International Journal of Current Science Research and Review
ISSN: 2581-8341
Volume 06 Issue 06 June 2023
DOI: 10.47191/ijcsrr/V6-i6-12, Impact Factor: 6.789
IJCSRR @ 2023
www.ijcsrr.org

Evaluating Encryption Algorithm Method Based on Software Encryption Tools for Information Security

Dr. Khaled Musa

ABSTRACT: Information security is the combination of policies, rules and practices to prevent any unauthorized access or attacks that causes corruption to data, information, and computing services. Information security techniques and programs are built around the core objective to secure data and information by adapting encryption algorithms methods. Encryption algorithm methods impeded in the information security programs or encryption software tools enforce more security by encrypting and decrypting data and information. Encryption algorithm methods are based on algorithms that scramble data and information by converting them into unreadable text. There are various encryption methods used in various encryption software tools. The more encryption algorithm methods used within the encryption software tool, the more security provided on data and information effective data and information security. In this paper, the most used encryption algorithm methods are analyzed and evaluated based on their usage in encryption software tools to determine the most encryption algorithm method that is used ensure more security on data and information.

KEYWORDS: Cryptography, Cipher Text, Encryption algorithms, Encryption, Information security, Security algorithms.

1. INTRODUCTION

Information security is defined as a combination of policies and practices to protect data and information and all resources such as computers, networks, programs from any unauthorized access and to prevent intruder attacks that causes corruptions (Gupta & Sharma, 2018).

Information security is a set of strategies that enforce rules and regulations to prevent, detect, document from threats on data and information. Information security programs and tools are built around the core objectives to maintaining confidentiality, integrity and availability on information technology systems, business data and information (Jain & Pal, 2017).

Security on data and information is important by preventing threats on systems used by individuals, businesses, and agencies (Roozbahani & Azad, 2015). Encryption software tools are used to secure data and information using encryption methods to secure sensitive data and information (Jain & Pal, 2017).

Encryption algorithm methods impeded in the encryption software tools are one of the techniques that include controls to ensure secure computing environment through web interfaces and programs to provide security, high computing efficiency and performance on information systems (Senyoa et al., 2018).

In this paper, the used encryption algorithm methods will be analyzed and evaluated based on their implementations in the encryption software tools. The encryption algorithm methods and encryption software tools are gathered, evaluated, and analyzed to determine the most used encryption algorithm method used in the various encryption software tools to ensure more security to data and information.

The rest of this paper is organized as follows: Section 2, presents encryption algorithm. Section 3 discusses the various encryption algorithms methods. Section 4, the most used software encryption tools. Section 5, evaluating encryption algorithm methods based on software encryption tools. Section 6 concludes the paper.

2. ENCRYPTION ALGORITHM

Encryption algorithm is the process of scrambling messages by converting text, data, and information into unreadable cipher text to provide for more security (Singh & Spriya, 2013). Encryption algorithm is a method that performs various substitutions and transformations techniques on the original message to turn it into cipher text (Ramaporkalai, 2017).

Data encryption is known for protecting data and information from any tampering by transforming data of a given format called plaintext, to another format, called cipher text using encryption keys and further decrypting the text to its original state (Kumari, 2017). Cryptography is the security mechanism of the transformation process using encryption and decryption methods that comes from the Greek word “Kryptos” which means hidden (Joshi & Karkade, 2015).

Cryptography is the process of encrypting and decrypting text and messages using symmetric and asymmetric keys (Joshi & Karkade, 2015). Symmetric encryption uses one key to encrypt and decrypt text and messages. Asymmetric encryption uses two keys, private and public keys encryptions (Kumari, 2017). Symmetric and Asymmetric encryption schemas secure communication between sender and receiver by using various encryption keys (Maqsood et al., 2017) to protect data and information from tampering and malicious attacks (Joshi & Karkade, 2015).

3. ENCRYPTION ALGORITHM METHODS

Encryption algorithm method is the process of applying complex mathematical algorithms to convert meaningful data into meaningless data format, then reconverting them back to their original meaningful format (Mehta, et al., 2015).

