REiD (Research and Evaluation in Education), 6(1), 2020, 20-31
Available online at: http://journal.uny.ac.id/index.php/reid

Testing the influence of SDES instructional media on the results of cryptography learning

[*1]Soeprijanto; [1]Aodah Diamah; [1]Prasetyo Wibowo Yunanto
[1]Faculty of Engineering, Universitas Negeri Jakarta
Jl. Rawamangun Muka, Rawamangun, Pulo Gadung, Kota Jakarta Timur, DKI Jakarta 13220, Indonesia
[*]Corresponding Author. E-mail: soeprijanto@unj.ac.id

Submitted: 6 February 2020 | Revised: 2 April 2020 | Accepted: 6 April 2020

Abstract

This study aims to examine the influence of Simplified Data Encryption System (SDES) simulation on student learning outcomes in Cryptography lessons. The research employed a quasi-experiment. Data analysis to test the SDES simulation model was performed using ANOVA 2x2. The U-Mann Whitney Test was chosen to examine differences in student learning outcomes of treatment groups and control groups, while the effectiveness of the media is determined by differences in student learning outcomes between the pre-test and post-test results in the two groups. The test results show that: (1) There is a difference between the treatment group and control group, indicated by the U-Mann Whitney Test result (U_{count} = 15 < U_{table} = 23; α = 0.05), which means there is a difference of student learning outcome between students given learning by DES simulation media and those by PowerPoints Media. (2) There is a difference in the cryptography learning outcomes for the students with the high initial ability between the treatment group and the control group. The test result is U_{count} = 0.5 < U_{table} = 2; at α = 0.05. (3) There is no difference in student learning outcomes for low initial ability student groups using the DES simulation media, with high ability students group using PowerPoints Media; the statistical test results show U_{count} = 11 > U_{table} = 2; at α = 0.05. This study concludes that using U-Mann Whitney, it can prove that the SDES simulation model developed is effective for improving student learning outcomes in Cryptography lessons.

Keywords: *SDES, student learning outcomes, cryptography lessons*

How to cite: Soeprijanto, S., Diamah, A., & Yunanto, P. (2020). Testing the influence of SDES instructional media on the results of cryptography learning. *REiD (Research and Evaluation in Education), 6*(1), 20-31. doi:https://doi.org/10.21831/reid.v6i1.30024.

Introduction

Learning media plays an important role in achieving learning objectives by providing an opportunity for teachers to develop students' knowledge, motivation, and classroom engagement. One of the learning media is a computer simulation that can be used by teachers for developing students' conceptual understanding. Computer simulation can facilitate students to develop knowledge and construct their understanding of the topics. In the computer simulation, students can repeat and explore the process to understand the concepts.

Researchers have successfully developed a Data Encryption System (DES) simulations using effective simulation design principles and avoiding cognitive overload on students. Excess Simulation DES development results include: (1) attention cueing to make it easier for students to focus and understand the simulations presented; (2) navigation and control feature to enable students to control

the simulation; and (3) only use dynamic visualization if necessary. After all of the activities during the assessment, analysis, design, and development, are completed, then we are ready for summative evaluation, to judge the effectiveness of the solution.

Data Encryption Standard (DES) and Simplified Data Encryption Standard (SDES) are designed to assist students in learning of modern cryptoanalytic techniques. Properties and structure in SDES are similar to those in DES, but SDES is simpler and makes students easier for encryption and decryption by hand with a pencil and paper. The simplified DES is designed only for educational purposes. Learning SDES provides insights on DES and other block ciphers and insights on various cryptanalytic approaches. Four levels of evaluation are identified, including reaction, learning, behavior, and results, to see the effectiveness of media influence of DES simulation of the development result on students' learning outcomes.

The research employed experimental research to prove the improvement of student learning outcomes. The problem arises when the number of students who joined the course of Cryptography as a respondent is limited, so the data obtained during potential research is not normally distributed. As an alternative data analysis solution is no longer conducted with parametric statistics, instead, to prove differences in student learning outcomes between treatment groups and control groups, Non-Parametric Statistics was used.

The Mann−Whitney U-test and the Kolmogorov−Smirnov two-sample test are non-parametric statistical procedures for comparing two independent samples. The parametric equivalent to these tests is the t-test for independent samples.

This research problem includes: (1) whether through the characteristic of the U-Mann Whitney Test, the differences in student learning outcomes between treatment groups and control groups can be demonstrated; (2) whether there is a difference in student learning outcomes of the group of students who have low initial ability given cryptographic learning with DES simulation media and a group of high initial ability students who were given cryptographic learning with PowerPoint media; (3) whether there is any influence of using DES simulation to the student learning outcomes of Cryptography. Meanwhile, the novelty of this study is the existence of a solution to the testing of educational media toward a relatively small number of student samples where the data obtained are not normally distributed and to support the learning process effectively in the cryptography course. Thus, this study aims to examine the influence of Simplified Data Encryption System (SDES) simulation on student learning outcomes in Cryptography lessons.

