The Eurasia Proceedings of
Educational & Social Sciences (EPESS)
ISSN: 2587-1730

The Eurasia Proceedings of Educational & Social Sciences (EPESS), 2015

Volume 2, Pages 68-73

ICEMST 2015: International Conference on Education in Mathematics, Science & Technology

IMPACT OF ENCRYPTED MULTIPLE CHOICE EXAM ON STUDENT SUCCESS

Mehtap KÖSE ULUKÖK
Departmet of Computer Engineering
Cyprus International University
Haspolat, Lefkoşa-KKTC

Zehra BORATAŞ ŞENSOY
Departmet of Computer Engineering
Cyprus International University
Haspolat, Lefkoşa-KKTC

Cagin KAZIMOGLU
Departmet of Information Systems Engineering
Cyprus International University
Haspolat, Lefkoşa-KKTC

ABSTRACT: Due to the rapid advancement of technology, the science of cryptography increasingly gained importance. Basically, the encryption algorithms used to encrypt the message or data. This work is motivated from *ÖSYM* (National University Entrance Exam of Turkey in 2011). The main aim of this study is to analyse the impact of encrypted multiple choice exam on students' success in Computer I course which is offered to Faculty of Law at Cyprus International University. Therefore, the study uses the results of an encrypted and non-encrypted multiple choice exam used in Computer I course. Encrypted multiple choice exam involves individual question sheets for each student having their own answer keys. For this reason, the original exam questions were arranged differently for each student. Thus, a separate answer key is created for each one of the students. While there were 150 students who took the course in fall 2011-2012, there was no assigned priority to any of the questions. In the implementation, the generated one-time pads (keys) are permutations of *n* numbers where *n* was the number of questions. This paper aims to compare effect of encrypted exam with non-encrypted exam results on different groups of students' success, using descriptive and inferential statistics. It is aimed to measure whether or not there is a correlation between the encrypted and non-encrypted exam results.

Key words: cryptography in education, encrypted exams, assessment in education, assessment methods to measure student success

INTRODUCTION

There are several studies searching the effect of examination types on students' success such as effect of assement techniques on programming courses are analyzed in (Yurtkan, K. Kazıımoglu C. Tekguc, U., 2014) and (Kazıımoglu, C. Tekguc, U. Yurtkan, K., 2014).

Multiple choice questions are generally generated from a list of questions. To prevent cheating, several booklets are prepared by shuffling the questions. There are some tools that generates tests from a databank of static questions (Fong, A.T. Siew, H.H. Yee, P.L. Sun, L.C., 2007). This online assesment system adaptively selects question indices. Another type of automatic question generation is based on estimating students' profile. Both of above systems require authoring and storing huge number of questions. Uğurdağ et. al. (Ugurdag, H. F. Argalı, E. Eker, O. E. Basaran, A. Gören, S. Ozcan, H., 2009) developed a tool that dynamically generates questions based on some parameters to have myriad number of question versions. This system also works online.

- Selection and peer-review under responsibility of the Organizing Committee of the conference

*Corresponding author: Mehtap KÖSE ULUKÖK- icemstoffice@gmail.com

This study is motivated from the national university entrance exam of Turkey in 2011 (*ÖSYM*). Same questions were used for all students' booklets having different answer keys. The examination was a written exam and it was performed in classrooms. Similarly, the encrypted multiple choice exam also uses same questions and individual answer keys are generated for all booklets.

Students' results of encrypted and non-encrypted multiple choice examinations are compared and analyzed using descriptive and inferential statistics.