The encryption algorithm methods effectively encrypt data and information following specific cryptographic techniques and key sizes. In this research, and based on other research, the most addressed encryption algorithm methods used within the encryption software tools are listed as follows:

- **Advanced Encryption Standard (AES):** also known by its original name Rijndael. AES is an encryption method that was established by the U.S. National Institute of Standards and Technology to protect sensitive data (Sawant et al., 2018). The AES method is symmetric key algorithm that provides strong security with less implementation complexity and most efficient algorithms among other algorithms methods (Kiran et al., 2016). To encrypt data and maintain its effective security, AES uses a variety of key sizes such as 128, 192, and 256 bits (Maqsood et al., 2107).
- **Data Encryption Standard (DES):** DES was developed by the International Business Machines Corporation (IBM) and is symmetric key algorithm that was further developed to Triple Data Encryption Standard (3DES) to maintain strong secure communication (Ratnadewi et al., 2018).

The DES and 3DES algorithms are symmetric key algorithms which are used in military, commercial, and security of communication system. DES and 3DES use different key sizes, where DES key size started as 56-bit and further developed to 168 bits in the triple DES (3DES) algorithm (Maqsood et al., 2017).

- **RC:** RC is an algorithm that was invented by Ron Rivest and may stand for either Rivest's cipher or Ron's code (El-Fishawy & Abu Zaid, 2007). RC algorithms started with RC2 and further developed several times to reach the RC6 version (El-Fishawy & Abu Zaid, 2007)

All versions of RC are considered symmetric key algorithms. From RC2 to RC6 encryption there were modifications on the way the encryptions were handled using varies of key sizes. To maintain secure communications RC2 started with 64-bit key sizes and was further developed to RC6 that supports 128, 192 and 256 bits key sizes (Mathur & Kesarwani, 2013).

- **RSA:** RSA stands for the names of its publishers Rivest, Shamir, and Adleman (Maqsood et al., 2017). RSA is an asymmetric key algorithm which uses private and public key encryptions for its communications (Kiran et al., 2016).

The encryption method, RSA, is used in transferring data over insecure channels using two keys, the public key is openly accessible to everyone, and the private key is kept secret by the authorized person (Maqsood et al., 2017). The current listed key size for RSA ranges between 512 as low-strength key and 4096 as high-strength key (IBM, 2018).

- **DSA:** Digital signature algorithm (DSA) was first published in 1991 by the National Institute of Standards and Technology (Subramanya & Byung, 2006) and further advanced by the NSA to be utilized by the United States government as a standard for virtual signatures (Sivaraman, 2017)

DSA is an asymmetric key encryption method where the encryption algorithm is designed to create an electronic private key signature and use it as public key (Lyasota, 2018).

The listed key size for DSA ranges between 512 as low-strength key and 4048 as high-strength key (IBM, 2018).

- **Serpent:** designed in 1998 by Ross Anderson, Eli Buham and Lars Knudsen. Serpent encryption algorithm is considered to have high security margin for its high number of processing cycles to perform its encryption (Nazlee et al., 2009).

The encryption method, serpent is symmetric key encryption (Ebrahim et al., 2013) that uses key size of 128-bits, 192 and 256-bits (Naeemabadi et al., 2015)

- **SHA:** Secure hash algorithm (SHA) designed by the National Security Agency (NSA) and published by National Institute of Standard and Technology (NIST) as a U.S Federal Information Processing Standard (Ibrahim et al., 2015).

The encryption method uses a hash algorithm to ensure data encryption. The hash algorithm concept is the use of mathematical function that condenses data to a fixed size (Sumagita & Riadi, 2018).

The variations of SHA algorithm are named are SHA-0, SHA-1, SHA-2, and SHA-3 with encryption key size of 512 (Sahu & Ghosh, 2017).

- **Twofish:** is an extended version of the earlier encryption method called blowfish with length of key size ranges from 32 bits to 448 bits (Mathur & Kesarwani, 2013).

The encryption method Twofish is a large and more complex symmetric key algorithm which uses one encryption key sizes 128 bits, 192 bits or 256 bits (Ma, C., Chandy, J., & Shi, Z. (2017).

