https://rijournals.com/engineering-and-physical-sciences/

RESEARCH INVENTION JOURNAL OF ENGINEERING AND PHYSICAL SCIENCES 4(1):90-98, 2025

©RIJEP Publications

ONLINE ISSN: 1115-9057

PRINT ISSN: 1597-8885

https://doi.org/10.59298/RIJEP/2025/419098

Design and Implementation of an enhanced Cryptography model using the combination of Blowfish and RSA for the Security of Computer-based Integrated School Information Management System

[1]Chinenye P. Ikeagwu; [2]Virginia E. Ejiofor; [3]Orji Everistus Eze and [4]Godspower Akawuku

[1,2,4]Department of Computer Science, Nnamdi Azikiwe University, Awka, Anambra State, Nigeria
[3]Department of Computer Science Federal Polytechnic Ohodo, Enugu, State, Nigeria
Email: Cp.ikeagwu@gmail.com

ABSTRACT

Data transmission threats have become a critical concern for organizations and individuals globally. Information's most valuable assets, alongside human resources, and the compromise of organizational data can lead to significant damage or even destruction. Consequently, organizations invest substantial resources to ensure the security of their data. The primary focus of the research is the development of a secure cryptographic model for a computer-based integrated school information management system (SIMS). The study addresses the critical need for secure data transmission between users and employs advanced cryptographic techniques to protect against intruders. To achieve this, the research integrates two cryptographic algorithms: RSA, an asymmetric encryption model, and Blowfish, a 64-bit symmetric system encryption model. This hybrid cryptographic framework referred to as Paschaline, is designed to enhance overall message security while improving system performance. The developed system incorporates biometric, and digital monitoring tools to ensure accurate supervision and inspection of school activities. Features include a surveillance camera for classroom monitoring biometric systems for teacher presence verification and teacher image capture for easy identification. The study utilized object-oriented Analysis and Design Methodology (OOADM) for system development and deployed technologies such as python, Django, PHP, and MYSQL for implementation, testing in selected schools in one of the zones in Ebonyi state demonstrated the efficiency of the online monitoring system and the reliability of the hybrid cryptographic model. The results confirm that the system ensures the availability, reliability and authenticity of secured data, thereby addressing the challenges of data transmission threats in educational institution.

Keywords: Cryptography, Blowfish, RSA, Information Management System.

Every educational institution has very high regards to their data because they are the force that propel their operations [1]. Compromising these data will definitely impact negatively on their operations. Therefore, security of Computer-based Integrated School Information Management System (CISIMS) has become a crucial component of educational institutions, for enabling the efficient management of student data, academic records, administrative processes, and other relevant information. However, despite the significance of CISIMS data. CISIMS often faces various security challenges, jeopardizing the confidentiality, integrity, and availability of sensitive data [2]. Although, various cryptographic model has been applied for the security of computer and for data authentications in the past. Such models like, Advanced Encryption Standard (AES), Digital Signature (DS) and RSA encryption model, and Elliptic Curve Cryptography (ECC), digital signature and image steganography amongst others. These Models have recorded certain limitations which include lack of integrity and reliability, violation of individual privacy, susceptible to brute force attack due to data symmetry, lack of terminal security leading to inability to implement end-to-end security and high computational cost that increases linearly with the number of messages [3]. It is against this background that the present study is set to create and develop cryptographic model for the security of computer based integrated school information management system [4]. To achieve this, the researcher adopted the use of two models such as Blowfish and RSA algorithms to create and develop a new model that will ensure accurate, efficient and effective Security of Computer-based Integrated School Information Management System (CISIMS). Moreover, to the best knowledge of the present researcher, these two models of cryptography (Blowfish and RSA algorithms) have not been

combined by other researchers for the development of the security of computer based integrated school information management system. Therefore, the present study will develop cryptographic model for the security of computer based integrated school information management system using RSA and Blowfish algorithms to help fill the limitations and the research gaps which other studies have created [5].