CRYPTOLOGY

Cryptography and cryptanalysis are two main fields of cryptology. Cryptography deals with the encryption of messages and data. Encryption algorithms are classified as symmetric and asymmetric encryption methods (Kodaz, H. Botsallı, F.M., 2010). Symmetric encryption uses single key and asymmetric encryption method uses two keys, general key and special key, for encryption and decryption. Cryptanalysis is the study of decryption or analysis of encrypted message. The first crypto system was used by Julius Caesar (Şahin, M. Ekin, A.B., 2011). Caesar encryption is one of the basic encryption method which based on the modular arithmetic. The process of encrypting a message in Caesar encryption can be performed by shifting the letters of an alphabet. An encryption of a letter x with key k is performed with encryption function (1) and the decryption of same letter is performed with decryption function (2).

$$E_k(x) = (x + k) \bmod 26 \quad (1).$$

$$D_k(x) = (x - k) \bmod 26 \quad (2).$$

For example, a message "CAN" is encrypted with function (1) and key k=3. The result of encryption is "FDQ" with Caesar encryption algorithm. The same key is used to decrypt the encrypted message to obtain the original one. Although Caesar algorithm is easy to use, it can be easily broken (Şahin, M. Ekin, A.B., 2011).

Vernam method is another symmetric encryption which also known as one-time pad encryption. One-time pad encryption firstly discovered in 1882 by Frank Miller (Markoff, 2011). The same method was reinvented in 1917 by Gilbert Stanford Vernam and Joseph Mauborgne without be aware of its first invention (Markoff, 2011). This encryption method based on a random key for each message which has the key length of original message length. One-time pad encryption is the only method which is theoretically proven as unbreakable (Shannon, 1949). However, this encryption method is not preferred in practice because of its implementation difficulty.

Implementation of Encrypted Multiple Choice

Symmetric key encryption methods encrypt and decrypt messages using the same key. Original message is called plain text and encrypted message is called as cipher text. In Vernam encryption, a message m having j number of characters (m_1, m_2,..., m_j) is encrypted using function (3), and a cipher text c (c_1, c_2, ..., c_j) with key k (k_1, k_2, ..., k_j) is decrypted using function (4).

$$E(m_j, k_j) = c_j \quad (3).$$

$$D(c_j, k_j) = m_j \quad (4).$$

Table 1. Multiple Choice Question Encryption

Student IDs	Randomly generated key for each student (k_j), $1 \le j \le N$, j is an integer	Encrypted answer keys for each student
546875	5, 9, 15, n, … , 20	a, c, a, b, …, d
…	…	…
153467	12, n, 3, 9, … , 17	c, b, a, b, …, a

In this study, modified Vernam encryption method is used to implement encrypted multiple choice exam. The difference comes from the nature of the problem. Instead of truly random keys, one-time pads are generated from a set of original question indices. The original exam questions are randomly ordered for each student. Thus, a separate answer key is created for each one. Each answer key is a sequence of length n. The possible number of randomly generated keys are permutations of n numbers where n is number of questions.

The student numbers are assumed to be eight digit positive integer M_i (i=1,...,N, N is the number of students). Students' questions and their corresponding encrypted correct answers are summarized in Table I.

In this application, the encrypted students' answer keys are calculated by the encryption function (5).

$$E(m_j, k_j) = (m_j + k_j) \bmod 4 \qquad (5).$$

In modular arithmetic operation, the second operand must be the number of choices. The result of mod operation is coded to "*a*, *b*, *c*, and *d*" respectively as correct answer choices. The encryption process produces answer keys for each student with the length of number of questions.

The number of possible keys is 1.55×10^{25} for 25 questions. Even if the same key is randomly generated for more than one student, different answer keys are created. This is because, unique student numbers are used in encryption process. If any of the students in the exam tries to decrypt the corresponding answer key, s/he needs to guess the original question index in their questions. The probability to find the possible key is 1/(25!). The student's encrypted multiple choice exam preparation process is shown in Figure 1.

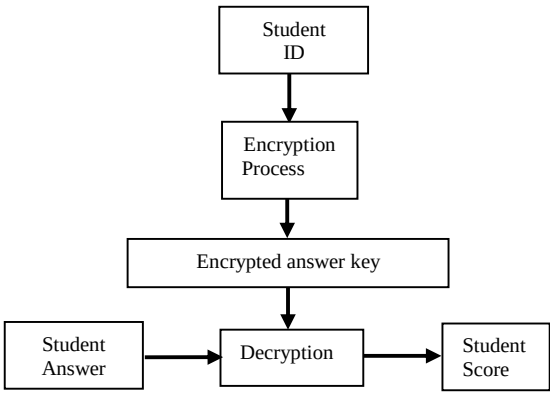

Figure 1. Encryption And Decryption Processes For Individual Student's Question Booklet.