4. ENCRYPTION SOFTWARE TOOLS

Software encryption tools are applications that encapsulate and impede specific encryption/decryption methods to protect data and information from any hacking and tampering (Roozbahani & Azad, 2015).

Encryption software tools were introduced by various information security specialists to assist businesses and agencies in implementing the best encryption software tool that protects sensitive data and information. Various information security specialists had tested various encryption software tools where they recommended several encryption tools for businesses and agencies to maintain data and information security. Each security specialist provided a list of recommended encryption software tools.

In data and information security protection, security specialist Johnston addressed the top 10 encryption software. Another security specialist, Rubenking, discussed the best encryption software for 2019. Shaleynikov addressed the top 6 encryption tools. Fearn addressed the best encryption software tools of 2018. Rijnetu discussed the encryption software tools to protect data. Security specialist Manes addressed the top 24 data encryption tools.

The major encryption software tools that effectively apply encryption algorithm methods as security mechanism to maintain information security and used by various organizations and businesses and listed as follows:

- **The Linux Unified Key Setup:** Linux Unified Key Setup (LUKS) is a disk encryption specification tool created by Clemens Fruhwirth in 2004 that was originally intended for GNU/Linux to encrypt data in Linux computers (Menéndez, 2014).
- **OpenSSL:** the encryption tool that is considered a library written programming language that provides cryptographic implementation in the secure socket layer (SSL) protocol through command line interface using private key certificate authentication (Sorenson, 2001).
- **PuTTY:** the encryption tool was originally written for Microsoft Windows, but later imported into various operating systems such as Unix and Mac operating systems. The encryption tool is a program that generates public and private keys to encrypt network connection and online communications (Rackspace Support, 2016)
- **LASTPASS:** the encryption tool uses two keys, hash key and encryption key, to secure data and information (Gibson, 2019). LastPass provides consumers and businesses security on password related breaches incidents using password vaulting and single sign-on solution (Constantin, 2017).
- **GPG:** GPG stands for Guu privacy guard (GPG) and is an encryption software program originally written by Phil Zimmermann in 1991 to securely store messages (Walfield, 2017).

PGP encrypt or decrypt files and folders (Tech148865, 2012) using compression and modification techniques to generate random session keys that is used to encrypt messages into cipher text (Poddebniak, 2018)

- **Stunnel:** Stunnel is software encryption tool that uses external libraries to encapsulate data (Banakar et al., 2019). The encryption software tools are designed to work as secure socket layer to encrypt data in transit through the network transport layer between remote clients and local servers (Fisher, n.d).
- **FileVault:** FileVault is created by Apple and is a full desk encryption software tool (Cobb, 2013) that uses keys to prevent unauthorized access to the information on Mac Operating systems (Kaelin, 2018).
- **DiskCryptor:** DiskCryptor is an open-source disk encryption software application that uses a combination of encryption algorithms for stronger security (Olson, 2012). The encryption tool is known as windows system tool that uses encryp-

tion techniques to encrypt the full disk and partition with the ability to encrypt the partition and disk on which the operating systems installed in (Greenwald, 2014).

- **7-Zip:** the encryption software tool has the ability to compress files and folders with encryption option (Shaleynikov, 2018). 7-Zip is an open-source platform and well-known for its simplicity in extracting most archives with strong encryption method (Rijnetu, 2018). The 7-Zip is easily integrated to Windows Explorer browser to allow flexible compression and encryption files and folders into various formats (Manes, 2015).
- **Bitlocker:** is a Microsoft encryption tool that is available in most Windows operating systems (Rijnetu, 2018). Bitlocker is a barebones program that protects files within Windows operating systems (Johnston, 2019). The encryption tool is used to prevent data breaches, data extraction, and has a strong encryption method for encrypting hard drives (Manes, 2015).
- **Folder Lock:** is one of the fastest encryption tools that implements strong encryption method to protect files and data with the ability to hide files and clean up footprints when deleting files (Shaleynikov, 2018). The tool consists of features to decoy passwords, hacker preventions, log unauthorized login attempts, back up passwords and get notification on potential attacks (Fearn, 2018). Folder Lock has encryption method that encrypt files, lock files, shred files, and secure online backup (Rubenking, 2018)
- **OpenPuff:** is an encryption tool with strong encryption methods that securely encrypt and hide files within other files (Manes, 2015). The encryption tool has embedding schemes to protect vulnerable systems (Cervantes et al., 2018). OpenPuff is a multi-format and semi-open-source encryption tool with security and privacy implications (Sloan & Hernandez-Castro, 2018).
- **AxCrypt:** is an encryption software tool that can be integrated with Windows Explorer browser to provide strong security encryption method to stop any intruders (Fearn, 2018). AxCrypt is an open-source tool used to encrypt and protect files (Rijnetu, 2018), the asymmetric cryptography impeded into the encryption tool secures file deletion and online password storage (Rubenking, 2018).