Analysis of the Proposed System

Due to the emergence of the information technology in the world today, most institution seek to develop information management system that manage their data and information. Every educational institution has very high regards to their data because they are the force that propel their operations. Compromising these data will definitely impact negatively on their operations [6]. And that exactly what most institutions are suffering because they leave the developed system open and it becomes vulnerable to third parties. Therefore, security of Computer-based Integrated School Information Management System (CISIMS) using cryptographic model has become a crucial component of educational institutions, for enabling the efficient management of student data, academic records, administrative processes, and other relevant information [7]. However, despite the significance of CISIMS data, CISIMS often faces various security challenges, jeopardizing the confidentiality, integrity, and availability of sensitive data.

As a result of the above challenges, the researcher adopts the use of two methods of the algorithm

Blowfish Algorithm

The Blowfish encryption approach is applied for data security on the client-side, which saves time consumed on the server-side instead [8]. The weakness of this approach is that as the file size increases, more time is required for compression and encryption, and hence, performance is compromised. Blowfish is a symmetric encryption algorithm, meaning that it uses the same secret key to both encrypt and decrypt messages. Blowfish is also a block cipher, meaning that it divides a message up into fixed length blocks during encryption and decryption. The block length for Blowfish is 64 bits; messages that aren't a multiple of eight bytes in size must be padded. Blowfish is public domain, and was designed by Bruce Schneier expressly for use in performance-constrained environments such as embedded systems. It has been extensively analyzed and deemed "reasonably secure" by the cryptographic community. Implementation examples are available from several sources, including the one by [9]. The proposed methodology for blowfish resolves the issue of reducing encryption time and space by compressing the data file. The time efficiency of the proposed approach is tested by using three different file sizes. The results are then compared by calculating encryption time for non-compressed and compressed files. Using this approach, if the file is compressed before applying encryption strategy, encryption time and the space required to save this file can be decreased [10]. However, for larger files sizes, its performance is not discussed. As the number of users increases, key management will be a challenging issue.

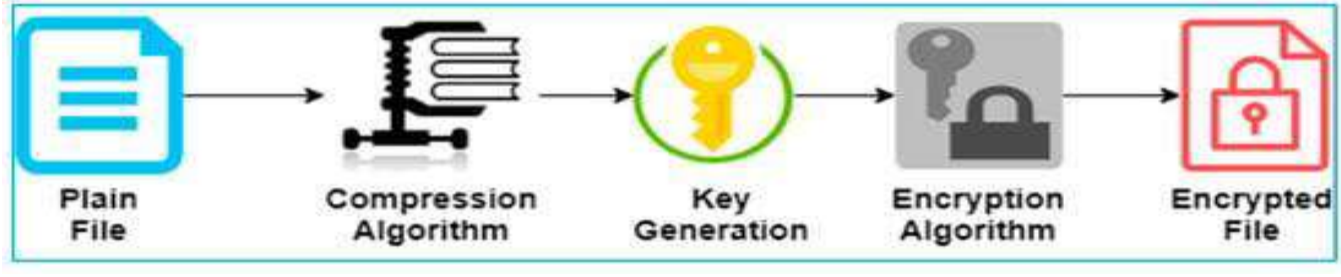


Figure 1 Blowfish encryption process adapted from [9].

Step-by-step implementation of Blowfish Algorithm.

Step1: Generation of sub keys:
Step2: initialize Substitution Boxes:
Step3: Encryption:
Step 4: Post-processing:

RSA Algorithm

RSA encryption is a public-key encryption technology developed by RSA Data Security. The algorithm is based on the difficulty in factoring very large numbers. Based on this principle, the RSA encryption algorithm uses prime factorization as the trap door for encryption. Deducing an RSA key, therefore, takes a huge amount of time and processing power. It is the standard encryption method for important data, especially data that is transmitted over the Internet. RSA is built into many common software products, including Microsoft's Internet Explorer. In this technique the message sender generates a public key to encrypt the message and a private key is generated by the receiver by using the secured database. The attacker can be confused by this technique because the incorrect private key can still decrypt the data but that data will be in another form i.e. that will not be the original message. This is a much complex technique. After generating the public and private keys, the process of

encryption is started. In both encryption and decryption methods the functions are created relative to the value of public and private keys [11].
Methodologically, the RSA algorithm falls under asymmetric cryptography algorithm. Asymmetric actually works on two different keys i.e. Public Key and Private Key. The Public Key is given to everyone and the Private Key is kept private.

