The Review of Contemporary Scientific and Academic Studies
An International Multidisciplinary Online Journal
www.thercsas.com
ISSN: 2583-1380 Vol. 4 | Issue No. 7 | July 2024 Impact Factor: 6.53

Electronic Signature as a Tool to Improve Government Transactions

Turturean Emanuela (turturean_emanuela@yahoo.com), Ph. D. Student, Faculty of Philosophy and Socio-Political Sciences, Political Sciences and International Relations Department, Alexandru Ioan Cuza University of Iasi, Romania

 Crossref/DOI: https://doi.org/10.55454/rcsas.4.07.2024.004

Abstract: *Electronic signature is used in government and economy transactions, becoming a significant component of digital public administration. This article aims to analyze the role of electronic signature in improving government transactions. Focus is on presenting the main security and integrity issues in the case of electronic signature. We will see how electronic signature is created and verified. The methodology used is a qualitative one and is based on the literature review on the importance of the electronic signature in government transactions, on European and Romanian legislation and also on international reports on the use of electronic signatures in public administration. No application or service can be completely secure, but we can say that the electronic signature service is an effective means of preventing data theft. An argument in support of this idea is that the electronic signature cannot be forged; a digitally signed message or document cannot be altered without invalidating the signature or document. This fact ensures the integrity of the documents transmitted between the institutions of government administrations.*

Keywords: Cryptography, Decryption, Electronic Signature, Encryption, Government Transactions

Article History: **Received: 20 July- 2024;** **Accepted: 26 July- 2024;** **Published/Available Online: 30 July- 2024**

1. Introduction

The use of electronic signature has become popular on the Internet, e-government, telecommunications systems, and computer networks (Bui, Nguyen, Luu and Dao, 2022: 23) especially after many countries adopted electronic signature laws, giving electronic signatures the same legal validity as handwritten signatures (holographic signatures). Electronic signature is used in government and economy transactions (Zubov, 2020: 624) becoming a significant component of digital public administration.

The rapid evolution of new information technologies in an increasingly digitized world has also caused electronic signature technologies to change and develop new ways for institutions to communicate, transmit, and archive documents. (Indu, N., Seetharaman, A, Veena, J and Arindam, B., 2016: 216). By using the electronic signature service, risks of e-government systems being attacked by hackers may be minimized during e-government transactions (Barman, Saha, 2013: 10), moreover, two of the most important principles of e-government are trust and security, so even if the digital document is attacked by intruder then also he cannot use it (Narayan, Shadab, Gaikwad, Sayyed and Bhawale, 2020:4327).

Therefore, by adopting electronic signature in the interactions between citizens and the government, the integrity and security of the data and the fact that the documents have not been altered, are ensured.

2. Literature Review

The main concern of the legislation in the field of digital signature was electronic documents, sometimes also called electronic records, but also signatures that are created, communicated and stored in electronic form. This type of signature is known to the general public as electronic signature or digital signature. Since 1997, the countries of the European Union have been concerned with the presentation of a framework project, which would help the states in harmonizing the legislation in the field of electronic signature, so that on December 14, 1999, Directive 1999/93 was published. The Directive defines the electronic signature as representing data in electronic format that is attached to, or is linked with other electronic data which serve as a method of authentication (Directive 1999/93/EC: 2 article, paragraph 1). This definition is a broad one, it includes both the stage of transposition of data in electronic form and the stage of authentication. Directive 1999/93/EC has been replaced by eIDAS from July 23, 2014. In Romania, the digital signature began to be used with the adoption of Law 455/2001 which establishes the legal regime of the digital signature and documents in electronic form.

Also, in a broad sense we can define the electronic signature as a technological term that refers to all the methods by which an electronic record can be signed (Amza and Amza, 2008:19). We can appreciate this definition is incomplete and does not capture all aspects of the digital signature process such as

The Review of Contemporary Scientific and Academic Studies
An International Multidisciplinary Online Journal
www.thercsas.com
ISSN: 2583-1380 Vol. 4 | Issue No. 7 | July 2024 Impact Factor: 6.53

authentication or integrity of data. From the perspective of authentication, originality and integrity of data, digital signature is a result of a cryptographic transformation (encoding) of data, than when properly implemented, provides an authentication mechanism for verifying the originality, integrity of data and signature recognition (Liţan, 2013:85). This definition brings to our attention an extremely important element in the electronic signature process, namely data encryption, involves data protection and the use of 'electronic keys'.

