I.J. Modern Education and Computer Science, **2016, 10, 1-8**
Published Online October 2016 in MECS (http://www.mecs-press.org/)
DOI: 10.5815/ijmecs.2016.10.01

Test Bank Management System Applying Rasch Model and Data Encryption Standard (DES) Algorithm

Maria Ellen L. Estrellado
Technological Institute of the Philippines, Cubao, Quezon City, 1109, Philippines
Email: ellen_estrellado@yahoo.com

Ariel M. Sison, Bartolome T. Tanguilig III
Technological Institute of the Philippines, Cubao, Quezon City, 1109, Philippines
Email: ariel.sison@aec.edu.ph, bttanguilig_3@yahoo.com

***Abstract*—**Online examinations are of great importance to education. It has become a powerful tool for evaluating students' knowledge and learning. Adopting modern technology that saves time and ensures security. The researcher developed a Test Bank Management System that can store test items in any subjects. The system is capable of conducting item analysis using the Rasch model scale. Items that undergo analysis based on Rasch scale helped faculty by quantifying each item as "good", "rejected", or "revised". For securing items in the test bank, Data Encryption Standard (DES) algorithm was successfully applied thus ensuring the safety and reliability of the questions in the test bank. Only items that are ready for deployment to the student's computer during the examinations will be decrypted. In conclusion, the system passed the evaluation process and eliminates redundancy of manual work.

Index Terms—Test Bank Management System, Rasch Model, Data Encryption Standard, Test Items, Item Analysis.

I. Introduction

One of the bases for evaluating or giving grades to the students is the examination or test. Examination or test serves as an assessment intended to measure the examinees' knowledge in a particular subject or topic. Examinations are a crucial part of both the academic teaching and learning process and of the school/university's administration procedures [1].It is one aim of an institution to gauge their students' ability and competitiveness. To the student, examination gives them goals toward which they are directed, pushing them to attain that goal within a specified period. For teachers, the result of examination also gives them drive and work direction, towards the better learning.

The preparation of the exam is a repetitive task and a very tedious process. It includes: (a) developing the exam, (b) digitizing it with text editor such as Microsoft Word, (c) piloting and reviewing the quality of each question, and finally, (d) printing out the exam papers [2]. So in order to precisely and reliably measure the proficiency of students and discern examinees with different levels of ability, items should be subjected to thorough investigation using some psychometric methods. That is, to item analyze. The basic idea of item analysis is that the statistical behavior of "bad items" is fundamentally different from that of "good items" [3].

However, conducting item analysis manually can cause a lot of time and effort, which may have inaccurate data, unreliable, and inefficient results. This procedure is an important technique for teachers to identify the effectiveness of the examination they have created.

Item analysis is a type of statistical technique that helps instructors determines the effectiveness of their test items [5]. A basic assumption made by ScorePak® [4] is that the test under analysis is composed of items measuring a single subject area or underlying ability. The quality of the test as a whole is assessed by estimating its "internal consistency". With item analysis, sorting questions could be easily quantified as "good", "rejected", or "revised". There would be no need for the instructors/faculty to do it manually.

There are several tools that can be utilized in analyzing data. One of these tools is the Rasch Model Analysis. Rasch model is the only item response theory (IRT) model in which the total score across items characterizes a person's totality. It is also the simplest of such models having the minimum of parameters for the person corresponding to each category of an item. This item parameter is generically referred to as a threshold. It provides teachers with two types of information: Difficulty Index and Discrimination Index.

Due to the different issues involved in the examination management, the author proposed to develop a web – based Test Bank Management System applying Rasch Model and Data Encryption Standard (DES) algorithm. The proposed system is capable of storing test questions that would be readily available for students and can be taken online. For the analysis of the test results from the students' answer sheet, the Rasch model would be used. Rasch analysis is employed to evaluate this assessment as a measurement tool. This produces measures for ability and item difficulty that are independent of both the specific items on the assessment and the sample of test-takers [6] while DES (Data Encryption Standard) algorithm will be used for securing the test questions in the test bank by encrypting each item. This algorithm uses a symmetric key (secret key) for the security of the test questions.

The rest of this paper is organized as follows: Section II is dedicated to related studies relevant to the present studies. Section III, is the operational framework. Section IV presents the design architecture of the TBMS. Then in Section V, is dedicated to conclusion and future works.

II. Related Studies

This section presents the studies reviewed which are relevant to the present study.