Cryptographic Learning Outcomes

Learning outcomes are abilities obtained by individuals to get learning experiences. According to Briggs (1979, p. 149), learning outcomes are all competencies that are obtained through the learning process.

Further, Bloom, Englehart, Hill, Furst, and Krathwohl (1978, p. 7) state that learning outcomes can be classified into three domains: cognitive, affective, and psychomotor domains. Gagné (1983, pp. 27–28) believes that learning outcomes are competencies that include verbal information, intellectual skills, motor skills, attitudes, and cognitive strategies and values. Verbal information and cognitive skills are students' knowledge or understanding of theory, while motor skills are students' skills, and attitudes are the values of student work, all of that as learning outcomes. Based on the aforementioned opinions, in this study, learning outcomes are defined as individual competencies including knowledge, skills, and attitudes obtained by students through the learning process.

Cryptography comes from the word *Crypto* which means secret, and *Graphy* which means writing (Sasongko, 2005, p. 160). Ariyus in Pratama and Latifah (2014, p. 19) asserts that in general, cryptography consists of three important main parts, namely, the encryption section, the description, and the key sections. The encryption algorithm is a function used to perform encryption and decryption work. According to Kromodimoeljo (2010, p. 5), the encryption technique is a way in which the original text is changed using an

encryption key into a random script that is difficult to read by someone who does not have a decryption key to decrypt the key using the so-called "decryption key" in order to get the original data back.

In modern cryptography, there are various kinds of algorithms that are intended to secure information sent over a computer network. According to Insights for Professionals (IFP) (2018, p. 1), modern cryptographic algorithms consist of three parts: (1) Symmetric Algorithm, (2) Asymmetric Algorithm, and (3) Hybrid Algorithm. Symmetric algorithm is an algorithm that uses the same key for encryption and description. The application of the symmetric algorithm is used by several prayer algorithms, one of which is the Data Encryption Standard (DES).

Based on the aforementioned studies, it can be concluded that Cryptographic learning outcomes are students' knowledge and skills towards data encryption and description techniques, as well as attitudes obtained by students through the learning process of cryptography. Operationally, the learning outcomes measured in this study are only the knowledge and skills of students about cryptography, while the aspects of attitude are not measured.

SDES Instructional Media

Levie and Lentz in Arsyad (2016) suggest four functions of instructional media, especially visual media, namely: (1) attention function, which sees that visual media is interesting and directs the students' attention to concentrate on the content of the lesson; (2) affective function, i.e. the visual media seen in student's enjoyment when studying; (3) cognitive function, i.e. the visual or image symbols that facilitate the learning outcome of goals for understanding and remembering information; (4) the compensatory function, that is, to provide a context for understanding the text and help the weak student in reading to organize the information in the text and recall it. Thus, the use of media in the learning process can generate new desires and interests, ease in remembering information, and assist students in organizing and recalling text lesson material that will ultimately affect student learning outcomes. Cheung (2009, p. 9) states that media production goes beyond mere comprehension and analysis in Bloom's taxonomy. Those involved in media production have to include the production of meaning and design using a range of symbol systems in evaluating the availability of a wide range of media resources.

Media production is not just mere understanding and analysis as in Bloom's taxonomy. Media production must include meaning and design using various symbol systems in evaluating the availability of various media resources. The effectiveness of media influences can be determined at least with two criteria, namely, (1) the difference in the mean of a result of student learning when compared with other media usage, and (2) an increase in average student learning outcomes when the learning media is used. Moreover, Lee and Owens (2004, p. 162) insist that successful multimedia development methodologies tend to include these elements: (1) *Design-time prototyping:* creating an early application-system prototype so as to review, test, and approve the interface design, media elements, script, or map. This is an efficient method for rapid development. (2) *Evolutionary development:* using each stage of prototyping and development as the basis from which to evolve the next prototype. For this to be successful, design decisions that do not involve the content must be locked in. (3) *The use of rapid development tools (RDT):* templates are useful for parallel development projects. They are particularly useful in projects where content is added in an iterative process, as it is made available. Templates are created and used as a framework for content as it is identified. Computer simulation design to support the learning process effectively should consider several factors, one of which, according to Plass, Homer, and Hayward (2009), is a control and navigation feature that allows students to simulate Plass et al's opinion is in line with the arguments of Hennessy et al. (2007) and Windschitl (1998). Controls that allow students to stop, repeat, or manage speed simulations, facilitate them to consolidate what they are learning. Another factor to consider is the cognitive load that students will experience when running the simulation. The information that is dynamically visualized in the simulation according to