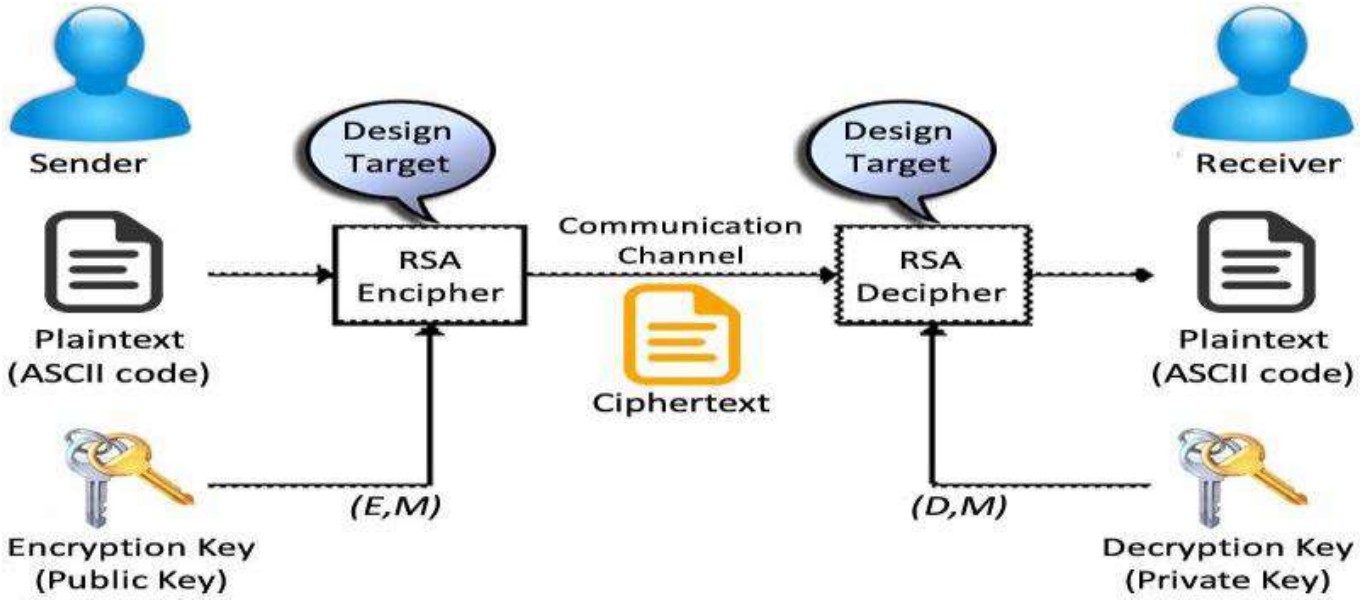


Figure: 2 RSA Encryption structure

Step by Step implementation of RSA Algorithm

Step 1: Choose two large prime numbers (p and q)
Step 2: Calculate n = p*q and z = (p-1)(q-1)
Step 3: Choose a number e where 1 < e < z.
Step 4: Calculate d = e-1mod(p-1)(q-1)
Step 5: You can bundle private key pair as (n,d)
Step 6: You can bundle public key pair as (n,e)

To create a new model for the security of computer based integrated school information management system. Moreover, to the best knowledge of the researcher, the related work above was focused on other types of cryptographic model for the security of computer and not necessarily the combination of Blowfish and RSA based integrated school information management system. It is against this backdrop that the present study attempts to fill the gap by creating a new model, developing and implementing it through the combination of these two models (Blowfish and RSA) for the security of computer based integrated school information management system.

Input Analysis of the New System

This refers to the various data that are supplied to the system that determine the output of the system. Users' data are supplied into the system through the input forms such as the subscription forms, evaluation response form, and user bio-data form.

Output Analysis of the New System

Output comprises of a set of processed input from the system. The system can produce output in various formats. However, in this work our output shall be generated from notification alerts, dialog messages and feedback requests.

