A. Project Tittle

File Encryption and Decryption System

B. Brief description on project background. (i.e. problem context, rationale, description problem area, nature of challenge)

For a better understanding about the study, cryptography processes have been combined with encryption approaches. Encryption methods are followed by other techniques like the Rivest Shamir Adleman (RSA) algorithm with public-key cryptography, 3DES (Triple-DES) algorithm with secret key cryptography and Advanced Encryption Standard (AES) algorithms. These methods are used to secure data that is sensitive. However, in recent situations, attackers have had the credibility and capability to get access to sensitive data by breaching encrypted files and modifying or viewing them without the users consent. Even if encryption is improved, weak algorithms may be quickly broken using a number of cracking tools that are available for free in order to obtain access to confidential data.

Furthermore, if the developer does not consider an appropriate type of encryption technique and cypher algorithm, implementing encryption to secure the information might cost the developer high risk. To give an example, the DES or also known as Data Encryption Standard is a usual standard where even technology present till date still utilizes it although it is no longer available at the market. In order to bring in encryption process for a number of gigabytes (GB) using similar key, it uses 64-bit blocks, despite the fact that GB is no longer considered large data. In a different perspective, hacker might easily penetrate the encryption in a matter of a few days. Furthermore, there are few types of cypher encryption that can be listed such as Caesar Cipher, Vigenere Cipher, and Vernam Cipher. Caesar Cipher can be derived as quite a basic substitution cypher that substitutes alphabet s each and every plain-text letter with a letter that is three places ahead of it. For instance, DEF will be the end result of ABC. To conclude, if the system s encryption technique is poor, hacker can eventually crack it by analyzing the cipher-text then reverse engineering the plain-text to access it.

**Rationale**

The suggested system is a stand-alone system that is capable of allowing users to secure the sensitivity of data, files, and folders. The system will come up with three identical principles, Confidentiality, Integrity and Availability (CIA), that will be utilized to protect files and data, as a result of the following method of this suggested system. It was necessary to improve the level of security algorithm, ciphertext, implemented in order to guarantee the integrity of files to be protected securely. To guarantee that the file s confidentiality was secured at all times, the transformation of ciphertext needed to be enhanced with encryption keys. Files and data will be accessible using the validated key (Availability).

Furthermore, it is clear that a system that can hide communications so that they are not accessible to anybody other than the owner or authorized users. As a result, the developer will construct an application that will allow users to encrypt and decrypt files and folders of their own choosing. By encrypting the real data, the data s confidentiality, integrity, and availability are preserved, and unauthorized users will not be able to access the concealed data. Furthermore, it will decrease the probability of data being stolen or exploited. Internet users do not have to worry about their data being leaked to third parties if they use this program because the data will be kept hidden.

**Tangible Benefits:**

* Authentication and authorization - For users to download the file.  Security clearance is based on the decryption key and determines which user is permitted to open the file.
* Cost saving by eliminating options to purchase external encryption software.
* Keeping files from falling into the wrong hands - File can be downloaded easily despite not having permission.

**Intangible Benefits:**

* Database - It is necessary to specify which user or individuals have permission to open the file when encryption is used.
* Encryption - To make a secure encryption for files and folders.

**Nature of Challenge**

First and foremost, learning how to implement encryption and decryption is one of the developer s main challenges. Cryptography can be branched out to various types and to get the most suitable method that secures data, comparison needs to be done. Since a drastic change would attract attention among unwanted or unauthorized individuals, it’s critical to keep the alterations to a minimum level.

Aside from that, developer has to contribute on doing study about various algorithms for encryption and has to choose the most suitable one to be used in the system. To make sure system works perfectly fine, affecting factors like time consumption to encrypt data as well as file size must be compared and studied among different methods. Not to forget that data that has been encrypted as well as concealed must be retrieved which leads to another challenge for the developer.

**Project Aim**

To build a system that does file encryption and decryption in a secured approach.

**Project Objectives**

* To study about issues of data breaches/data confidentiality and also methods used to secure.
* To design a suitable method to secure the data/information before sending over to recipient.
* To develop a tool incorporating both encryption and decryption to secure files and data.

C. Brief description of project objectives. (i.e. scope of proposal and deliverables)

**Deliverables**

* The system offers users to encrypt files in order to give a higher level of security for the user s files, and as a result, the system must be able to decrypt the user-encrypted files.
* The system enables the user to encrypt as well as decrypt data, including files and their contents. The user needs to browse and select the file that he/she wants to encrypt.
* Password verification will be another feature that has been included to the system. When a user wishes to encrypt or conceal a file, he or she must first set a password and when decrypting the file, it requires the same password. This feature prevents unauthorized users from reading the original file s content.

D. Brief description of the resources needed by the proposal. (i.e. hardware, software, access to information / expertise, user involvement etc.)

**Hardware**

The following are the minimal hardware requirements to achieve the system s objectives:

* 8 GB RAM or higher
* Keyboard
* Mouse
* Wi-Fi

**Software**

The following are the minimal software requirements to achieve the system s objectives:

* Microsoft SQL Server
* Windows 7 or higher
* PyCharm
* Microsoft Word 2016
* Microsoft Project 2016

**Access to information/expertise**

For developing this particular system, consultation from supervisor as well as lecturers involved to security field is required. Questionnaire will be circulated to students from APU campus and also from the outer circle to get better response regarding the system to proceed with evaluation.