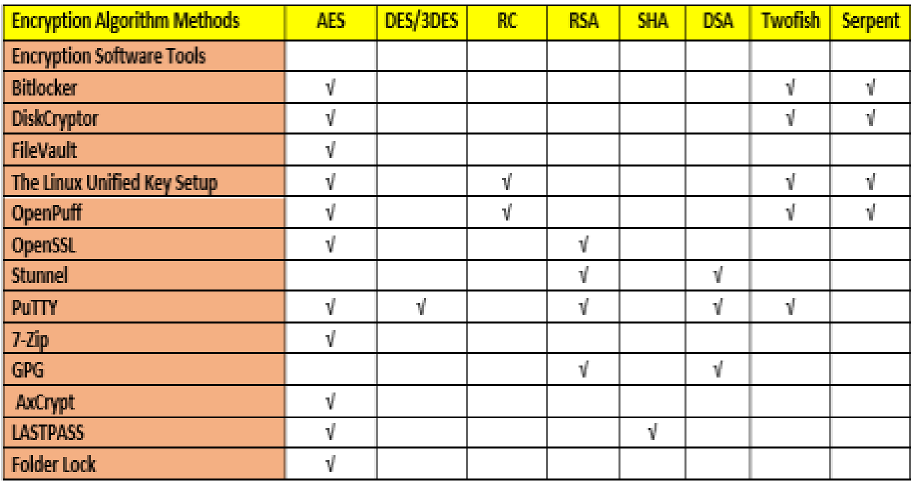
5. EVALUATING ENCRYPTION ALGORITHM METHODS BASED ON SOFTWARE ENCRYPTION TOOLS

The information on encryption algorithm methods were gathered through many searches from within the encryption software tools themselves and through many of published searches on security information systems written by information security specialist and scholars. The commonly used encryption algorithm methods addressed by professional security specialists and scholars were gathered, analyzed, and evaluated based on the basis of the encryption software tools.

Cross referencing the encryption algorithm methods (AES, DES/3DES, RC, RSA, SHA, DSA, Twofish, and Serpent) and the encryption software tools (Bitlocker, Diskcryptor, FileVault, Linux Unified Key Setup, OpenPuff, OpenSSL, Stunnel, PuTTY, 7-Zip, GPG, AxCrypt, LASTPASS, and Folder Lock) the results are presented as shown in Figure 1:

1. There are several encryption software tools that use several encryption algorithm methods to ensure more security on data and information. An encryption software tool at least has one encryption algorithm method implemented in it to ensure data and information security.
2. The encryption algorithm methods DES/3DES is used only in PuTTY encryption software tool and SHA is used in LASTPASS encryption software tool.
3. The encryption algorithm method RC is used in two encryption software tools, the Linux Unified Key Setup and OpenPuff, whereas DSA is used in three encryption software tools Stunnel, PuTTY, and GPG.
4. The encryption algorithm methods RSA and Serpent are used in four encryption software tools and Twofish is used in five encryption software tools.
5. The encryption algorithm method, AES, is used in eleven encryption software tools which are most of the encryption software tools used in applications and systems.
6. Among the several encryption algorithm methods, the most dominated and used method is The Advance Encryption Standard (AES) method uses symmetric key algorithm which provides strong and more efficient security mechanism with less implementation complexity.

