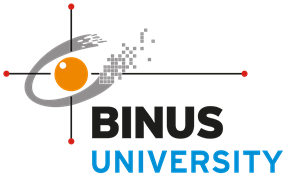
**BINUS INTERNATIONAL**

**DATA STRUCTURE**

**FINAL PROJECT PROPOSAL**

**CipherShield: Encrypt and Decrypt**

****

**Submitted by**

**Ari Jaya Teguh - 2702403996**

**Michael Lee Koesumo - 2802470553**

**Riki Awal Syahputra - 2802471404**

**28/03/2024**

**Submitted to**

**MARIA SERAPHINA ASTRIANI, S.KOM., M.T.I.**

# **TABLE OF CONTENTS**

[**TABLE OF CONTENTS 2**](#_84bv2es6oe54)

**1. Background………………………………………………………………………...……………………**[**3**](https://docs.google.com/document/d/19i4fmPCuoOSDux7QQuN88jZnz2G5BgAWpgxaI0vnyL4/edit#heading=h.9fpjxrvdof1j)

**2. Problem Description……………………………………………………………………………………4**

**3. Solution…………………………………………………………………………………………………..5**

**4. Team Workload…………………………………………………………………...…………………….7**

**5. Backup Plan….……………………………………………………………………………………..…...7**

**References……………………………………………………………………………………………….....8**

1. **Background**

Encryption and decryption are crucial security measures in the modern digital landscape. The process of encryption involves the utilization of cryptographic algorithms and keys to convert data into ciphertext. The data required an accurate decryption key to be readable. Once the file has been encrypted, it becomes inaccessible to unauthorized individuals who lack the appropriate key to decrypt or access the file.

In contrast, the process of decryption involves the reversal of encryption, wherein ciphertext is transformed back into plain text. This procedure enables individuals with proper authorization to access and understand the material that has been encrypted. The implementation of robust encryption and decryption techniques is necessary to protect sensitive data from unauthorized access and uphold its confidentiality and security.

Apple Inc. is an exemplary corporation that places a high priority on data protection. Encryption and decryption play a crucial role in safeguarding sensitive information and mitigating the risk of illegal data intrusions. A range of encryption techniques and algorithms, including the Vigenère cipher, the RSA algorithm, the AES algorithm, and the modified Playfair algorithm, contribute to the enhancement of data security through the provision of distinct levels of security and complexity. Organizations possess the ability to select the most suitable approach or algorithm to optimize the efficacy of protecting sensitive data.

Safeguarding extremely sensitive and valuable data from cyber threats necessitates the implementation of a comprehensive strategy that encompasses strong encryption and decryption methodologies. The comprehension and proficient application of these techniques are imperative in upholding integrity, confidentiality, and security in the contemporary digital environment.

1. **Problem Description**

Organizations have numerous challenges in the era of digitalization. An illustration of this is the safeguarding and secrecy of delicate data. Organizations are confronted with substantial risks in preserving the integrity and privacy of their data due to the escalating prevalence of cyber threats and data breaches. The appropriate implementation of encryption and decryption techniques is crucial in safeguarding sensitive data from unwanted access and potential data breaches.

The issue at hand arises due to a prevalent deficiency in the comprehension of encryption and decryption methodologies within numerous businesses, or their inadequate implementation thereof. Consequently, their susceptibility to cyberattacks, data breaches, and potential financial and legal ramifications arises from their compromised data security stance.