Process Flow in the New System

Processes describe how data is being managed in order to generate an output from the system. That is, the steps that data must pass through for it to generate the needed result from the system. Our model shall use cryptographic algorithms and keys to convert plaintext data into cipher text. This is to protect sensitive data from unauthorized access or interception during transmission or storage. Secondly, the model shall use harsh function to convert data of any size into a fixed-size string of characters. The resulting hash value will be unique to the input data, such that, even a slight change in the input will produce a significantly different hash value [12]. This will be very useful in verifying the integrity of data by warding off data alterations. Thirdly, our model shall use Digital signatures to authenticate the integrity and origin of digital documents or messages. By using asymmetric cryptographic algorithms, such as RSA or ECDSA, to generate a unique signature for a specific piece of data. The signature can be verified using the corresponding public key, ensuring that the data has not been tampered with and that it originated from the expected sender [13].

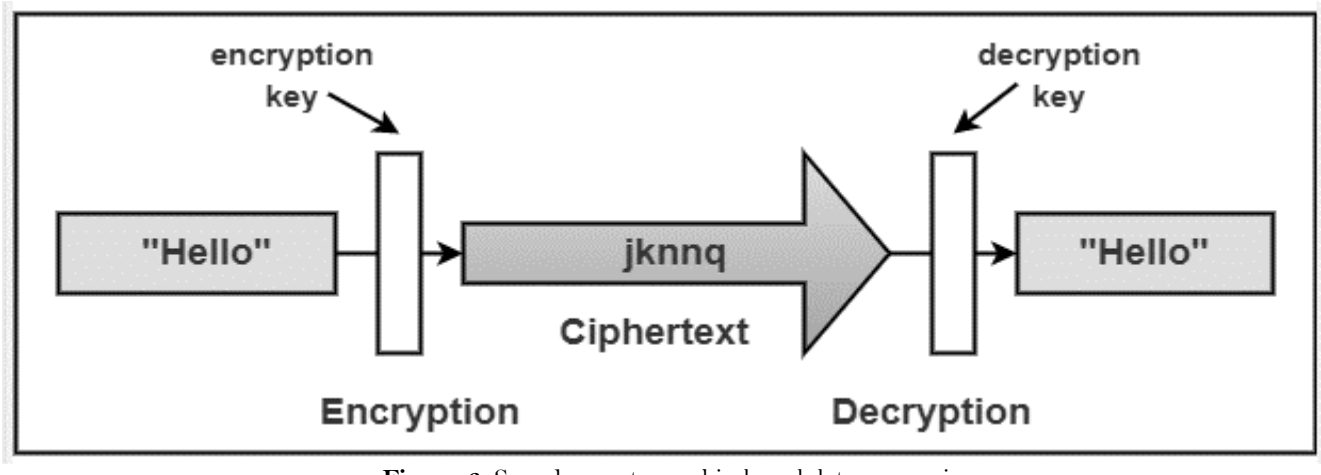


Figure 3: Sample cryptographic-based data processing

Class Diagram of the Proposed System

In software engineering, a class diagram in the Unified Modelling Language (UML) is **a** type of static structure diagram that is used to model the structure of a system by showing the system's classes, their attributes, operations (or methods), and the relationships among objects. It illustrates the relationships and source code dependencies among classes

The purposes of class diagram therefore are to:

i. Show the static structure of classifiers in a system

ii. provide basic notation for other structure diagrams prescribed by UML

iii. model systems from business perspective

Use Case Diagram of the Proposed System

Use case modelling was originally developed by Jacobson in the 1990s and was incorporated into the first release of the UML in 1999. A use case modelling is widely used to support requirements elicitation. It can also be taken as a simple scenario that describes what a user expects from a system. Each use case represents a discrete task that involves external interaction with a system. In its simplest form, a use case is shown as an ellipse with the actors involved in the use case represented as stick figures, describing the interactions between a system and its environment. The details of the interactions involved in a high-level use case may be documented in a sequence diagram.

