International Journal of Communication and Information Technology

E-ISSN: 2707-6628
P-ISSN: 2707-661X
www.computersciencejournals.com/ijcit
IJCIT 2022; 3(1): 16-21
Received: 15-11-2021
Accepted: 16-12-2021

Application of cryptography in enhancing privacy of personal data in medical services

Xavier Francis Oduor and Zachary Bosire Omariba

Xavier Francis Oduor
Department of Computer Science, Egerton University, Njoro, Kenya

Zachary Bosire Omariba
Department of Computer Science, Egerton University, Njoro, Kenya

Corresponding Author:
Zachary Bosire Omariba
Department of Computer Science, Egerton University, Njoro, Kenya

DOI: https://doi.org/10.33545/2707661X.2022.v3.i1a.41

Abstract

Computer security began decades ago in an era where there was no internet or network to take into consideration. During this era, the top priority was to protect data based on physical measures. Furthermore, security largely focused on preventing individuals with enough knowledge about how to operate an electronic device. Over the years, the security of data has greatly evolved with the evolution in technology. The scope of data security has also enlarged making it a sensitive area in contemporary society. This paper analyses cryptography in securing the privacy of personal data transmission in medical services. It focuses on the evolution of these strategy, the need for cryptography, and some of the given instances that cryptography is applied in medical services. Additionally, this paper provides code-based examples of cryptography with a real-time demonstration using an Integrated Development Environment (IDE).

Keywords: Cryptography, security, encryption, decryption, algorithms, plain text, cipher text

1. Introduction

Securing personal data forms one of the core objectives of modern-day organizations. Data security is made up of four basic components that represent the main objective of computer security. These components include integrity, accountability, confidentiality, and availability [1]. The evolution of technology has brought the internet closer to the public. To promote collaboration and ensure a continuum of care, healthcare organizations record personal data in electronic health records (EHRs) and electronic medical records (EMRs). These devices build enterprise-wide data patient data to be shared with other organizations. Furthermore, technological advancements have brought the world into a "global village" [2]. This contribution makes it possible for healthcare providers to easily share data with other professionals. However, these advancements have brought challenges to healthcare organizations. For instance, data security concerns have risen as a result of technological advancements. According to Russel, the opportunities for data breaches are increasing drastically as a result of these advancements [3]. Personal data, both in transit and at rest, face a potential threat of being hacked, manipulated, or destroyed by external or internal users in healthcare organizations. This data includes patient health records and healthcare professionals' credentials.

Factors such as error and omission, unauthorized access, excess privilege, identity theft, malware, and phishing put personal data transmission in medical services at risk. Due to these challenges, several strategies have been put in place to act as countermeasures. In particular, this paper focuses on cryptographic as an efficient method used to promote data security [4]. This technique act as an important line of defense by preventing malicious entities from getting access to sensitive data in healthcare organizations.

This paper is organized into chapters. Chapter two gives the literature review which gives the theoretical background of cryptography and the aspects of cryptography that this paper will focus on in securing personal information in medical sector. Chapter three focuses on the aspects of cryptography which include encryption and decryption and how these aspects help in securing information. Chapter four addresses the need for cryptography in medical sector. It addresses the major cryptographic attacks in the medical sector and the possible solutions to these attacks. This paper concludes by highlighting some of the main points to focus on when addressing cryptography in medical services.

Cryptography involves secure communications techniques that enables only the sender and the intended recipient of a message to view its contents. Cryptography is derived from mathematical concepts and algorithms which refer to a set of rule-based calculations.

This technique is intended to transform original messages into forms that are hard to decipher [5]. Modern cryptography aims to accomplish certain objectives in protecting information and communications. These objectives include confidentiality, integrity, non-repudiation, and authentication [6]. Confidentiality ensures that information being sent cannot be understood by unintended recipient. Integrity ensures that the information cannot be altered in transit or storage between the sender and the receiver without the alteration being detected. The objective of non-repudiation ensures that the sender cannot deny their intentions in the creation or transmission of the information at a later stage [7]. Authentication ensures that the sender and the receiver can confirm each other's identity and the origin and destination of the information.

Cryptography involves the process of encrypting and decrypting data. These two schemes are crucial in securing privacy of personal data transmission in medical services. This paper focuses on these two schemes in to show how cryptography can be utilized in securing the privacy of personal data in transit or storage in medical sector.

