JOURNAL OF SCIENCE TECHNOLOGY AND EDUCATION 10(4), DECEMBER, 2022
ISSN: 2277-0011; Journal homepage: www.atbuftejoste.com

# A Secured CBT Examination Question Using Data Encryption Standard Algorithm

Siyaka, Opotu Hassan
*Computer Science Department,*
*Faculty of Comuputing and Informatics,*
*Confluence University of Science and Technology, Osara, Kogi State.*

**ABSTRACT**
*Giving exams, from the smallest level, such as daily tests and semester exams, to the highest level, such as the national exam, is one approach to measure the success of the academic process and accomplishment of student competency. Cryptography is a data security approach that is used to ensure the security of data. Using the Data Encryption Standard (DES) algorithm, a security system was created to protect exam questions so that data could not be read by a student or unauthorized user before the exam time. The DES algorithm is a symmetric algorithm in which the encryption and decryption processes use the same key Processes. The Caesar Cipher algorithm will be used to create an additional key that will be kept hidden from the public in the system that will be developed. The findings of this study show that the DES encryption method provides the best results, indicating that it can be used to protect transmitted data in a virtual data storage system. The C#.Net is used to develop the software for this project in other to achieve the aim of this project.*

**ARTICLE INFO**
Article History
Received: June, 2022
Received in revised form: July, 2022
Accepted: August, 2022
Published online: December, 2022

**KEYWORDS**
Cryptography, DES, unauthorized, symmetric, Caesar cipher

## INTRODUCTION

Data protection from hostile computer users is critical in our daily lives, and securing confidential data such as examination questions is a top priority to prevent the student or penetrator from seeing the questions before the exam begins. Securing data from unkind computer users is still highly vital nowadays, (Plata et al., 2019) all procedures require greater security to protect data from smart hackers, whether it's preventing unwanted access to individual images, guaranteeing data privacy compliance, or maintaining the stability of company information. To prevent unauthorized users from abusing information and unlawful penetrations, the importance of having secure exam questions for computer-based testing (CBT) should be emphasized, Security for computer-based testing examination questions is required for access into equipment, such as a computer, as well as access to other personal data via their connections. Data security is a top priority in every business, organization, or computer-based testing (CBT) assessment institution. This application is intended to encrypt examination questions, store the encrypted question, and decrypt the question only by admin with access to the application during the examination period before it is sent down to the database of the computer-based testing (CBT) examination platform where the exam will begin, preventing assaults.

According to (Sumartono et al., 2018) Information security is the protection of personal and non-personal data from various threats in order to ensure privacy. Data security can help businesses reduce risk while also increasing return on investment and business opportunities. There are information security elements to consider while designing information system security systems. Many hazards will emerge before the information is widely disseminated. Information is something that wild parties will go after. To protect data from these threats, cryptographic algorithms are required. The Data Encryption Standard (DES) is a block cipher that belongs to the symmetrical cryptography scheme. The DES algorithm uses a 64-bit block size. DES uses 56 private key bits or sub keys to encrypt 64 plaintext bits into 64-bit cipher text.

It is undeniable that developments in technology and the quick transmission of information are also followed by a surge in crime in the IT area; very valuable information is sought by criminals in the IT field in order to be misused so that they obtain large profits (Permana et al., 2020). One of the pieces of information is student value data, hence a

**Corresponding author: Hassan, O. S. ✉ alhassan77077@gmail.com ✉ Department of Computer Science, University of Science and Technology, Osara, Kogi State.* 

system that uses a cryptographic algorithm to secure it is required. In this situation, the Data Encryption Standard (DES) algorithm is employed to secure student value data.

Data security is a system for protecting data from potential threats and assuring the delivery of information. Its purpose is to reduce risk while simultaneously improving or speeding up decision-making. The sensitivity of the data in the database also influences the level of security; data that isn't too sensitive to the security system isn't too tight, whereas sensitive data necessitates a more strict security level setting for access (Sumartono et al., 2018).