Plass et al. (2009) requires a more severe mental process than information which is presented in the static form, however, properly designed dynamic visuals can help students learn more effectively. Cueing is one of the effective ways examined by de Koning, Tabbers, Rikers, and Paas (2007). Cueing in dynamic visualization can help students focus on specific processes they need to understand. According to de Koning et al., cueing in visualization can be a color or arrow that guides the students to an important aspect of the simulation. Associated with cognitive loads, according to Höffler and Leutner (2007), dynamic visualization will only be more effective than static visualization if its nature does represent the process to be studied and not merely decorative. Data Encryption Standard (DES) is one of the topics in Cryptography Courses. DES is originally designed to be implemented only in hardware systems and is, therefore, extremely slow in software applications (Rabah, 2005, p. 312). DES is a symmetric-key algorithm for the encryption of digital data. Compared to classical cryptographic algorithms, DES includes complex and elusive algorithms. DES was originally designed by IBM before it became the standard set by the National Institute of Standards and Technology in 1977. Technically, the DES algorithm was resolved when published a scientific article containing an analysis for brute-force attack DES (Biham & Shamir, 1991, p. 4). However, at that time to carry out the attacks proposed by Biham and Shamir, it takes a lot of plaintexts so that the attack is not practical to do. When the computer becomes faster, the attack becomes possible and triple-DES and AES finally appear in place of DES. Nevertheless, DES remains widely used (Burr, 2006). In addition, DES is an important algorithm studied due to the basis of the triple-DES algorithm and its AES continuation algorithm. Due to the long process of DES, a simplified version of the DES called Simplified Data Encryption System (SDES). Cohen (2007, p. 14) believes that SDES was developed by Professor Edward Schaefer of Santa Clara University. The SDES algorithm is instructive and is not a secure encryption algorithm. As seen in Figure 1 and Figure 2, SDES has a process and structure similar to DES, but all the parameters have been made as simple as possible. For example, 16 rounds on DES are simplified into two rounds. According to Schaefer, with simpler structures and parameters, SDES will be more easily understood by undergraduate students.

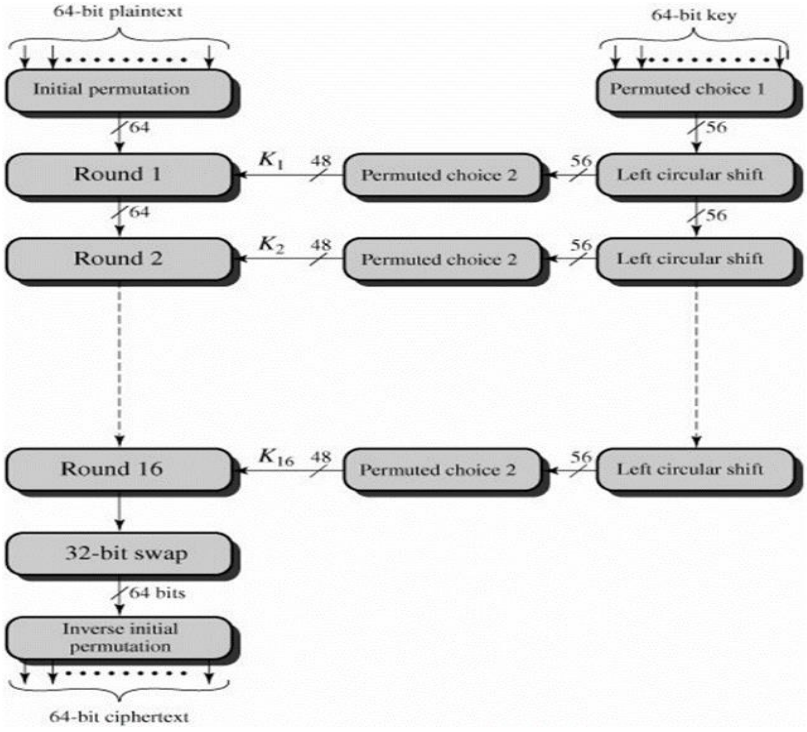

Figure 1. Data Encryption Standard (DES) (Stallings, 2002)