Therefore, the electronic signature provides a high degree of data security, the recipient of the electronically signed message can verify both the fact that the original message belongs to the person whose signature was attached and the fact that the message has not been altered, intentionally or accidentally, from the moment to which was signed (Ţacu, 2012: 55). From this definition it follows that the electronic signature corresponds to a single person and the integrity of the signed data is ensured. The transfer of the signature to other persons is impossible. Three of the most important features of the electronic signature are that: electronic signature ensure identification and creates a connection between the person who signed the document and the document itself; and detects any changes made to the electronic signed document (Lax, Buccafurri, Serena Nicolazzo, Nocera, Fotia, 2015: 440). These features apply in the context where users have already agreed to the protocol of an electronic signature.

From technical point of view, in both cases of creating and verifying the electronic signature, the same procedure is used, but with different keys (Egerszegi, Erdosi, 2003: 69). We will see in the next section that the electronic signature involves two keys: the public key and the private key.

We could not complete the process of defining the concept of electronic signature without distinguishing between simple electronic signature, advanced electronic signature and qualified electronic signature. **Simple electronic signature** it is the most widely used and involves a minimum requirement for identity assurance. Simple electronic signature does not fulfill any of the following elements such as: authenticity, authentication, integrity, and does not involve the use of a certificate or e-token.

According to eIDAS an electronic signature can be defined as an **advanced electronic signature** if it meets the following condition: it is exclusively connected by the signer; identify the signatory; it is created using digital signature creation; and it is connected to the data signed in such a way that every intervention on the signed data can be identified (eIDAS, 2014). We can conclude that advanced electronic signature ensures authenticity, integrity, identity and involves authentication.

If advanced electronic signature is created with a device or e-token based on a qualified certificate, then the signature is a **qualified electronic signature**. Also, qualified electronic signature enjoys the highest level of validity in the member states of the European Union by being given the same legal recognition as a holographic signature (Deloitte, 2017). A more specific definition of qualified electronic signature is given from the perspective of a system that provides two guarantees: ensuring that a document`s signatory can be identified, and the most important guarantee, the fact that once the electronic signature has been applied to the document, any change or intervention on the document can be detected (Martoni and Palmirani, 2013:311).

3. Electronic Signature Process

Electronic signature process consists of three steps: mathematical algorithms, encryption and certification (Ksketri & Dholakia, 2001: 1668). Electronic signature use a mathematical algorithms which enables the receiver know the person who created the message and it is untampered while on transit. (Ahmed, 2022: 66).

The two major categories of algorithms that are the basis of an electronic signature are algorithms that are responsible for the electronic signature generation process and algorithms that are responsible for the process of verifying the authenticity of the signature.

From the point of view of some authors, there are at least three categories of algorithms that are the basis of an electronic signature, namely: symmetric or asymmetric algorithms which are key generation algorithms; signing algorithms and verification algorithms (Alrehily, Alotaibi, Almutairy, Alqhtani and Kar, 2015:60).

The process of generating an electronic signature involves two keys, the private key and the public key. The private key, as the name suggests, is secret and can only be used by the owner of the signature, while the public key can be used by anyone to verify whether the owner of the private key was the person who signed

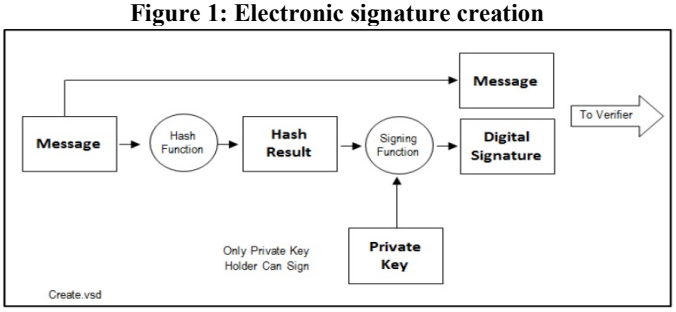
The Review of Contemporary Scientific and Academic Studies
An International Multidisciplinary Online Journal
www.thercsas.com
ISSN: 2583-1380 Vol. 4 | Issue No. 7 | July 2024 Impact Factor: 6.53

the document or not. (Bartok, Erdosi, 2017: 455). So, the private key is used in the signature generation process and the public key is used in the signature verification process.