The decryption process of the implementation is performed by comparing the student answers with the corresponding answer keys. Student scores are calculated as the result of decryption. The implementation details of encrypted multiple choice exam can be found in (Ulukok, M.K. Sensoy, Z.B., 2012).

EXPERIMENTAL STUDY

A total of 150 comparable valid results from non-encrypted and encrypted exams were gathered and entered into IBM software package used for statistical analysis (SPSS). The results of the exams were gathered randomly without considering whether or not students have prior knowledge in the subject. The encrypted and non-encrypted exam results are used as raw data to investigate the following research question:

Research Question	Null Hypothesis (H_o1)	Alternative Hypothesis (H_a1)
Is there a significant correlation between student's encrypted and non-encrypted exam results?	There is no significant correlation between students' encrypted and non-encrypted exam results.	Students' encrypted and non-encrypted exam results are significantly and strongly correlated with each other.

In order to examine the results accurately in the context of the above research question, it was important to identify the correct method for an inferential statistical analysis. As the experimental structure is based on investigating the correlations in a sample group, it was essential to investigate the distribution of data before evaluating the correlations. Therefore, a procedure for carrying out either a Pearson's product-moment correlation coefficient or a Spearman's rank-order correlation could be performed. A Pearson's r was to be selected should the data captured comes from a normally distribution and similarly, Spearman's correlation was available if the data captured did not come from a normally distributed population.

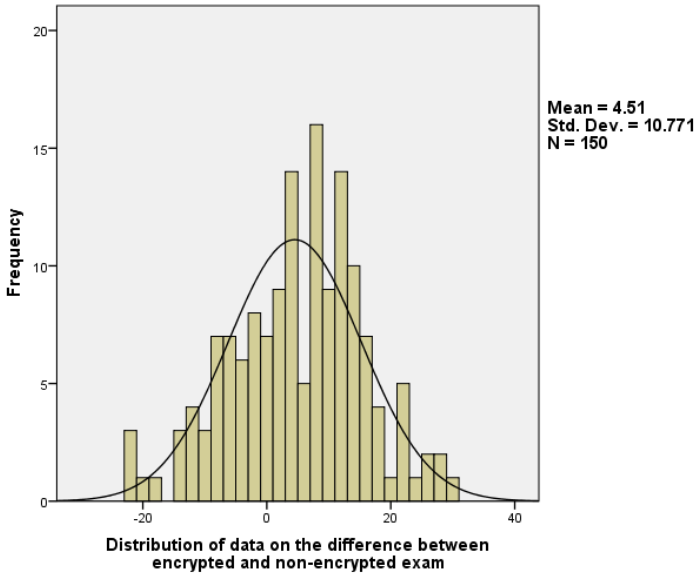

Figure 2. Shows The Histogram Distribution Of Data Based On The Difference Between Encrypted And Non-Encrypted Exam.

Figure 2 illustrates the histogram distribution of data collected from the difference of encrypted and non-encrypted exam results. As seen from the figure, the histogram indicates the distribution of data as skewed to the right. Additionally, the difference between encrypted and non-encrypted exams was found to be positive. Based on the distribution of data, there are skewness issues on the data distribution as considerable number of responses are on the right side of the histogram. Although the distribution of data on the histogram provides an initial overview for the normal data distribution, the histogram itself is arguable tool to determine whether or not data came from a normally distributed population. To investigate the distribution of data distribution further, it was essential to analyse the Normal Q-Q Plot of distribution.