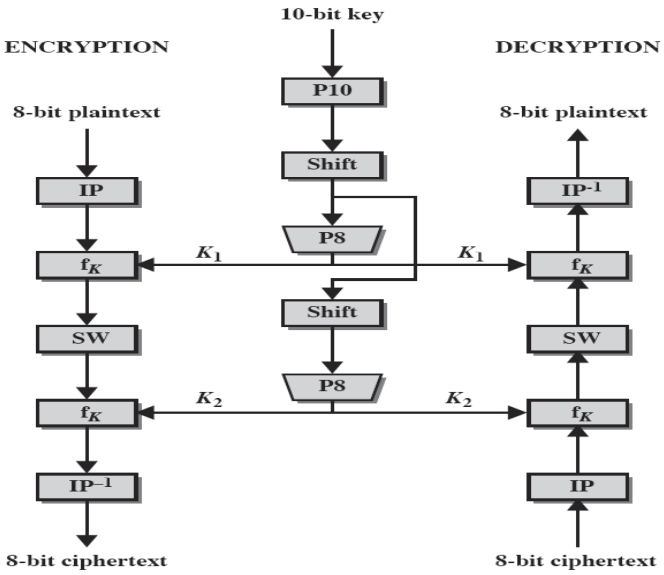

Figure 2. Structure of Simplified Data Encryption Standard (SDES) (Stallings, 2002)

The comparison between DES and SDES can be seen in Table 1. The purpose of SDES for education is that students can more easily learn about modern cryptanalytic techniques. Table 1 shows the differences between DES and SDES. SDES is similar to DES but has simpler properties and structures that are easier to understand.

Table 1. Comparison of DES and SDES

	DES	SDES
Key	64 Bit	10 Bit
Sub Key	56 Bit	8 Bit
Plain Text Processed	64 Bit	10 Bit
Number of Rounds	16	2

The Mann-Whitney (U-test)

Corder and Foreman (2014, pp. 69–70) explain that the Mann−Whitney U-test is non-parametric statistical procedures for comparing two samples that are independent, or not related. The parametric equivalent to these tests is the t-test for independent samples. Mann−Whitney U-test is used to compare two unrelated, or independent, samples. The two samples are combined and rank-ordered together. The strategy is to determine if the values from the two samples are randomly mixed in the rank-ordering or if they are clustered at opposite ends when combined. A random rank-ordered would mean that the two samples are not different, while a cluster of one sample's values would indicate a difference between them. According to Ho (2014, p. 518), the Mann-Whitney test is a non-parametric statistic used to find out whether there are differences in responses from two independent data populations when data are weaker than the interval scale. This test can be likened to a t-test test for two independent groups when a violation of the assumption of normality or data scale is not appropriate for the t-test. From Corder and Foreman (2014), Ho (2014), and Berry, Mielke Jr., and Johnston (2012, pp. 9–11), we can conclude that the U-Mann Whitney has a characteristic as an alternative test to the independent group t-test when the assumption of normality is not met. Formula (1) is used to determine a Mann-Whitney U-test statistic for each of the two samples (Corder & Foreman, 2014, p. 70). The smaller two U statistics is the obtained value:

$$Ui = n_1.n_2 + \frac{ni(ni+1)}{2} - \sum R_i \quad \ldots\ldots\ldots\ldots\ldots\ldots \quad (1)$$

Annotation:
U_i is the test statistic for the sample of interest,
n_i is the number of values from the sample of interest,
n_1 and n_2 are the numbers of values from the first and second sample,
Σ_{Ri} is the sum of the ranks from the sample of interest.

According Susetyo (2017, p. 236), the level of significance uses α =0.05, and rejection criteria H_0 for one side if $U_{count} \leq U_{table}$ formulated at an opportunity value (p) compared to the specified real level. U_{price} is selected as the smallest value from the calculation results in each group.

Method

This study utilizes the characteristic of U-Mann Whitney's Test to prove the effectiveness of learning media influence SDES simulation development result in learning cryptography. The research was conducted in Informatics and Computer Technology Education Study Program, Faculty of Engineering, in Jakarta. The study was conducted in the even semester of the academic year 2016/ 2017. The research method used to test the DES Simulation model is a quasi-experimental method with treatment by level. The quasi-experiment method is meant to see the causal relationship between two factors deliberately caused by the researcher by eliminating other disturbing factors. This research uses treatment design by level 2x2 because there are two types of treatment on independent variables. This study also controls two attribute variables consisting of two levels. The variable has the potential to affect the dependent variable. Experimental design treatment by level 2 x 2 is described in Table 2.

The variables studied consist of the independent variable and bound variable. The dependent variable is the student learning outcome of the independent variable consisting of one active variable and one attribute variable. The pre-test is considered an attribute, while the active variables in the form of learning by using PowerPoints (PPT) media. The hypothesis was tested with two levels. This variable has the potential to affect the dependent variable. Experimental ANOVA model requires sample data requirement that is used come from a population that has normal and homogenous distribution, so, before data analysis is done or hypothesis testing is done, Normality and Homogeneity need to be tested first. When it is not normal, the use of Parametric Statistics cannot proceed. In this research, the experiment was conducted by the steps illustrated in Figure 3.