Chieh-Ju and Wang [19] provided a baseline results of the item analysis for the English Proficiency Test where it offered guidelines to know which items need to be discarded or could be maintained. It contributed to the assessments of English major students' language proficiency.

On the same manner, Bermundo and Bermundo [20] in their study developed software that checks and analyzes the test items. This is in response to the needs of developing a system that lessens, if not eliminate the said difficulty and complexity of the process to item analyze the exam. They reiterated the difference of having such system helped in the analysis as compared to the traditional method. It also showed how the teachers perceived the level of usability and acceptability of the design of the TCIAS regarding feasibility, functionality, accuracy and efficiency.

Likewise, in the study of Dio [21], he developed a Mathematics Proficiency Test that determined the proficiency level including the competencies that are needed to be enhanced in general education mathematics of the pre-service elementary teachers. He also proposed an enhancement in the syllabus based on the identified needs of the students. The MPT developed a used test method and tested internal consistency to determine the reliability level of the MPT. He used Cronbach's alpha for testing the validity of the test items.

Chang [22] investigated the differences in the partial scoring performance of examinees in elimination testing and conventional dichotomous scoring of multiple-choice tests implemented on a computer-based system. They used multiple-choice items to eliminate examinees with partial knowledge over those who are simply guessing.

While, Muddu [23] mentioned in his study, that online test, exam, and contest are part of online education but not widely implemented due to lack of resources and security related issues. He proposed a solution to the security issues and cheating, in an online exam. Two cryptographic algorithms namely RSA and Data Encryption Standard are used. The RSA algorithm was used for securing the users credentials, and the DES are used for securing online test environment.

Zughoul et.al. [24] proposed a new method for key generation based on Data Encryption Standard Algorithm for online examination to make it more secure. They reiterated the encryption of the Online Examination System particularly the privacy of the users' credentials. Furthermore, they proposed that users should have a personal space such that there is user control on what and how much personal information could be shared with others. They proposed an improvised algorithm of DES.

III. Operational Framework

Figure 1 shows the framework of the proposed system. The faculty would prepare all the test questions in the subjects they handle based on the covered topics in the syllabus. The Chairperson, would review, check and approve all the items. The remaining questions would then be encoded in the system subject for DES encryption to ensure the security and confidentiality of the test questions before saving it in the Test Bank. A maximum of one hundred (100) test items per subject would be stored in the test bank. The system would randomly select items in the Test Bank. Randomly selected questions would then be decrypted using DES algorithm again before it could be deployed in the students' computer and could be taken by the students online. After the examination, the system would automatically check the answer sheets. Results of the exam would be displayed by the system and Rasch model tool would be utilized for item analysis. The answer sheets would serve as the point reference for the process of weighing if the test questions are "good"; "rejected", or "revised".

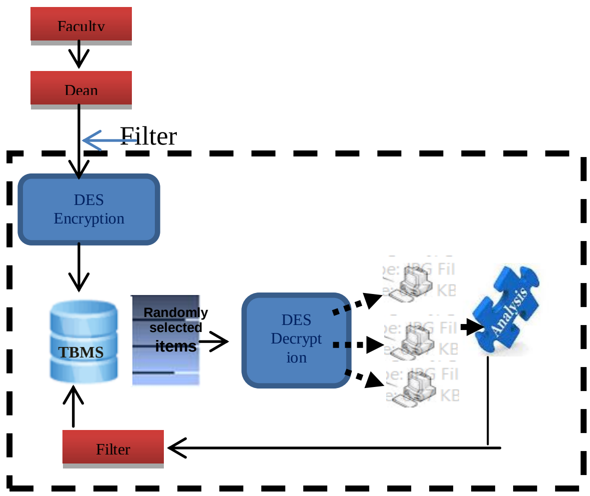

Fig.1. Conceptual Framework of Test Bank Management System Applying Rasch Model and Data Encryption Standard Algorithm.

IV. Design Architecture of the TBMS

This part of the documentation presented the design architecture of the system. It includes application of Rasch model as analysis tools for the analysis of each item and for the security of the test items in the test bank using the DES algorithm.

A. Item Analysis Using Rasch Model Scale

Based on Item Response Theory (ITR), quantitative method is the key to conduct item analysis in any exams as stressed by Stanley [16]. Rasch model is the simplest form among IRT (Item Response Theory) models. It has been taken by many researchers in different subject as a criterion for the structure of the responses, rather than a mere statistical description of the responses.