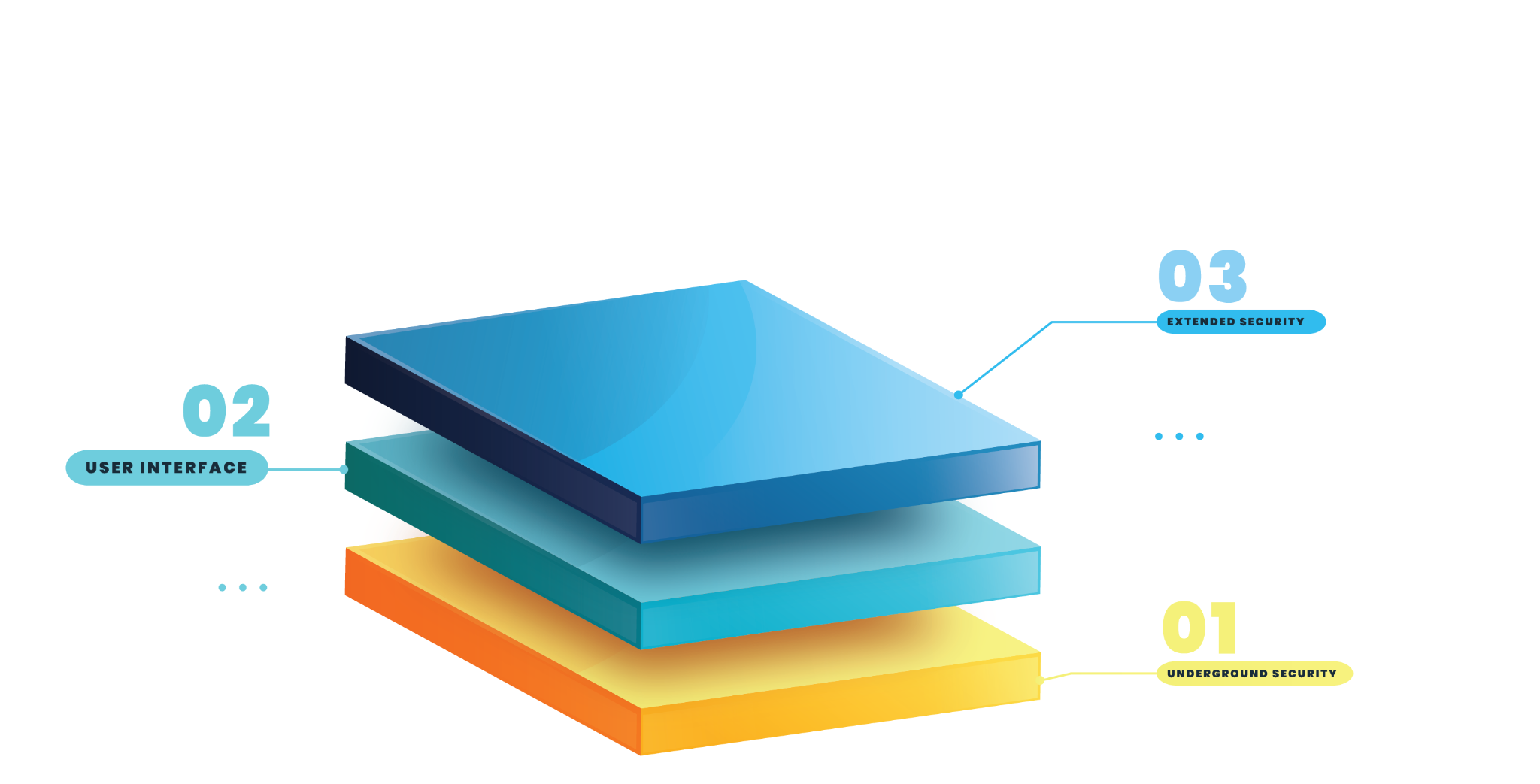
Furthermore, the intricate nature of encryption algorithms and the ongoing development of cybersecurity threats present supplementary obstacles for firms, necessitating their continuous awareness of contemporary security standards and optimal methodologies to mitigate risks to a tolerable extent.

The complexity of encryption and decryption operations is heightened due to the diverse array of data forms and types, encompassing both structured and unstructured data. The implementation of customized encryption solutions that effectively cater to the unique requirements and attributes of an organization's digital assets, while also adhering to regulatory mandates, constitutes a fundamental element of its cybersecurity strategy.

In essence, the issue at hand pertains to the imperative for enterprises to enhance their encryption and decryption skills to successfully safeguard sensitive information. To accomplish this, it is crucial to tackle technical obstacles, be vigilant against emerging risks, establish strong encryption protocols, and adhere to industry-specific data protection rules.