1.1 Analysis of Data Encryption and Decryption

Data encryption and decryption are both important algorithms when it comes to protecting personal data transmission in medical services. These algorithms help to promote confidentiality when data is transmitted using the internet or other computer networks. Furthermore, they ensure key security services such as integrity, authentication, access control, and non-repudiation [8]. Data encryption and decryption began as classic cryptographic schemes. These schemes made use of pen and paper to encrypt data. As technological inventions and innovations started creeping into the world of computing, the development of electromagnetic equipment offered more complex and efficient means of encryption and decryption. The introduction of electronics further enabled intricate schemes with greater complexity. Therefore, what began as a classic scheme utilizing a pen and a paper has developed into a complex scheme that makes use of mathematical algorithms to securely encrypt and decrypt data [9]. Furthermore, the need to make systems more secure and free from vulnerabilities has also fueled these advancements.

1.1.1 Data Encryption

This technique involves the process of converting data from a readable form (plain text) to an encoded format (ciphertext). It involves converting data into a format that can only be read after it has been decrypted [8]. Encryption, therefore, forms the basic building block of information security. Encryption can be applied to various forms of digit data. For instance, it can be applied to messages, files, and documents. It can also be applied to any other form of communication over a network.

1.1.2 The General Mechanism of Encryption

Plaintext, which refers to data that needs to be encrypted has to undergo certain stages during encryption. Additionally, an encryption key is also required for successful encryption. The plain text data has to be passed through some algorithms [8]. These algorithms refer to mathematical calculations that are applied on plaintext. Using the encryption key and an appropriate encryption algorithm, the plain text is converted into an encrypted format referred to as cipher text.

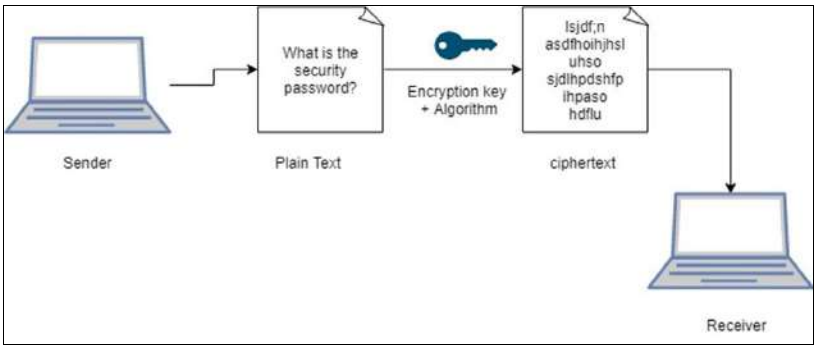
What is the security password?
Encryption key + Algorithm
lsjdf;n asdfhoihjhsl uhso sjdlhpdshfp ihpaso hdflu
Sender
Plain Text
ciphertext
Receiver

Fig 1: Encryption using Advanced Encryption Standard (AES) 128

1.1.3 Types of Data Encryption

Data encryption is categorized into two techniques namely symmetric and asymmetric encryption.

Symmetric encryption utilizes a single key for both encryption and decryption. This method ensures that a secure method is utilized to transfer the key between the sender and the receiver.

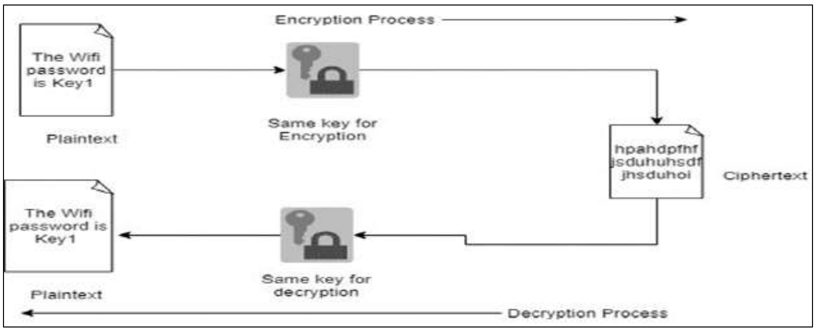

Fig 2: Visual breakdown of symmetric encryption

Asymmetric encryption, on the other hand, utilizes the idea of a key pair. This technique utilizes a different key for the encryption and decryption process. The first key is referred to as a private key. This key is kept secret by the sender. The second key is referred to as the public key. This key can either be shared by a group of recipients or it can be available to the general public. When data is encrypted using the receiver's public key, it can only be decrypted with the matching private key. This method ensures that data is transferred without the risk of unauthorized access.