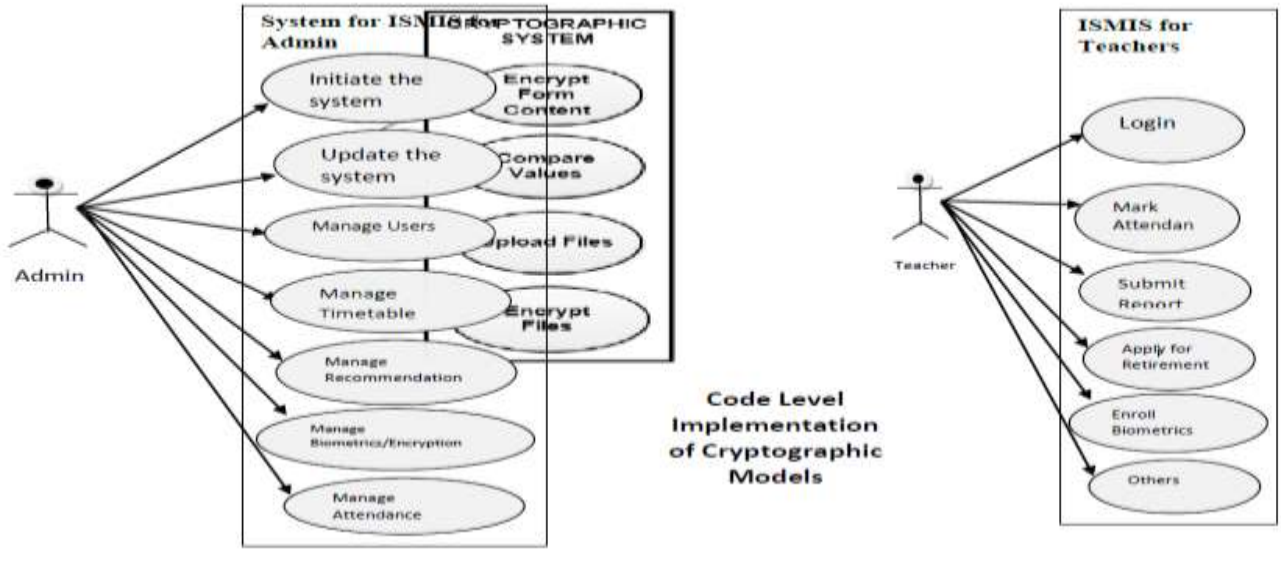


Figure 4: The Cryptographic Process in the New System

The figure 4 above illustrates how the new system works. The users which is otherwise referred to as actors comprises of the users which is made up of the students, the teachers and the system administrators [14]. Whatever information/data that is

passed into the system is encrypted, with the value calculated and stored and during future operation on the submitted data, the value is once again calculated and compared with the initial value. If discrepancy is found, the system raises alarm but if none, the process continues peacefully. More so, every file and folder uploaded into the system is encrypted but when a legitimate user requests for the file, it will be decrypted before it is displayed to the user.
For instance, the student can create and maintain their profile in the system while a teacher can create profile, upload course materials, upload assignments and grade them while the system administrator can log into the system, generate report, manage students and staff records, including courses. All these activities are duly protected cryptographically in the system.

RSA (Rivest-Shamir-Adleman)

Purpose: RSA is a public-key encryption algorithm used for securing data during transmission. It is particularly effective for encrypting small amounts of data and for digital signatures.

Features:

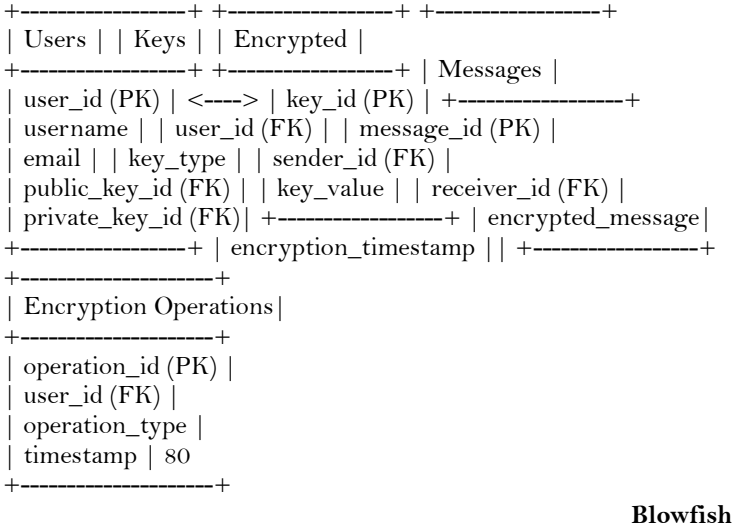
Public and Private Keys: RSA uses a pair of keys – one for encryption (public key) and one for decryption (private key).
Encryption and Digital Signatures: It ensures secure data transmission and verifies the authenticity and integrity of messages.
Computational Intensity: RSA is computationally expensive and is not ideal for encrypting large volumes of data directly.
Using an ORM like **SQLAlchem**Using an ORM like **SQLAlchemy** (Python) or **Hibernate** (Java), we can map these database tables to objects. Here's a simplified example using Python and SQLAlchemy:

