International Journal of Advanced Research and Development
ISSN: 2455-4030, Impact Factor: RJIF 5.24
www.advancedjournal.com
Volume 2; Issue 1; January 2017; Page No. 69-73

DSE-Tutor: An intelligent tutoring system for teaching DES information security Algorithm

Abed Elhaleem A Elnajjar, * Samy S Abu Naser

Department of Information Technology, Faculty of Engineering & Information Technology, Al-Azhar University, Gaza, Palestine

Abstract
Lately there is more attention paid to technological development in intelligent tutoring systems. This field is becoming an interesting topic to many researchers. In this paper, we are presenting an intelligent tutoring system for teaching DES Information Security Algorithm called DES-Tutor. The DES-Tutor target the students enrolled in cryptography course in the department Information Technology in Al-Azhar University in Gaza. Through DES-Tutor the student will be able to study course material and try the exercises of each lesson. An evaluation of the DES-Tutor was carried out and the results were promising.

Keywords: tutoring system, teaching, information security, expert system, des algorithm, and e-learning

1. Introduction
Intelligent Tutoring Systems is a multidisciplinary field that examines how to contrive educational systems that offer custom-made instruction to individual students, as good teachers try to do. Research in Intelligent Tutoring Systems has positively elated techniques and systems that offer adaptive sustenance for student when solving problem in a diversity of domains. On the other hand, there are other educational undertakings that can take advantage from personalized computer-based provision, for example discovering interactive simulations, learning examples, and playing instructive games. Offering individualized help for these actions postures exclusive challenges, since it needs an ITS that can simulate and adapt to student performances, skills and rational states frequently not as organized and well-defined as those complicated in old-style problem solving. This paper presents DES-Tutor projects that illustrate some of these challenges [38].

Intelligent Tutoring Systems can be defined as a computerized learning settings that include computational modules in learning sciences, computational linguistics, cognitive sciences, mathematics, artificial intelligence, and other areas that create intelligent systems that are well-established computationally [38].

At its early stages ITS got a robust input from the joint need of AI and of the educational system to discover effective applications that could illustrate the power of ICAI by enhancing instruction in the delivery of efficient tutoring for each student, customized to his/her requirements and pace of learning [38]

2. Literature Review
There are many tutoring systems designed and developed for the purpose of education, some dedicated to teaching computer science students [3, 4, 8, 14, 31, 38], Arabic and English language [10], teaching programming languages [3, 4, 8, 32, 35], for debugging skills [2], Linear Programming [33, 36], effectiveness of e-learning [5, 30. 37], computer aided instruction [39], teaching AI searching algorithms [41], teaching database [9, 18, 20, 34], teaching different health topics [12, 13], teaching Computer Networks [11], teaching Computer Theory [15], teaching biology [19, 39], teaching advanced topics in information security [21], Big O Notation for Measuring Expert Systems complexity [40], intelligent tutoring system for teaching the right letter pronunciation in reciting the Holy Quran [7].

3. DES-Tutor
In this paper, we used ITSB authoring tool [38] for building the DES-Tutor. This tool designed and developed using Delphi Embarcadero XE8, 2015; this tool supported two languages: Arabic and English. It has two systems in one software. The first system is teacher system where it allows him/her to add course content, questions, answers, student profile, adjust colors and fonts of all screens, basic data for the DES-Tutor, choose the language of the interface, and level of difficulty. The second system is the student system where it allows the student to learn the lessons and try the exercises.

4. DES-Tutor Architecture
This DES-Tutor has four modules: student model, domain model, teaching model, and user interface model. The domain model presents and organizes the content in lessons/chapters. The teaching model works as controller of the whole DES-Tutor system. The student model provides the system with all needed data so it can adapt itself with the student. The user interface model has two sections - one for the teacher and the other for the student as shown in Fig 1.

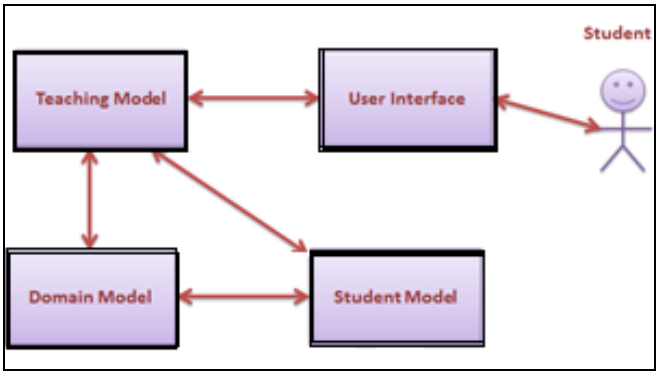

Fig 1: DES-Tutor Architecture.