A secure system ensures the confidentiality of data. This means that, it allows individuals to see only the data which they are supposed to see. It was observed that examination questions are confidential data and need to be safeguarding while they are stored in the database, not allowing intruders to abuse the information when there get hold of it. The requirement to protect examination questions in the event of unauthorized access to locations where such data is stored is a must. Data stored in plain text that is not encrypted can be easily viewed and misused, jeopardizing examination operations. The loss of data has already been mentioned as a factor that can delay the start of an examination as a result, it's critical to develop strategies for encrypting and decrypting exam questions. A technique will be devised that can guarantees a high level of assured accuracy for securing the examination questions.

Securing data in the current cyber world we find ourselves in is very important, and it helps a lot of organizations, firms, and academic data to be kept in safe and secure manners when the data is encrypted, unauthorized users cannot penetrate through your data because any attempt made, the penetrator will see the data in cipher text, which will not be understandable to him, but only the admin alone or any other authorized user will see the data in cipher text, which will not be understandable to him.

This research aims at securing CBT examination questions using DES algorithm to prevent unauthorized users to get access to the examination questions. The work is carried out to make sure for maximum computerized data security system. It also proves the usefulness of data security. It will also enlighten other researchers to study relating field of work related to data security.

This research will also provide detailed information on the concept of data security. The importance of data security in this field. There is always the need in lives of individuals and corporation for privacy and secrecy. The purpose of study of this project securing CBT examination questions using data encryption standard (DES).

## LITERATURE REVIEW

This section provides a brief reference to the literature articles which suggest the techniques for data encryption. It is split into further subsections based on the different types of algorithm. According to (Akande et al., 2020) safeguard sensitive data from illegal access and alteration, cryptographic techniques have been widely used. The Data Encryption Standard (DES) is one of the most extensively used cryptographic algorithms, however it is vulnerable to key and differential attacks. Several DES improvements have been proposed in the literature to combat these attacks.

Image Composition Using Data Encryption Standard (DES) Output Result across the Internet (Mohammed, 2021). For information security specialists, data protection is a crucial problem because of the rapid growth of techniques for transferring information via the Internet, as well as its vast volumes, it is vital to develop methods to protect information from intruders (Hackers or Crackers) by using cryptographic algorithms such as (AES, DES, RSA...etc.) that allow for fast processing and data protection. Other methods of data protection include disguising it in a specific media, such as an image, video, or audio file. This research encrypts the data using the Data Encryption Standard (DES), and then converts it to a picture of a specific pattern that is used to randomize the distribution of data in the form of different point colors and sites before sending it over the internet.

According to (Zebua, 2018) Computer utilization in the execution of the computer-based test is currently no strange. The problem of question security and exam answers to abuse actions is a key aspect to consider and maintain in the execution of computer-based exams. Cryptographic techniques are one strategy that can be used to overcome the challenges mentioned above. The outcomes of the encoding procedure can make it more difficult for attackers to figure out the exam's original text, reducing exam abuse. Utilization of cryptographic algorithm techniques is one alternative solution to solve the above problems. One method of securing

*Corresponding author: Hassan, O. S. ✉ alhassan77077@gmail.com ✉ Department of Computer Science, University of Science and Technology, Osara, Kogi State. 

data by encrypting it is to use cryptographic techniques. The technique or the cryptographic algorithm can encrypt text exam records that have been stored in the database. Minimizing exam misuse by parties other than the legitimate stakeholders can have a substantial influence on the business.

Counterparts, with the goal of preventing the misuse of information by non-eligible parties. Security has been a top priority for every faction of society over the years (Yazdeen et al., 2021) Security has been enforced over time through many means, including digitization. Virtually every company in today's world stores its data in digital databases. It was formerly imposed through physical occurrences.

