International Journal of Academic and Applied Research (IJAAR)
ISSN: 2000-005X
Vol. 2 Issue 2, February – 2018, Pages: 1-11

An Intelligent Tutoring System for Learning Classical Cryptography Algorithms (CCAITS)

Jihan Y. AbuEl-Reesh
Department of Information Technology
Faculty of Engineering & Information Technology
Al-Azhar University, Gaza, Palestine

Samy S. Abu-Naser
Professor of Artificial Intelligence, Department of Information Technology
Faculty of Engineering & Information Technology
Al-Azhar University, Gaza, Palestine

Abstract: *With the expansion of computer and information technologies, intelligent tutoring system are becoming more prominent everywhere throughout the world, it influences the scene to wind up plainly genuine that anyone could learn at anyplace in whenever. Be that as it may, without the help of intelligent tutoring system, the learning questions students' response can't be understood in time. Thus it is important to create intelligent tutoring system (ITS) keeping in mind the end goal to give learning support service for students. In this paper, we present an intelligent tutoring system for Learning Classical cryptography algorithms. The structure of this system and the elements of every part are presented in the first place, and then the program flow on which the agents in this system base to participate with the others to suggest reasonable learning pedagogical for individual student according to the evaluation of students' cognitive capability level is discussed. Moreover, the algorithm and procedure which are sophisticated to execute the designed functions of the agents will be explained. The suggested system for Learning Classical cryptography algorithms will derive adaptive learning pedagogical for individual student to learn in compelling and effective way. This an intelligent tutoring system concentrate on the students registered in Advanced Topics in Information Security in the faculty of Engineering and Information Technology at Al-Azhar University in Gaza and we suggest reasonable and suitable learning pedagogical for individual student to perform adaptive learning. During which the student will be able to think about the course and deal with related issues and solving the problems. An evaluation of the Learning Classical cryptography algorithms system was finished and the results were positive.*

Keywords: Intelligent Tutoring System, Classical Cryptography Algorithms, CCAITS, Learning Strategies, Unified Modeling Language (UML).

1. INTRODUCTION

CCAITS is an intelligent tutoring system for learning Classical cryptography algorithms. The Tutor progressively presents student with the concept of Classical cryptography algorithms and portrays most repeatedly utilized classes of Classical cryptography algorithms. Cryptography is Considered an intrinsic and tricky part of Computer Security for the novice, for the master, and for software designed to help in the Cryptography. Intelligent Tutoring Systems are computer-based coaching programs that apply artificial intelligence. ITS are further developed, enabling students to enhance their skills by accomplishing tasks as part of the reactive discourse hall environment[2-15]. ITS can answer questions and give customized support to the students[16-24]. ITS, contrary other educational technologies, to evaluate every student's response because to estimate his/her knowledge and skills. ITS can change learning strategies; provide illustrations, explanations[25-30], demonstrations, examples exercises and reasonable activities where you require them. Research in Intelligent Tutoring Systems has emphatically delighted techniques and systems that offer adaptive support for student when solving problem in various domains[31-37]. otherwise, there are other learning projects that can pick advantage from personalized computer-based provision, for instance playing instructive games, covering interactive simulations, and learning example Offering individualized help for these activities stances restrictive difficulties, since it needs an ITS that can simulate and adapt to student skills, skills and rational cases repeatedly not as systematic and well defined as those complex in prior-style problem solving. Intelligent Tutoring Systems (ITS) have made extraordinary walks as of late. The objective of these learning technology systems is to give intelligent, one-on-one, computer-based aid to students as they learn to solve problems in a kind of instruction that is often not available because of scarce (human) resources [38].The basic rationale subordinate conventional ITS systems is that by using module domain knowledge and dynamic student modules, matching student's problem solving Procedures to the explicit domain modules, it is likely to adapt instruction to the needs of certain students and efficiently support their learning. Two outstanding methodologies that both utilize such unequivocal domain modules have exhibited noteworthy practical accomplishment in learning domains, for example database design or UML, algebra, programming, geometry [39, 40]. This paper presents Classical cryptography calculations Tutor extends that represent some of these challenges. system gives an intelligent representation of educational subject altered to student performance, such as desirable detail level, degree of backward knowledge, estimate of the system on the level of student's knowledge with the case being presently educated, as well as with the full subject, of the framework on the level of student's acquaintance with the issue being at present educated, and additionally with the whole material. The case imposed in course realization of this problem, "Classical cryptography " [41] should bolster this course, and we explained The lessons in Arabic in order to make it easier for students to understand the subjects by using their native language. The ITS system for learning the Classical cryptography algorithms, illustrated in this paper, makes pedagogical module of learning the demonstrate possible, and in addition independent study of Classical cryptography algorithms for more advanced students. The course for learning Classical cryptography algorithms is divided into two main sections, Preliminaries section, and Classical Cipher section which consists of four subsection (Monoalphabetic Substitution Cipher, Polyalphabetic Substitution Cipher, PolyGram Substitution Cipher, and Homophonic Substitution Cipher). over interaction of a user with the system, the Tutor observe and monitors the performance of the student, same bringing about difference in student' characteristics in the Student module. These given are given through interaction of a user with the system by method for tests and solving problems. Evaluations acquired through such interactions are contrasted and alternate parameters and appraisals with a specific end goal to get the last judgment of a student. Figure1 describes the system's architecture, consist of the Domain module, Student module, Pedagogical module, User Interface module.