Table 2. Design of ANOVA Experiments (2x2)

Level	SDES Simulation Media (Treatment Group)	PowerPoint Media (Control Group)
High initial ability (Pre-Test)	A_1B_1	A_2B_1
Low initial ability (Pre-Test)	A_1B_2	A_2B_2

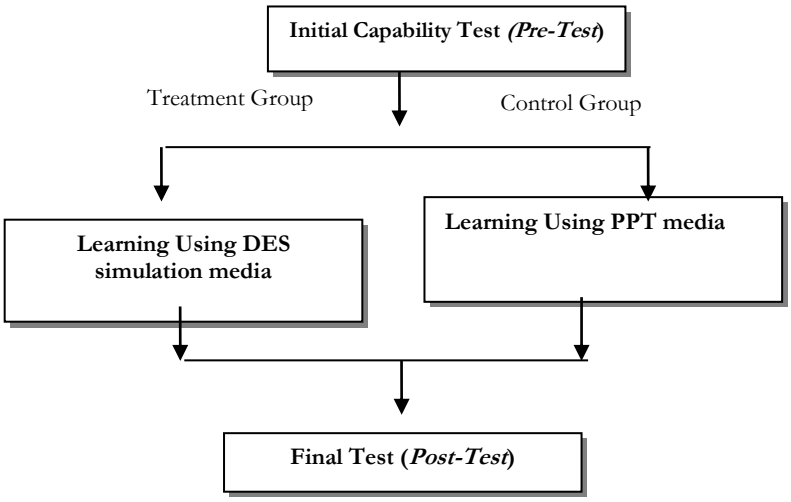

Figure 3. Experiment Steps

Table 3. Distribution of Research Respondents

Level of Ability	SDES (Treatment Group)	PPT (Control Group)	Total
High Ability Pre-Test Results	5	5	10
Low Ability Pre-Test Results	5	5	10
Total	10	10	20

Table 4. Data of Pre-Test and Post-Test Results

	Mean	Median	Modus	Deviation Standard
Pre-Test	55.70	53.00	44.00	14.40
Post-Test (Treatment Group)	87.60	80.00	80.00	0.00
Post-Test (Control Group)	65.00	65.00	65.00	9.78

Table 5. The Value of *Lilliefors*

Group	L_{count}	L_{table}	Conclusion
Simulation DES(Treatment)	0.6895	0.2580	Abnormal
Power Points (Control)	0.0763	0.2580	Normal
Treatment High Level Pre-Test	0.6134	0.3370	Abnormal
Treatment Low Level Pre-Test	0.5707	0.3370	Abnormal
Control High Level	0.6188	0.3370	Abnormal
Control Low Level	0.5870.	0.3370	Abnormal

Each step in Figure 3 is elaborated as follows. (1) A pre-test is the initial test performed using an objective test in the form of multiple-choice questions. Preliminary test results were used to divide the respondents into two groups: high initial ability group and low initial ability group. Based on the results of the grouping of respondents at each level, 50% taken to be treated as the Treatment group is taught using DES simulation media, while others are given lessons by using PowerPoint media. (2) In the experimental step, the participants were divided into two groups, namely, the treatment group and the control group. Each group consists of students who have low initial ability and who have high initial ability. Treatment Group was taught by using DES Simulation Media. The control group was taught using PowerPoint media. (3) In the provision of Post-Test, the final test is done with the same problem as the initial stage. The final test result is used to test the research hypothesis.

The sample size is 20 students. The sample distribution in each group is presented in Table 3.

Findings and Discussion

The research data are presented under the form of a summary of information, including the minimum, maximum, mean, or median, standard, deviation, variance, and theoretical ranges of each variable. This research data are obtained from 20 respondents. Data of the research results consist of initial ability and result data of the Post-Test. The description of the research results for each complete variable can be seen in Table 4.

Test Requirements Analysis

Before the data analysis was carried out to test the hypothesis, the analysis requirements need to be tested first. One of the tests is the normality test. The normality test was performed using the Lilliefors test of the null hypothesis which states that the sample originated from a normally distributed population versus an alternative hypothesis states that the sample is from a population that is not normally distributed. The calculation value of Lilliefors is presented in Table 5.

From the calculation of the value of Lilliefors, it turns out that from almost all of the groups tested, the data are not normal. Only one variable has normal data, namely, on the control group student learning outcomes. On that basis, the researchers decided that ANOVA analysis cannot proceed. Instead, non-parametric statistics are used to prove the difference in student learning outcomes between the treatment group and the control group. The statistic used to test the

hypothesis is the U-Mann Whitney Test. U-Mann Whitney Test can be equated with a t-test for two independent groups drawn from one population-scale lower than interval and assumption of the distribution of sample normality (Ho, 2014).