According to (Yazdeen et al., 2021) increasing numbers of Internet and wireless network users have helped accelerate the need for encryption mechanisms and devices to protect user data sharing across an unsecured network. Because of these features, data security, integrity, and verification may be used. Symmetrical block chips are crucial in the encryption of internet data. The Data Encryption Standard (DES) and Advanced Encryption Standard (AES) are data encryption technologies that preserve privacy. Encryption - Encryption is the translation method of plain text to cipher text. This unreadable message can be easily transmitted over an unreliable network. The encryption process requires encryption algorithms.

1. **Decryption** - Decryption is the opposite of encryption. To make cipher text out of plain text.
2. **A Key** - A key is a binary text (mathematical formula). In data encryption, it operates on plain text, and in decryption, it takes place on the cipher text.
3. **Key Size** - Key size, used in any algorithm, calculates required length in bits.
4. **Block Size** - Key cipher is based on a fixed length of bits. It is a predetermined length of "Block" bits in the machine. The block size depends on the algorithm selected.
5. **Round** - Encryption round means that before it gives cipher text as output, the encryption feature is performed in the complete encryption process.

To protect data from unauthorized users, data security strategies are required. One of the essential methods used for data security is the encryption of data Two fundamental forms of cryptography are available:

• Cryptography with Symmetric Key (Secret Key).
• Cryptography with Asymmetric Key (Public Key).

The study identified that there was a lot of deficiencies when it comes to the coverage of security of data such as examination questions which is a sensitive data. This made it difficult to acquire data with regard to the aforementioned research.

## METHODOLOGY

### FACT FINDING METHODS USED

In order to complete this research, information was gathered from both Primary source and Secondary source. The primary source of information for my research was an interview with the management information system (MIS) department, which we conducted by asking questions and also utilized an observational strategy in which we were alert to all of the department's operations, examining them and recording them as needed.

The importance of secondary data sources for this type of endeavor cannot be overstated. The research acquired secondary data from journals, the majority of which were addressed in our literature evaluation of this research.

### DESCRIPTION AND ANALYSIS OF THE NEW SYSTEM

By applying the DES algorithm method to the new system, securing computer-based testing examination questions focus on ensuring the security of the questions by creating an application software that will be responsible for the encryption and decryption of the examination questions before they are sent down to the database to prevent access by unauthorized users. The following is descriptions of the new develop system for this research:

1. The encryption of the examination questions is more secure than the existing system.
2. The login interface is build where the admin will go through authentication process in order to access the main encryption/decryption environment.
3. The user can easily upload the examination question file and encrypt the file then store in a folder which will be link to the database.
4. We can find the most accurate security using the DES algorithm technique to secure the examination question.

### GRAPHICAL STRUCTURE

The software approach for this paper is based on the unified software development process,

*Corresponding author: Hassan, O. S. ✉ alhassan77077@gmail.com ✉ Department of Computer Science, University of Science and Technology, Osara, Kogi State. 

JOURNAL OF SCIENCE TECHNOLOGY AND EDUCATION 10(4), DECEMBER, 2022
ISSN: 2277-0011; Journal homepage: www.atbuftejoste.com

block diagram, and flowchart. This entire process is used to explain the new system's visual view, which is used to model the different interacting processes, applications, and systems in order to articulate and come up with robust system architecture.

## UNIFIED MODELING LANGUAGE (UML) OF THE NEW SYSTEM

The UML describe the visual view of how the develop system operate and also the processes involved shown in figure 1.