python Copy code

```
from sqlalchemy import create_engine, Column, Integer, String, ForeignKey
from sqlalchemy.ext.declarative import declarative_base
from sqlalchemy.orm import relationship
Base = declarative_base()
# User table
class User(Base):
__tablename__ = 'users'
user_id = Column(Integer, primary_key=True)
username = Column(String)
public_key_id = Column(Integer, ForeignKey('keys.key_id'))
private_key_id = Column(Integer, ForeignKey('keys.key_id'))
public_key = relationship("Key", foreign_keys=[public_key_id])
private_key = relationship("Key", foreign_keys=[private_key_id])
# Key table (public/private keys)
class Key(Base):
__tablename__ = 'keys'
key_id = Column(Integer, primary_key=True)
user_id = Column(Integer, ForeignKey('users.user_id'))
key_type = Column(String) # 'public' or 'private'
key_value = Column(String) # Key value (e, n) or (d, n)
user = relationship("User", back_populates="keys")
# Prime Numbers table
class Prime(Base):
__tablename__ = 'primes'
prime_id = Column(Integer, primary_key=True)
prime_value = Column(Integer)
# Encrypted Messages table 79
class EncryptedMessage(Base):
__tablename__ = 'encrypted_messages'
message_id = Column(Integer, primary_key=True)
sender_id = Column(Integer, ForeignKey('users.user_id'))
receiver_id = Column(Integer, ForeignKey('users.user_id'))
encrypted_message = Column(String)
sender = relationship("User", foreign_keys=[sender_id])
receiver = relationship("User", foreign_keys=[receiver_id])
# Create engine and session
engine = create_engine('sqlite:///:memory:')
Base.metadata.create_all(engine)
```

Concept of RSA cryptographic model

Here is an illustratiion of how RSA encryption integrates with an Object-Relational Database in the context of a system:
plaintext
Copy code



Blowfish

Purpose: Blowfish is a symmetric-key block cipher designed for fast encryption and decryption. It is efficient and suitable for encrypting large volumes of data.

Features

Symmetric Key: Blowfish uses the same key for both encryption and decryption, requiring secure key management.
Speed and Efficiency: It is fast and supports variable key lengths, making it suitable for encrypting large datasets.
Block Cipher: It operates on blocks of data, which is effective for securing large chunks of information.

Program Algorithm

The algorithm could be a pseudocode or a flowchart that represent the logic flow of the program operations. It shows the flow of control of the application for the implementation of the information management system. The flow of logic makes it easy for the implementation since users can follow the steps to implement the system. This provides the developer a guide in the process of developing and integrating the system into design provided for the information management system and security system in the previous [15]. The algorithm also helps in the process of providing the avenue for the system to process its major task using the steps outlined in the system.

Integrated School Monitoring System Pseudo code

Step 1: Start
Step 2: server variables
Step 3: Declare variable for school integrated monitoring system
Step 4: Create user interface
Step 6: Create style sheet component for the system presentation
Step 7: Create database Components for integrated school monitoring system
Step 8: Assign fields' variable
8.1 Assign content record parameters for the integrated School monitoring system
8.2 create database components
8.3 store components using necessary SQL query
Step 9: Using java script facility
Step 10: Create a class of the objects and their attributes (properties)
Step 11: Assign classes for property operations of events
Step12: Determine identifiers for server-side PHP event properties
Step 13: Determine MYSQL-PHP operations
Step 14: Connect PHP logic with queries and with GUI browsers forms and java script components.
Step 15: Using MYSQL
15.1: Link input object data to databases
15.2: Add content to Database
Step 16: Using the form Object variable
16.1: integrate form object with modules.