Analyzing data according to the Rasch model, or conducting Rasch analysis, gives a range of details for checking whether adding the scores is justified or not in the data. This is called the test of fit between the data and the model. As cited in the study of Khairani and Razak [15], Rasch analysis provides reliability indices for both item and examinee's measure. High reliability for both indices was desirable since they indicate a good results if the comparable items/examinees were employed.

When performing item analysis, the following statistical information was analyzed:

Index of Difficulty

The Index of Difficulty is the percentage of students that correctly answered the questions. It calculates the proportion of students in a class who got an item correct, then divide it by a total number of students who took the exams. Below is the formula:

$$\frac{\text{No. of Correct answer}}{\text{Total number of students}} \tag{1}$$

Index of Discrimination

The discrimination index is a basic measure of the validity of an item. It is a measure of an item's ability to discriminate between those who scored high on the total test and those who scored low. In the equation below, UG refers to the right response of the upper group; LG refers to the right response of the lower group; and NG is the total number of each group.

$$\frac{(UG)-(LG)}{(NG)} \tag{2}$$

Table 1. Parameters of Item Analysis

Item Difficulty	Interpretation	Index of Discrimination	Remarks
<0.20	Difficult Item	Positive/ Negative (+/-)	Rejects
0.20 to 0.80	Average to Moderately Difficult Item	Positive (+)	Retain
		Negative (-)	Revise
>0.80	Easy Item	Positive/ Negative (+/-)	Rejects

Table 1.shows the parameters of analyzing test items using the Rasch Model. To elaborate precisely the scale in Rasch: if the value of an item is greater than 0.80, the test item is "Very Easy", if the value is less than 0.20, the item is considered as "Very Difficult"; items that have a value between 0.20 to 0.80 is considered as "Average" or Moderately Difficult".

Table 2 are sample computations for items# 1, 2 and 18 on the first try out of the Mock Exam using Equation 1 and 2.

B. Applying Data Encryption Standard Algorithm

Data Encryption Standard (DES) algorithm as used in this study is a symmetric key algorithm. Keys are the same for both encryption of plaintext and decryption of cipher text. Items inside the test bank will be encrypted for security purposes. Only items for deployment or to be taken by the students during a scheduled online exam will be decrypted.

Figure 2 shows the key generation process. The key in plaintext was converted into hexa value, then converted into binary value. Next is to perform initial permutation before going to 16 rounds of the key generation process. The result is reduced to 56-bit block for parity checking. Then it is divided into two halves (as shown in the detailed process in Table 3). A circular shift(left shift) for both values of L_0 and R_0 were performed. Then it assigns the value of L_0 to L_1 and R_0 to R_1. Combined values of L_1 and R_1 to produce the 48-bit output or the key in Round 1. For the succeeding round, the values of L1 and R1 were combined, then generate the next keys by conducting a left circular shift. Processed 6 and 7 was repeated generate the key for Round 2 until Round 16. Binary result was then converted to hexa value. The generated key values of each round after the processes are shown in Table 4.

Table 2. Result of the analysis

Item #	Item Difficulty	Interpretation	Index of Discrimination	Interpretation	Remarks
1	1	Very Easy	0	positive value	Reject
2	0.76	Moderately Difficult	-0.3	negative value	Revised
18	0.33	Moderately Difficult	0.1	positive value	Retain/ Good Item