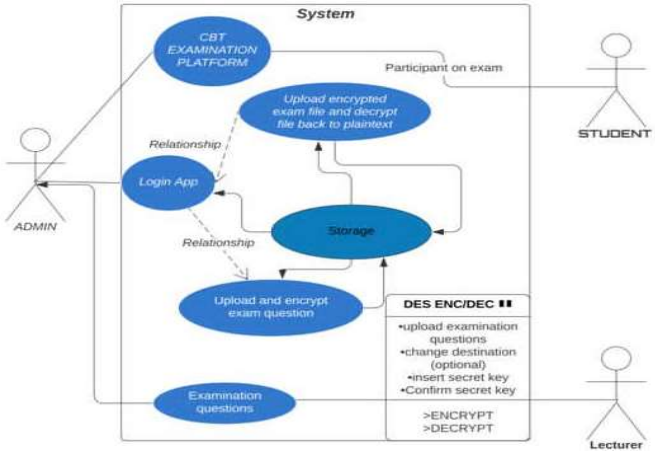


**Figure 1:-** UML activity diagram of the new system

The following are the features of the new system:

1. The new system features a data encryption authentication technique in addition to the traditional authentication methods (username and password).
2. Test questions are encrypted and stored in a database to prevent tampering, unauthorized or malicious access, and other unwanted behaviors that could threaten the integrity and confidentiality of the exam questions.

The encryption of exam questions before there are decrypted and uploaded to the database, which is done using the DES algorithm, is one of the most crucial features of the new system. The suggested cryptographic approach will be used to encrypt exams questions to ensure a secured spot for the questions. The questions will be decrypted during the examination period before uploading to the CBT platform, where a genuine participant who passes the authentication stage (Login stage) in the CBT exam platform would be able to participate in the exam.

## CONCEPTUAL FRAMEWORK

As earlier mentioned, this research employs the block cipher approach shown in figure 2. The data will be encrypted and decrypted using the DES block cipher. The CBT questions will be accessed after the security process has been successfully completed. The DES algorithm is used to encrypt the data into a secret key, which applies a 56-bit key to each 64-bit block of data and will be decrypted using that same secret key.

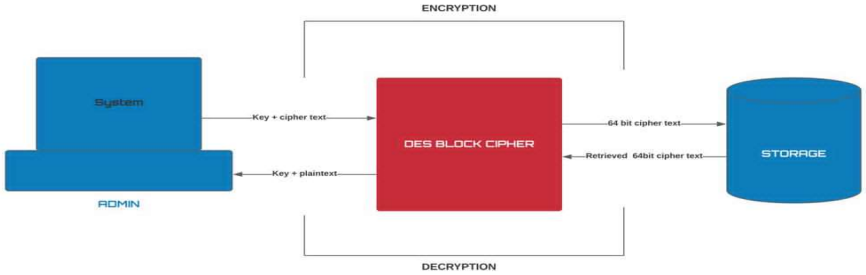


Figure 2:- **Encryption-Decryption Flow Mode**

*Corresponding author: Hassan, O. S. ✉ alhassan77077@gmail.com ✉ Department of Computer Science, University of Science and Technology, Osara, Kogi State. 

JOURNAL OF SCIENCE TECHNOLOGY AND EDUCATION 10(4), DECEMBER, 2022
ISSN: 2277-0011; Journal homepage: www.atbuftejoste.com

## FLOWCHART OF THE NEW SYSTEM

The flowchart of the new system describes the whole process of how the system operates.

