Implementation of Advanced Encryption Standard Cryptographic Algorithm in a Test Bank System

LAMPEL B. BEROL
http://orcid.org/0000-0002-2477-8971
lampelberol@gmail.com
Saint Michael College of Caraga
Nasipit Agusan del Norte
Philippines

Gunning Fog Index: 11.43 Originality: 98%
Flesch Reading Ease: 48.56 Plagiarism: 2%
Grammar Check: 99%

ABSTRACT

Cryptography is a method that provides assurance and validity from users to secure information from infiltrators. This study aimed to develop a Test Banking System with the integration of Advanced Encryption Standard cryptographic algorithm available to enhance the system vulnerability against any unexpected attacks, reliability, and speed of execution. The algorithm will be integrated for the secure generation and retrieval of information on the Test Bank system. The primary purpose was to create a storage of test questions that are based on Bloom’s Taxonomy six level cognitive domain. The proposed system followed the agile developmental model which promote quick response to changing environments, changes in user requirements, accelerated project deadlines, and the like. The respondents answered the survey instrument to evaluate the acceptability level of the project 4.34 as mean or the average score, which is considered an average rating in the scale range. As a result, the system will provide a more secure and private way in terms of questionnaire transmittal (which means that the sender will be able to send and receive encrypted test question over the network).
KEYWORDS

Cryptography, advanced encryption standard, algorithm, Bloom's Taxonomy, Philippines

INTRODUCTION

The Examination is a formal test of a person’s knowledge or proficiency in a particular subject or skill (Alagbe et al., 2017). It plays an important role as it provides benefits for both the instructor and the student. The instructor can assess the students through by giving direct assessment through an exam and students can use self-assessment for them to monitor their studies.

Through the interviews conducted by the proponent with the dean, instructors, and program heads in the different department, the proponent found out most of the higher education institutions (HEIs) are still using the manual process of producing test questionnaires. It starts with the instructors making the syllabus that contains the topics for the whole semester. It is followed by creating of test questionnaires based on the table of specification that follows Bloom’s taxonomy aligned to the topics indicated in the syllabus of the instructor (Adams, 2015). Then upon submission, the program head and dean of the specific department will now check the test questionnaire and table of specification of the instructor if the questions conform to the appropriate cognitive level domain requirements as specified in the syllabus (Musah, Al-Hudawi, Tahir, & Kamil, 2015).

Several problems were observed using the manual process of creating, submitting, checking and approving of test questionnaire and table of specification. The process is so tedious and time-consuming. No storing of test questions were done to make it reusable in the future (Khorsand, 2009. Also, it consumes a lot of papers during the revision of the test questionnaire and table of specification during checking (Ebadi, 2015).

The proponent came up with the idea of proposing a test banking system. The test banking system will enable the instructor to create syllabi, test questionnaire, and table of specification as well as retrieve test questions and test questionnaire depending on the subject they are teaching (Ahmad, Rifen, & Wahab, 2016). The program head can check, approve, reject and put remarks on the test questionnaire that the instructor created. The dean rechecks the test questionnaire then decides to reject or accept the test questionnaire for printing. The proposed system can queue the test questionnaire ready for printing with one default copy of each test questionnaire. The system generates reports such as approved, rejected, produced, pending and late test questionnaire and table of specification list. To secure stored data, an encryption system will be created. The proposed project also offers systems notification, chatting and SMS notification as additional features. By this, it can improve the way of creating, submitting, checking, printing, retrieving and storing of test questionnaires.
OBJECTIVES OF THE STUDY

Generally, the project aimed to design, develop and implement a Test Banking System with Advanced Encryption Standard Cryptographic Algorithm. Specifically, it aimed to:

1. Design and develop a Test Banking System consisting of the following components: user Account module, log-in module, syllabus module, subject list module, exam schedule module, notification module, and report module
2. Use symmetric cryptography algorithm in encrypting and decrypting plaintext data in the Test Bank System; and
3. Test the system performance using ISO 25010 and ISO 9126 software quality characteristics standard for system evaluation.