International Journal of Current Science Research and Review
ISSN: 2581-8341
Volume 06 Issue 06 June 2023
DOI: 10.47191/ijcsrr/V6-i6-12, Impact Factor: 6.789
IJCSRR @ 2023
www.ijcsrr.org



Encryption Algorithm Methods	AES	DES/3DES	RC	RSA	SHA	DSA	Twofish	Serpent
Encryption Software Tools								
Bitlocker	√						√	√
DiskCryptor	√						√	√
FileVault	√							
The Linux Unified Key Setup	√		√				√	√
OpenPuff	√		√				√	√
OpenSSL	√			√				
Stunnel				√		√		
PuTTY	√	√		√		√	√	
7-Zip	√							
GPG				√		√		
AxCrypt	√							
LASTPASS	√				√			
Folder Lock	√							

Figure 1. Encryption Algorithm Methods and Encryption Software Tools

6. CONCLUSION

Information security is the combination of policies, rules and practices to prevent any unauthorized access or attacks that causes corruption to data, information, and computing services. Securing data, information, and computing services from any attacks are key principles to information security for individuals, businesses, and agencies. Encryption software tools are programs used to maintain such security in information systems.

Information security techniques and programs are built around the core objective to secure data and information by adapting encryption algorithms methods. Encryption algorithm methods impeded in the information security programs or encryption software tools enforce more security by encrypting and decrypting data and information.

The most encryption algorithm methods were gathered, analyzed, and evaluated based on the software encryption tools. Cross referencing the encryption algorithm methods (AES, DES/3DES, RC, RSA, SHA, DSA, Twofish, and Serpent) with the encryption software tools (Bitlocker, Diskcryptor, FileVault, Linux Unified Key Setup, OpenPuff, OpenSSL, Stunnel, PuTTY, 7-Zip, GPG, AxCrypt, LASTPASS, and Folder Lock) to find the most used encryption algorithm method.

The results show there are several encryption software tools that use several encryption algorithm methods to ensure more security on data and information. Each encryption software tool at least has one encryption algorithm method implemented in it to ensure data and information security.

The encryption algorithm methods DES/3DES is used only in PuTTY encryption software tool and SHA is used in LASTPASS encryption software tool.

The encryption algorithm method RC is used in two encryption software tools, the Linux Unified Key Setup and OpenPuff, whereas DSA is used in three encryption software tools Stunnel, PuTTY, and GPG.

The encryption algorithm methods RSA and Serpent are used in four encryption software tools and Twofish is used in five encryption software tools.

The encryption algorithm method, AES, is used in eleven encryption software tools which are most of the encryption soft-ware tools used in applications and systems.

Among the several encryption algorithm methods, the most dominated and used method is The Advance Encryption Standard (AES) method uses symmetric key algorithm which provides strong and more efficient security mechanism with less implementation complexity.

REFERENCES

1. Cervantes, A., Sloan, T., Hernandez-Castro, J., & Isasi, P. (2018). System steganalysis with automatic fingerprint extraction. PLOS/One, 13(7).
2. El-Fishawy, N. &Abu Zaid, O. (2007). Quality of Encryption Measurement of Bitmap Images with RC6, MRC6, and Rijndael Block Cipher Algorithms. International Journal of Network Security, 5(3), 241–251.