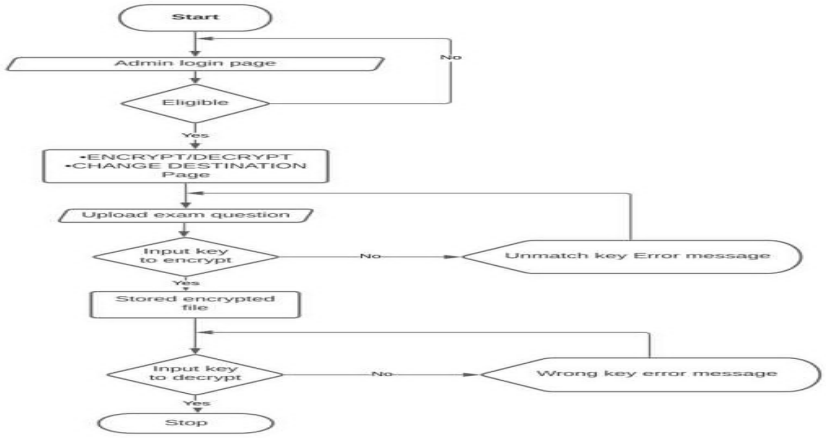


**Figure 3:** Flowchart design for the new system

## SYSTEM IMPLEMENTATION AND DOCUMENTATION

### Choice of Programming Language

Visual Studio 2017 (C#.NET) will be used for interface design and program operations (front end), and MySQL will be utilized for database (back end) in this research work. Advanced Windows features such as (object linking and embedding) and MDI are supported (Multiple Data Interface).
It's a programming language that focuses on objects that unbalances speed of work.

### Installation Requirement

The hardware and software requirements for the proposed system are evaluated from two (2) perspectives.

### Hardware Requirement

The computer and devices that make up the newly built system are known as hardware.
• At least an Intel two core processor is necessary (1.6 GHz), A minimum of 2GB of RAM is required. Also a hard disk with a capacity of 120 GB or more is required with Combo CD-drive or 52x CD-drive.

### Software Requirement

The following are the minimal software requirements:

i. Microsoft Windows 7 or a later version of Windows.
ii. Antivirus software to safeguard the system's architecture.
iii. Microsoft SQL Server is a database management system.
iv. Visual Studio 2017 (C#.NET) or a more recent version of Visual Studio.

### System Testing

This entails putting the proposed system to the test using real data to ensure that design and code flaws are addressed, as well as validating the overall system. When the subsystems are connected to a controller to form the overall system, system testing is performed. The following are the steps and processes that are involved in system testing: -

1. Testing of individual units.
2. Module evaluation.
3. Testing of subsystems
4. Acceptance Testing is a term that refers to the process of determining

**1. Unit Testing:** This is the most basic level of testing, in which the individual units that make up a module are tested to ensure that they work properly.
**2. Module Testing:** This technique entails testing each module individually as a new system is built.
**3. Subsystem Testing:** This is the next stage of the testing process, in which modules are combined to form subsystems. Subsystem testing is typically focused on module interfaces.
**4. Acceptance testing:** The system is run and it is discovered that the system works with genuine profiles or real data, i.e. data that is supposed to be manipulated.

### SYSTEM DOCUMENTATION

This provides an overview of the information contained in the program's main

*Corresponding author: Hassan, O. S. ✉ alhassan77077@gmail.com ✉ Department of Computer Science, University of Science and Technology, Osara, Kogi State. 

structure. The program is built in such a way that it will handle practically all aspects of protecting suitable data files and so on.