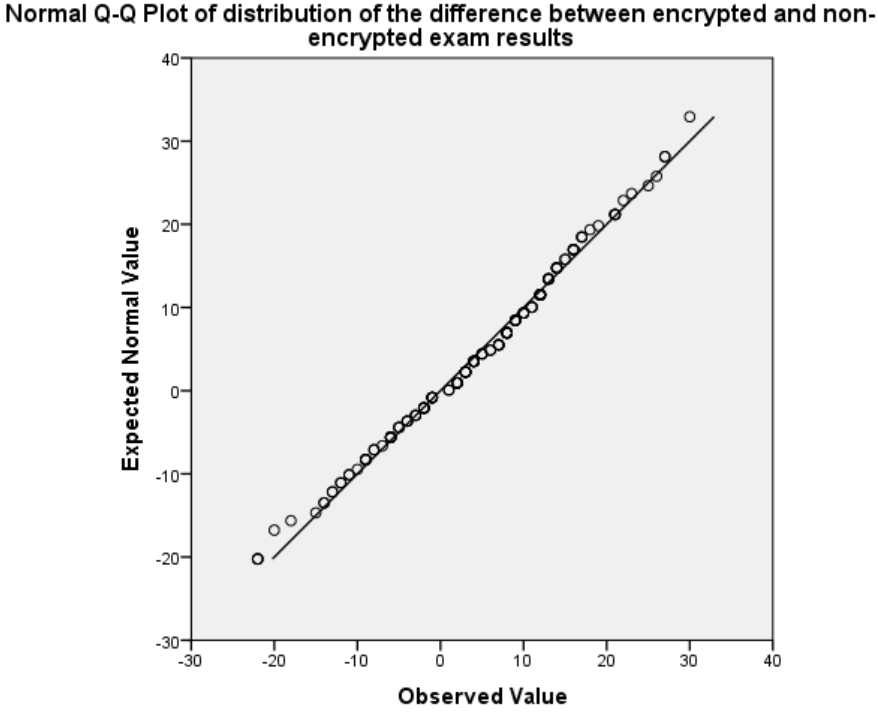

Figure 3. Normal Q-Q Plot Of Distribution Of Data On The Difference Between Encrypted And Non-Encrypted Exam Results.

Figure 3 illustrates the distribution of data collected from the difference between the encrypted and non-encrypted exam. As histogram is not a very reliable tool for measuring whether or not data came from a normally distributed popular, it was essential to look into Normal Q-Q plots and the results of a normality test (specifically *Shapiro-Wilk test* since the population number is not high). The linear line on the above figure represents a perfect normal distribution on data set. The Circles on the Q-Q plots are the observation nodes

which represents the difference of encrypted and non-encrypted exams. As it can be seen from the above figure, majority of data nodes embrace the linear line whereas those nodes at the edges are not on the line. Additionally, the expected normal values (i.e. the difference between the exams) go up to 40 whereas the same value only goes down to -30. Hence, the Q-Q plot supports the findings of the histogram and indicates that the data distribution is indeed skewed to the right. However, as majority of the nodes embrace the linear line, the Q-Q plot provides strong evidence that the data came from a normally distributed population.

Table 2. Shapiro-Wilk Normality Test

	Shapiro-Wilk		
	Statistic	df	Sig.
exam with encryption – exam without encryption	.989	150	**.282**

To validate the findings of Q-Q plot, a normality test (i.e. Shapiro-Wilk) was conducted to ensure whether or not the data came from a normally distributed population. Table 2 illustrates the findings of the Shapiro-Wilk normality test which is a normality test used especially when the sample size is not very large. If the Sig. value (P) of the Shapiro-Wilk Test is greater than 0.05 (P>0.05), this indicates that the data comes from a normally distributed population. On the other hand, if the Sig. value is below 0.05 (P<0.05), the data significantly diverge from a normal distribution. As it can be observed from the table, the Sig. value is greater that 0.05 (P=0.282), which provides strong evidence that the data came from a normally distributed population.