16.2: Test interaction
Step 17: Test Net connection string
Step 18: Initialize file Upload
Step 19: Check file size
19.1: if (size < max_size) then
Upload file
Else
Reject upload
Else if
Step 20: if file upload is successful then
Step 20.1: create storage for uploaded papers
Step 20.2 store paper files in approved other
Step 21: deploy in the web server for extension
Step 22: Stop

Code-Level Paschaline Model Code Implementation Using PHP

Paschaline combines RSA and Blowfish encryption cryptography model in PHP:

```
<?php
// RSA Encryption
function rsa_encrypt($public_key, $plaintext) { $encrypted = '';
openssl_public_encrypt($plaintext, $encrypted, $public_key);
 return base64_encode($encrypted);
 } function rsa_decrypt($private_key, $ciphertext) { $decrypted = ''; openssl_private_decrypt(base64_decode($ciphertext), $decrypted, $private_key);
 return $decrypted; }
// Blowfish Encryption
function blowfish_encrypt($key, $plaintext) {$iv = openssl_random_pseudo_bytes(8);
$ciphertext = openssl_encrypt($plaintext, 'BF-CBC', $key, 0, $iv); return base64_encode($iv . $ciphertext); } function blowfish_decrypt($key, $ciphertext) {$ciphertext = base64_decode($ciphertext);
$iv = substr($ciphertext, 0, 8);
$ciphertext = substr($ciphertext, 8);
$plaintext = openssl_decrypt($ciphertext, 'BF-CBC', $key, 0, $iv);
return $plaintext; }
// PASCHALINE MODEL
/*This model uses RSA for asymmetric encryption (to encrypt the Blowfish key) and Blowfish for symmetric encryption (to encrypt the data). The hybrid_encrypt function encrypts the Blowfish key with the public RSA key and then encrypts the data with the Blowfish key. The hybrid_decrypt function decrypts the Blowfish key with the private RSA key and then decrypts the data with the decrypted Blowfish key. Note that this example uses the `openssl` extension in PHP, which provides a wrapper for the OpenSSL library. Make sure to handle errors and exceptions properly, and use secure key management practices.
*/ // Combined Model resulting to Paschaline Model
function hybrid_encrypt($public_key, $blowfish_key, $plaintext) {$encrypted_blowfish_key = rsa_encrypt($public_key, $blowfish_key); $encrypted_data = blowfish_encrypt($blowfish_key, $plaintext); return $encrypted_blowfish_key . ':' . $encrypted_data; } function hybrid_decrypt($private_key, $ciphertext) { list($encrypted_blowfish_key, $encrypted_data) = explode(':', $ciphertext); $decrypted_blowfish_key = rsa_decrypt($private_key, $encrypted_blowfish_key); $decrypted_data = blowfish_decrypt($decrypted_blowfish_key, $encrypted_data); return $decrypted_data; }
// Usage:
$public_key = '-----BEGIN PUBLIC KEY-----
...your public key here...
-----END PUBLIC KEY-----';
$private_key = '-----BEGIN RSA PRIVATE KEY-----
...your private key here...
-----END RSA PRIVATE KEY-----';
$blowfish_key = 'your_secret_blowfish_key_here'; // 16-byte key
$plaintext = 'Hello, World!'; $ciphertext = hybrid_encrypt($public_key, $blowfish_key, $plaintext); echo 'Ciphertext: ' . $ciphertext . PHP_EOL; $decrypted_text =
hybrid_decrypt($private_key, $ciphertext); echo 'Decrypted text: ' . $decrypted_text . PHP_EOL; ?>
```

SUMMARY, CONCLUSION AND RECOMMENDATION

In this research, the development of a cryptographic model is a central focus, particularly its application within a computer-based integrated information management system. This initiative underscores the critical need for robust monitoring and security measures to ensure the confidentiality, integrity, and availability of sensitive school data. The importance of such system to schools cannot be overstated, as they play a pivotal role in streamlining operations, safeguarding information and enhancing overall institutional efficiency. For school to achieve positive outcomes and improve the standard of Education in Nigeria, securing Teachers' and students' data effectively is imperative. Monitoring within the school system involves a holistic approach to safeguarding both the structures and the content of information, particularly staff and student data. This includes implementing comprehensive measures to protect such data from damage, loss, or theft by enforcing strict control mechanism within the system. Schools rely heavily on their information management system and data security frameworks to prevent unauthorized access to critical organizational information. Despite this reliance, instances occur where teachers inadvertently expose sensitive information to hackers or vulnerabilities, allowing hackers, crawlers, spammers to invade privacy and gain unauthorized access. These challenges have necessitated the integration of ICT-based security solutions into school information management systems. The modern world is often referred to as a global village, with ICT playing a pivotal role across educational, political, economic, and social sectors. Technology has become an indispensable tool for organizations to compete and thrive, and data security is a cornerstone of any effective school management system. The stakes are particularly high in schools, as student records encompass sensitive personal information, academic data, financial details, and even health records. To address this concern, Cryptography has been adopted as a fundamental method for securing data within the the information management system. Cryptographic techniques are critical for ensuring the confidentiality of data communications, including telephone lines, fax transmissions, e-mails, financial transactions, medical histories, e-banking activities, and other sensitive operations requiring secure communication channels.