**Figure 4.2:** Admin Login page

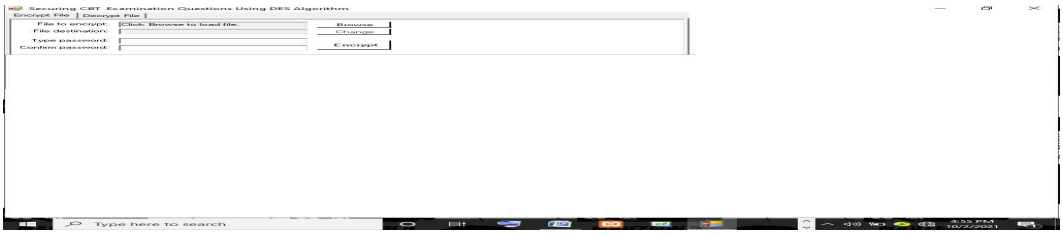


**Figure 5:** Front End

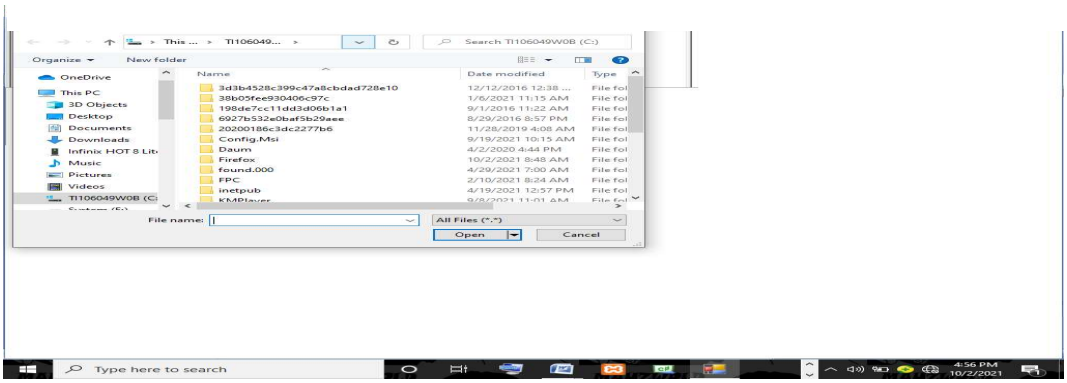


**Figure 6:** Select file to Encrypt

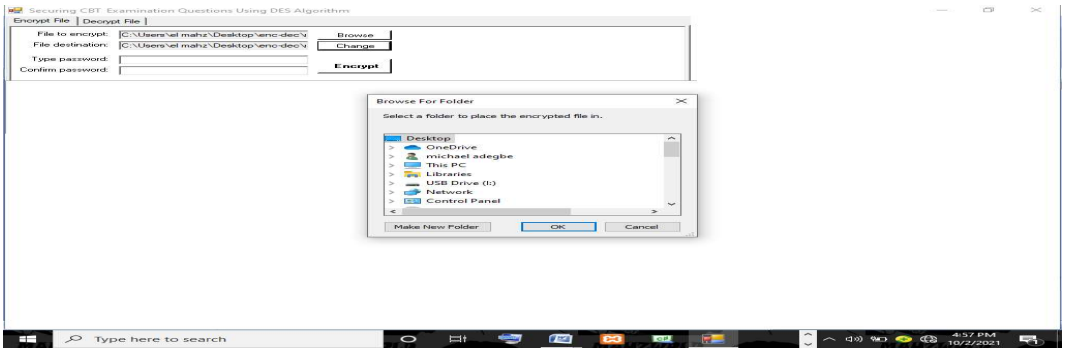


Figure 7: **Select Destination for Encrypt File**

*Corresponding author: Hassan, O. S. alhassan77077@gmail.com Department of Computer Science, University of Science and Technology, Osara, Kogi State. 

JOURNAL OF SCIENCE TECHNOLOGY AND EDUCATION 10(4), DECEMBER, 2022
ISSN: 2277-0011; Journal homepage: www.atbuftejoste.com