Hypothesis Testing

Hypothesis was tested using a formula previously presented in Formula (1) to determine the Mann−Whitney U-test statistic for each of the two samples. Meanwhile, the value of U_2 is calculated by the formula $U_2 = n_1.n_2-U_1$. The level of significance uses $\alpha = 0.05$, while the criteria rejection H_0 if the U_{value} of the calculated result is less than the value of U_{table} at probability 0.95 or at $\alpha = 0.05$. According Susetyo (2017, p. 236), the level of significance uses $\alpha = 0.05$ and rejection citeria H_0 for one side if $U_{count} \leq U_{table}$ formulated at an opportunity value (p) compared to the specified real level.

The First Hypothesis

The first hypothesis is elaborated as follows. H_0: there is no difference in student learning outcomes between the treatment group and the control group. H_1: there are differences in student learning outcomes between the treatment group and the control group.

Table 6. Data of Students' Learning Outcomes

Treatment Group	Rank	Control Group	Rank
95	20	75	13.5
85	19	70	10.5
75	13.5	70	10.5
80	16.5	65	7.5
80	16.5	65	7.5
70	12	55	3
80	16.5	60	4.5
50	2	40	1
65	7.5	60	4.5
80	16.5	65	7.5
Total Rank	**140**		**70**

The data on the students' learning outcomes are presented in Table 6. From Table 6, the value of $R_2 = 70$. When this value is entered to Formula (1), the value of U_1 obtained is elaborated as illustrated in Formula (2):

$$U_1 = 10.10 + \frac{10(10+1)}{2} - 70 = 85 \quad \ldots\ldots\ldots\ldots \quad (2)$$

Meanwhile, the value of $U_2 = n_1.n_2 - U_1 = 10.10 - 85 = 100 - 85 = 15$. The calculation results obtained value U arithmetic of 15 When this value is confirmed in table U for $n_1 = 10$ and $n_2 = 10$, $\alpha = 0.05$ got U table value of 23. Thus, statistical test results prove that $U_{count} < U_{table}$ ($15 < 23$). It is concluded that H_0 is rejected and H_1 is accepted. It means that there is a difference between the treatment group and the control group (see Table 7). The result of the calculation of the mean obtained that the mean to the treatment group is 87.5. This value is higher than the mean of the control group amounted to 65. It shows that the students' learning outcomes of the group of students who were given learning from the DES simulation media are higher than the students who were given the learning by using PowerPoints (PPT) media.

The Second Hypothesis

The second hypothesis is elaborated as follows. H_0: there is no difference in student learning outcomes of cryptography between those using SDES simulation media on high-ability cryptography (A1B1) and high-ability student group learning cryptography using PowerPoint media (A2B1). H_1: there is a difference in student learning outcomes of cryptography between those using DES simulation media on high ability students (A1B1), and those using PowerPoint media on the high-ability students (A2B1).

This hypothesis was tested in two stages. The first stage is to test the significance of differences in student learning outcomes between the treatment group and control group with the U-Mann Whitney Test. The second stage is to compare the mean values of both.

The result of the difference test of student learning outcomes at the students with high initial ability obtained U_{table} price with probability of 0.95 (U-α) or α (0.05) with the sample number 1 (n_1) and number 2 respectively = 5 and 2. The value U calculation result is 0.5, so the statistical test results $U_{count} < U_{table}$ ($0.5 < 2$). Thus, it is concluded that H_0 is rejected and H_1 is accepted (see Table 8).

Table 7. Hypothesis Test Results 1

Hypothesis 1	$U_{count} = 15$	$U_{table} = 23$	H_0 Rejected	H_1 Accepted
Mean Value	$\overline{A1}$ =87.5	$\overline{A2}$ =65		
Conclusion	There is a difference in post-test results between student learning outcomes with SDES (A_1) and with the result of learning with PowerPoint (A_2)			

Table 8. Hypothesis Test Result 2

Hypothesis 2	$U_{count} = 0.5$	$U_{table} = 2$	H_0 Rejected	H_1 Accepted
Mean Value	$\overline{A1B1}$ = 83	$\overline{A2B1}$ = 70		
Conclusion:	There is a difference between student learning outcomes with DES simulation media and student learning outcomes with PowerPoint media, in the both groups of high ability students			

Table 9. Hypothesis Test Result 3

Hypothesis 3	$U_{count} = 11$	$U_{table} = 2$	H_0 Accepted	H_1 Rejected
Mean Value	$\overline{A1B2}$ =69.00	$\overline{A2B1}$ =70.00		
Conclusion:	There is no difference in student learning outcomes between a group of low-level students who learn cryptography to using DES simulation media and high-ability student group learning cryptography using PowerPoint (PPT)			

The Third Hypothesis

The third hypothesis is elaborated as follows. H_0: there is no difference in student learning outcomes between low-grade students who learned cryptography using SDES (A1B2) simulation media and high-ability student group learning cryptography using PowerPoint media (A2B1). H_1: there is a difference in student learning outcomes between a group of low-performing treatment (A1B2) and a high initial-ability control group (A2B1).