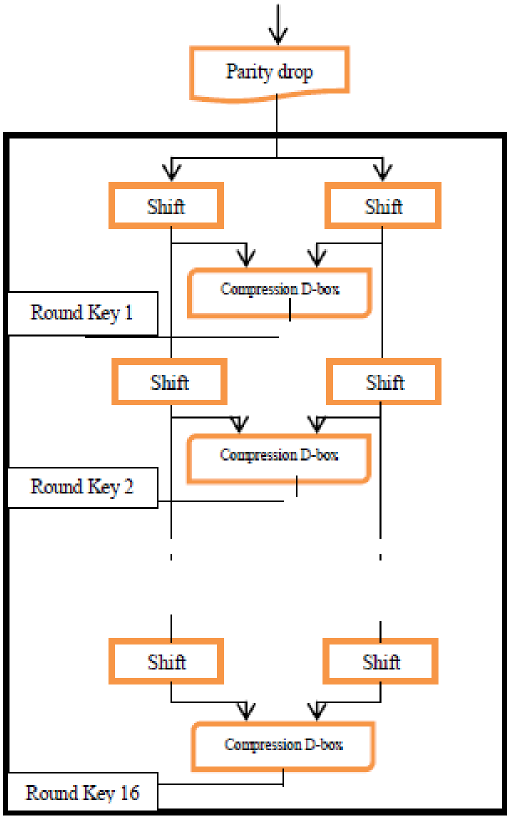

Fig.2. Key Generation Process

Table 3. Illustration of the Key Generation Process

Step	Process	Value	
1	(Thisismy) Hexa value 54686973697 36d79	0101010001101000011010010111 0011011010010111001101101101 0101111001	
2	64-bit binary value	01010100 01101000 01101001 01110011 01101001 01110011 01101101 01111001	
3	Remove the last bit of every 8bits	0101010 0110100 0110100 0111001 0110100 0111001 0110110 0111100	
4	Permuted Value	0101010 0110100 0110100 0111001 0110100 0111001 0110110 0111100	
5	Get the 1st half of binary and labeled as L_0 and R_0	L_0 0101010 0110100 0110100 0111001	R_0 0110100 0111001 0110110 0111100
6	Performed Circular Shift both for L_1 and R_1	L_1 101010100110 1000 11010001 1100	R_1 110100011100 101101100111 1000
7	Combine L_1 and R_1 then apply permuted choice 2	1001110001011000101100101010 0011110011011010011 1	
8	Convert binary result to hexa to produce key for 1st Round	9c58b2a3cda7	

Table 4. Key Generation Result

Round	Value	Round	Value
1	9c58b2a3cda7	9	e80d33d75314
2	da91ddd7b748	10	e5aa2dd123ec
3	1dc24bf89768	11	83b69cf0ba8d
4	2359ae58fe2e	12	7c1ef27236bf
5	b829c57c7cb8	13	f6f0483f39ab
6	116e39a9787b	14	0ac756267973
7	c535b4a7fa32	15	6c591f67a976
8	d68ec5b50f76	16	4f57a0c6c35b

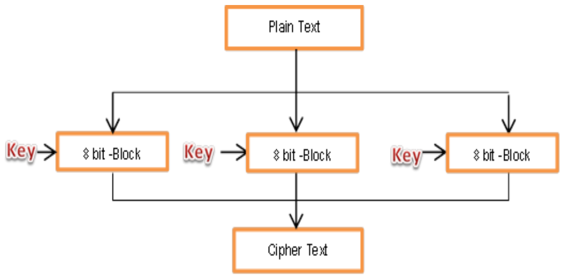

Fig.3. Division of Plaintext into 64-bit block

Table 5. Plaintext in 64-bit block

Block	Plaintext in 64-bit block
1	Which co
2	mputer h
3	as been
4	Designed
5	to be a
6	s compact
7	t as pos
8	sible?

Figure 3 shows the process of dividing the plaintext in 64-bit block, and Table 5, shows the result after the division of the plaintext. A sample test item, "Which computer has been designed to be as compact as possible?" was converted into a cipher text by grouping each character into eight (8) bytes per block as shown in Table 3.2. The last block is consisting only of six (6) characters. It is then automatically padded with three (3) spaces to complete the eight (8) characters. Padding in cipher happens when the plaintext to be encrypted is not an exact required length. Therefore it should be padded by adding a padding string [28]. Each block is encrypted using Round 1 to 16 keys in Table 4.

Figure 4 presents the flowchart of the plaintext encryption process. Table 6 shows the detailed encryption process of the plaintext using the 16-round key. The encryption function has two inputs; plaintext and the key. The first block is converted into hexa value then from hexa value to binary value. Then DES performs an initial permutation (IP) on the entire 64-bit block of data. It is then split into 2, 32 bit sub-blocks, L_0 and R_0. The