TECHNICAL BACKGROUND

Symmetric Key Algorithm

Advanced Encryption Standard (AES) is a symmetric block cipher. It means that this cryptographic algorithm uses the same key for both encryption and decryption process that can be used to protect electronic data. The receiver and the sender have to agree upon a single (shared) key (Patil, Narayankar, Narayan, & Meena, 2016).
Advanced Encryption Standard (AES) Algorithm Design

Operations performed in Rijndael state is 4 rows of bytes. The 128 bit key is expanded as an array of 44 entries of 32 bits words; 4 distinct words serve as a round key for each round; key schedule relies on the S-box. This algorithm composed of three layers the Linear Diffusion, Non-Linear Diffusion, and Key Mixing. The figure below shows the High-Level Description of Rijndel Algorithm.

```
State = X
AddRoundKey(State, Key0)
for r = 1 to (Nr - 1)
    a. SubBytes(State, S-box)
    b. ShiftRows(State)
    c. MixColumns(State)
    d. AddRoundKey(State, Keyr)
end for
SubBytes(State, S-box)
ShiftRows(State)
AddRoundKey(State, KeyNr)
Y = State
```

Advanced Encryption Standard Algorithm Steps

Substitution-permutation network is the design principle of AES which has a fixed block size of 128 bit and key a size of 128, 192 and 256 bits with 10, 12 and 14 rounds of encryption respectively. This particular work uses 128 bit key for 10 rounds (excluding initial add round key) of encryption. First and last round of algorithm are different while all other rounds are the same. Encryption and decryption operate 16 bytes of data as [4*4] array named as state arrays. While the encryption round consists of four main steps viz, shift row, substitution of bytes, mix column and add round key, the decryption round consists of inverse operations of encryption. Shift row operation shifts byte of first, second and third rows of state matrix to the left by an offset of 1, 2, and 3 respectively. However, Shift Row operation is not necessarily the first step of AES iteration. It can be interchanged with a byte substitution operation without affecting the results. This operation helps AES block cipher to become four dependent block ciphers. Each byte of state matrix is replaced by corresponding SBox entry in substitution byte step. This operation is highly nonlinear transformation and maps input state matrix to a highly nonlinear set of output state matrix. Mix column operation multiplies a fixed matrix with state matrix in GF(28) while adding round key operation adds state matrix with the key in GF(28). The key expansion module of AES algorithm generates all round key from key inputs and starts by taking substitution of the first four byte of data followed by cyclic rotation and addition of round constants. The result obtained is
added to the first four byte of previous key input to get first four bytes of a new key. It is then added to second row of input key byte to get the second row of a new key and so on.

**METHODOLOGY**

The proponent applies the agile developmental model because it is based upon iterative and incremental process models, it conveys increased value, visibility, and adaptability to changing product requirement and enhancing client satisfaction through fast delivery of working product features and client participation.

**Analysis Phase**

Series of interviews to the different respondents such as the faculty, program head, dean, and the printing in-charge of the institution was conducted during this phase. The researcher gathered the user requirements then analyzed. Data collected such as policies in creating syllabus, test questionnaire, and table of specification was interpreted to produce a complete and final specification of user requirement.

**A. Syllabi generation and approval**

Syllabi can be created when the faculty is loaded with the subject in the indicated semester and the approval can only be done by the department dean. Syllabi must contain the topics, sub topics and the period a topic must be taught by the faculty. It would be the basis of the construction of the test questionnaire.
B. Test questionnaire and Table of specification submission and approval

Based on the policy of every institution, the submission of test questionnaire with the table of specification is a week before the set exam schedule. The construction of test questionnaire must follow the six cognitive domain of Bloom’s taxonomy which includes knowledge, application, comprehension, evaluation, analysis, and synthesis.

C. Printing of test questionnaire policy

Test questionnaire to be printed must be approved by the department dean and queued to the printing in-charge, copies of test questionnaire to be printed must base on the number of students enrolled in the subject.

Requirements Analysis

This phase shows the use-case description and class diagram of the system that illustrates where the actor can access the core functions and elements of the proposed system.

Use Case Diagram of Test Bank System with AES Cryptographic Algorithm

The use case log-in described in the figure above shows how the user logs into the system. The basic flow of this use case starts when an actor wishes to log into the system. The system request that the actor should enter his/her username and password. The system validates the entered username and password and logs the actor into the system. If in the basic flow the actor enters an invalid name or password, the system displays an error message. The actor can choose to either return to the beginning of the basic flow or
cancel the log-in, at which point the use case ends. If the use case was made successful, the actor is now logged into the system. If not, the system state is unchanged.