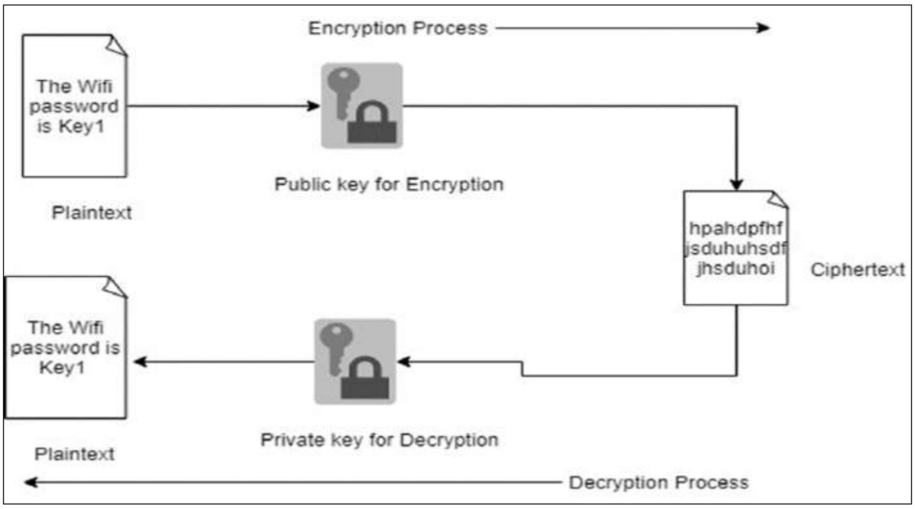
Encryption Process
The Wifi password is Key1
Plaintext
Public key for Encryption
hpahdpfhf jsduhuhsdf jhsduhoi
Ciphertext
The Wifi password is Key1
Plaintext
Private key for Decryption
Decryption Process

Fig 3: Visual breakdown of asymmetric encryption

These two schemes of encryption and decryption are different from each other as captured in TABLE 1 in terms of number of keys, security, resource utilization, size of cipher-text and speed.

Table 1: Differences between symmetric and asymmetric encryption

Differences	Symmetric Encryption	Asymmetric Encryption
Number of keys	uses a single key for encryption and decryption	uses two keys for encryption and decryption
Security	Less secured due to use a single key for encryption	Much safer as two keys are involved in encryption and decryption
Resource utilization	Works on low usage of resources	Requires high consumption of resources
Size of Ciphertext	Smaller cipher text compared to original plain text file	Larger cipher text compared to original plain text file
Speed	Fast technique	Slower in terms of speed

Source: [1, 10, 11]

1.1.4 Data Decryption

This technique refers to converting ciphertext to plain text. Therefore, it involves converting encrypted data into its original form [8]. Logically, this process is the reverse of the encryption process. Decryption is done by "un-encrypting" the ciphertext into plain text using the encryption key.

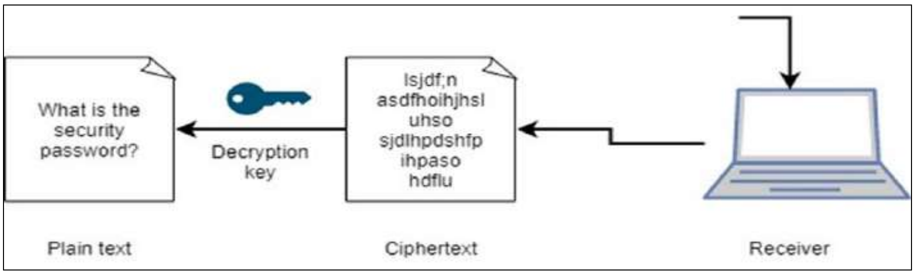
What is the security password?
Decryption key
lsjdf;n asdfhoihjhsl uhso sjdlhpdshfp ihpaso hdflu
Plain text
Ciphertext
Receiver

Fig 4: Visual breakdown of basic decryption

1.1.5 Principles of Data Encryption and Decryption

Encryption and decryption techniques offer effective ways to transform data without losing its meaning during transmission. However, despite their usefulness, these techniques do not solve all security problems within an organization. According to Oracle Corporation, these techniques may even worsen some problems. For instance, data encryption and decryption do not entirely solve access control problems [12]. Access to data should, therefore, be limited to those with a need to utilize it. This mechanism provides additional security to data. Data encryption does not protect against malicious database administrators [13]. A malicious database administrator may carry out several activities to a database such as corrupting and deleting data [12]. Data encryption may not protect against many such attacks. Therefore, encrypting every bit of data does not make data secure since it does not protect against security concerns such as access control. Additionally, these techniques may affect performance since they are both intensive operations. The process of encryption and decryption is shown in Table 2.