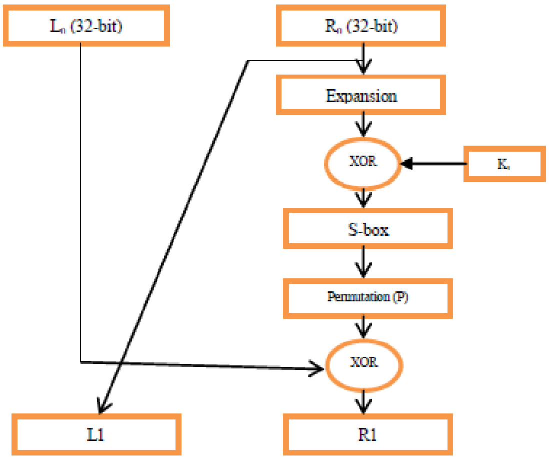

Fig.4. Plaintext Encryption Process

Table 6. Detailed Encryption Process of Plaintext

Step	Process	Result
1	Convert plaintext "which co" to hexa, hexa to binary	776869636820636f 1110111011010000110100101 1000110110100000100000011 0010000000000
2	Apply IP to the result then convert to hexa value	11110101 00101100 00111100 00110101 01101100 00100000 01100100 00000000 eed0d2c6 d040c800
3	Divide the result into two halves	L0 / R0 eed0d2c6 / d040c800
4	Apply Expansion/ Permutation to the Result of R_0	6f80fe8a17a9
5	Use Key in Round 1(Table 3.1), performed XOR with R_0	9c58b2a3cda7
6	Apply S-box substitution	ae1ba189
7	Apply permutation function to the result of R0	dc1f10f4
	XOR the value of L0 to R0 the Assigned the new value to R1	86ed743c
9	Assign the value of R0 to L1	d040c800
10	Repeat steps 3 to 9, having R_1 and L_1 as input to the next round. Perform this for 16 Rounds using the keys in Table 3.1	
11	Concatenate the result to get the value of the 1st block cipher. The result of the plaintext "which co"	10b08248abd41bec

expansion/permutation process was applied to the value of R_0. The result will be XORed to the 1st key in Table 4. The XOR result will then be grouped to 8 blocks. Each block consists of 6 bits. Afterwards, the S-box substitution was applied to the result. Then, permutation function was applied to the result of R_0. Performed XOR to L_0 with the permuted value of R_0, and then assigned the value to R_1. Assigned R_0 to L_1. The output of this final permutation is the 64-bit cipher text of the 1st block of plaintext. After performing the process, the output is shown in Table 7 while in Table 8 is the encryption value of the 1st block of cipher text after using round 1 to 16 keys.

Table 7. Encryption Value of the Plaintext in 64-bit block

Plaintext in 64 bit block	Ciphertext
Which co	10b08248abd41bec
mputer h	d1ae1cab11eff016
as been	9cc65bac958beb20
Designed	bab9939dba901eee
to be a	47084d57cc02fcdc
s compact	498ed7ab2a973244
t as pos	5e013cdbc46ec58d
sible?	b8153403ea57c015

Table 8. Encryption Value of the 1st block of Ciphertext

Index	Left	Right
1	d040c800	86ed743c
2	86ed743c	e0e7a039
3	e0e7a039	61123d5d
4	61123d5d	a6f29581
5	a6f29581	c1fe0f05
6	c1fe0f05	8e6f6798
7	8e6f6798	6bc34455
8	6bc34455	ec6d1ab8
9	ec6d1ab8	d0d10423
10	d0d10423	56a0e201
11	56a0e201	b6c73726
12	b6c73726	6ff2ef60
13	6ff2ef60	f04bf1ad
14	f04bf1ad	f0d35530
15	f0d35530	10b08248
16	10b08248	abd41bec

Figure 5 shows the cipher text decryption process. The process is performed in reverse order using the same key. If at random selection the sample test item were selected, the process starts by getting the value of L_1 and R_1 then performed XOR to the value. Get the value of R_1, performed expansion permutation. S-box substitution is then applied to get the value of L1. XORed the result of R1 to the first key in Table 4. Concatenate R1 ll L1 to produce the value. Finally, the 1st block of cipher text is recovered. The detailed process is shown in Table 9. Figure 5 below is the Ciphertext Decryption Process.