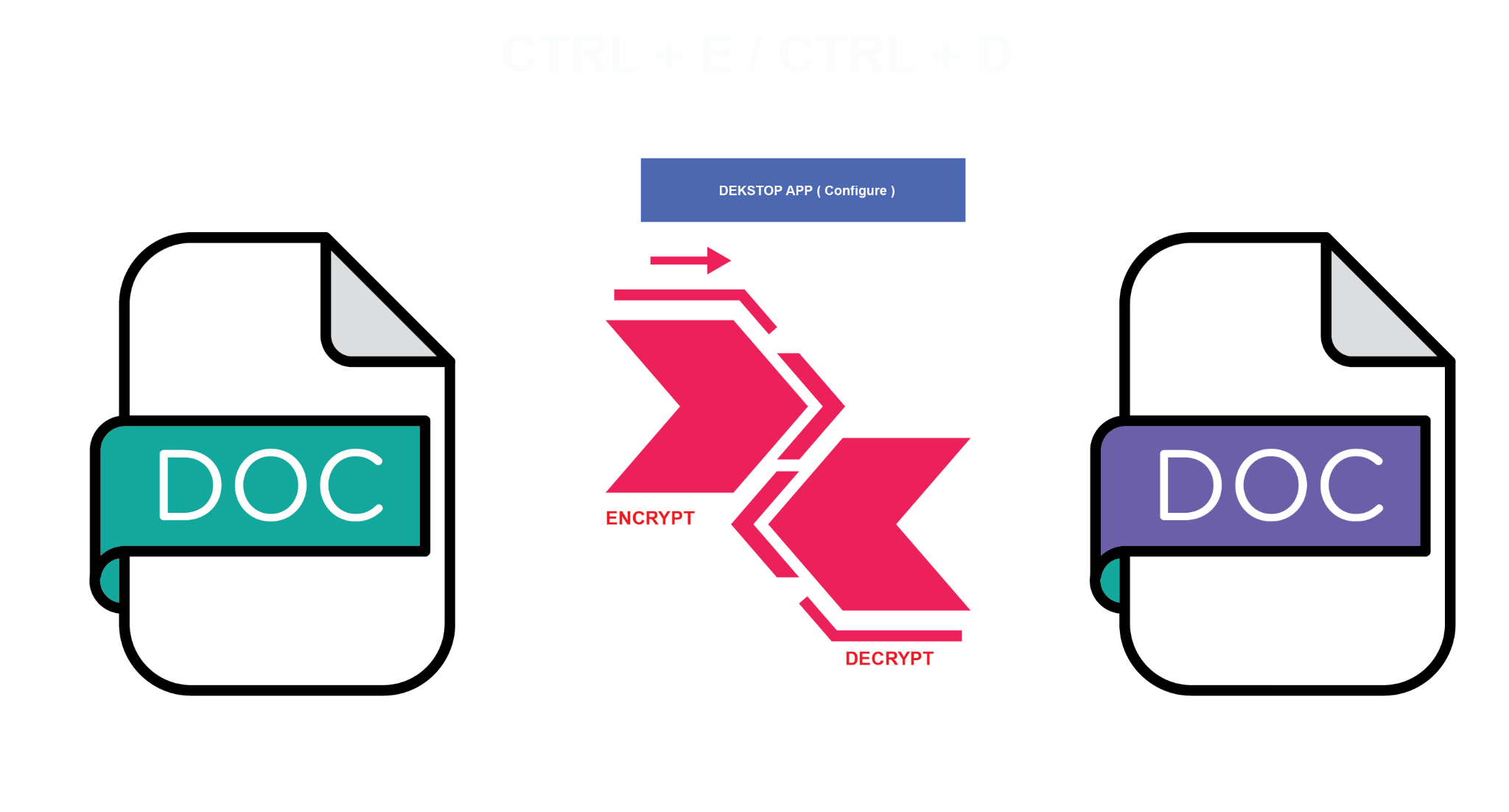
1. **Solution**

While the world is already familiar with security with its massive implementation worldwide, our team wants to extend the ability of security to the new layer standard on the Windows operating system. The extended version of security will enable the next level of security with its more interactive feature to encrypt and decrypt data with the use of a shortcut.

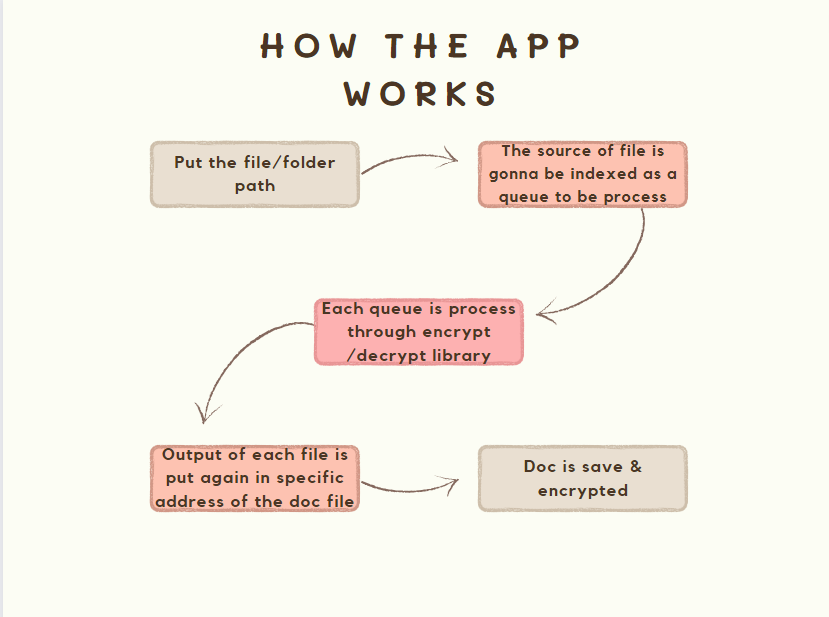


In simple terms, our team decided to define two layers of components in our computer: the first is underground security, where everything is running in abstraction to protect our data, and a huge amount of instruction where the user does not have to know the process, and the second layer is the interface of interaction that the user can see.

With the Ciphershield project, we extend the layer into layer 3, which is our team that brings the extra solution for a more secure system that can be customized as needed; it combines customization, background security, and interaction between the decision of the user and the cryptography software.