The use case Manage Syllabus Module describes how the user view loaded subjects and create syllabus. The user can add, edit, and search specific subjects for them to create the syllabus. If the user wants to delete the syllabus generated the user should contact and get permission from the admin.

The provide subject lists module offer the user to create test questionnaire and table of specification based on the syllabi/ syllabus made in the Manage Syllabus module. The use case illustrates the process of how the user can select and provide question type per item and assign a point.

Further, Set Exam Schedule use case allows a user that has administrative or delegated administrative role privileges to set the date of the examination, the start and end date of the submission of test questionnaire and table of specification.

On the other hand, the use case Queue of examination papers shows the user the sequence of the submitted test questionnaire that is already checked by the program head and approved by the respective department deans. Therefore, the user can be notified that shown in the notification use case on what is the status of the submitted requirements.

Lastly, the Use case manage report demonstrates how the user retrieves reports from the system. If the user wants to retrieve and print files from records, the user clicks print and in the outset, the use case ends.

**Design Phase**

In this phase, the systems analysts developed models and prototypes that represented all system processes, inputs, and outputs. The system design was based on the module and scope that the proponent constructed and approved by the end user.
The system design requires hardware infrastructure which includes a server, computers and another communication medium. A server can guarantee that records are stored in a specific location. For later use, records can be accessed from the server. The system is useful and runs in personal computers: desktop or laptop. Computers can communicate with other computers if it is connected to a network. A shared printer plays a big role in generating a report. User can print report in a shared printer even it is not directly connected to the unit.

Implementation Phase

In this phase the software and hardware requirements specifications are discussed; the distribution of the user respondents and the survey tool used to evaluate the system.

Hardware Requirements

The following hardware requirements are needed to run the Test Bank System with AES Cryptographic algorithm application.

Table 1. Personal Computer/Laptop Hardware Requirements

<table>
<thead>
<tr>
<th>Specification Name</th>
<th>Minimum Requirements</th>
</tr>
</thead>
<tbody>
<tr>
<td>Hard disk</td>
<td>120gb or higher</td>
</tr>
<tr>
<td>Memory</td>
<td>2gb or higher</td>
</tr>
<tr>
<td>CPU</td>
<td>1.90ghz Intel Celeron</td>
</tr>
</tbody>
</table>

Personal Computer/ Laptop with minimum hardware requirements stated above is the primary requirement to deploy the Test Bank system. The PC shall be connected to a Local Area Network accessing the server that stores the database of the proposed system (Erickson, Lyytinen, & Siau, 2005).

1. Printer: The system generates the hardcopy of syllabus, test questionnaire and table of specification as output. It will be delivered via a connected printer.

Software Specification

The following are the system requirements needed to run the Test Banking system with Advanced Encryption Standard Algorithm.

Software Requirements:

1. Bootstrap. This software was used for the front-end web framework for designing websites and web applications. The proponents used this for the graphical user interface (GUI) to have a more professional approach for the system.

2. Sublime Text. A proprietary cross-platform source code editor with a Python application programming interface (API). It natively supports
many programming languages and markup languages, and its functionality can be extended by users with plug-in, typically community-built and maintained under free-software licenses. The proponents will use this as the code editor to create the back-end of the system.

3. MySQL is an open-source relational database management system (RDBMS). The proponents use this as the storage for data. This will be the database for the system.

4. PHP is a popular general-purpose scripting language that is especially suited to web development. The proponents will use this scripting language to create the system.

5. Navicat is a series of graphical database management and development software produced by PremiumSoft CyberTech Ltd. For MySQL, MariaDB, Oracle, SQLite, PostgreSQL, and Microsoft SQL Server.

6. DeZign for databases is a database design tool that helps you model, create and maintain databases. It uses entity relationship diagrams to graphically design databases and automatically generates the most popular SQL and desktop databases.

7. XAMPP is a free and open source cross-platform web server solution stack package developed by Apache Friends, consisting mainly of the Apache HTTP Server, MariaDB database, and interpreters for scripts written in the PHP and Perl programming languages.

