KNOWLEDGE – International Journal
Vol. 28.4
December, 2018

CRYPTOGRAPHIC ALGORITHM FOR DEFENDING INFORMATICS TEST RESPONSES

Ilhan Istikbal Ibryam
"Dimitar Talev" Secondary School, Dobrich, Republic of Bulgaria i.ibryam@shu.bg
Byulent Mustafa Mustafa
Konstantin Preslavsky University of Shumen, Faculty of Mathematics & Informatics, Republic of Bulgaria byulent_mustafa@abv.bg
Atti Rashtid Mustafa
Konstantin Preslavsky University of Shumen, College in Dobrich, Republic of Bulgaria
atti_mustafa@abv.bg

Abstract: With the introduction of Information Technology in educational process we need more often to use electronic evaluation. The examples of test variants in the secondary school are often prepared with the help of word processing editors as WordPad that has good opportunities for elementary text formatting. Another part of the teachers often use Microsoft Word when preparing their tests. It is true that Microsoft Word has much more editing and formatting instruments than WordPad. For access to electronic educational resources suggested by the school teachers two or more computer networks are built (teachers' and learners'). Using these networks and their access rights, each user, learner or teacher, has the opportunity to add files and directories into the school database (DB). Learners can add files with the exercises they have done during their classes. Teachers suggest through the database the electronic lessons they have developed. At the end of each unit each teacher prepares an electronic test. In it there are described the evaluation criteria depending on the number of points the student has gathered through correct responses. In most cases we notice that in the teachers' network files with the responses of the tests are added later on. Not always the means for defence offered by the system administrators at the school can guarantee the safety of our files and more exactly the manipulation of the answers of the electronic forms of check up. Aiming at more effective defence of the text files, this article views an algorithm created by us for cryptographic defence of text files and it's application in secondary school. The effective use of cryptographic information defence minimises the opportunity to decipher the coded information aiming at its misuse by the learners. Providing safe defence against unsanctioned access in computer communication is a complex and extensive task which is solved by means of a set of measures of organisation and programme-technical character. The defence of the process of submitting data requires utmost attention because it concerns the most vulnerable and accessible for violation points in the communication systems.
Keywords: cryptographic algorithm, defence of text data, information defence

КРИПТОГРАФСКИ АЛГОРИТЪМ ЗА ЗАЩИТА НА ОТГОВОРИ НА ТЕСТ ПО ИНФОРМАТИКА

Илхан Истикбал Ибрям
СУ „Димитър Талев“, гр. Добрич, Република България i.ibryam@shu.bg
Бюлент Мустафа Мустафа
Шуменски университет „Епископ Константин Преславски“, Факултет по Математика и информатика, Република България byulent_mustafa@abv.bg
Атти Рашид Мустафа
Шуменски университет „Епископ Константин Преславски“, Колеж - Добрич, Република България
atti_mustafa@abv.bg

Анотация: С внедряването на информационните технологии в образователният процес все по-често се налага и формата за проверка и контрол да се извършва посредством електронно оценяване. Примерните варианти на тестовете в средните училища често се подготвят с помощта на текстов редактор като WordPad, притежаващ добри възможности за елементарно оформление на текст. Друга част от преподавателите често се възползват при подготовката на тестовете си от възможностите, които предлага текстообработващата система Microsoft Word. Неоспорим е факта, че Microsoft Word притежава много повече инструменти за

редактиране и форматиране на текста в сравнение с WordPad. За достъп до електронните образователните ресурси, които се предлагат от учителите в училищата са изградени две и повече компютърни мрежи (преподавателска и ученическа). Използвайки тези мрежи и техните права за достъп всеки потребител било то обучаем или обучаващ има възможност да добавя файлове и директории в базата данни (БД) на училището. От страна на учениците те могат да добавят файловете с упражненията, които са правили по време на час. Учителите от своя страна предлагат с помощта на БД разработените в електронен вариант от тях уроци. В края на всеки раздел всеки преподавател подготвя и електронен вариант на тест. В него са описани и критериите за оценяване според броя точки, на които е отговорил правилно ученикът. В повечето случаи се забелязва, че в преподавателската мрежа се добавят и файловете с отговорите на съответните тестове. Не винаги средствата за защита предлагани от системните администратори в съответните училища могат да ни гарантират сигурността на файловете и по-точно манипулирането на отговорите на електронните форми за проверка и конторл на знанията. Именно с цел по-ефективна защита на текстовите файлове в тази статия разглеждаме създаден от нас алгоритъм за криптографска защита на текстови файлове и приложението му в средните училища. Ефективното използване на криптографска защита на информацията свежда до минимум възможноста да се дешифрира кодираната информация с цел нейното нежелано използване от страна на обучаемите. Обеспечаването на достатъчно сигурна защита срещу несанкциониран достъп в компютърните комуникации е сложна и широкообхватна задача, която се решава с помощта на комплекс от мерки с организационен и програмно-технически характер. Защитата на процеса на предаване на данни изисква най-сериозно внимание, тъй като тя обхваща най-уязвимите и достъпни за нарушения точки в комуникационните системи.
Ключови думи: криптографски алгоритъм, защита на текстови данни, защита на информацията