The signatory of the document can be both a natural person, provided that person possesses an electronic signature creation device, and a digital certificate obtained by law from an authorized provider. Digital certificate is used to verify the public key belongs to the individual (Patel, Patel, Suthar, 2019: 39) and involves also the metadata attached to the digital certificate.

To avoid any fraud attempt, as seen in figure 1 and 2, both keys are actually a string of bits, created by algorithms that generate such pairs.

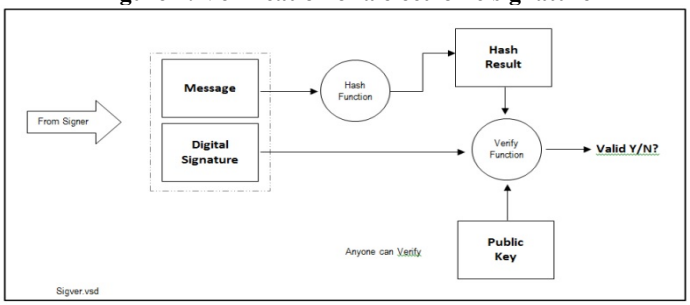
Figure 1: Electronic signature creation



Source Heyink (2014)

As we can see, a hash-code function is applied to the document, obtaining the fingerprint of the document. Through an algorithm, the private key is applied over the fingerprint of the document, resulting in the electronic signature. This operation is applied to a file opened and saved in Open Office and consists in creating a file with the same name and extension as the original file. In this way, a file is obtained that can only be decrypted by the persons possessing the certificates from the list of recipients of the document. It is important to note that when encrypted the data, the hash code is different every time, even if it is used the same password. (Shaker & Jumaa, 2017: 91).

Figure 2: Verification of a electronic signature



Source Heyink (2014)

After signing the document, it will be sent to the recipient, who can check if the document has really been signed and verify that the data message is the same as the sent data message (Pathak, Sharma and Sharma, 2020: 132). Data message are not being signed directly, they are first hashed then signed (Ali, 2020:33) and the person who receives the data message then applies his public key and verify the validity of data (Prakash, Purohit, 2013: 28).

The verification of the electronic signature is an important process which ensure data integrity (Kavin & Ganapathy, 2021: 180). Data integrity, in the case of electronic signature refers to the fact that the data inside the signed document has not been tampered with during their transmission. If the document has been tampered with, then the signature becomes invalid.

In summary, the verification of the electronic signature is done by using the public key. The private key is known only to the signatory, the public key can be found out by all users in the network under the conditions of accessing the website of the provider of electronic signature certification services.

No application or service can be completely secure, but we can say that the electronic signature service is an effective means of preventing data theft. An argument in support of this idea is that the electronic signature

The Review of Contemporary Scientific and Academic Studies
An International Multidisciplinary Online Journal
www.thercsas.com
ISSN: 2583-1380 Vol. 4 | Issue No. 7 | July 2024 Impact Factor: 6.53

cannot be forged, a digitally signed message or document cannot be altered without invalidating the signature or document (Pooja & Yadav, 2018: 72).

4. Data Encryption and Decryption

Encryption involves encoding data in order to protect it and keep it secret. Encryption it is a method of securing information and can only be accessed by the person with the valid decryption key (Mangal, Arora, Goyal, 2021: 1). Encryption is the fundamental structure square of data security (Pronika, 2021: 1031), and it is used for keeping data and documents confidential and private. In a digital era, a lot of confidential data is transmitted electronically, so that such data does not reach those who are looking for it, we must refer to cryptography.