3. Fearn, N. (April 26, 2018). The best encryption software tools of 2018. TechradarPro, from https://www.techradar.com/news/top-5-best-encryption-tools
4. Gupta, M. & Sharma, A. (2018). A Review Article on Cyber Security, Web Security and Cyber Crime. University Research Resource Journal, 1(2), 70-74.
5. IBM. (2018). Size considerations for public and private keys, IBM Knowledge Center, from https://www.ibm.com/support/knowledgecenter/en/SSLTBW_2.3.0/com.ibm.zos.v2r3.icha700/keysizec.htm
6. Jain, J. & Pal, P. (2017). A Recent Study over Cyber Security and its Elements. International Journal of Advanced Research in Computer Science, 8(3), 791- 793.
7. Johnston, N. (Jan 8, 2019). The Best Encryption Software. ToptenReviews, from https://www.toptenreviews.com/software/security/best-encryption-software/
8. Joshi, M. & Karkade, R. (2015). Network Security with Cryptography. International Journal of Computer Science and Mobile Computing, 4(1), 201-204.
9. Kiran, J., Anusha, M., kumar, A., & Kavya, M. (2016). Cryptography: The Sciene of Secure Communication. International Journal of Computer Science and Network Security (IJCSNS), 16(4), 129-134.
10. Kumari, S. (2017). A research Paper on Cryptography Encryption and Compression Techniques. International Journal of Engineering and Computer Science, 6(4), 20915-20919.
11. Ma, C., Chandy, J., & Shi, Z. (2017). Algebraic Side-Channel Attack on Twofish. Journal of Internet Services and Information Security (JISIS), 7(2) 32-43.
12. Manes, C. (June 12, 2015). The top 24 free tools for data encryption. TechTalk from https://techtalk.gfi.com/the-top-24-free-tools-for-data-encryption/
13. Maqsood, F., Ahmad, M., Ali, M., & Shah, M. (2017). Cryptography: A Comparative Analysis for Modern Techniques. International Journal of Advanced Computer Science and Applications (IJACSA), 8 (6), 442-448.
14. Mathur, M. & Kesarwani, A. (2013). Comparison between DES, 3DES, RC2, RC6, BLOWFISH and AES. Proceedings of National Conference on New Horizons in IT (NCNHIT 2013), 143-148.
15. Mehta, P., Bansal, M., & Upadhyaya, A. (2015). Stream Cipher and Block Cipher Based Performance Analysis of Symmetric Cryptography Algorithms: AES and DES. International Journal of Modern Trends in ENgneering and Research, 2(7), 262-366.
16. Ramaporkalai, T. (2017). Security Algorithms in Cloud Computing. International Journal of Computer Science Trenda and Technology (IJCST), 5(2), 500-503
17. Ratnadewi, Adhie, R., Hutama, Y., Ahmar, A., & Setiawan, M. (2018). Implementation Cryptography Data Encryption Standard (DES) and Triple Data Encryption Standard (3DES) Method in Communication System Based Near Field Communication (NFC). IOP Conf. Series: Journal of Physics: Conf. Series 954 012009, 1-9.
18. Rijnteu, I. (March 13, 2018). 9+ Free Encryption Software Tools To Protect Your Data. Heimdal Security, from https://heimdalsecurity.com/blog/9-free-encryption-software-tools/
19. Roozbahani, F. & Azad, R. (2015). Security Solutions against Computer Networks Threats. International Journal of Advanced Networking and Applications, 7(1), 2576-2581.
20. Rubenking, N. (July 17, 2018). The Best Encryption Software for 2019. PC, from https://www.pcmag.com/article/347066/the-best-encryption-software
21. Sawant, A., Nitnaware, V., & Deshpande, A. (2018). Advanced Encryption Standard Block Cipher Algorithm. International Journal of Electronics, Electrical and Computational System (IJEECS), 7(3), 366-371.
22. Senyoa, P. K., Addaeb, E., & Boatenga, R. (2018). Cloud computing research: A review of research themes, frameworks, methods and future research directions. International Journal of Information Management, 38(1), 128–139.
23. Shaleynikov, A. (Oct 13, 2018). The Top 6 Encryption Tools. D Zone, from https://dzone.com/articles/top-6-encryption-software-tools
24. Singh, G. & Spriya. (2013). A Study of Encryption Algorithms (RSA, DES, 3DES, and AES) for information security. International Journal of Computer Applications, 67(19), 33-38
25. Sloan, T., & Hernandez-Castro, J. (2018). Dismantling OpenPuff PDF steganography. ELSEVIER ScienceDirect, 25 (2018), 90-96.