4.1 Domain Model of DES-Tutor

This model of DES-Tutor deals with the lessons in cryptography and Information Security content, studying of (DES) algorithm encryption and decryption technology.

This model works on the ordering of the lessons/chapters. There are two main ingredients in it. The first one is the organization which deals with the organization and the ordering of lessons and themes. Where the chapters are: Chapter 1, Chapter 2, Chapter 3, and Chapter 4.

The second component, warehouse, deals with the material being taught in itself.

The material of the DES-Tutor Information Security Algorithm consists of the followings [1, 6-16, 17, 22-29]:

i) Chapter one includes

This chapter is to illustrate the principles of modern symmetric ciphers. For this purpose, the emphasis on the most widely used symmetric cipher: the Data Encryption Standard (DES). Though many symmetric ciphers have been established since the introduction of DES, and though it is meant to be replaced by the Advanced Encryption Standard (AES), DES stills the most significant algorithm. Furthermore, a detailed study of DES offers an understanding of the philosophies used in other symmetric ciphers.

ii) Chapter two includes

Key Security Concepts, Levels of Impact, Computer Security Challenges, Assets of a Computer System, Vulnerabilities & Threats & Attacks, Countermeasures, Threat Consequences & the Types of Threat Actions That Cause Each Consequence-Based on DES and Double DES and Triple DES, Computer & Network Assets, Examples of Threats, Passive & Active Attacks, Security Requirements, Fundamental Security Design Principles, Attack Surfaces, Attack Surface Categories, Computer Security Strategy & Security implementation.

iii) Chapter three includes

This chapter discusses symmetric ciphers. Topics include multiple encryption, looking in particular at the most widely used multiple-encryption scheme: triple DES.

iv) Chapter four includes

This chapter explains the attacks just described seem impractical, anybody using two-key 3DES may sense some concern. Therefore, many researchers now feel that three-key 3DES is the favored alternative. Three-key 3DES has an operative key length of 168 bits and is well-defined as C = E(K3, D(K2, E(K1, P)))

Backward compatibility with DES is provided by placing K3 = K2 or K1 = K2.

4.2 Student Model of DES-Tutor

A student must have a profile in order to study course materials and try the exercises. The profile contain information about the student such as last time the student used DES-Tutor, student number, student name, level difficulty reached, current score, overall score, how many exercises attempted in each session. The current score represents student score for each difficulty level within a lesson. The overall score represents student score for all level in a lesson.

4.3 Teaching Module of DES-Tutor

Teaching module works as an expert coach that controls the functionality of the system. Through this model, a student can try to answer all questions in the first difficulty level and if the student gets 75% score or more, the expert coach moves the student to second level of difficulty of the same lesson. However, if the student does not get that score, the expert coach make the student repeats the exercises of the same difficulty level. In the case the student get score Less than 50%, expert coach force the student to breach back to lessons then allows him to come back to try the exercises.

4.4 User Interfaces of DES-Tutor

The ITSB tool used for building the DES-Tutor support two type of users: teachers and students. When the teacher log into the DES-Tutor, the teacher can add initial information about the student, configure and adjust the color, font name, and size of all buttons, menus, combo boxes, add lessons, add exercises, and add answers. A screenshot of the teacher interfaces is shown in Fig 2, Fig 3, Fig 4, and Fig 5.

However, when the student log into the system, he/she will be able to see the lessons, examples and exercises, performance (See Fig 6, Fig 7, Fig 8 and Fig 9).