Acceptance and Deployment Phase
The respondents of the study were the faculty, program heads, department deans and printing-in-charge. The researcher used purposive sampling techniques in conducting the study.

The primary source of information was taken from the respondents. Survey instrument was distributed for them to answer, collected and outputs were recorded. The data was analyzed and interpreted for the development of the project.

However, to ensure the validity of the result the researcher conducted a focus group discussion and project demonstration. The participants tested and evaluated the system.

Table 2. Respondent’s distribution

<table>
<thead>
<tr>
<th>Position</th>
<th>N (Population)</th>
<th>Percentage</th>
</tr>
</thead>
<tbody>
<tr>
<td>Faculty</td>
<td>7</td>
<td>70</td>
</tr>
<tr>
<td>Program head</td>
<td>2</td>
<td>20</td>
</tr>
<tr>
<td>Dean</td>
<td>1</td>
<td>10</td>
</tr>
<tr>
<td>Total</td>
<td>10</td>
<td>100</td>
</tr>
</tbody>
</table>
RESULTS AND DISCUSSION

Table 3. Respondents Evaluation Result in terms of system usability

<table>
<thead>
<tr>
<th>A. Usability of the system</th>
<th>MEAN</th>
<th>VERBAL INTERPRETATION</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. The system is easy to use and quick to learn.</td>
<td>3.52</td>
<td>SA</td>
</tr>
<tr>
<td>2. The system manages error filtering from user-input through error handlers</td>
<td>3.65</td>
<td>SA</td>
</tr>
<tr>
<td>3. The system functionality can be easy to remember</td>
<td>3.40</td>
<td>SA</td>
</tr>
<tr>
<td>4. The User Interface components are accessible</td>
<td>3.47</td>
<td>SA</td>
</tr>
<tr>
<td>5. The System Design Aesthetic and User Interface are visually attractive</td>
<td>3.40</td>
<td>SA</td>
</tr>
<tr>
<td><strong>Weighted Mean</strong></td>
<td><strong>3.48</strong></td>
<td><strong>SA</strong></td>
</tr>
</tbody>
</table>

Legend:
SA – Strongly Agree (3.26 – 4.00)  
A – Agree (2.51 – 3.25)  
D – Disagree (1.76 – 2.50)  
SD – Strongly Disagree (1.00 – 1.75)

Table 3 shows the mean distribution and verbal interpretation. In terms of “Usability,” an overall mean of 3.48 was garnered with a verbal description of “Strongly Agree.” The Table also showed that the item, “The system manages error filtering from user-input through error handlers” has the highest mean of 3.65 verbally described as the user “Strongly Agree”. This means that the system provides user-friendly graphical reviewed by the user.

Table 4. Respondents Evaluation Result in terms of system Maintainability/Efficiency

<table>
<thead>
<tr>
<th>B. Maintainability/ Efficiency of the system</th>
<th>MEAN</th>
<th>VERBAL INTERPRETATION</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. The system provides results in a timely manner.</td>
<td>3.45</td>
<td>SA</td>
</tr>
<tr>
<td>2. The system prints the TQ and TOS clearly.</td>
<td>3.50</td>
<td>SA</td>
</tr>
<tr>
<td>3. The system provides a hardcopy of the generated result.</td>
<td>3.63</td>
<td>SA</td>
</tr>
<tr>
<td>4. The system loads fast.</td>
<td>3.30</td>
<td>SA</td>
</tr>
<tr>
<td>5. The system can cater to a large amount of data.</td>
<td>3.30</td>
<td>SA</td>
</tr>
<tr>
<td><strong>Weighted Mean</strong></td>
<td><strong>3.43</strong></td>
<td><strong>SA</strong></td>
</tr>
</tbody>
</table>

Legend:
SA – Strongly Agree (3.26 – 4.00)  
A – Agree (2.51 – 3.25)  
D – Disagree (1.76 – 2.50)  
SD – Strongly Disagree (1.00 – 1.75)
Table 4 shows the mean distribution and the verbal description in terms of “Maintainability/Efficiency” with a total mean of 3.43 verbally described as “Strongly Agree.” The table shows that the question, “The system provides a hardcopy of the generated result” has the highest mean of 3.63, this only means that the system alters and adapts to new conditions like adding features, can be used without written instructions. The system was efficient enough to adopt external changes like system updates.