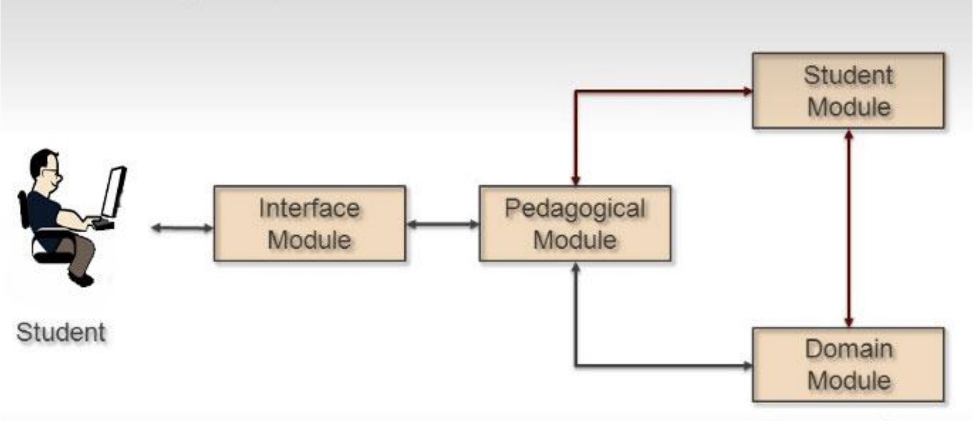


Figure1: Classical cryptography algorithms –Tutor Architecture

2. LITERATURE REVIEW

In the modern day we have a massive expansion of Intelligent Tutoring System, ITS has fetch much attention of the researchers. There are numerous intelligent tutoring systems, such as Knowledge-based program debugging (PROUST) developed by Johnson and Littman Soloway to check non syntactic bugs for students in the Pascal programs [56]. SQL-Tutor, designed by Mitrovic and Ohlsson, demonstrates and teaches to students the way of writing queries in relational database through various lessons in the basics of writing query, and also the student writes the query into the system, thereafter the system analyzes the query to discovery errors and weakness. Based on the errors, the system gives a set of notes and hints by showing a short text describing the error and how to solve it [43-61]. Dance Learning from Bottom-Up Structure (DL-BUS) depend on automated lesson generation systems, learns juniors basic dance movements through analyzing and separator dance into lessons. At the beginning: split the dance to small movements then show them to the student. Thereafter: learn students joint dance movements during a part of time [62]. Affective tutoring systems (ATS) depend on embedded devices is a system that leans on embedded devices for detecting the emotion, feelings, psychology student and also adapt to the student's mood such as frustrated and fatigued, angry etc. Based on the feelings and mood of the student, the student will learn [63, 64]. The Andes physics tutoring system is a system that learns student's methods to solve physics problems [64]. PIXIE developing by Sleeman in 1987 is depends on Leeds Modeling System (LMS) to check errors in algebra [64]. MYCIN [51] is expert system for diagnosing diseases such as cancers, depend on MYCIN, developed GUIDON to show the lessons of the symptoms and disease, displaying rules in the knowledge base of the student [52]. An ITS teach students English dialogues during interaction with students and it takes into account the individual differences of students during levels [52]. A comparative study between Animated Intelligent Tutoring Systems (AITS) and Video-based Intelligent Tutoring Systems (VITS) [54], teaching AI searching algorithms[24], Linear Programming[21,36], Java Expression Evaluation [36], Parameter Passing In Java Programming[37], Java Objects[38], effectiveness of e-learning[39], effectiveness of the CPP-Tutor[40], computer aided instruction[41], learning to program in C++ [26], Predicting learners performance using NT and ITS [43]. There are various systems developed and designed for the aim of education. These systems assist students to learn fast and build their self-confidence. Some of these systems devoted to learning computer science such as [38,42, 60, 61], English and Arabic language such as [62, 63] and Mathematics for example [64]. A recent ITS is called COMET [64] that are used for medical problem-based learning; Another one is for Mentoring Diabetes [64]; The Major of these ITS are specialized in one specific disease and other in a few diseases. However, the existing suggests ITS system is expert in the video games.

3. CLASSICAL CRYPTOGRAPHY ALGORITHMS-TUTOR(CCAITS)

In this paper, we utilized ITSB authoring tool. This tool created and developed by prof. Samy S. Abu Naser [1] by using Delphi Embarcadero XE8, 2015; this tool supported English and Arabic languages, and consist of two systems in one application: The first Dedicated to with teacher system where it authorize the teachers to add course subjects, questions and answers. The second system Dedicated to the student system where it authorize the student to study course subjects and solve exercises.

3.1 DOMAIN MODULE ARCHITECTURE

The domain module comprises information about classical cryptography algorithms to illustrate the course; intelligent tutoring system utilizes a domain module to solve problems or solutions cases. The module displays the subjects and the learning in a simple way and it products a lot of problems for every lesson taking into consideration individual differences. When a student reply to the problem, determines if correct or wrong, moreover it assess the student. The domain module presented lessons, its arrangement and a scope of components. The subjects enveloped in this ITS as follows[63-73]:

Preliminaries section

- The Division Algorithm
- Prime Number
- Trial Division.rtf
- Sieve of Eratosthenes
- Greatest Common Divisor
- Euclidean Algorithm
- Extended Euclidean Algorithm
- The Fundamental Theorem of Arithmetic
- Least Common Multiple
- XOR – Exclusive-Or
- Logarithms

Classical Cipher section

- Coding
- Classical Method
- Monoalphabetic Substitution Cipher
- Caesar Cipher
- Atbash Cipher
- ROT 13 Cipher
- Affine Cipher
- Monoalphabetic
- Polyalphabetic substitution cipher
- Simple Shift Vigenere Cipher
- Break the simple Vigenere Cipher
- Key Length KAISISKI
- The Full Vigenere Cipher
- The Auto-Key Vigenere Cipher
- The Running Key Vigenere Cipher
- PolyGram Substitution Cipher
- The Playfair Cipher
- Hill Cipher
- Break the PolyGram Substitution Cipher
- The Jefferson Cylinder
- Homophonic Substitution Ciphers
- Transposition Ciphers
- The One-Time Pad
- Combination between Substitution/Transposition Cipher

3.2 STUDENT MODULE ARCHITECTURE

The student module is crossing with the domain module. It features subjective and influencing conditions of the student in respect to his development as the learning movement progresses. As the student advance well ordered through the critical thinking process, the wise mentoring system includes itself in module following procedure. Whenever there is any deviation from the predefined module, the astute mentoring system stamps it as a blunder. Each new student must have his own account to have a profile where it enables the student to think about course subject and do the exercises. The profile has data about the student, for example, date of last visit, login date, student number, student name, current score, and general score. The present score speaks to student score for each level. The general score speaks to student for all levels. Student module stores insights about the student’s present critical thinking state and long haul information advance, fundamental for adjusting the material to the student 's qualities (characteristics). In this paper, three classifications of student’s attributes are thought about: 1- Personal information (name, ID, email ...). 2-Performance information - the student’s intellectual and individual attributes, and in addition other general long haul qualities. 3- Overlay information - the present level of dominance of Classical cryptography Algorithms identified with the comparing components in the area module. The current IT’S for Classical cryptography algorithms has two main interfaces: user interface and teacher interface. Configuration Pattern bit by bit brings different attributes into the student module in view of the assessed student’s knowledge, for example, experience level, degree of mastery, education style, etc. In the student module Attribute values are calculated by implementing a devoted group of rules and simple procedures from Pedagogical module. The values are adjusted during the session. At the close of each session, the system memorizes the student module as report. Whenever the student sign onto the system, the data stored report record are utilized to set the student module.

3.3 PEDAGOGICAL MODULE ARCHITECTURE

This module is presented the essence of the whole system; it administers all the Procedures and tasks in system. It has been observed that students are having difficulties in understanding Classical cryptography algorithms. To overcome this distress, an Intelligent Tutoring System for teaching Classical cryptography algorithms called CCAITS have been developed to students registered in Advanced Topics in Information Security in the faculty of Engineering and Information Technology at Al-Azhar University in Gaza. It works like a coordinator that administer, controls, monitors the functionality of the system. During this module, the student can answer questions on the first level, and if he gains 75% score or more, he can shift to the second level. But if he brings low scores, he iterates the exam at the same level. The pedagogical module works like learning strategies or academic outlines. This module needs information on the points given in the student's interaction. Depending on these facts, the Pedagogical module can generate tutorial procedure early interaction activities. But the system must to realize what the right method or how to display the same work for various students that they may have various skills, cognitive reasoning. CCAITS by degrees introduces students to the concept of Classical cryptography algorithms and automatically generates exercises for the students to resolve.

3.4 USER INTERFACE MODULE ARCHITECTURE

This is the Interactive interface of the CCAITS. It amalgamates all types of information wanted to interact with student, out of shape, text, graphics, keyboard, mouse-driven menus, multimedia, etc. Main factors for user-acceptance are user-friendly and display. Figure 2 showed login screen for CCAITS. The current IT'S for Classical cryptography algorithms has two main interfaces: user interface and teacher interface.