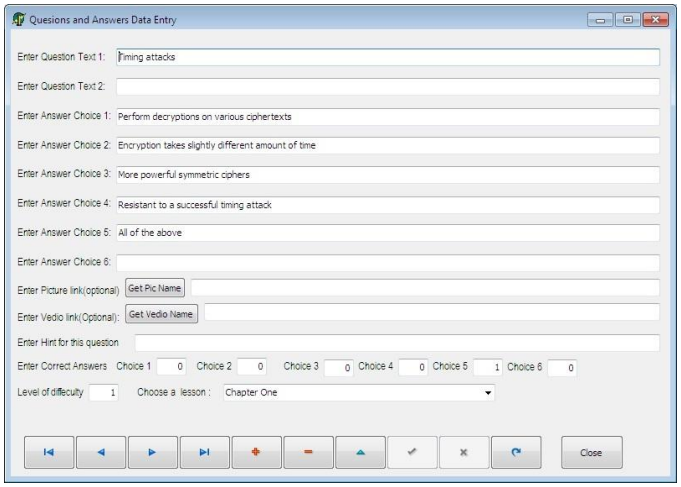

Fig 2: Form for adding questions and answers

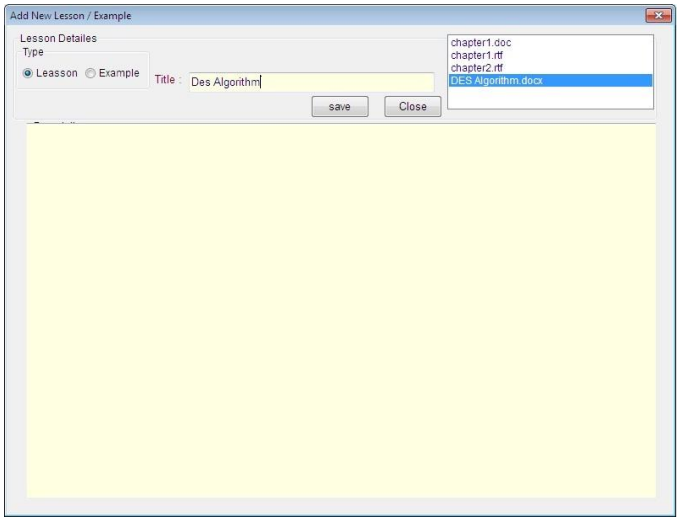

Fig 3: Form for adding Lessons and Examples

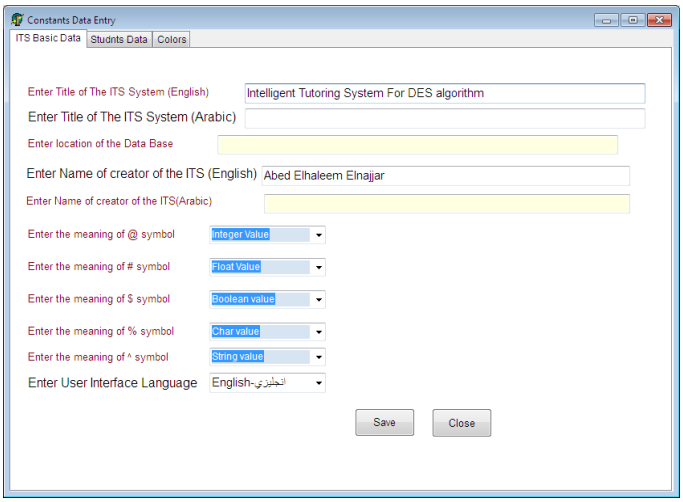

Fig 4: Form for adding constants of the system

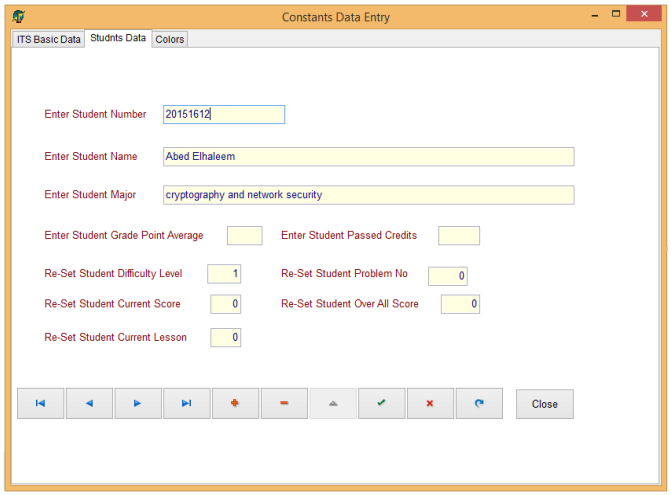

Fig 5: Form for adding initial students' information