Table 2: Encryption vs Decryption

Characteristic	Encryption	Decryption
Definition	Process of converting plain text information (plaintext) into a form that appears random and meaningless (ciphertext)	The process of converting ciphertext to plaintext
Method	Encryption is done automatically with the help of a secret key during transmission of data	Decryption is done automatically into its original form using the data that was sent
Location	Data is encrypted on the sender's side	Data is decrypted on the receiver's side.
Major Function	Convert human readable texts into random and incomprehensible form that cannot be interpreted	Convert random and incomprehensible texts into a form that is comprehensible by human
Algorithm	Similar algorithm is used for encryption and decryption with a pair of keys each used for the two schemes	Similar algorithm is used for encryption and decryption with a pair of keys each used for the two schemes

Source: [1, 11, 10]

2. Application of Cryptography in Medical Services

Cryptography has been integrated into medical systems with an aim of promoting data security. Personal data in healthcare organizations are stored in different locations. These locations include EHRs or EMRs systems, mobile devices, computers, applications, and workstations. Health organizations at large have seen the need of utilizing these techniques in their daily operations. They have become an indispensable tool for healthcare organizations that use large volumes of data [14]. Cryptography has, therefore, been applied in different contexts within these organizations. For instance, this technique has been applied in the application layer encryption. This method is a data security solution that encrypts different types of data passing through an application. Application layer encryption encrypts data across multiple layers which include files, disks, and databases. This encryption technique reduces attack surfaces and helps in hardening systems. Therefore, if one application is compromised, the rest of the system is secured and does not become at risk. This technique has also been applied in security of medical images in health information systems [14].

Furthermore, cryptography helps to protect transmissions of data and promote secure communications between organizations. According to Security Metrics, over a hundred organizations have had personal data stolen due to inadequate email encryptions [4]. Therefore, cryptography helps to protect both individuals and organizations from simple and complex attacks from criminals and repressive governments. It also helps to protect electronic commerce transactions. For instance, cryptography makes it possible to safely transmit patients' and healthcare providers' credentials. Additionally, it protects data stored in electronic devices such as organization computers through disk encryption [8]. Therefore, cryptography is important in day-to-day operations in healthcare organizations. It promotes safety and ensure the successful completion of medical operations that require safe storage and transfer of personal data.

2.1 Need for Cryptography in Medical Sector

Healthcare organizations have become major targets for cyber-attacks [15]. It is increasingly necessary to protect healthcare data through cryptographic schemes. Cyber-attacks target healthcare organization stakeholders such as payers, insurance companies, and healthcare providers. According to Lauren *et al.*, healthcare cybersecurity attacks increased by 320% between 2015 and 2016 [15]. Most attacks resulted from the desire to access private information which could be utilized to commit identity theft and other criminal activities.

2.2 Cybersecurity attacks in Medical Sector

Most security breaches in healthcare aim to access personal data such as patient information. These criminals can then utilize this information to perform different activities that meet their personal interests. Some of these activities include:

1. Commit identity theft and health insurance fraud

Identity theft refers to the deceitful practice of using another person's information to commit fraud. For instance, attackers may steal an individual's information to get medical services. On the other hand, health insurance fraud occurs when a dishonest person intentionally submits false or misleading information to obtain additional payments for medical expenses than were actually incurred.

2. Expose private information to the public

Attackers may breach a healthcare database to expose private information of individuals in an attempt to get revenge or fulfill their personal desires. This action affects the confidentiality between patients and their healthcare providers. It also affects the integrity and availability of private information since authorized parties may have access to such information after exposure.

3. Damage a person's reputation

Attackers may manipulate a user information and perform informal actions on the behalf these individuals such as sharing confidential information and end up damaging their reputation.