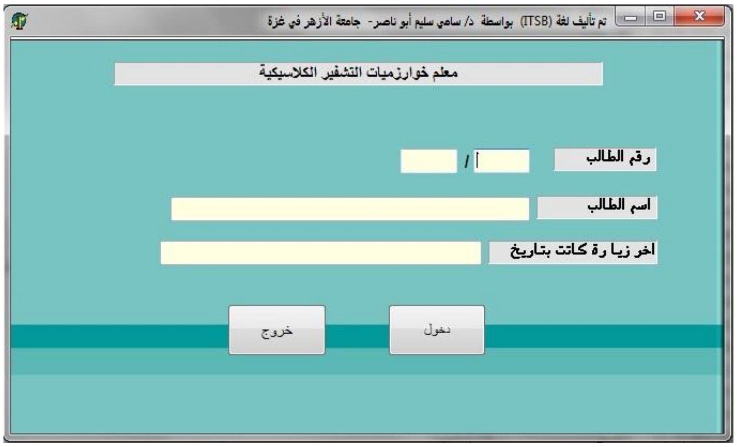
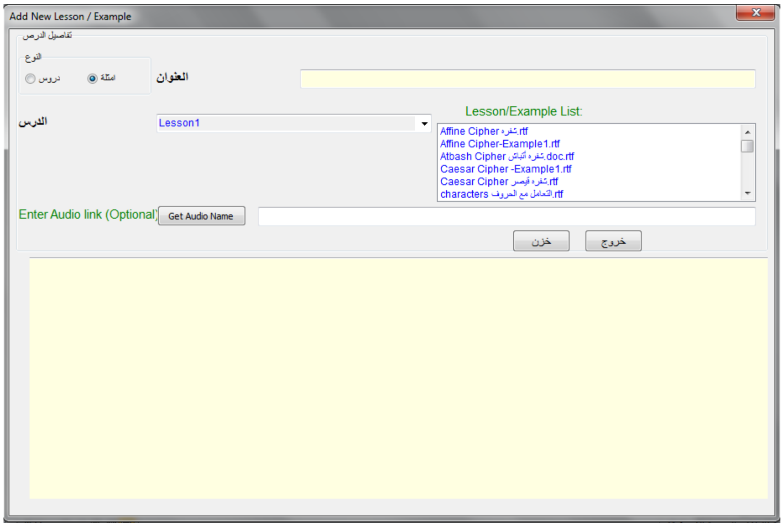

تم تأليف لغة (ITSB) بواسطة د/ سامي سليم أبو ناصر- جامعة الأزهر في غزة
معلم خوارزميات التشفير الكلاسيكية
رقم الطالب
/
اسم الطالب
اخر زيا رة كانت بتاريخ
دخول
خروج

Figure2: Shows Form for login screen for CCAITS

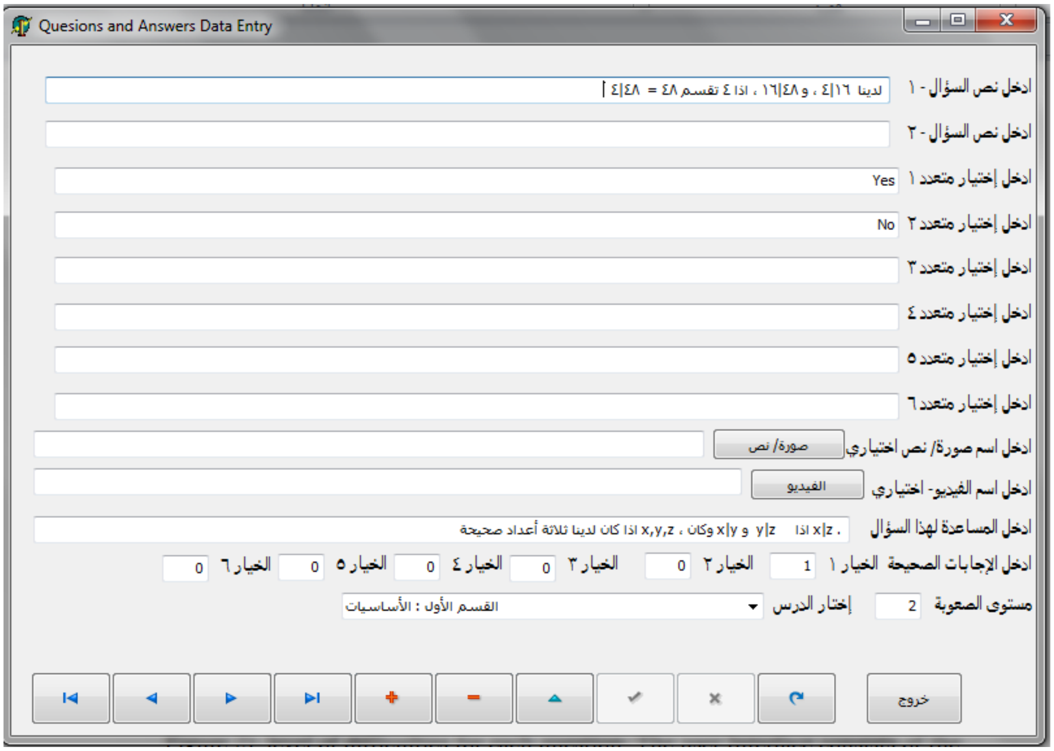
The teacher interfaces includes four parts to build the student model and domain model. The first interface is to add examples and lessons with the capability to supply video, sound, and pictures with lessons to help and simplify the learning of students(as in Figure 3).



Affine Cipher شفره.rtf
Affine Cipher-Example1.rtf
Atbash Cipher شفره أتباش.doc.rtf
Caesar Cipher -Example1.rtf
Caesar Cipher شفره قيصر.rtf
characters التعامل مع الحروف.rtf

Figure3: Shows form for adding Lessons and Examples

The second interface is to add questions and answers with the capability of adding video, picture and hints to simplify the questions answer, and join a level of difficulty for each question(as in Figure 4).


Quesions and Answers Data Entry

ادخل نص السؤال - ١ لدينا ٤|١٦ ، و ٤٨|١٦ ، اذا ٤ تقسم ٤٨ = ٤|٤٨

ادخل نص السؤال - ٢

ادخل إختيار متعدد ١ Yes

ادخل إختيار متعدد ٢ No

ادخل إختيار متعدد ٣

ادخل إختيار متعدد ٤

ادخل إختيار متعدد ٥

ادخل إختيار متعدد ٦

ادخل اسم صورة/ نص اختياري

ادخل اسم الفيديو- اختياري

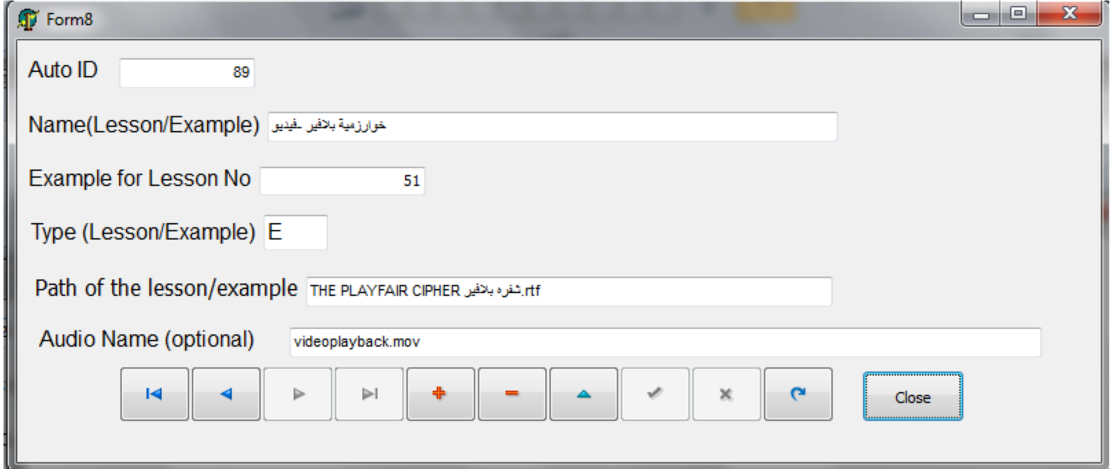
ادخل المساعدة لهذا السؤال اذا كان لدينا ثلاثة أعداد صحيحة x,y,z ، وكان x|y و y|z اذا x|z .