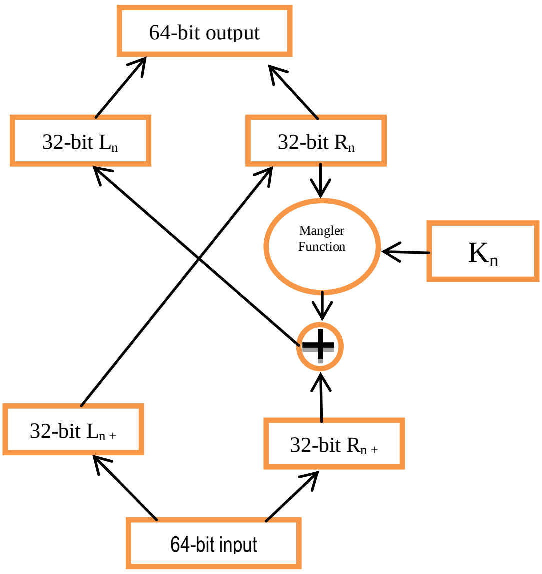

Fig.5. Ciphertext Decryption Process

Table 9. Decryption Result of the 1st block of Ciphertext

Step	Process	Result
1	Get the value of L1 and R1	L1 = d040c800 R1=86ed743c
2	XOR R1 to L1	dc1f1cf4
3	Get the value of R1, performed expansion permutation	86ed743c
4	Apply S-Boxes Substitution	ae1ba189
5	XOR the result to the key in round 1	9c58b2a3cda7
6	New Value for R1	R1 = 07b5cf4c
7	R1 II L1	4713b8f45cd9b326
8	Plaintext value of the 1st cipher after 16 Rounds.	776869636820636f

C. Evaluation of the developed system/software using the ISO 9126 standard.

In any project development, a certain design methodology is employed in order to come up with an effective and desirable result. However, in order to achieve the goal of having an affective and desirable result, the system has to undergo the evaluation using the ISO 9126 Standard. Below are the activities performed in the evaluation of the developed system.

The system was presented to the evaluators-respondents consisting of thirty (30) students and three (3) Faculty members of the Engineering Department. The functions and processes of the software were discussed during the presentation to ensure that the developed system is evaluated properly. During the final evaluation, survey questionnaires were distributed.

The evaluation survey for this system is based from the external and internal quality model adopted from the ISO / IEC 9126 standard. The primary goal of the survey is to test the performance of the system in view of its users. The criteria used are composed of six (6) main quality characteristics that are defined in the ISO9126 [28] standards as follows:

- Functionality – the ability of the software product to provide functions which meet stated or implied needs of the users.
- Reliability – the ability of the system to functions as specified, and the capability of the system to maintain its service provisions under defined conditions for defined period of time.
- Efficiency – the ability of the software to provide appropriate performance in relation to the amount of resources used. This is used to measure how well the system works.
- Usability –the ability of the software to be easily operated by a given user in a given environment and the ease of which the system functions could be understood by the intended users.
- Portability – characterizes the ability of the software/system to change to new specifications or operating environments or the measure of the effort that is needed to move software to another computing platform.
- Maintainability – it is the ability to identify the root cause of a failure within the software, the amount of effort to change a system and the effort needed to verify (test) a system change.

An evaluation sheet was distributed to different respondents. The questionnaire uses the scale of 1 to 5, with 1 as the lowest and 5 as the highest. The evaluation sheet enumerates six (6) indicators: functionality, reliability, efficiency, usability, maintainability, and portability. Table 11 is the over-all tabulated results based on the respondents evaluation.

Table 10. Tabulated Rating of the Respondents – Overall

	Criteria	**Mean**	**Qn**	**Ql**
1.	Functionality	4.6	5	E
2.	Efficiency	4.6	5	E
3.	Usability	4.8	5	E
4.	Reliability	4.15	4	VG
5.	Portability	4.85	5	E
6.	Security	4.8	5	E
	Overall Mean	**4.63**	**5**	**E**

Legend:

Mean Range	Quantitative Value (Qn)	Qualitative Value(Ql)
4.51 – 5.00	5	(E) Excellent
3.51 – 4.50	4	(VG) Very Good
2.51 – 3.50	3	(G) Good
1.51 – 2.50	2	(F) Fair
1.00 – 1.50	1	(P) Poor

Table 10 shows the overall mean of the criteria used in the evaluation of the system quality. The overall mean is 4.63, which has an equivalent qualitative result of "Excellent". The result simply implied that respondents found the system useful and was able to attain the goals and objectives of the study.

V. Conclusion and Future Works

The developed system is capable of storing test items in the test bank per subject. Random selection of the test items ready for deployment to the student's computer is one of the functions of the system. It automatically checked the answer sheet of each student. The Rasch model was successfully applied by conducting an analysis of each item based on the result of the exams of the students, as it was part of the function of the system, thus eliminating redundancy of manual work. After analysis faculty members could now easily quantify all the items in the exams as *good, rejected or revised items.*

The integrity and confidentiality of the test items stored in the test bank was successfully secured using DES algorithm by automatically encrypting all the test items in the test bank. Only items ready for deployment after randomly selected by the system will be decrypted.

Functions like editing/saving items are embedded in the system.

With the developed system, manual work of the faculty when it comes to preparation of the exams is reduced if not eliminated.

The system passed the evaluation process based on the ISO 9126 standard as perceived by the respondents.

Full implementation of the developed system is recommended.