Cryptography has the role of solving two big problems of data security namely privacy and authentication (Whitfield, Hellman, 1976: 645). The flow of information in a conventional cryptographic system used for the privacy of communications has several components: a sender, a receiver and a hacker. The sender generates a plaintext or unencrypted message to be communicated over an insecure channel to the legitimate receiver, to prevent the hacker from discovering the message, the sender operates on the message with an irreversible transformation to encrypt the text. The key is transmitted only to the legitimate recipient through a secure channel. The problem of authentication is one of the most important obstacles to the universal adoption of electronic signature in government transactions.

More precisely, according to the instructions of the electronic signature providers, the encryption of a file is done with the recipient`s public key, and if the certificate expires or the recipient loses/damages the private key the encrypted file can no longer be recovered, (DigiSign, 2020: 12) the file is accessible by the recipient and the sender as long as the cryptographic key pair exists. Encryption is insufficient, because it provides no proof of the identity of the sender of the encrypted information (Al-Khouri, 2012: 17) that`s way electronic signature was created to ensure the integrity and security of the information.

Decoding the data is called decryption. From a technical point of view, decryption involves opening the received file, and type the password. After entering the password, the data is converted and decoded into word and images. Decryption is the process of transforming data message sent in the form of a secret code, back into a form that can be understood. Sarkar & Noel (2020: 734) conclude that the strength of an encryption system depend on the strength of its algorithm and on the length of the keys used for encryption and decryption.

5. Electronic Signature as a Tool to Improve Electronic Government

In the electronic government age, each government sector moves away from paper documents with ink signatures or authenticity stamps, to electronic signatures (Barik, Karforma, 2012: 10). In most parts of the world, public authorities and institutions determine the type of electronic signature applicable (advanced or certified) for use by natural or legal persons.

Successful implementation of quality e-government services involves specific legislation, regulations and also a better understanding of the requirements of the citizen as they will be the ultimate end-users (Roy and Karforma, 2014: 652). The failure of quality implementation of e-government services leads to the decrease of citizens trust in the government and the stagnation of the development of the information society. For example, electronic signature, which is a service used in e-government transactions is increasing, starting from document management in official correspondence until used in the government`s licensing documents (Budiarti, Putra and Nurmandi, 2020: 632).

Electronic signature is an essential component of an e-gov infrastructure (Fonseca, Castro, Gonzalez, Chavarria, Raventos, 2016: 225) and is the method which is used to validate and authorize the content and users who are going to involve in the e-governance system (Pancholi, Patel, Hiran, 2018: 7).

Electronic signature contributes to the improvement of electronic government services by ensuring a high degree of security and data confidentiality. Akotam, Kontoh and Ansah argue that government can reduce data theft by employing the right mix of authentication, encryption and digital signatures; governments can significantly reduce risk of forgery, theft or abuse of identification credentials. One of the most common problems regarding data security in e-government is to grant access to authorized users as well as the need to

verify that users are real who they claim to be (Alijeaid, Ma, Langensiepen, 2014:1) this problem is solved by adopting and implementing electronic signature in e-government systems.

5. Conclusion

We have attempted to discuss the role of electronic signature in government transactions. We conclude that the problem of authentication is one of the most important obstacles to the universal adoption of electronic signature in government transactions.

We saw that the process of electronically sig a document consists of two steps, the signature creation process and the signature verification process. The process of generating an electronic signature involves two keys, the private key and the public key. The private key, as the name suggests, is secret and can only be used by the owner of the signature, while the public key can be used by anyone to verify whether the owner of the private key was the person who signed the document or not.

Electronic signature contributes to the improvement of electronic government services by ensuring a high degree of security and data confidentiality

References

***Deloitte Report (2017) on Electronic Signature Platforms. Key Contractual issues, 2017: 29. https://www2.deloitte.com/content/dam/Deloitte/ch/Documents/technology/deloitte-ch-PLC-ELECTRONIC%20SIGNATURE%20PLATFORMS.pdf.

***DigiSign (2020), Instructions for using the program DigiSigner, 2020: 1-15. https://digisign.ro/uploads/Instructiuni-utilizare-DigiSigner.pdf.