ادخل الإجابات الصحيحة الخيار ١ 1 الخيار ٢ 0 الخيار ٣ 0 الخيار ٤ 0 الخيار ٥ 0 الخيار ٦ 0

مستوى الصعوبة 2 إختار الدرس القسم الأول : الأساسيات

Figure4: Shows Form for adding questions and answers

The third interface is to modify lessons and examples with the capability of adding video, picture (as in Figure 5).


Form8

Auto ID 89

Name(Lesson/Example) خوارزمية بلافير ـ فيديو

Example for Lesson No 51

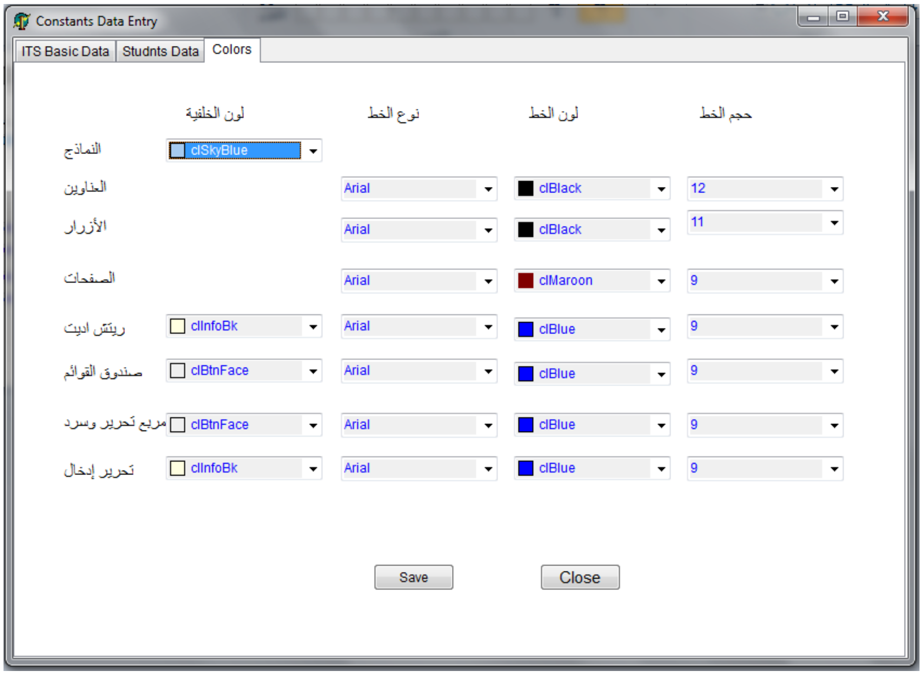
Type (Lesson/Example) E

Path of the lesson/example THE PLAYFAIR CIPHER شفره بلافير.rtf

Audio Name (optional) videoplayback.mov

Figure5: Shows Form for modifying questions and answers

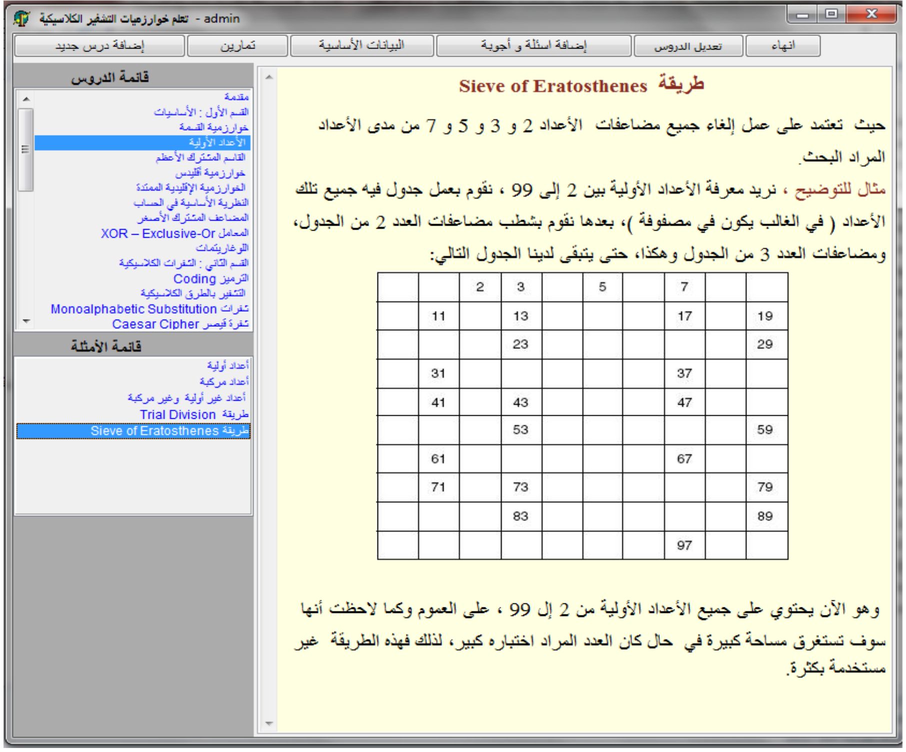
The fourth interface to adjust the background color, font, size, for system components, furthermore build basic data about the student and system. Fig 6 shows the teacher interfaces (See Figure6).



	لون الخلفية	نوع الخط	لون الخط	حجم الخط
النماذج	🟦 clSkyBlue			
العناوين		Arial	⬛ clBlack	12
الأزرار		Arial	⬛ clBlack	11
الصفحات		Arial	🟥 clMaroon	9
ريتش اديت	⬜ clInfoBk	Arial	🟦 clBlue	9
صندوق القوائم	⬜ clBtnFace	Arial	🟦 clBlue	9
مربع تحرير وسرد	⬜ clBtnFace	Arial	🟦 clBlue	9
تحرير إدخال	⬜ clInfoBk	Arial	🟦 clBlue	9

Figure6: Shows form for adjusting Fonts of all screens of the system

A screenshot of the student's interface is appears in Figure7, Figure8, Figure9, Figure10 and Figure11. The student Interfaces has been prepared for the student to interact with the system out of which shows exams for each lesson (as in Figure9). The student selects a lesson from the menu of lessons (as in Figure7); the system shows the first difficulty level of the exam questions randomly. If the student finished all questions correctly on the first level, the system moves the student to the following level of difficulty automatically. The interface and responses are fundamental to the process of adaptation of the system with the student. So, the evolution in the adaptation process depend on it(as in Figure10).