As for future works The TBMS may be further secured by using other security algorithm aside from DES. The developed TBMS can still be improved by adding other features/functions that will help ease-up the usage of the system, like: to restore the discarded questions automatically if needed; choices for multiple choice format can be re-arranged together with the correct answers; graphic choices can be considered; and the system can provided audit trail or report of faculty who contributed the questions or faculty who modified the question.

Acknowledgement

I would like to express my sincerest gratitude to my thesis adviser, Dr. Ariel M. Sison, for his guidance and his valuable suggestions for the improvement of the study. He consistently allowed this paper to be my own work, but steered me in the right direction whenever he thought I needed it. Thank you, Sir Ariel.

Also to all the Panel of Examiners, for their comments and suggestion for the improvement of the research paper.

I would also like to thank the experts who were involved in the validation survey of this research project: particularly the Statistician, Computer Analysts, and the SSC Research Director who participated/contributed in the making of this study. Without their inputs, the validation of survey could not have been successfully conducted.

I would also like to acknowledge the former President of the Sorsogon State College Dr. Antonio Fuentes and the present president Dr. Modesto D. Detera for their invaluable support in the conduct of this study. I am gratefully indebted.

Appreciation is extended to the Commission on Higher Education (CHED), for the scholarship granted to the proponent.

I must also express my profound gratitude to my parents, brothers and sister for their unfailing support and continuous encouragement throughout the years of my study.

To my children Erika, Oli and Julia for their understanding during the time when I cannot give my 100% attention during the course work and for continuously providing me an inspiration to keep me going and work on this project.

Finally to my husband Rico, for the love and for providing me with unfailing support, continuous encouragement and understanding throughout the years of study and through the process of researching and writing. This accomplishment would have not been possible without them. Thank you so much.

Above all, to the ALMIGHTY GOD for His blessings.

References:

[1] Bauer, Dr. Yvonne,Degenhardt, Dr. Lars, Kleimann, Dr. Bernd, and Wannemacher, Dr. Klaus,"Online Exams as Part of the IT – supported Examination Process Chain",Higher Education Information System.

[2] YewTzeHui, Cheong Soon Nyean, Yap Wen Jiun, NordinAbdRazak 2 and Ahmad ZamriKhairani, "Development of Mathematics Question Banking System for Secondary School in Malaysia, 2012 International Conference on Management and Education Innovation, IPEDR Vo, 37, pp. 12-16.

[3] Kehoe and Jerard, Basic Item Analysis for Multiple-Choice Tests, Practical Assessment, Research & Evaluation, 4(10), 1995.

[4] Scorepak, "Score Pak: Item Analysis",Office of the Educational University of Washington. August 2005.

[5] "Scatron Guide", Educational Management Center.

[6] Ahmad Zamri Khairani, "Development of Mathematics Question Banking System for Secondary School in Malaysia,2012 International Conference on Management and Education Innovation IPEDR vol.37 (2012)© .

[7] Camero, Joseph T., "The Role of Online Grading Programs in School/Community Relations";New Southern International School, Bangkok Thailand, July 2011, Vo. 1, pp.91-105.

[8] Elaine Barker, William Barker, William Burr, Wiliam Pork, Mike Smid; "Computer Security", National Institute of Standard and Technology, July, 2012.

[9] MwaiNyaga, Hassan Bundu; "The Impact of Examination Analysis for Improving the Management of public Examination or Otherwise"; 27th Annual Conference of the Association for Educational Assessment in Africa; August 2009, pp. 1-20.

[10] Dr.Roberta N. Chinn, Dr. Norman R. Hertz and Dr. Barbara A. Showers; "Building and Managing Small