Table 3. Pearson Product-Moment Correlation Coefficient Showing Relationship Between Exams Without Encryption And Exams With Encryption

		Exam without Encryption	Exam with Encryption
Exam without Encryption	Pearson Correlation	1	**.387****
	Sig. (2-tailed)		.000
	N	150	150
Exam with Encryption	Pearson Correlation	**.387****	1
	Sig. (2-tailed)	.000	
	N	150	150

**. Correlation is significant at the 0.01 level (2-tailed).

A *Pearson's r* was computed to assess the relationships among the exams (i.e. encrypted and non-encrypted) since the Normal Q-Q plots and the Shapiro Wilk normality test provided strong evidence that data came from a normally distributed population. Although there are only crude estimates available for interpreting the strength of a correlation, a strong positive correlation between two or more variables is identified when *Pearson's r* is equal or greater than +0.7. Correspondingly, a modest strong correlation ranges from +0.49 to +0.69 and a weak relation is recognized to be between +0.2 and +0.39. Any correlation that ranges between +0.01 and +0.019 is often accepted as negligible. In addition to these, the negative correlations follow the same guidelines but with a negative value rather than positive.

As shown in Table 2, the correlations between the encrypted and non-encrypted exams are in positive direction, significant but weak. According to the results of the Pearson's correlation, there is a positive, significant but a weak association in between encrypted and non-encrypted exams (r=0.387, n=150, p=0.001). This means that the Pearson's coefficient provides strong evidence that the association between the encrypted and non-encrypted exams is feeble (r^2=0.149, 15%).

CONCLUSION

Based on the analysis of data, two different conclusions can be drawn from the Pearson's correlation result. Firstly, those students who did well in their non-encrypted exams also did reasonably well in their encrypted exams as the difference between the coefficient numbers is small. Secondly, there is a significant but a very weak relationship between the difference of students' encrypted and non-encrypted exam results (r^2=0.14). The correlation percentage between the two exam results was found to be 14% which is low. This provides strong reasons to believe that those students who did well in their non-encrypted exams also did well in their encrypted exams. In other words, there is strong evidence from the Pearson's correlation test that proves preparing an exam encrypted or non-encrypted has negligible effect on students' exam results. There is another sample of size 220 (students' results in fall 2012-2013), which will be analyzed in future work.

REFERENCES

Fong, A.T. Siew, H.H. Yee, P.L. Sun, L.C. (2007). An intelligent online assessment system. *Journal of WSEAS Transactions on Computers.*, 552-559.

Kazimoglu, C. Tekguc, U. Yurtkan, K. (2014). Correlations Among Assessment Techniques Used In An Introductory Programming Course. *International Conference on Education in Mathematics, Science and Technology*. Konya, Turkey.

Kodaz, H. Botsallı, F.M. (2010). Simetrik ve asimetrik şifreleme algoritmalarının karşılaştırılması. *Journal of Technical-Online.*, 10-23.

Markoff, J. (2011, July 25). *Codebook shows an encription form dates back to telegraphs.* Retrieved from The Newyork Times.: http://www.nytimes.com/2011/07/26/science/26code.html?ref=science

Shannon, C. (1949). Communication theory of secrecy sytems. *Bell systemtechnical journal.*, 656-715.

Şahin, M. Ekin, A.B. (2011). *Kriptoloji: Ankara Üniversitesi Açık Ders Materyalleri.* Retrieved from http://acikders.ankara.edu.tr/course/view.php?id=42

Ugurdag, H. F. Argalı, E. Eker, O. E. Basaran, A. Gören, S. Ozcan, H. (2009). Smart Question (sQ): Tool for Generating Multiple-Choice Test Questions. *8th WSEAS International Conference on EDUCATION and EDUCATIONAL TECHNOLOGY*. Italy.

Ulukok, M.K. Sensoy, Z.B. (2012). Encrypted Individual Multiple Choice Questions. *5th International Conference on Information Security&Cryptology*, (pp. 319-321). Ankara, TURKEY.

Yurtkan, K. Kazimoglu C. Tekguc, U. (2014). Evaluation of algorithm implementation assessment methods based on a data structure course. *International Conference on Education in Mathematics, Science and Technology*. Konya, Turkey.