Sieve of Eratosthenes طريقة

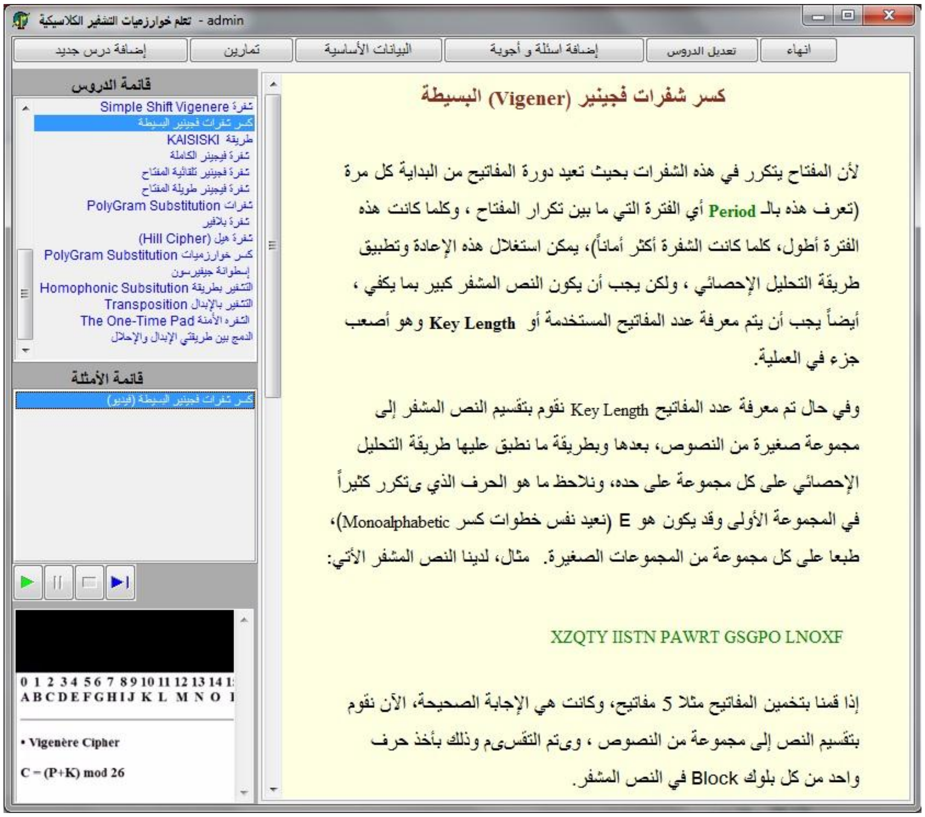
حيث تعتمد على عمل إلغاء جميع مضاعفات الأعداد 2 و 3 و 5 و 7 من مدى الأعداد المراد البحث.

مثال للتوضيح ، نريد معرفة الأعداد الأولية بين 2 إلى 99 ، نقوم بعمل جدول فيه جميع تلك الأعداد (في الغالب يكون في مصفوفة)، بعدها نقوم بشطب مضاعفات العدد 2 من الجدول، ومضاعفات العدد 3 من الجدول وهكذا، حتى يتبقى لدينا الجدول التالي:

		2	3		5		7		
	11		13				17		19
			23						29
	31						37		
	41		43				47		
			53						59
	61						67		
	71		73						79
			83						89
							97		

وهو الآن يحتوي على جميع الأعداد الأولية من 2 إل 99 ، على العموم وكما لاحظت أنها سوف تستغرق مساحة كبيرة في حال كان العدد المراد اختباره كبير، لذلك فهذه الطريقة غير مستخدمة بكثرة.

Figure7: Shows Student lessons and examples interface.


admin - تعلم خوارزميات التشفير الكلاسيكية
إضافة درس جديد
تمارين
البيانات الأساسية
إضافة اسئلة و أجوبة
تعديل الدروس
انهاء
قائمة الدروس
شفرة Simple Shift Vigenere
كسر شفرات فجينير البسيطة
طريقة KAISISKI
شفرة فيجينر الكاملة
شفرة فجينير تلقائية المفتاح
شفرة فيجينر طويلة المفتاح
شفرات PolyGram Substitution
شفرة بلافير
شفرة هيل (Hill Cipher)
كسر خوارزميات PolyGram Substitution
إسطوانة جيفيرسون
التشفير بطريقة Homophonic Subsitution
التشفير بالإبدال Transposition
الشفره الأمنة The One-Time Pad
الدمج بين طريقتي الإبدال والإحلال
قائمة الأمثلة
كسر شفرات فجينير البسيطة (فيديو)
0 1 2 3 4 5 6 7 8 9 10 11 12 13 14 1:
A B C D E F G H I J K L M N O I
• Vigenère Cipher
C = (P+K) mod 26

كسر شفرات فجينير (Vigener) البسيطة

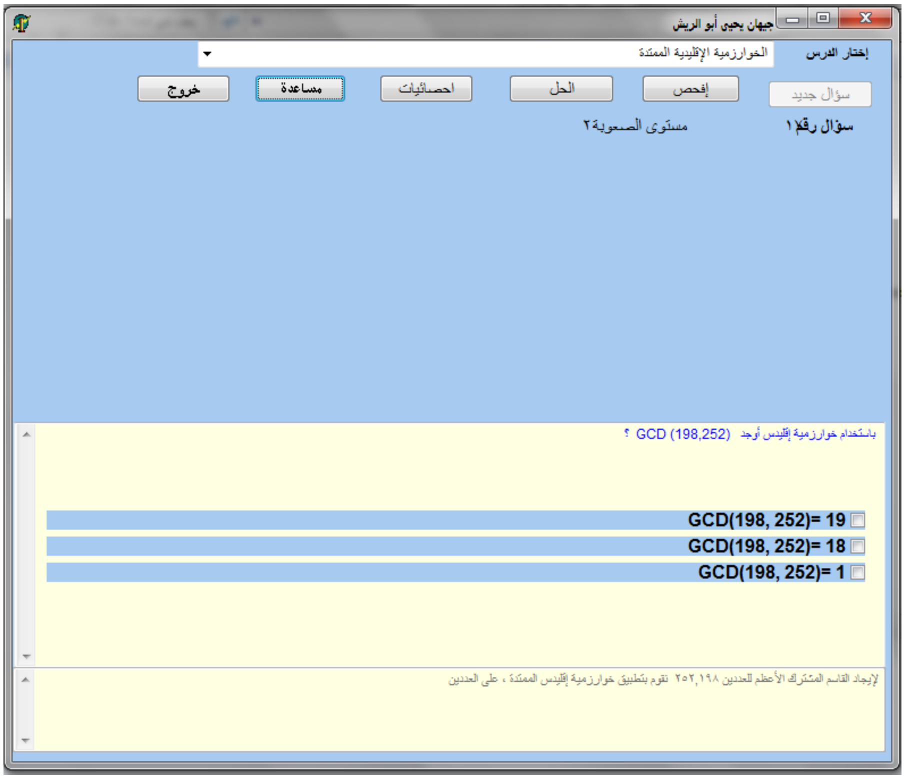
لأن المفتاح يتكرر في هذه الشفرات بحيث تعيد دورة المفاتيح من البداية كل مرة (تعرف هذه بالـ Period أي الفترة التي ما بين تكرار المفتاح ، وكلما كانت هذه الفترة أطول، كلما كانت الشفرة أكثر أماناً)، يمكن استغلال هذه الإعادة وتطبيق طريقة التحليل الإحصائي ، ولكن يجب أن يكون النص المشفر كبير بما يكفي ، أيضاً يجب أن يتم معرفة عدد المفاتيح المستخدمة أو Key Length وهو أصعب جزء في العملية.

وفي حال تم معرفة عدد المفاتيح Key Length نقوم بتقسيم النص المشفر إلى مجموعة صغيرة من النصوص، بعدها وبطريقة ما نطبق عليها طريقة التحليل الإحصائي على كل مجموعة على حده، ونلاحظ ما هو الحرف الذي ىتكرر كثيراً في المجموعة الأولى وقد يكون هو E (نعيد نفس خطوات كسر Monoalphabetic)، طبعا على كل مجموعة من المجموعات الصغيرة. مثال، لدينا النص المشفر الأتي:

XZQTY IISTN PAWRT GSGPO LNOXF

إذا قمنا بتخمين المفاتيح مثلا 5 مفاتيح، وكانت هي الإجابة الصحيحة، الآن نقوم بتقسيم النص إلى مجموعة من النصوص ، وىتم التقسىم وذلك بأخذ حرف واحد من كل بلوك Block في النص المشفر.