***DIRECTIVE 1999/93/EC OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL from December 13, 1999 *on a Community framework for electronic signatures,* 2 article, paragraph 1. https://eur-lex.europa.eu/eli/dir/1999/93/oj.

***Regulation (EU) No 910/2014 of the European Parliament and of the Council *on electronic identification and trust services for electronic transactions in the internal market*. https://eur-lex.europa.eu/eli/reg/2014/910/oj.

Ahmed, M., M., (2022), Digital Signature with RSA Public Key Cryptography for Data Integrity in SOSE- Based E-Government Systems, *International Journal of Management, Technology, and Social Sciences (IJMTS)*, 7(1), 2022: 59-70. https://srinivaspublication.com/journal/index.php/ijmts/article/view/1146/579.

Akotam, A., W., Kontoh, M., S., and Ansah, A., K., (2013), E-governance public key infrastructure (PKI) model, *Int. J. Electronic Governance*, 6 (2), 2013: 133-142. https://www.researchgate.net/publication/264821916_E-governance_public_key_infrastructure_PKI_model.

Ali, A., Md., (2020) Digital Signature- The Security Tool, *International Journal for Research in Applied Science & Engineering Technology* (IJRASET), 8, (6), 2020: 32-37. https://www.ijraset.com/fileserve.php?FID=29163.

Alijaid, D., Ma, X., Langensiepen, C., (2014), Biometric Identity-Based Cryptography for e-Government Environment, *Science and Information Conference*, 2014: 581-588. https://www.researchgate.net/publication/286297661_Biometric_identity-based_cryptography_for_e-Government_environment.

Alrehily, A., D., Alotaibi, A., F., Almutairy, S., B., and Alqhtani, M., S., Kar, J., (2015), Conventional and Improved Digital Signature Scheme: A Comparative Study, *Journal of Information Security*, (6), 1, 2015: 59-67. https://www.scirp.org/pdf/JIS_2015012216263196.pdf.

Al-Khouri, A., M., (2012), The role of digital certificates in contemporary goverment systems: The case of UAE Identity Authority, *International Journal of Computer Science Engineering and Information Technology Research (IJCSEITR)*, 2 (1), 2012: 17-25. https://www.academia.edu/7340016/THE_ROLE_OF_DIGITAL_CERTIFICATES_IN_CONTEMPORARY_GOVERNMENT_SYSTEMS_THE_CASE_OF_UAE_IDENTITY_AUTHORITY.

Amza, T., Amza C. P., (2008). *Electronic signature*. București: Lumina Lex Publishing.

Barik, N., Karforma, S., (2012) A study on Efficient Digital Signature Scheme for E-Governance Security, *Global Journal of Computer Science and Technology*, 12, (3), 2012: 6-11. https://globaljournals.org/item/197-a-study-on-efficient-digital-signature-scheme-for-e-governance-security.

Barman, P., Saha, B., (2013), E-Governance Security using Public Key Cryptography With special focus on ECC, *International Journal of Engineering Science Invention*, (2), 8, 2013: 10-16. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4771424.

Bartok, S., Erdosi, P. M, (2017) May the advanced biometric electronic signature be applicable in public administration?, *Conference paper Central and Eastern European e-Dem and e-Gov Days 2017*, Digital Divide in the Danube Region: Is it still significant in explaining ICT adoptions in e-Democracy and e-Government?, 2017: 455-461. https://ejournals.facultas.at/index.php/ocgcp/article/view/1577.

Budiarti, N., Putra Y., P., Nurmandi A., (2020), Digital Signature Implementation as a New Smart Governance Model, *Society, 8 (2)*, 2020: 628-639. https://www.researchgate.net/publication/348556987_Digital_Signature_Implementation_as_a_New_Smart_Governance_Model/link/60574b06299bf1736759d958/download?_tp=eyJjb250ZXh0Ijp7ImZpcnN0UGFnZSI6InB1YmxpY2F0aW9uIiwicGFnZSI6InB1YmxpY2F0aW9uIn19.

