F. (2013) Personal Data Processing: The Legal Guide. Eyrolles, Paris.

[21] Eastaway, R. and Wyndham, J. (2001) Why Do Buses Always Come in Threes? Flammarion, Paris, 95-107.

[22] Hill, L.S. (1929) Cryptography in an Algebraic Alphabet. *American Mathematical Monthly*, **36**, 306-312. https://doi.org/10.1080/00029890.1929.11986963

[23] Edward, L.R. (2000) Cryptological Mathematics. The Mathematical Association of America, Washington DC, 124-140. https://doi.org/10.1090/clrm/016

[24] Douglas, S. (2001) Cryptographie, Théorie et pratique. Vuibert, Paris, 12-16.