Figure8: Shows Student lessons and examples interface supported by using video.



سؤال رقم ١

مستوى الصعوبة ٢

باستخدام خوارزمية إقليدس أوجد GCD (198,252) ؟

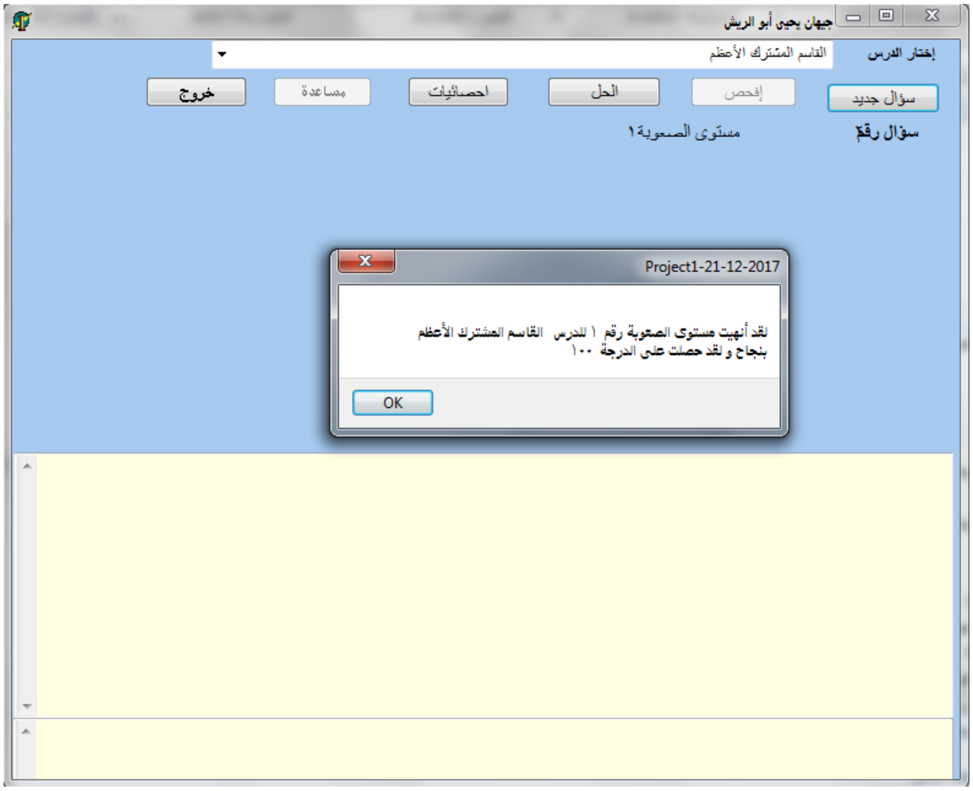
□ GCD(198, 252)= 19

□ GCD(198, 252)= 18

□ GCD(198, 252)= 1

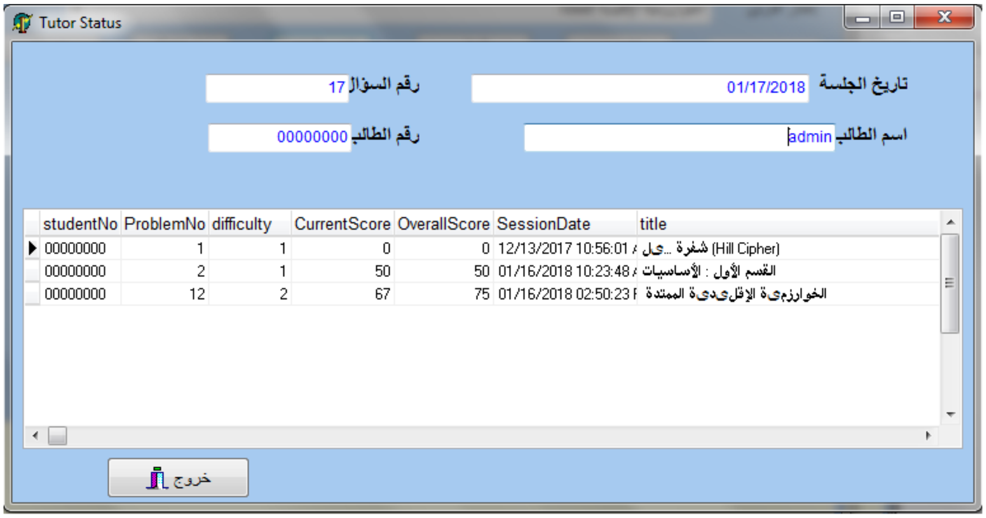
لإيجاد القاسم المشترك الأعظم للعددين ٢٥٢,١٩٨ نقوم بتطبيق خوارزمية إقليدس الممتدة ، على العددين

Figure9: Shows Student Exercises interface.



لقد أنهيت مستوى الصعوبة رقم ١ للدرس القاسم المشترك الأعظم
بنجاح و لقد حصلت على الدرجة ١٠٠

Figure10: Shows Student Exercises Difficulty Level Score Interface.



تاريخ الجلسة 01/17/2018

رقم السؤال 17

اسم الطالب admin

رقم الطالب 00000000

studentNo	ProblemNo	difficulty	CurrentScore	OverallScore	SessionDate	title
00000000	1	1	0	0	12/13/2017 10:56:01	شفرة …ىل (Hill Cipher)
00000000	2	1	50	50	01/16/2018 10:23:48	القسم الأول : الأساسيات
00000000	12	2	67	75	01/16/2018 02:50:23	الخوارزمىة الإقلىدىة الممتدة

Figure11: Shows Student statistics Interface.

4. EVALUATION

The evaluation was carried out to test the CCAITS intelligent tutoring system. The evaluation was to let a group of students examine the materials: lessons, examples, exercises, answers, student information, and system constants etc. for Classical cryptography algorithms individually. Then we gathered the opinion of each student in team of how easy, efficient, and friendly was the CCAITS tool. Several empirical evaluations have shown a positive impact on learning and suggested that other intelligent tutoring systems be designed for other courses.

5. CONCLUSION AND FUTURE WORKS

In this research of Learning Classical cryptography algorithms system so that the system can run on heterogeneous platforms. The work is dedicated to those the students registered in Advanced Topics in Information Security in the faculty of Engineering and Information Technology at Al-Azhar University in Gaza, It involves four modules mainly Domain module, student module, Pedagogical module, Interface module. The student module of the Learning Classical cryptography algorithms ITS is functionally fully decoupled from the other components of the system. This approach to student modeling uses a combination of stereotype and overlay techniques. Its main advantage compared to other similar modules is a universal approach to module creation. The approach is not strictly related to design patterns as the domain of teaching/learning. It can be applied to ITS in any domain without changes or with a few changes, depending on the requirements of the pedagogical module. Curriculum sequencing is based on execution of instructional plan generated based on student knowledge of domain matter. Course units are generated dynamically from domain module by using adaptive presentation templates. in module maintenance. The tutoring system is developed and implemented to increase and/or enhance the skills to the students in the adopted domain. The system is briefly explaining the chosen domain. The system supports the explanation process using the multimedia facilities such as images, sound, animation and text as well. The system involves also the question analysis as well as the domain knowledge expert. The knowledge of the Expert Module is important for presenting the correct answer. The system also is supported by a graphical user interface to ease the interaction with the students. This work is considered prototype as it can be scaled up to cover other subject curricula. There are several directions in future research and future development of the Design Pattern system: 1 development of a case-based generator of new problems for student, 2- development of a graphical authoring tool for domain module maintenance. Finally we suggested that other intelligent tutoring systems be designed for other courses. We recommend a comprehensive evaluation of the system to be carried out next time the course is offered.