Bui, T., T., Nguyen, D., T., Luu, H., D., Dao, K., H., (2022), A new method for constructing digital signature scheme based on new hard problem, *Journal of Science and Technique,* 11, (2), 2022: 23-33. https://jst.lqdtu.edu.vn/index.php/ict/article/view/535/378.

Egerszegi, K., Erdosi, P., (2003) Problems in the implementation of the electronic signature, *Periodica Polytechnica Ser. Soc. Man. Sci.* 1, (11), 2003: 67-82. https://pp.bme.hu/so/article/view/1681/999.

Fonseca, R., V., Castro, M., A., Gonzalez, R., B., Chavarria, M., C., and Raventos, G., M., (2016), Promoting Quality e-Government Solutions by Applying a Comprehensive Information Assurance Model: Use of Cases for Digital Signature, 6th *IFIP World Information Technology Forum (WITFOR)*, 2016: 223-234. https://link.springer.com/chapter/10.1007/978-3-319-44447-5_21.

Heyink, M., (2014) Electronic Signatures for South African Law Firms, *Low Society of South Africa*, 2014: 21.

Indu, N., Seetharaman, A, Veena, J and Arindam, B., (2016), The Impact of Electronic Signatures on Internet Control Systems, *International Journal of Academic Research*, 4, (4), 2016: 216-238. https://www.researchgate.net/publication/325018677_The_Impact_of_Electronic_Signatures_on_Internal_Control_Systems.

Kavin, B., P., and Ganapathy, S., A, (2021) New Digital Signature Algorithm for Ensuring the Data Integrity in Cloud using Elliptic Curves, *The International Arab Journal of Information Technology*, 18, (2), 2021: 180-190. https://www.iajit.org/portal/PDF/Vol%2018,%20No.%202/18839.pdf.

Kshetri, N., Dholakia, N., (2001) Impact of Cultural and Political Factors on the Adoption of Digital Signatures in Asia, *Association for Information Systems, AIS Electronic Library (AISeL), Americas Conference on Information Systems (AMCIS)*, 2001: 1666-1673. https://core.ac.uk/download/pdf/301346373.pdf.

Lax, G., Buccafurri, F., Nicolazzo, S., Nocera, A., Fotia, L., (2015), A new aproach for electronic signature, *International Conference on Information Systems Security and Privacy ICISSP*, 1, 2015: 440-447. https://air.unimi.it/retrieve/01ccb108-8d1e-4a65-a7e4-247a82651e08/57434.pdf.

Lițan, D. E., (2013), *The Information Technologies systems of the e- government type or electronic government between the present and future*, București: Matrix ROM Publishing, 2013: 85.

Mangal, S., Arora, P., Goyal, S., (2021), A study on encryption and decryption system, *2nd International Conference on IoT Based Control Networks and Intelligent Systems (ICICNIS)*, 2021: 1-3. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3883878.

Martoni, M., and Palmirani, M., (2013), Remote signatures for e-Government: The Case of Municipal Certification in Itlay, *Proceedings of the 13th European Conference on e-Government*, 2013: 310-318. https://www.researchgate.net/publication/303686224_Remote_Signatures_for_e-Government_The_Case_of_Municipal_Certification_in_Italy/link/574d6f4108aec988526b12e7/download?_tp=eyJjb250ZXh0Ijp7ImZpcnN0UGFnZSI6InB1YmxpY2F0aW9uIiwicGFnZSI6InB1YmxpY2F0aW9uIn19.

Narayan, S., Shadab, S., Gaikwad, P., Sayyed, H., Bhawale, K., (2020), Digital document signature, *International Research Journal of Engineering and Technology (IRJET)*, (7), 4, 2020: 4327- 4330. https://www.irjet.net/archives/V7/i4/IRJET-V7I4831.pdf.

Pancholi, V., R., Patel, B., P., Hiran, D., (2018) A Study on Importance of Digital Signature for E-Governance Schemes, *International Journal for Innovative Research in Science & Technology- IJIRST*, 4, (10), 2018: 7-10. https://www.ijirst.org/articles/IJIRSTV4I10012.pdf.