Through the U Mann Whitney Test, U_{table} price is obtained with probability 0.95 (U-α) or at α (0.05) with sample number 1 (n_1) and sample 2 (n_2) respectively = 5 and 2. The value of U calculation result is 11, so the statistical test results is $U_{count}<U_{table}$ (11>2). Thus, it can be concluded that H_0 is accepted and H_1 is rejected, meaning that there is no difference in student learning outcome in the low-skilled student group treated with learning using DES simulation media (A1B2) and student learning outcome in the group of high-ability students who are not treated (control group) (A2B1), as presented in Table 9.

Viewed from the average indigo obtained, it shows that the mean of the Treatment Group is 69 and the control group's average rating is 70. Therefore, it can be concluded that the student learning outcomes of low-skilled students who were given lessons with DES simulation media are more comparable than the high initial ability students who were given learning using PowerPoint (PPT) media.

When examined thoroughly from testing Hypotheses 1 to 3, the influence of learning media DES simulation on the development of students' cryptography learning results can be proven. More detail information is presented in Table 10.

Other findings through the first hypothesis calculation through U-Test also prove that the learning outcomes of the treatment group students differ from the learning outcomes of the control group students. In other words, the results of the students who were given the lesson of cryptography using DES simulation media and those who were given the lesson of cryptography using PowerPoint media is different.

This finding is also supported by the fact that the average post-test result from the treatment group reached 87.5 is much higher than the average over the control group's post-test outcome of 65. From this first hypothesis, it also shows that the U test results also correspond with the result of the student's average grade.

In line with the findings of the second hypothesis that tested the use of DES simula-

Table 10. U-test Value, Mean Comparison, and Conclusion

Hypothesis	U-Test Value	Conclusion	Findings	Mean Comparison
1	$U_{count}=15<U_{table}=23$	H_0 rejected H_1 accepted	There is a difference in student learning outcomes of cryptography between those using SDES simulation media and those using PowerPoint on all samples	87.5 : 65
2	$U_{count}=0.5<U_{table}=2$	H_0 rejected H_1 accepted	There is a difference in the student learning outcomes of studying cryptography on student with high ability between those who were taught using SDES simulation media and those taught using PowerPoint media	83 : 70
3	$U_{count}=11>U_{table}=2$	H_0 accepted H_1 rejected	There is no difference in the students' cryptography learning outcomes between the group of low ability students when learning by SDES simulation media, and a group of high-ability students learning by PowerPoint.	69 : 70

tion media in the group of high-ability students, a match of the U-Mann Whitney statistical test results with the mean of each test group is also found, where the second hypothesis proves that there is a difference between the students' learning outcomes using DES simulation media and the students' learning outcomes using PowerPoint media in a group of high-ability students, by comparison of the mean of 83.00 compared to 70.00.

Thus, the first and second problems raised in this study were answered that this study proves that the U-Mann Whitney Test can prove differences in student learning outcomes between treatment group, i.e. groups of students given learning by DES simulation media and control group, i.e. students given learning using PowerPoint. The result of statistical analysis to prove the fourth hypothesis also explains at the same time answer the third problem in this research. The results of the analysis prove that DES simulation media is an effective development result for use as a medium in teaching cryptography. It is shown that the learning outcomes of students with low initial ability can be increased so that they are not different from the high-ability students given learning cryptography using conventional media (PowerPoint). Hence, the developed DES simulation works well and can be recommended as an alternative media for cryptographic learning, especially in achieving the competence of DES mastery goals.

Conclusion

Through the U-Mann Whitney Test, it is proven that there are differences in the result of cryptography learning between students taught using SDES simulation media and those taught using PowerPoint. Then, the learning media obtained from the developed DES simulation works well and improves the students' learning in cryptography.

According to the research findings and discussion, several conclusions are drawn as follows. (1) There is a difference in terms of the post-test results between the learning outcomes of students taught using SDES (A1) and the learning outcome of students taught using PowerPoint. (2) There is a difference between the learning outcomes of students taught using DES simulation media and the learning outcomes of those taught using PowerPoint media in both groups of high ability students. (3) There is no difference in terms of the learning outcomes between the group of low-ability students who learn cryptography using DES simulation media and the group of high-ability students learning cryptography using PowerPoint (PPT).

References

Arsyad, A. (2016). *Media pembelajaran*. Jakarta: Raja Grafindo Persada.