REFERENCES

[1] Abu Naser, S. S. (2016). ITSB: An Intelligent Tutoring System Authoring Tool. Journal of Scientific and Engineering Research, 3(5), 63-71.

[2] Mrouf, A., Albatish, I., Mosa, M., & Abu Naser, S. S. (2017). Knowledge Based System for Long-term Abdominal Pain (Stomach Pain) Diagnosis and Treatment. International Journal of Engineering and Information Systems (IJEAIS), 1(4), 71-88.

[3] Qwaider, S. R., & Abu Naser, S. S. (2017). Expert System for Diagnosing Ankle Diseases. International Journal of Engineering and Information Systems (IJEAIS), 1(4), 89-101.

[4] AbuEl-Reesh, J. Y., & Abu Naser, S. S. (2017). An Expert System for Diagnosing Shortness of Breath in Infants and Children. International Journal of Engineering and Information Systems (IJEAIS), 1(4), 102-115.

[5] Al Rekhawi, H. A., Ayyad, A. A., & Abu Naser, S. S. (2017). Rickets Expert System Diagnoses and Treatment. International Journal of Engineering and Information Systems (IJEAIS), 1(4), 149-159.

[6] Abu Ghali, M. J., Mukhaimer, M. N., Abu Yousef, M. K., & Abu Naser, S. S. (2017). Expert System for Problems of Teeth and Gums. International Journal of Engineering and Information Systems (IJEAIS), 1(4), 198-206.

[7] Almurshidi, S. H., & Abu Naser, S. S. (2017). Design and Development of Diabetes Intelligent Tutoring System. EUROPEAN ACADEMIC RESEARCH, 6(9), 8117-8128.

[8] Al-Bayed, M. H., & Abu Naser, S. S. (2017). An intelligent tutoring system for health problems related to addiction of video game playing. International Journal of Advanced Scientific Research, 2(1), 4-10.

[9] Hamed, M. A., & Abu Naser, S. S. (2017). An intelligent tutoring system for teaching the 7 characteristics for living things. International Journal of Advanced Research and Development, 2(1), 31-45.

[10] Almurshidi, S. H., & Abu Naser, S. S. (2017). Stomach disease intelligent tutoring system. International Journal of Advanced Research and Development, 2(1), 26-30.

[11] El Agha, M., Jarghon, A., & Abu Naser, S. S. (2017). Polymyalgia Rheumatic Expert System. International Journal of Engineering and Information Systems (IJEAIS), 1(4), 125-137.

[12] Khella, R. A., & Abu Naser, S. S. (2017). Expert System for Chest Pain in Infants and Children. International Journal of Engineering and Information Systems (IJEAIS), 1(4), 138-148.

[13] Akkila, A. N., & Abu Naser, S. S. (2017). Teaching the right letter pronunciation in reciting the holy Quran using intelligent tutoring system. International Journal of Advanced Research and Development, 2(1), 64-68.

[14] AbuEloun, N. N., & Abu Naser, S. S. (2017). Mathematics intelligent tutoring system. International Journal of Advanced Scientific Research, 2(1), 11-16.

[15] Bakeer, H. M. S., & Naser, S. S. A. (2017). Photo Copier Maintenance Expert System V. 01 Using SL5 Object Language. International Journal of Engineering and Information Systems (IJEAIS), 1(4), 116-124.

[16] Nabahin, A., Abou Eloun, A., & Abu Naser, S. S. (2017). Expert System for Hair Loss Diagnosis and Treatment. International Journal of Engineering and Information Systems (IJEAIS), 1(4), 160-169.

[17] Al-Nakhal, M. A., & Abu Naser, S. S. (2017). Adaptive Intelligent Tutoring System for learning Computer Theory. EUROPEAN ACADEMIC RESEARCH, 6(10), 8770-8782.

[18] Abu Hasanein, H. A., & Abu Naser, S. S. (2017). An intelligent tutoring system for cloud computing. International Journal of Academic Research and Development, 2(1), 76-80.

[19] Abu Naser, S. (2008). An Agent Based Intelligent Tutoring System For Parameter Passing In Java

Programming. Journal of Theoretical & Applied Information Technology, 4(7).

[20] Abu Naser, S. (2008). JEE-Tutor: An Intelligent Tutoring System for Java Expression Evaluation. Information Technology Journal, Scialert, 7(3), 528-532.

[21] Abu Naser, S. S. (2001). A comparative study between animated intelligent tutoring systems AITS and video-based intelligent tutoring systems VITS. Al-Aqsa Univ. J, 5(1), 72-96.

[22] Abu Naser, S. S. (2006). Intelligent tutoring system for teaching database to sophomore students in Gaza and its effect on their performance. Information Technology Journal, 5(5), 916-922.

[23] Abu Naser, S. S. (2008). Developing an intelligent tutoring system for students learning to program in C++. Information Technology Journal, 7(7), 1055-1060.

[24] Abu Naser, S. S. (2008). Developing visualization tool for teaching AI searching algorithms. Information Technology Journal, Scialert, 7(2), 350-355.

[25] Abu Naser, S. S. (2012). Predicting learners performance using artificial neural networks in linear programming intelligent tutoring system. International Journal of Artificial Intelligence & Applications, 3(2), 65.

[26] Abu Naser, S. S. (2012). A Qualitative Study of LP-ITS: Linear Programming Intelligent Tutoring System. International Journal of Computer Science & Information Technology, 4(1), 209.

[27] Alawar, M. W., & Abu Naser, S. S. (2017). CSS-Tutor: An intelligent tutoring system for CSS and HTML. International Journal of Academic Research and Development, 2(1), 94-98.

[28] Al-Bastami, B. G., & Abu Naser, S. S. (2017). Design and Development of an Intelligent Tutoring System for C# Language. EUROPEAN ACADEMIC RESEARCH, 6(10), 87-95.

[29] Aldahdooh, R., & Abu Naser, S. S. (2017). Development and Evaluation of the Oracle Intelligent Tutoring System (OITS). EUROPEAN ACADEMIC RESEARCH, 6(10), 8711-8721.

[30] Alhabbash, M. I., Mahdi, A. O., & Abu Naser, S. S. (2016). An Intelligent Tutoring System for Teaching Grammar English Tenses. EUROPEAN ACADEMIC RESEARCH, 6(9), 7743-7757.

[31] Al-Hanjori, M. M., Shaath, M. Z., & Abu Naser, S. S. (2017). Learning computer networks using intelligent tutoring system. International Journal of Advanced Research and Development(2), 1.

[32] El Haddad, I. A., & Abu Naser, S. S. (2017). ADO-Tutor: Intelligent Tutoring System for leaning ADO. NET. EUROPEAN ACADEMIC RESEARCH, 6(10), 8810-8821.

[33] Elnajjar, A. E. A., & Abu Naser, S. S. (2017). DES-Tutor: An Intelligent Tutoring System for Teaching DES Information Security Algorithm. International Journal of Advanced Research and Development, 2(1), 69-73.

[34] Hilles, M. M., & Abu Naser, S. S. (2017). Knowledge-based Intelligent Tutoring System for Teaching Mongo Database. EUROPEAN ACADEMIC RESEARCH, 6(10), 8783-8794.

[35] Mahdi, A. O., Alhabbash, M. I., & Abu Naser, S. S. (2016). An intelligent tutoring system for teaching advanced topics in information security. World Wide Journal of Multidisciplinary Research and Development, 2(12), 1-9.