Pathak, A., K., Sharma, K., Sharma, K., R., (2020) To Improve Working of Digital Signature Using Public Key Cryptography, *International Research Journal of Modernization in Engineering Technology and Science*, (2), 9, 2020: 130-143. https://www.irjmets.com/uploadedfiles/paper/volume2/issue_9_september_2020/3327/1628083131.pdf.

Patel, Patel, Suthar, (2019), The Study of Digital Signature Authentication Process, *Journal of Information, Knowledge and Research in Computer Science and Applications*, 1, (2), 2019: 38-43. https://www.researchgate.net/publication/336603564_THE_STUDY_OF_DIGITAL_SIGNATURE_AUTHENTICATION_PROCESS.

Pooja, Yadav, M., Digital Signature, (2018), *International Journal of Scientific Research in Computer Science, Engineering and Information Technology IJSRCSEIT*, (3), 6, 2018: 71-75. https://ijsrcseit.com/paper/CSEIT18364.pdf.

Prakash, S., Purohit, M., (2013), An Efficient implementation of PKI architecture based Digital Signature using RSA and various hash functions (MD5 and SHA variants), IOSR *Journal of Computer Engineering (IOSR-JCE),* (15), 6, 2013: 27-33. https://www.iosrjournals.org/iosr-jce/papers/Vol15-issue6/E01562733.pdf.

Pronika, S., S., T., (2021) Performance analysis of encryption and decryption algorithm, *Journal of Electrical Engineering and Computer Science*, (23), 2, 2021: 1030-1038. https://www.researchgate.net/publication/353753142_Performance_analysis_of_encryption_and_decryption_algorithm/link/610e83590c2bfa282a2bb23a/download?_tp=eyJjb250ZXh0Ijp7ImZpcnN0UGFnZSI6InB1YmxpY2F0aW9uIiwicGFnZSI6InB1YmxpY2F0aW9uIn19.

Roy, A., and Karforma, S., (2014) A study on Implementation of security in E-Governance using Cryptography, *International Journal of Advanced Research in Computer Science and Software Engineering*, 4, (4), 2014: 652-659. https://www.researchgate.net/publication/262315385_A_study_on_implementation_of_security_in_E-Governance_using_cryptography/link/02e7e5385fb4717c55000000/download?_tp=eyJjb250ZXh0Ijp7ImZpcnN0UGFnZSI6InB1YmxpY2F0aW9uIiwicGFnZSI6InB1YmxpY2F0aW9uIn19.

Shaker, H. Shaima, Jumaa, Ghzwh, G., (2017), Digital Signature Based on Hash Functions, *International Journal of Advancement in Engineering Technology, Management and Applied Science* (IJAETMAS), (4), 1, 2017: 88-99. https://www.researchgate.net/publication/336603564_THE_STUDY_OF_DIGITAL_SIGNATURE_AUTHENTICATION_PROCESS/link/60af5698a6fdcc647edf665d/download?_tp=eyJjb250ZXh0Ijp7ImZpcnN0UGFnZSI6InB1YmxpY2F0aW9uIiwicGFnZSI6InB1YmxpY2F0aW9uIn19.

Sharkar, Punyaslok and Noel, Sherly, Cipher: Encryption & Decription, *International Research Journal of Engineering and Technology (IRJET)*, (7), 10, 2020: 731-737. https://www.researchgate.net/publication/344950501_CIPHER_ENCRYPTION_DECRYPTION/link/5f9ab708299bf1b53e4ef9c0/download?_tp=eyJjb250ZXh0Ijp7ImZpcnN0UGFnZSI6InB1YmxpY2F0aW9uIiwicGFnZSI6InB1YmxpY2F0aW9uIn19.

Țacu, C. D., (2012), *Data encryption*, Craiova: Arves Publishing, 55.

Whithield, D., Hellman, M., (1976), New Directions in Cryptography, *IEEE TRANSACTION ON INFORMATION THEORY* (22), 6, 1976: 644-654. https://ee.stanford.edu/~hellman/publications/24.pdf.

Zubov, V., V., (2020) Global Challenges and Prospects of the Modern Economic Development, *European Proceedings of Social and Behavioural Sciences*, 2020: 621-625. https://www.europeanproceedings.com/article/10.15405/epsbs.2020.03.89.