REFERENCES

1. Dale R. Globalization and education: Demonstrating a" common world educational culture" or locating a" globally structured educational agenda"? Educational Theory. 2000 Oct 1;50(4):427.
2. Ahanger AS, Masoodi FS, Khanam A, Ashraf W. Managing and Securing Information Storage in the Internet of Things. InInternet of Things Vulnerabilities and Recovery Strategies 2024 (pp. 102-151). Auerbach Publications.
3. Wornow M, Xu Y, Thapa R, Patel B, Steinberg E, Fleming S, Pfeffer MA, Fries J, Shah NH. The shaky foundations of large language models and foundation models for electronic health records. npj digital medicine. 2023 Jul 29;6(1):135.
4. Crowley E. Information system security curricula development. InProceedings of the 4th conference on Information technology curriculum 2003 Oct 16 (pp. 249-255).
5. Murtaza MH, Tahir H, Tahir S, Alizai ZA, Riaz Q, Hussain M. A portable hardware security module and cryptographic key generator. Journal of Information Security and Applications. 2022 Nov 1;70:103332.
6. Wasserman EA. Detecting response-outcome relations: Toward an understanding of the causal texture of the environment. InPsychology of learning and motivation 1990 Jan 1 (Vol. 26, pp. 27-82). Academic Press.
7. Csapó B, Ainley J, Bennett RE, Latour T, Law N. Technological issues for computer-based assessment. Assessment and teaching of 21st century skills. 2011 Oct 13:143-230.
8. Hassinen M, Mussalo P. Client controlled security for web applications. InThe IEEE Conference on Local Computer Networks 30th Anniversary (LCN'05) l 2005 Nov 17 (pp. 7-pp). IEEE.
9. Josephra V. and Shamina, R. B. (2017). Performance Enhancement of Blowfish Encryption Using RK-Blowfish Technique. *International Journal of Applied Engineering Research*; 12, (20); pp. 9236-9244. Research India Publications. http://www.ripublication.com 9236
10. Seth B, Dalal S, Jaglan V, Le DN, Mohan S, Srivastava G. Integrating encryption techniques for secure data storage in the cloud. Transactions on Emerging Telecommunications Technologies. 2022 Apr;33(4):e4108.
11. Yadav J,, Sharma S, Sharma P. (2012). Modified RSA Public Key Cryptosystem Using Short Range Natural Number Algorithm,*Computer Science, Mathematics* https://api.semanticscholar.org/CorpusID:124243881
12. Chi L, Zhu X. Hashing techniques: A survey and taxonomy. ACM Computing Surveys (Csur). 2017 Apr 4;50(1):1-36.
13. Caelli WJ, Dawson EP, Rea SA. PKI, elliptic curve cryptography, and digital signatures. Computers & Security. 1999 Jan 1;18(1):47-66.
14. Lamb R, Kling R. Reconceptualizing users as social actors in information systems research. MIS quarterly. 2003 Jun 1:197-236.
15. Peffers K, Tuunanen T, Rothenberger MA, Chatterjee S. A design science research methodology for information systems research. Journal of management information systems. 2007 Dec 1;24(3):45-77.

CITE AS: Chinenye P. Ikeagwu; Virginia E. Ejiofor; Orji Everistus Eze and Godspower Akawuku (2025). Design and Implementation of an enhanced Cryptography model using the combination of Blowfish and RSA for the Security of Computer-based Integrated School Information Management System. RESEARCH INVENTION JOURNAL OF ENGINEERING AND PHYSICAL SCIENCES 4(1):90-98