Berry, K. J., Mielke Jr., P. W., & Johnston, J. E. (2012). The two-sample rank-sum

test: Early development. *Electronic Journ@l for History of Probability and Statistics*, *8*(December), 1–26. Retrieved from http://www.jehps.net/decembre2012/BerryMielkeJohnston.pdf

Biham, E., & Shamir, A. (1991). Differential cryptanalysis of DES-like cryptosystems. *Journal of Cryptology*, *4*(1), 3–72. https://doi.org/10.1007/BF00630563

Bloom, B. S., Englehart, M. D., Hill, W. H., Furst, E. J., & Krathwohl, D. R. (1978). *Taxonomy of educational objectives - The classification of educational goals; Handbook I: Cognitive domain*. New York, NY: David McKay.

Briggs, L. J. (1979). *Instructional design: Principles and applications*. Englewood Cliffs, NJ: Prentice Hall.

Burr, W. (2006). Cryptographic hash standards: Where do we go from here? *IEEE Security & Privacy*, *4*(2), 88–91.

Cheung, C.-K. (Ed.). (2009). *Media education in Asia*. Dordrecht: Springer Netherlands.

Cohen, A. E. (2007). *Architectures for cryptography accelerators* (Doctoral thesis, University of Minnesota, Minneapolis, MN.). Retrieved from https://pqdtopen.proquest.com/doc/304824471.html?FMT=ABS

Corder, G. W., & Foreman, D. I. (2014). *Nonparametric statistics: A step-by-step approach* (2nd ed.). Hoboken, NJ: John Wiley & Sons.

de Koning, B. B., Tabbers, H. K., Rikers, R. M. J. P., & Paas, F. (2007). Attention cueing as a means to enhance learning from an animation. *Applied Cognitive Psychology*, *21*(6), 731–746. https://doi.org/10.1002/acp.1346

Gagné, R. M. (1983). *The conditions of learning*. New York, NY: Holt, Rinehart and Winston.

Hennessy, S., Wishart, J., Whitelock, D., Deaney, R., Brawn, R., Velle, L. la, … Winterbottom, M. (2007). Pedagogical approaches for technology-integrated science teaching. *Computers & Education*, *48*(1), 137–152. https://doi.org/10.1016/j.compedu.2006.02.004

Ho, R. (2014). *Handbook of univariate and multivariate data analysis with IBM SPSS* (2nd ed.). Boca Raton, FL: CRC Press.

Höffler, T. N., & Leutner, D. (2007). Instructional animation versus static pictures: A meta-analysis. *Learning and Instruction*, *17*(6), 722–738. https://doi.org/10.1016/j.learninstruc.2007.09.013

Insights for Professionals (IFP). (2018). 3 Types of encryption to protect your data. Retrieved from Tech Insights for Professionals website: https://www.insightsforprofessionals.com/it/security/types-of-encryption-protect-your-data

Kromodimoeljo, S. (2010). *Teori dan aplikasi kriptografi*. Sunnyvale, CA: SPK IT Consulting.

Lee, W. W., & Owens, D. L. (2004). *Multimedia-based instructional design: Computer-based training, web-based training, distance broadcast training, performance-based solutions* (2nd ed.). San Francisco, CA: John Wiley & Sons.

Plass, J. L., Homer, B. D., & Hayward, E. O. (2009). Design factors for educationally effective animations and simulations. *Journal of Computing in Higher Education*, *21*(1), 31–61. https://doi.org/10.1007/s12528-009-9011-x

Pratama, R. K. P., & Latifah, F. (2014). Implementasi enkripsi dekripsi pesan teks menggunakan model Julis Caesar berbasis Object Oriented Programme. *Jurnal Techno Nusa Mandiri*, *XI*(1), 17–26. https://doi.org/10.33480/techno.v11i1.167

Rabah, K. (2005). Theory and implementation of Data Encryption Standard: A review. *Information Technology Journal*, *4*(4), 307–325. https://doi.org/10.3923/itj.2005.307.325

Sasongko, J. (2005). Pengamanan data informasi menggunakan kriptografi klasik. *Dinamik*, *10*(3), 160–167. Retrieved from https://www.unisbank.

ac.id/ojs/index.php/fti1/article/view/25

Stallings, W. (2002). The advanced encryption standard. *Cryptologia*, *26*(3), 165–188. https://doi.org/10.1080/0161-110291890876

Susetyo, B. (2017). *Statistik untuk analisis data penelitian*. Bandung: Refika Aditama.

Windschitl, M. A. (1998). A practical guide for incorporating computer-based simulations into science instruction. *The American Biology Teacher*, *60*(2), 92–97. https://doi.org/10.2307/4450426