[36] Naser, S. (2009). Evaluating the effectiveness of the CPP-Tutor an intelligent tutoring system for students learning to program in C++. Journal of Applied Sciences Research, 5(1), 109-114.

[37] Shaath, M. Z., Al-Hanjouri, M., Abu Naser, S. S., & Aldahdooh, R. (2017). Photoshop (CS6) intelligent tutoring system. International Journal of Academic Research and Development, 2(1), 81-87.

[38] Vanlehn, K.; The behavior of tutoring systems. International Journal of Artificial Intelligence in Education, 16:227–265, August 2006.

[39] Koedinger, K; Anderson, J; Hadley, W; and Mark, M; Intelligent tutoring goes to school in the big city. International Journal of AI in Education, 8:30–43, 1997.

[40] Mitrovic , A; Mayo, M; P. Suraweera, and B. Martin. Constraint-based tutors: A success story. In Proceedings of the 14th International conference on Industrial and engineering applications of artificial intelligence and expert systems, pages 931–940, London, UK, 2001. Springer-Verlag.

[41] https://www.3asfh.com/, Available at 15/1/2018.

[42] Graesser, A.C., Lu, S., Jackson, G.T. et al. 2004. Auto Tutor: A tutor with dialogue in natural language. Behaviour Research Methods, Instruments, & Computers 36: 180.

[43] Mitrovic, A. (1998a). A Knowledge-Based Teaching System for SQL. In T. Ottmann, I. Tomek (Eds.) Proceedings of ED-MEDIAÕ98 (pp. 1027-1032). VA: AACE.

[44] Mitrovic, A. (1998b). Experiences in Implementing Constraint-Based Modeling in SQL-Tutor. In Proceedings of 4th International Conference on Intelligent Tutoring Systems, ITSÕ98 (pp. 414-423).

[45] Mitrovic, A. 2003. An Intelligent SQL Tutor on the Web. International Journal of Artificial Intelligence in Education 13. 171Ð195 IOS Press. University of Canterbury, Private Bag 4800, Christchurch, New Zealand.

[46] Yang, A, Leung, H. Yue, L., Deng, L. 2013. Generating a two-phase lesson for guiding beginners to learn basic dance movements. Computers and Education, 61, pp 1-20.

[47] Picard, R. W., 1997. Affective Computing, MIT Press.

[48] Sarrafzadeh, A., 2008, How do you know that I don't understand? A look at the future of intelligent tutoring systems, Computers in Human Behavior, Vol 24, no 4, pp 1342-1363.

[49] VanLehn1, K., Lynch, C.,Schulze, K., Shapiro, J., Shelby, R., Taylor, L., Treacy, D., Weinstein, A., and Wintersgill, M. 2005. The Andes Physics Tutoring System: Lessons Learned. International Journal of Artificial Intelligence in Education, 15(3).

[50] Sleeman, D. H., 1987. PIXIE: a shell for developing intelligent tutoring systems, AI & education: Learning environments and intelligent tutoring systems, pp. 239-265.

[51] Shortliffe, E. H., 1976, Computer based medical consultations, MYCIN.

[52] Hyacinth S.N, 1990, Intelligent tutoring Systems: An Overview, AI Review, pp 251-277.

[53] Johnson, W. L, Soloway, E. M., 1984. PROUST: Knowledge-based program debugging. Proc: The 7th International Software Engineering. Conference, Orlando, Florida, pp. 369-380.

[54] Dede, C. 1986. A review and synthesis of recent research in intelligent computer-assisted instruction. International man-machine studies, 24, pp 329-353.

[55] Free English Grammar E-Book Level 2, In: Expresso English, The link: https://www.espressoenglish.net/.

[56] Graesser, A.C., Lu, S., Jackson, G.T. et al. 2004. Auto Tutor: A tutor with dialogue in natural language. Behaviour Research Methods, Instruments, & Computers 36: 180.

[57] Garito, M.A. 1991. Artificial intelligence in education: evolution of the teaching-learning relationship. British journal of educational technology, 22(1),pp 41-47.

[58] Johnson, W. L,Soloway, E. M., 1984. PROUST: Knowledge-based program debugging. Proc: The 7th International Software Engineering. Conference, Orlando, Florida, pp. 369-380.

[59] Hyacinth S.N, 1990, Intelligent tutoring Systems: An Overview, AI Review, pp 251-277.

[60] C. J. Butz, S. Hua, R. B. Maguire, "A web-based Bayesian intelligent tutoring system for computer programming", Web Intelligence and Agent Systems, Vol.4, No.1, pp.77-97 · January 2006.

[61] Carter, Elizabeth and Blank, Glenn D, "An Intelligent Tutoring System to Teach Debugging", Artificial Intelligence in Education: 16th International Conference, AIED 2013, Memphis, TN, USA, July 9-13, 2013.

[62] Peter Haddawy, Siriwan Suebnukarn. COMET: A Collaborative Tutoring System for Medical Problem-Based Learning, IEEE Intelligent Systems, 2007; 22:70-77. July/August 2007, doi:10.1109/MIS.2007.66

[63] Mahmoud, Ahmed Y and Chefranov, Alexander G, (2009) Hill cipher modification based on eigenvalues hcm-EE,Proceedings of the 2nd international conference on Security of information and networks ACM, pp. 164-167

[64] Ahmed, Y Mahmoud and Chefranov, Alexander, (2011)Hill cipher modification based on pseudo-random eigen values HCM-PRE, journal of Applied Mathematics and Information Sciences (SCI-E), vol (8:2), pp. 505-516

[65] Mahmoud, Ahmed Y and Chefranov, Alexander G (2010) Secure Hill cipher modifications and key exchange protocol, Automation Quality and Testing Robotics (AQTR), 2010 IEEE International Conference, vol 2, pp.1-6

[66] Doukhnitch, Evgueni and Chefranov, Alexander G and Mahmoud, Ahmed, (2013) Encryption Schemes with Hyper-Complex Number Systems and Their Hardware-Oriented Implementation, Theory and Practice of Cryptography Solutions for Secure Information Systems},vol 110, IGI Global

[67] Mahmoud, AY and Chefranov, Alexander G, (2012), Secure hill cipher modification based on generalized permutation matrix SHC-GPM, journal of Information Sciences Letters, pp. 91-102

[68] Chefranov, Alexander G and Mahmoud, Ahmed Y, (2013), Commutative Matrix-based Diffie-Hellman-Like Key-Exchange Protocol, Information Sciences and Systems 2013, pp. 317-324,Springer, Cham

[69] Mahmoud, Ahmed Y and Chefranov, Alexander G, (2014), A Hill Cipher Modification Based on Eigenvalues Extension with Dynamic Key Size HCM-EXDKS, International Journal of Computer Network and Information Security, vol 6:5, Modern Education and Computer Science Press

[70] Chefranov, Alexander G and Mahmoud, Ahmed Y, (2010), Elgamal public key cryptosystem and signature scheme in GU (m, p, n), Proceedings of the 3rd international conference on Security of information and networks, pp. 164-167, ACM

[71] Mahmoud, Ahmed Yehya Ahmed, (2012) Development of Matrix Cipher Modifications and Key Exchange Protocol, Ph.D thesis, Eastern Mediterranean University (EMU)

[72] Mahmoud, Ahmed Y. and Mahdi, Ali Osama, (2016) Comments On Multi-window Against Mobile Application Lock, Journal of Multidisciplinary Engineering Science Studies (JMESS), vol 2:5, May – 2016, pp. 494-497, JMESS

[73] Abdelwahed, Ann S. and Mahmoud, Ahmed Y. and Bdair, Ramiz A. (2017), 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, vol 15:1, pp. 1-26