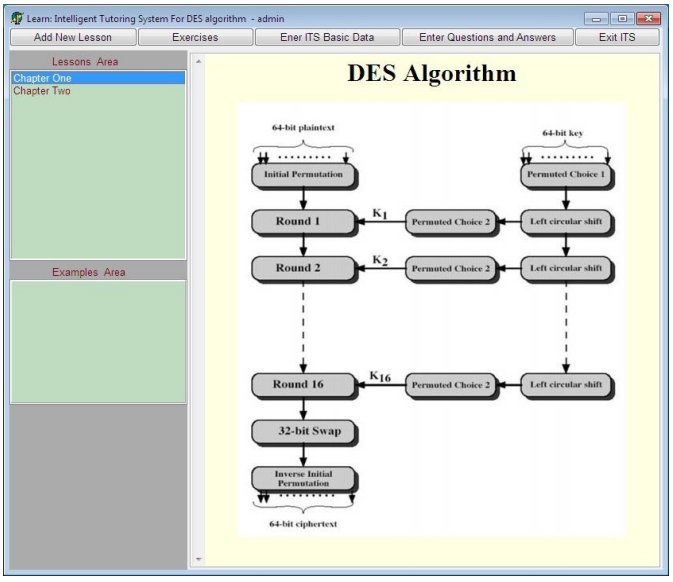

Fig 6: Student lessons and examples form

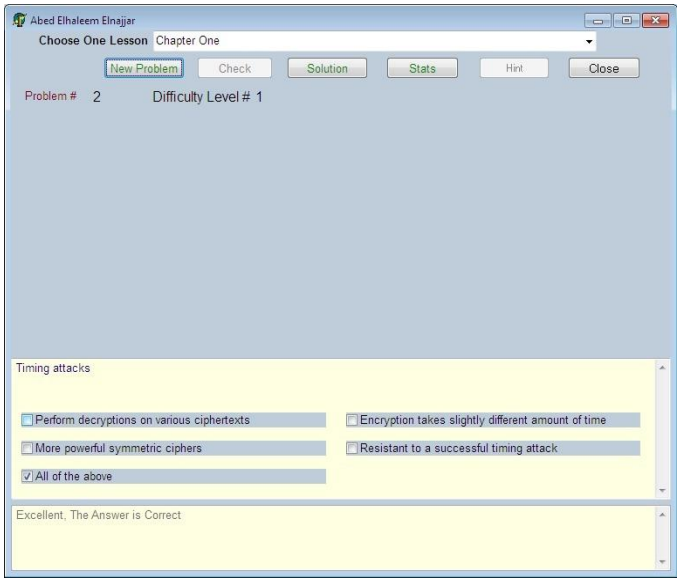

Fig 7: Student Exercises form.

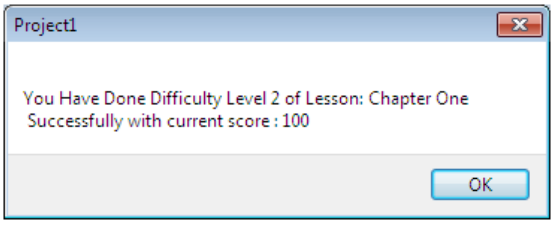

Fig 8: Message to tell student that he/she successfully finished in this level

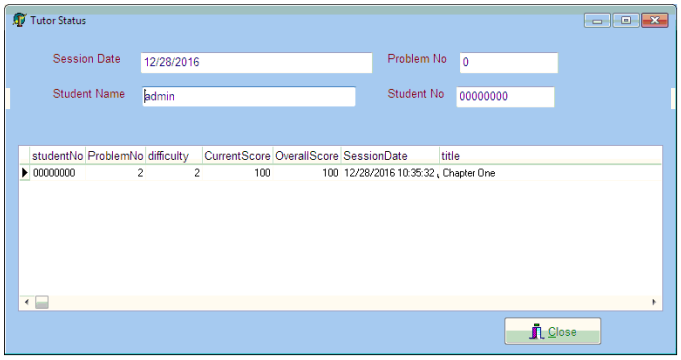

Fig 9: Student performance form.