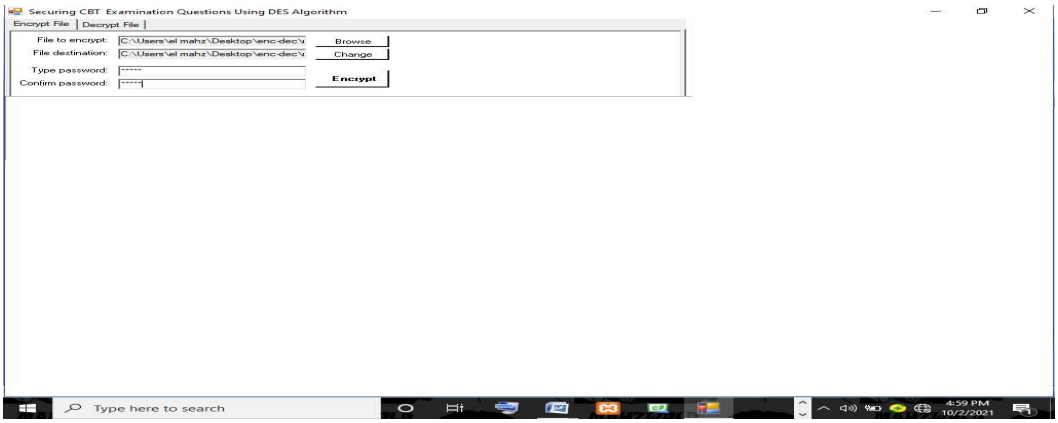


**Figure 8:-** Insert a secret key

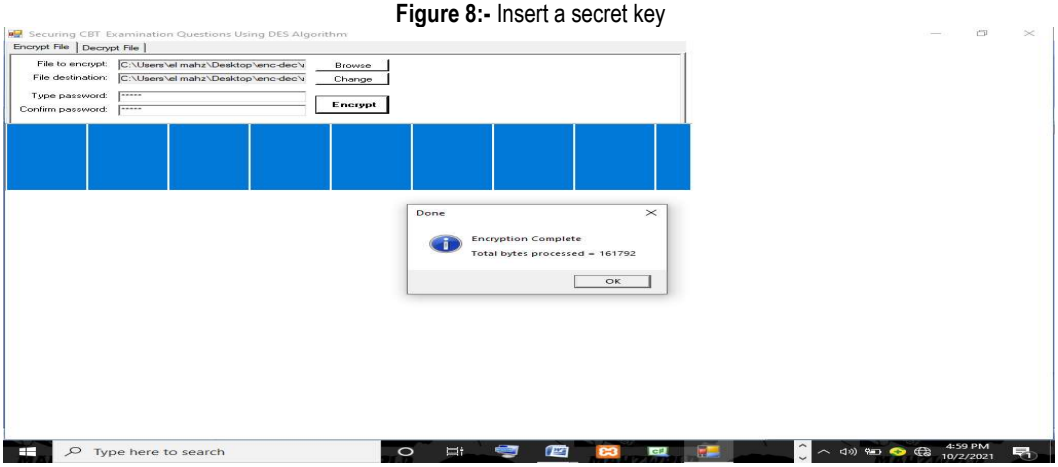


**Figure 9:- File successfully Encrypt**

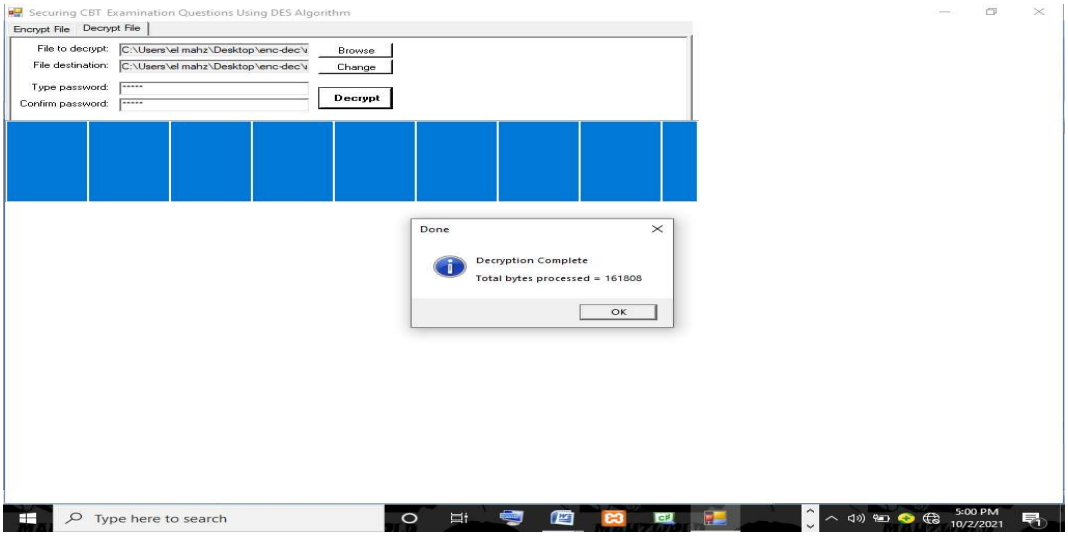


**Figure 10:-**File successfully Decrypt

*Corresponding author: Hassan, O. S. ✉ alhassan77077@gmail.com ✉ Department of Computer Science, University of Science and Technology, Osara, Kogi State. 