4. Cause personal distress

When attackers expose confidential information to the public, the involved parties may experience stigma and discrimination which may result in personal distress.

Based on the increased attacks over the recent years that have focused on medical sector, all healthcare organizations need to embrace cryptography in the day-to-day operations. The two cryptographic schemes, encryption and decryption, have formed an important part of operations in some healthcare organizations. These strategies ensure that these organizations achieve certain goals during their operations. For instance, cryptographic schemes such as data encryption and decryption ensure security of data [8]. These techniques protect information from data breaches during data transit or when data is stored. Healthcare organizations also need these techniques to ensure privacy. Cryptography offers more dynamic data protection by ensuring that only authorized parties can access data within an organization [14]. They ensure data remain confidential. Furthermore, these techniques ensure authentication. They also ensure sources of data remain legitimate.

2.3 Challenges in Cryptography

The application of data encryption and decryption presents certain technical challenges. For example, encrypting indexed data may make the index to be unusable for any other purpose. It may render a query useless in a given database. As a result, despite its additional security, encryption cannot be applied to indexed data since it may make data unusable in a given database [16]. Another difficult aspect of cryptography is the key transmission. Cryptographic key on transit can be grabbed by an attacker who may gain access to sensitive data afterward. Additionally, key storage also presents a challenge. A database administrator with all privileges can access tables containing encryption keys [16]. Keys stored on an operating system are only as secure as the protections in the operating system. Therefore, an attacker who has access to the operating system can get access to the keys.

Additionally, cryptography does not offer protection against the vulnerabilities and threats that result from design of medical devices such as EHRs and EMRs. Cryptography does not ensure high availability which is a fundamental aspect of information security [16]. Additional techniques are required to guard against threats such as breakdown of information system and denial of service attacks. Furthermore, a system that utilizes a strongly encrypted and authentic source of information can be difficult to access even for a legitimate user. An attacker can render such system non-functional [16]. Such challenges make it difficult for most organizations to fully embrace the use of cryptography in their systems. Cryptography comes at a cost in terms of money and time. Addition of cryptographic techniques in the information processing leads to time delay and the use of public key cryptography requires setting up and maintenance which can be costly [16]. These factors make organizations to weigh the benefits against the cost of integrating cryptography in their operations. The cryptographic security attack, attack aspects and the cryptographic solution are shown in Table 3.

Table 3: Security attacks and solutions

Type of Attack	Security Aspect	Cryptographic solution
Denial of Service (DOS)	Availability	Digital signature
Eavesdropping	Confidentiality	Symmetric encryption of messages
Brute Force	Confidentiality	Strong encryption and key generation algorithms
Impersonation	Authentication	Variable MAC and IP addresses
Unlawful monitoring	Privacy	Anonymous key changes
Message tempering	Integrity	Integrity metrics, similarity algorithm

Source: [17, 1]

The instance of Symmetric encryption and decryption is shown in the appendix 1.

3. Conclusion

Cryptographic algorithms form the basis of data security. These algorithms have evolved from simple classical schemes to advanced schemes with greater complexities that ensure data is secure. These techniques have been incorporated by organizations and governments to ensure that confidentiality, integrity, availability, and accountability of data are maintained at all times. Medical sector has also incorporated cryptography in its operations. With attackers increasing their focus on healthcare data, one of the safest ways to protect medical information from such breaches is through utilizing cryptography. It offers more robust protection from cyber-criminals by encoding data in such a way that only authorized parties can access it. However, this technique also experiences certain challenges associated with its use. For instance, despite its additional security, encryption cannot be applied to indexed data since it may make data unusable in a given database. Additionally, key storage also presents a challenge as any individual with all the privileges can access tables containing cryptographic keys. With the advancements in technology, more complex and secure cryptographic algorithms will continue to be developed to offer more secure means to share messages between entities.