26. Lyasota, Z. (August, 2018). A Guide to Digital Signature Algorithms. Security Zone, from https://dzone.com/articles/digital-signature-1
27. Subramanya, S. & Byung, K. (2006). Digital Signatures. IEEE Potentials. 5-8
28. Sivaraman, K. (2017). A Comparision Study of RSA and DSA Algorithm in Mobile Cloud Computing. International Journal of Pure and Applied Mathematics, 116(8), 247-253.
29. Ebrahim, M., Khan, S. & Khalid, U. (2013). Symmetric Algorithm Survey: a Comparative Analysis. International Journal of Computer Applications, 61(20), 12-19.
30. Nazlee, A., Hussin, F., & Ali, N. (2009). Serpent Encryption Algorithm Implementation on Compute Unified Device Architecture (CUDA). Proceedings of 2009 Student Conference on Research and Development (SCOReD 2009), 1-4.
31. Naeemabadi, M., Ordoubadi, B., Dehnavi, A., Bahaadinbeigy, K. (2015). Comparison of Serpent, Twofish and Rijndael encryption algorithms in tele-ophthalmology system. Advances in Natural and Applied Sciences, 9(1), 137-149.
32. Sumagita, M. & Riadi, I. (2018). Analysis of Secure Hash Algorithm (SHA) 512 for Encryption Process on Web Based Application, 7(4), 373-381.
33. Ibrahim, R., Hussain, A., & Kadhim, R. (2015). Implementation of Secure Hash Algorithm Sha-1 by Labview. International Journal of Computer Science and Mobile Computing, 4(3), 61-67.
34. Sahu, A. & Ghosh, S. (2017). Review Paper on Secure Hash Algorithm with Its Variants. International Journal of Technical Innovation in Modern Engineering & Science (IJTIMES), 3(5), 1-7.
35. Menéndez, M. (2014). How to encrypt a USB storage device with ‘Linux Unified Key Setup’ (LUKS). Miguel Menéndez Pro, from https://miguelmenendez.pro/en/blog/2014/10/encrypt-usb-storage-device-linux-unified-key-setup-luks/
36. Sorenson, H. (2001). An Introduction to OpenSSL Part One. Symmantic.Connect, from https://www.symantec.com/connect/articles/introduction-openssl-part-one?page=1
37. Rackspace Support (2016). Generate RSA keys with SSH by using PuTTYgen. Rackspace, from https://support.rackspace.com/how-to/generating-rsa-keys-with-ssh-puttygen/
38. Constantin, L. (2017). LastPass is scrambling to fix another serious vulnerability. PCWorld, from https://www.pcworld.com/article/3185731/security/lastpass-is-scrambling-to-fix-another-serious-vulnerability.html
39. Gibson, S. (2019). Proven security model. LastPass, from https://www.lastpass.com/enterprise/security
40. Walfield, N. (2017). An Advanced Introduction to GnuPG. g10 Code GmbH. 1-130.
41. Poddebniak, D., Dresen, C., M¨uller, J., Ising, F., Schinzel, S., Friedberger, S., Somorovsky, J., & Schwenk, J. (2018). Efail: Breaking S/MIME and OpenPGP Email Encryption usingExfiltration Channels. SEC'18 Proceedings of the 27th USENIX Conference on Security Symposium. 549-566.
42. Tech148865. (2012). Encrypt or Decrypt Files and Folders with PGP Zip (Windows). Symantec, from https://support.symantec.com/en_US/article.TECH148865.html
43. Banakar, V., Shah, A., Shastri, S., & Chidambaram, V. (2019). nalyzing the Impact of GDPR Compliance on Storage Systems. University of Texas at Austin, 1-7.
44. Fisher, C. (n.d). STunnel security for Oracle Replace Database TLS for Simplified Best Practice Compliance, from http://syro.org/systemd/otunnel.html.
45. Kaelin, M. (2018). Protect sensitive data with these five free encryption apps. TechRepublic, from https://www.techrepublic.com/article/protect-personal-and-sensitive-data-with-these-five-free-encryption-apps/
46. Cobb, N. (2013). A Problem Solving Approach to Enterprise FileVault 2 Management and Integration. Western Kentucky University Topscholar, Masters Theses &Specialist Projects. Paper 1296.
47. Olson, R. (2012). Performance differences in encryption software versus storage devices. Linnaeus University, School of computer science, physics, and Mathematics, 1-40.
48. Greenwald, G. (2014). Why privacy matters. TED Talk, from https://www.privacytools.io/