Table 5. Respondents Evaluation Result in terms of system functionality

<table>
<thead>
<tr>
<th>B. Functionality of the system</th>
<th>MEAN</th>
<th>VERBAL INTERPRETATION</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. The system gives exact generation of TQ and TOS.</td>
<td>3.60</td>
<td>SA</td>
</tr>
<tr>
<td>2. The system gives almost exact output of what is expected by the user.</td>
<td>3.20</td>
<td>SA</td>
</tr>
<tr>
<td>3. The system has met the institution’s appropriate laws and guidelines need to be complied with.</td>
<td>3.33</td>
<td>SA</td>
</tr>
<tr>
<td>4. The system delivers the precise result of storing TQ and TOS</td>
<td>3.53</td>
<td>SA</td>
</tr>
<tr>
<td>5. The system does not give erroneous display during storage and retrieval.</td>
<td>3.40</td>
<td>SA</td>
</tr>
</tbody>
</table>

Weighted Mean 3.41 SA

Legend:

SA – Strongly Agree (3.26 – 4.00)  D – Disagree (1.76 – 2.50)
A – Agree (2.51 – 3.25)           SD – Strongly Disagree(1.00 – 1.75)

Table 5 shows the mean distribution and the verbal description in terms of “Functionality” with a total mean of 3.41 verbally described as “Strongly Agree.” This means that the system as perceived by the user provides convenience in terms of functionality. The system can be easily accessed by the user and is deemed easier to use. As perceived by the user, the system provides convenience in the accession of the system, creation of data and generation of a report.
Table 6. Summary Table of the Over-all Mean and Grand Distribution of the Acceptability Level

<table>
<thead>
<tr>
<th>Acceptability Level of Test Bank System with AES Cryptographic Algorithm in terms of:</th>
<th>Over-all Mean</th>
<th>Rating</th>
</tr>
</thead>
<tbody>
<tr>
<td>Usability</td>
<td>3.48</td>
<td>SA</td>
</tr>
<tr>
<td>Functionality</td>
<td>3.41</td>
<td>SA</td>
</tr>
<tr>
<td>Maintainability/Efficiency</td>
<td>3.43</td>
<td>SA</td>
</tr>
<tr>
<td><strong>Grand Mean</strong></td>
<td><strong>3.44</strong></td>
<td><strong>SA</strong></td>
</tr>
</tbody>
</table>

After conducting the survey which the proponents used the questionnaire shown above, the gathered ratings from the 10 respondents were calculated using mean/average. The proponents come up to the result of 3.48 as maximum score, 3.41 as a minimum, and 3.44 as mean or the average score. Since the mean result was 3.44, it is considered as average in the scale range, which means that the user from faculty, program heads, and dean agree that the system was usable in terms of its functions that are based on the given user requirements. It means that the system was deemed useful to the department because it provided accurate creation and generation of a report.

**CONCLUSIONS**

This study introduces Test Bank System with less usage of papers and more reliable process in such a way that it has security measures, it can be accessible anytime and anywhere inside the school premises. And it improves the productivity of the faculty. Also, this system will be beneficial in the way of maximizing the faculty’s time and effort and the company’s resources. With the use of this system, creating TQ, TOS and Syllabi, submitting TQ, checking of TQ and TOS to program head and dean will be more efficient in such a way that TQ and TOS will automatically queue to the program head and dean page upon submission of the instructor.

At the end of the development phase, the system was able to achieve its objectives. The administrator created add user that allowed them to log in. The users are allowed to create syllabus, test questionnaire and table of specification. The program head and dean can able to monitor the submission compliance per faculty, to add data to put into records, manage files along with its permissions, and generate a report. The user activities are well saved in the MySql database and with more secure privacy in exchanging information because of the embedded Advanced Encryption Standard Cryptographic algorithm which means the system remains protected from unauthorized access.
RECOMMENDATIONS

Based on the conclusions, some crucial recommendations are stated as follows:

1. The instructor, program head and department dean are encouraged to implement and utilize the system. Particularly as to substitute for the traditional way of creating a syllabus, test questionnaire, and table of specification.

2. The system needs an Artificial Intelligence system support that has an automatic decision upon filtering cognitive domain level in every question to fulfill more of the user’s preferences.

LITERATURE CITED