In our initial project, our focus lies on securing the .doc type file, which is as simple as encrypting all the content on the file, and can be decrypted as well by only using a shortcut on the keyboard, such as CTRL + E for encrypting the content and CTRL + D for decrypting the content.



The algorithm that we are going to use for the encryption is our own. We are planning to make an algorithm using hash tables. The types of encryption that we are going to use are symmetric and asymmetric. A symmetric algorithm uses a shared secret key to be able to encrypt and decrypt the data. In contrast, an asymmetric algorithm allows us to use a pair of mathematically related keys, a public key as well as a private key, to be able to encrypt and decrypt the data.

The data structures that we will use for the encryption and decryption processes are hashmaps, hashtables, arrays, linked lists, and trees. HashMaps and HashTables are useful for storing key-value pairs, which can be operated in cryptographic applications for mapping keys to encrypted data or decryption data to ciphertext. Hashmaps provide efficient lookup and compensation operations, making them suitable for managing encryption keys and associated data. Arrays are used to store fixed-size sequences of elements, such as bytes, in encryption algorithms like AES (Advanced Encryption Standard) or RSA (Rivest-Shamir-Adleman). They provide efficient access to elements based on indexes, which is crucial for processing data in encryption and decryption processes. People primarily choose arrays due to their simplicity and direct access to memory location attributes. You can use linked lists to manage variable-length data structures, like storing encrypted blocks of data that change in size depending on the input. They also offer dynamic memory allocation and insertion capabilities, making them beneficial for handling data streams in encryption and decryption processes. On the other hand, data structures like binary search trees (BST) or balanced trees can be used for organizing and searching encrypted data efficiently. Trees provide logarithmic time complexity for search operations, which is very helpful in cryptographic applications where quick access to data is vital.

1. **Workload:**
2. Ari: Making the encryption and decryption library. We decided to use Hashtable for our encryption and decryption library. Cryptographic hash functions rely on hash tables, which are utilized in encryption techniques. Efficient storage and retrieval of massive data sets are facilitated by these systems, ensuring the preservation of data security and integrity.
3. Mike: Making the app able to convert and change the content in Microsoft Word for the encryption & decryption process to work correctly and efficiently.
4. Riki: Building the GUI and adding shortcuts to make the user easier to encrypt and decrypt sensitive information.
5. **Backup Plan**

Our backup plan is to make an app that recommends movies to the user. People often don’t know or spend a lot of time choosing a movie to watch. So to not waste time choosing movies, we decided to make a movie recommendation for the user. The basic idea is that the user is asked general questions like the genre, year, actor (not required), etc. Based on the answer, the app decides what movie is best for the user. The machine learning that is used to support the app is TensorFlow Lite. The data structures that we are going to use are hash, linked list, and array list.

**References**

Andoque, Twinkle. “Chapter 1 Introduction Background of the Study.” *Www.academia.edu*, [www.academia.edu/7835291/Chapter\_1\_Introduction\_Background\_of\_the\_Study](http://www.academia.edu/7835291/Chapter_1_Introduction_Background_of_the_Study).

Cash, David, et al. “Dynamic Searchable Encryption in Very-Large Databases: Data Structures and Implementation.” *Cryptology EPrint Archive (Eprint.iacr.org)*, 2014, [eprint.iacr.org/2014/853](http://eprint.iacr.org/2014/853).

“Encrypt Your Data and Devices / Safecomputing.umich.edu.” *Safecomputing.umich.edu*, [safecomputing.umich.edu/protect-yourself/encrypt-your-data#:~:text=Encryption%20helps%20protect%20confidential%20data](http://safecomputing.umich.edu/protect-yourself/encrypt-your-data#:~:text=Encryption%20helps%20protect%20confidential%20data).

M. R. Alves, Pedro G., and Diego F. Aranha. “A Framework for Searching Encrypted Databases.” *Journal of Internet Services and Applications*, vol. 9, no. 1, 3 Jan. 2018, <https://doi.org/10.1186/s13174-017-0073-0>.

Mahajan, Dr. Prerna, and Abhishek Sachdeva. “A Study of Encryption Algorithms AES, DES and RSA for Security.” *Global Journal of Computer Science and Technology Network, Web & Security*, vol. 13, no. 15, 2013, [s.id/24m7I](http://s.id/24m7I).

Pitchay, Sakinah Ali, et al. “A Proposed System Concept on Enhancing the Encryption and Decryption Method for Cloud Computing.” *IEEE Xplore*, 1 Mar. 2015, [ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=7576545](http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=7576545).

Shrestha, Kapil, et al. “Data Encryption and Decryption | PDF | Encryption | Cryptography.” *Scribd*, 2019, [www.scribd.com/document/508179120/Data-encryption-and-decryption](http://www.scribd.com/document/508179120/Data-encryption-and-decryption).