5. Evaluation

We have evaluated the DES-Tutor by presenting it to a group of teachers who specialize in teaching cryptography and a group of students in Al-Azhar University taken this course. We asked both groups to evaluate the DES-Tutor. Then we requested from them to fill questionnaire DES-Tutor. The result of the evaluation by the students and the teachers were promising.

6. Conclusion

In this paper, we have designed an Intelligent Tutoring System for teaching DES Information Security Algorithm by

using ITSB authoring tool. The system is called DES-Tutor. DES-Tutor was designed to facilitate the study of learning cryptography and Information Security by the students. DES-Tutor architecture and requirements of each model in the system have been explained. We conducted an initial evaluation of the DES-Tutor by a group of teachers and students and the results were promising.

7. References

1. Abdelwahed AS, Mahmoud AY, Bdair RA. Information Security Policies and their Relationship with the Effectiveness of the Management Information Systems of Major Palestinian Universities in the Gaza Strip. International Journal of Information Science and Management. 2017; 15(1):1-26.
2. Abu Naser S. A methodology for expert systems testing and debugging, North Dakota State University, USA 1993; 1:1-130.
3. Abu Naser S. JEE-Tutor: An Intelligent Tutoring System for Java Expression Evaluation, Information Technology Journal, Scialert. 2008; 7(3):528-532.
4. Abu-Naser S, Ahmed A, Al-Masri N, Deeb A, Moshtaha E, AbuLamdy M. An Intelligent Tutoring System for Learning Java Objects. International Journal of Artificial Intelligence and Applications (IJAIA). 2011; 2(2).
5. Abu-Naser S, Al-Masri A, Sultan YA, Zaqout I. A prototype decision support system for optimizing the effectiveness of elearning in educational institutions. International Journal of Data Mining & Knowledge Management Process (IJDKP). 2011; 1:1-13.
6. Ahmed YM, Chefranov A. Hill cipher modification based on pseudo-random eigen values HCM-PRE. Applied Mathematics and Information Sciences (SCI-E), 2011; 8(2):505-516.
7. Akkila AN, Naser SSA. Teaching the Right Letter Pronunciation in Reciting the Holy Quran Using Intelligent Tutoring System. International Journal of Advanced Research and Development. 2017; 2(1).
8. Al-Bastami BH, Naser SSA. Design and Development of an Intelligent Tutoring System for C# Language, European Academic Research. 2017; 4(10).
9. ALDahdooh R, Naser SSA. Development and Evaluation of the Oracle Intelligent Tutoring System (OITS), European Academic Research. 2017; 4(10).
10. Alhabbash MI, Mahdi AO, Abu Naser SS. An Intelligent Tutoring System for Teaching Grammar English Tenses. European Advanced Research. 2016; 4(9):7743-7757.
11. Al-Hanjori MM, Shaath MZ, Naser SSA. Learning Computer Networks Using Intelligent Tutoring System. International Journal of Advanced Research and Development. 2017; 2(1).
12. Almurshidi SH, Naser SSA. Design and Development of Diabetes Intelligent Tutoring System. European Academic Research, 2017; 4(9):8117-8128.
13. Almurshidi SH, Naser SSA. Stomach Disease Intelligent Tutoring System. International Journal of Advanced Research and Development. 2017; 2(1).
14. Alnajjar M, Naser SSA. Improving Quality Of Feedback Mechanism In Un By Using Data Mining Techniques, International Journal of Soft Computing, Mathematics and Control. 2015; 4(2).
15. Al-Nakhal MA, Naser SSA. An Intelligent Tutoring System for learning Computer Theory, European Academic Research. 2017; 4(10).
16. Chefranov AG, Mahmoud AY. Elgamal public key cryptosystem and signature scheme in GU (m, p, n). In Proceedings of the 3rd international conference on Security of information and networks. ACM. 2010, 164-167
17. Doukhnitch E, Chefranov AG, Mahmoud A. Encryption Schemes with Hyper-Complex Number Systems and Their Hardware-Oriented Implementation. Theory and Practice of Cryptography Solutions for Secure Information Systems, 2013, 110.
18. El Haddad IA, Naser SSA. ADO-Tutor: Intelligent Tutoring System for leaning ADO.NET. European Academic Research. 2017; 4(10).
19. Hamed MA, Naser SSA. An Intelligent Tutoring System for Teaching the 7 Characteristics for Living Things. International Journal of Advanced Research and Development. 2017; 2(1).
20. Hilles MM, Naser SSA. Knowledge-based Intelligent Tutoring System for Teaching Mongo Database, European Academic Research. 2017; 4(10).
21. Mahdi AO, Alhabbash MI, Naser SSA. An intelligent tutoring system for teaching advanced topics in information security. World Wide Journal of Multidisciplinary Research and Development. 2016; 2(12):1-9.
22. Mahmoud AYA. Development of Matrix Cipher Modifications and Key Exchange Protocol, 2012.
23. Mahmoud AY, Chefranov AG. Hill cipher modification based on eigenvalues hcm-EE. In Proceedings of the 2nd international conference on Security of information and networks ACM. 2009, 164-167.
24. Mahmoud AY, Chefranov AG. Secure Hill cipher modifications and key exchange protocol. In Proc of 17 th IEEE International Conference on Automation, Quality and Testing, Robotics AQTR, 2010.
25. Mahmoud AY, Chefranov AG. Secure hill cipher modification based on generalized permutation matrix SHC-GPM. Information Sciences Letters, 2012, 91-102.
26. Mahmoud AY, Chefranov AG. A Hill Cipher Modification Based on Eigenvalues Extension with Dynamic Key Size HCM-EXDKS. International Journal of Computer Network and Information Security, 2014; 6(5):57.
27. Mahmoud AY, Mahdi AO. Comments On Multi-window Against Mobile Application Lock. Journal of Multidisciplinary Engineering Science Studies (JMESS), 2016; 2(5):494-497.
28. Mahmoud AY, Barakat MS, Ajjour MJ. Design And Development Of Elearning University System. (Journal of Multidisciplinary Engineering Science Studies (JMESS), 2016; 2(5):498-504.
29. Mahmoud A, Chefranov A. Hill cipher modification based on pseudo-random eigenvalues. Appl. Math, 2014; 8(2):505-516.
30. Naser S. Evaluating the effectiveness of the CPP-Tutor an intelligent tutoring system for students learning to program in C++. Journal of Applied Sciences Research; www.aensiweb.com/JASR/. 2009; 5(1):109-114.