E. Academic research being carried out and other information, techniques being learnt. (i.e. what are the names of books you are going to read / data sets you are going to use)

In order to carry out the deliverables, the preliminary list of books and web pages I will study are as follows.

**Books**

Name: Understanding Cryptography

Author: Christof Paar, Jan Pelzi

Publisher: SpringerLake

Name: Data Hiding Fundamentals and Applications

Author: Husrev T.Sencar, Mahalingam Ramkumar, Ali N. Akansu

Publisher: Elsevier Science Publishing Co Inc

Name: Understanding Privacy

Author: Daniel J. Solove

Publisher: Harvard University Press

Name: Practical Cryptography in Phyton

Author: Seth James Nielson, Christopher K. Monson

Publisher: Apress Media LLC

Name: The Hash Function BLAKE

Author: Jean-Philippe Aumasson, Willi Meier, Raphael C.-W. Phan, Luca Henzen

Publisher: SpringerLake

**Online Resources**

1. W.H. (2020, February 7). *CIA in shipping, part 1: How to ensure data confidentiality*. Dualog. Retrieved January 16, 2022, from https://www.dualog.com/blog/how-to-ensure-data-confidentiality-in-shipping

2. Allan, M. (2021, July 9). *6 Types of Encryption That You Must Know About*. GoodCore Blog. Retrieved January 16, 2022, from https://www.goodcore.co.uk/blog/types-of-encryption/

3. Sharma, K. (2020, December 25). *Top 12 Software Development Methodologies & its Advantages & Disadvantages*. TatvaSoft Blog. Retrieved January 16, 2022, from https://www.tatvasoft.com/blog/top-12-software-development-methodologies-and-its-advantages-disadvantages/

4. Sv, M. (2021, December 16). *Encrypt and Decrypt Files using Python — Python Programming*. Towards Data Science. Retrieved January 16, 2022, from https://towardsdatascience.com/encrypt-and-decrypt-files-using-python-python-programming-pyshark-a67774bbf9f4

5. Martin, M. (2021, November 9). *Difference Between Encryption and Decryption*. Guru99. Retrieved January 16, 2022, from <https://www.guru99.com/difference-encryption-decryption.html>

6. S. (2020a, November 25). *What is Cryptography? – An Introduction to Cryptographic Algorithms*. Edureka. Retrieved January 16, 2022, from https://www.edureka.co/blog/what-is-cryptography/

7. Thakkar, J. (2021, March 11). *Types of Encryption: 5 Encryption Algorithms & How to Choose the Right One*. Hashed Out by The SSL StoreTM. Retrieved January 16, 2021, from https://www.thesslstore.com/blog/types-of-encryption-encryption-algorithms-how-to-choose-the-right-one/

F. Brief description of the development plan for the proposed project. (i.e. which software methodology and why, the major areas of functions to be developed and the order in which developed)

The image for the preliminary of project progress is the system development methodology. "These are often used as a framework to structure, plan, and control the development process of an information system." Depending on environment in which it operates, organizational team as well as project, a number of methodologies can be implemented based on factors listed.

"The system development approach will be chosen based on how well it defines the precise goals for each stage and the outcomes required before the next one can begin." It may include specific structures for providing documentation that describes each stage." Rapid Unified Process (RUP) and Rapid Application Development (RAD) are two types of system development methods and methodologies that will be discussed. RUP provides systematic and stable way to software development where it comes with a mix of principles, practices as well as procedures that directly represent the approach itself. RUP comes with five phases that can be arranged starting from the very first phase, inception, followed by elaboration, construction, transition and production. Besides that, RAD s method is focused on adaptability and the capability to adjust with acquired knowledge, and it requires a rigid framework with defined standards. Meanwhile RAD consist of four major phases which can be arranged in ascending order starting from planning requirements, user design, rapid construction and cutover.

G. Brief description of the evaluation and test plan for the proposed project. (i.e. what is the success criteria and how will be evaluated and implementation will be tested, indicate the estimated size of the demonstration / test database)

**Success Criteria**

To determine project s success by looking at how effectively the encryption and decryption are working based on the users level clearance.

**Unit Testing**

Users will evaluate each session of system implementation to check if anything goes wrong and provide feedback on any suggestions for improving the system s functionality. However, the encrypt and decrypt phases are the most crucial of these testing processes. Because the primary aim of this system is to run based on the objectives, the developer can concentrate on other criteria to bring to the system.

**Integration Testing**

The system will be deployed in groups of people to test whether it can handle more than one user operating the system at the same time. This will certainly be stored in order to determine if the database can capture the user decryption key and execute it for the entire group at once. In addition, to test the system by sending the file to more than one receiver.

**Usability Testing**

For this phase, a random user will attempt to test the system to see whether it can provide them the system s actual output. An actual data or file will be entered into the system by the user. Furthermore, they will provide feedback on the system and what they think of it, whether it is to add new functionalities or to fix some of the ones that are malfunctioning.