## PERFORMANCE EVALUATION

Table 1 below describes the difference between the old system and the new system performance.

**Table 1:-** Performance rate of the two system

| S/N | Performance | New system | Old system |
|---|---|---|---|
| 1 | Speed | 90% fast | 60% |
| 2 | Security method used | Encryption/Decryption process (secret key) | Authentication process (username & password) |
| 3 | Safety rate | More secured and safeguard | Can be easily cracked |
| 4 | Efficiency | More efficient | Less efficient |

The new system will be a stand-alone system in which CBT examination questions will be encrypted and downloaded before being stored in a folder where a penetrator will be unable to access the questions if an attempt is made, because when encrypted, the questions will be downloaded in cipher form and can only be in plaintext when the encrypted file containing the questions is uploaded from the stored folder into that same system.

## CONCLUSION AND RECOMMENDATIONS

We were able to demonstrate the implementation of the Data Encryption Standard and how it works through this academic work, achieving the whole goal of informing the public about the importance of securing test questions and data in computer systems.

We therefore recommend that staff and management, as well as any other institution with a similar structure and organizational framework, use this Academic work for the following reasons:

1. The research study was successful in resolving the data security issue.
2. It also assists the admin in logging in and viewing the encryption/decryption platform, which allows them to encrypt and decrypt data.

## REFERENCES

Adil Yazdeen, A., Zeebaree, S. R. M., Mohammed Sadeeq, M., Kak, S. F., Ahmed, O. M., & Zebari, R. R. (2021). FPGA Implementations for Data Encryption and Decryption via Concurrent and Parallel Computation: A Review. *Qubahan Academic Journal*, *1*(2), 8–16. https://doi.org/10.48161/qaj.v1n2a38

Akande, O. N., Abikoye, O. C., Kayode, A. A., Aro, O. T., & Ogundokun, O. R. (2020). A Dynamic Round Triple Data Encryption Standard Cryptographic Technique for Data Security. In *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics): Vol. 12254 LNCS*. Springer International Publishing. https://doi.org/10.1007/978-3-030-58817-5_36

Mohammed, M. S. (2021). *Image Composition Using Data Encryption Standard ( DES ) Output Result Over the Internet 48*, 199–214.

Permana, A. A., Nurnaningsih, D., Studi, P., Informatika, T., Teknik, F., & Tangerang, U. M. (2020). *Application of cryptography with data encryption standard (des) algorithm in picture 1,2*. 82–87.

Plata, I. T., Panganiban, E. B., & Bartolome, B. B. (2019). *International Journal of Advanced Trends in Computer Science and Engineering Available Online at http://www.warse.org/IJATCSE/static/pdf/file/ijatcse30852019.pdf A Security Approach for File Management System using Data Encryption Standard ( DES ) algorithm*. *8*(5).

Sumartono, I., Putera, A., & Siahaan, U. (2018). *Encryption of DES Algorithm in Information Security*. 264–274.

Zebua, T. (2018). *Encoding the Record Database of Computer Based Test Exam Based on Spritz Algorithm*. *April*. https://doi.org/10.24843/LKJITI.2018.v09.i01.p06

*Corresponding author: Hassan, O. S. ✉ alhassan77077@gmail.com ✉ Department of Computer Science, University of Science and Technology, Osara, Kogi State.* 