31. Naser SA. A comparative study between Animated Intelligent Tutoring Systems (AITS) and Video-based Intelligent Tutoring Systems (VITS). Al-Aqsa University Journal. 2001; 5(1):1.
32. Naser SA. An Agent Based Intelligent Tutoring System For Parameter Passing In Java Programming. Journal of Theoretical & Applied Information Technology. 2008; 4(7).
33. Naser SA, Ahmed A, Al-Masri N, Sultan YA. Human Computer Interaction Design of the LP-ITS: Linear Programming Intelligent Tutoring Systems. International Journal of Artificial Intelligence & Applications (IJAIA). 2011; 2(3):60-70.
34. Naser SSA. Intelligent tutoring system for teaching database to sophomore students in Gaza and its effect on their performance. Information Technology Journal; Scialert. 2006; 5(5):916-922.
35. Naser SSA. Developing an intelligent tutoring system for students learning to program in C++. Information Technology Journal, Scialert. 2008; 7(7):1055-1060.
36. Naser SSA. A Qualitative Study of LP-ITS: Linear Programming Intelligent Tutoring System. International Journal of Computer Science & Information Technology, 2012; 4(1):209-220.
37. Naser SSA. Predicting learners performance using artificial neural networks in linear programming intelligent tutoring system. International Journal of Artificial Intelligence & Applications, 2012; 3(2):65-73.
38. Naser SSA. ITSB: An Intelligent Tutoring System Authoring Tool. Journal of Scientific and Engineering Research. 2016; 3(5):63-71.
39. Naser SSA, Sulisel O. The effect of using computer aided instruction on performance of 10th grade biology in Gaza. Journal of the College of Education. 2000; 4:9-37.
40. Naser SSA. Big O Notation for Measuring Expert Systems complexity, Islamic University Journal – Gaza. 1999; 7(1):77-57.
41. Naser SSA. Developing visualization tool for teaching AI searching algorithms, Information Technology Journal, Scialert. 2008; 7(2):350-355.