4. References

1. Chadwick DW, *et al.* A cloud-edge based data security architecture for sharing and analysing cyber threat information, Futur. Gener. Comput. Syst. 2020;102:710-722. DOI: 10.1016/j.future.2019.06.026.
2. Srinivasan R. Whose global village?: Rethinking how technology shapes our world. NYU Press, 2018.
3. Revill Jr DK. The Value of Artificial Intelligence when Mitigating Data Breaches, Dr. Diss. Capitol Technol. Univ., 2021.
4. Mousavi HA, Seyyed Keyvan, Ali Ghaffari, Sina Besharat. Security of internet of things based on cryptographic algorithms: a survey. 2021;27(2):1515-1555. DOI: https://doi.org/10.1007/s11276-020-02535-5.
5. Qadir AM, Varol N. A review paper on cryptography, 2019. DOI: 10.1109/ISDFS.2019.8757514.
6. Sharma JS, Dilip Kumar, Ningthoujam Chidananda Singh, Daneshwari Noola A, Amala Nirmal Doss. A review on various cryptographic techniques & algorithms. Materials Today: Proceedings. 2022;51:104-109. DOI: https://doi.org/10.1016/j.matpr.2021.04.583.
7. Thilakarathne NN. Security and privacy issues in iot environment, Int. J Eng. Manag. Res. 2020;10:4. [Online]. Available: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3559982.
8. Yazdeen RRZ, Abdulmajeed Adil, Subhi Zeebaree RM, Mohammed Mohammed Sadeeq, Shakir Fattah Kak, Omar Ahmed M. FPGA Implementations for Data Encryption and Decryption via Concurrent and Parallel Computation: A Review, Qubahan Acad. J. 2002;1(2):8-16. AD, DOI: https://doi.org/10.48161/qaj.v1n2a38.
9. Mohd Zaid Waqiyuddin MZ. Evolution of Cryptography, Obtenido Evol. Cryptogr. 2007;6:8. https//idazuwaika.files.wordpress.com/28.. [Online].

Available: https://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.698.2641&rep=rep1&type=pdf.

10. Parms J. Symmetric vs. Asymmetric Encryption – What are differences? SSL2BUY Wiki-Get Solution for SSL Certificate Queries. SSL2BUY Wiki-Get Solution for SSL Certificate Queries, 2020.
11. Martin M. Difference between Encryption and Decryption, Guru. 2022, 99. https://www.guru99.com/difference-encryption-decryption.html#6.
12. Zhang XL, Peng, Joseph Liu K, Richard Yu F, Mehdi Sookhak, Man Ho Au. A survey on access control in fog computing. IEEE Commun. Mag. 2018;56(2):144-149. DOI: 10.1109/MCOM.2018.1700333.
13. Mousa TM, Abdulazeez, Murat Karabatak. Database security threats and challenges, 2020 8th Int. Symp. Digit. Forensics Secur., no. IEE, 2020, 1-5. DOI: 10.1109/ISDFS49300.2020.9116436.
14. Kester QA, Nana L, Pascu AC, Gire S, Eghan JM, Quaynor NN. A Cryptographic Technique for Security of Medical Images in Health Information Systems, Procedia Comput. Sci. 2015 Jan;58:538-543. DOI: 10.1016/J.PROCS.2015.08.070.
15. Branch JB, Lauren, Warren Eller, Tom Bias, Michael McCawley. Douglas Myers, Brian Gerber, “Trends in malware attacks against United States healthcare organizations, Glob. Biosecurity, 2019, 1(1). [Online]. Available: https://jglobalbiosecurity.com/articles/10.31646/gbio.7/.
16. Menezes DS. Alfred, Challenges in Cryptography, IEEE Secur. Priv. 2021;19(2):70-73. DOI: 10.1109/MSEC.2021.3049730.
17. Shahid IS, Muhammad Anwar, Arunita Jaekel, Christie Ezeife, Qasim Al-Ajmi. Review of Potential Security Attacks in VANET, Majan Int. Conf., vol. IEEE, 2018, 1-4. DOI: 10.1109/MINTC.2018.8363152.

5. Appendix 1

An instance of Symmetric encryption and decryption

These two codes illustrate symmetric encryption and decryption done on a file with important information. During the encryption, the code prompts a user to select the file to be encrypted. The text file in this illustration is named “important.txt.” The code then prompts a user to enter a passphrase which acts as the encryption key. The code then utilizes the passphrase to encrypt the text file to “encrypted File des” file. This encrypted file has incomprehensible data that cannot be read by human.

During the decryption, the code prompts a user to select the file to be decrypted. The encrypted file in this illustration is “encrypted File des.” The code then prompts a user to enter the passphrase which acts as the decryption key. Since this illustration involves a symmetric encryption and decryption, the same encryption key is used for decryption. This code then utilizes this key to decrypt the selected file back to its original content “decryptedFile.txt”. The output is the initial file with contents that are readable to a human.