Examination Program", presented at Annual meeting of the Council on Licensure, Enforcement, and Regulation in Las Vegas, NV, September 2002.
[11] Qingchun Hu and Yong Huang; "An Approach for Designing Test Bank in Adaptive Learning System"; The9th International Conference on Computer Science & Education (ICCSE 2014); Vancouver, Canada; August 22-24, 2014, pp.462-464.
[12] Osama Almasri, Hajar Mat Jani, Zaidah Ibrahi3, Omar Zughoul; "Improving Security Measuresof E-Learning Database"; IOSR Journal of Computer Engineering Volume 10, Issue 4 (Mar. - Apr. 2013).
[13] NikhileshBarik and Dr. Sunil Karforma; "Risks and Remedies in E-Learning System"; International Journal of Network Security & Its Applications (IJNSA), Vol.4, No.1, January 2012.
[14] Jose F .Calderon and Expectacion C. Gonzales; Measurement and Evaluation; Printed by J. Creative Label Enterprise, Copyright, 1993.
[15] Ahmad Zamri bin Khairani and Nordin bin Abd. Razak; "Advance in Educational Measurement: A RaschModel Analysis of Mathematics Proficiency Test"; International Journal of Social Science and Humanity, Vol. 2, No. 3, May 2012.
[16] Julian C. Stanley, Educational and Psychological Measurement and Evaluation, 6th Edition; National Bookstore.
[17] Madhu Babu anumolu, "An Online Examination System Suing Wireless Security application", Internation Journal on Engineering Trends and Technology, Vo. 4, September, 2013.
[18] Chieh-Ju Emily Wang, "Item Analysis of a Test Bank Developed for University English Major Student"s; Department of Applied Languages, Ming Chuan University; April 2012.
[19] Cesar B. Bermundo and Alex B. Bermundo, Test Checker and Item Analyzer with Statistics; 10th National Convention of Statistics (NCS); October 2012.
[20] Ryan V Dio; NCBTS – Based Mathematics Proficiency Test (MPT) for Pre-Service Elementary Teachers; Bicol University, July 2012.
[21] Shao- Hua Chang, Pei-Chun Lin, zihChuan Lin; Measure of Partial Knowledge and Unexpected Responses in Multiple Choice Tests; Educational Technology and Society; Page 95-109.
[22] Ramchander Muddu; "Design and Implementation of a Monitoring System to Prevent Cheating in Online Test"; Texas A & M university – Corpes Christ; TX 2012.
[23] Omar Zughoul, Hajar Mat Jani, AdibahShuib, Osama Almasri, Privacy and Security in Online Examination System; OSR Journal of Computer Engineering, Mar-April 2013.
[24] "Cryptography",http://www.di-gt.com.au/cryptopad.html
[25] http://www.iusmentis.com/technology/encryption/des/
[26] "ISO 9126 standard", www.whatis.com
[27] "ParityChecking",https://en.wikipedia.org/w/index.php?se arch =parity=Go

Authors' Profiles

Maria Ellen L. Estrellado was born in Casiguran, Sorsogon. She earned her Master's Degree in Master in Management major in Public Administration at Sorsogon State College, Sorsogon City in 2005 She obtained her baccalaureate degree in BS Computer Science at Aemilianum Institute, Sorsogon in 1997.

After receiving her baccalaureate degree, she worked as a Clerk at Allied Banking Corporation, Sorsogon City branch in 1997. Afterwards, she worked as a clerk at the Sorsogon State College until October 2005. At present she is a college instructor of the said institution and teaching computer subjects at the Engineering/Architecture Department.

Dr. Ariel M. Sison earned his Doctor of Information Technology (DIT) at the Technological Institute of the Philippines Quezon City in 2013 and graduated with Highest Honors. He took up his master's degree in Computer Science at De La Salle University Manila in 2006 and obtained BS Computer Science at Emilio Aguinaldo College Manila in 1994.

He is currently the Dean, School of Computer Studies, Emilio Aguinaldo College Manila. His research interests include Data Mining and Data Security.

Dr Sison is a member of International Association of Engineers (IAENG), Philippine Society of IT Educators and Computing Society of the Philippines. Currently, he is a Technical Committee Member of International Academy, Research, and Industry Association (IARIA) for International Conference on Systems (ICONS)

Dr. Bartolome T. Tanguilig III took his Bachelor of Science in Computer Engineering in Pamantasan ng Lungsod ng Maynila, Philippines in 1991. He finished his Master's Degree in Computer Science from De La Salle University, Manila, Philippines in 1999, and his Doctor of Philosophy in Technology Management from Technological University of the Philippines, Manila in 2003. He is currently the Assistant Vice President for Academic Affairs and concurrent Dean of the Graduate Programs of the Technological Institute of the Philippines, Quezon City.

Dr. Tanguilig III is a member of the Commission on Higher Education (CHED) Technical Panel for IT Education (TPITE), the chair of the CHED Technical Committee for IT (TCIT), the founder of Junior Philippine ITE Researchers (JUPITER), Vice President – Luzon of the Philippine Society of IT Educators (PSITE), board member of the PCS Information and Computing Accreditation Board (PICAB), member of the Computing Society of the Philippines (CSP) and a program evaluator / accreditor of the Philippine Association of Colleges and Universities Commission on Accreditation (PACUCOA).