1. ВЪВЕДЕНИЕ

Актуален проблем е определянето на критерий за ефикасност и ефекивност на криптографските системи. Ефективността може да се определи като величина, с която се измерва количествено полезността на дадена система. Тя може да се измери с някакви показатели, например ресурси, време, вероятности и т.н. За разлика от ефективността, ефикасността не се оценява от количеството на използваните ресурси за постигане на дадена цел, а само от факта на постигането на поставената цел. [1]. В тази статия ние използваме карта на Tinkerbell като основна за генериране на ключове. То е рекурсивно дефиниран по формула (1).

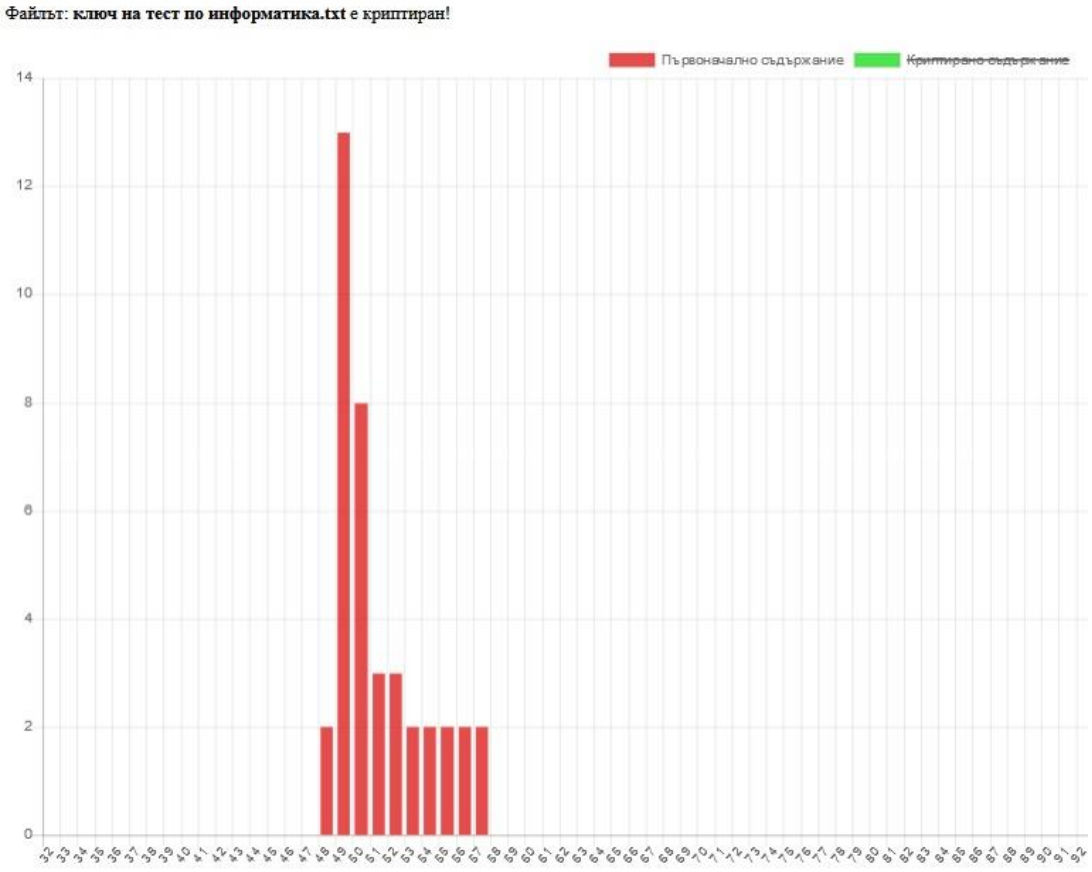
2. ИЗЛОЖЕНИЕ

В годишното разпределение по дисциплината „Информатика“ в Ха клас са предвидени 36 часа (по 1 час седмично). Точно толкова е и разпределението по дисциплината „Информационни технологии“ в Хб клас. По „Информатика“ учебният материал е разпределен на две основни теми: Алгоритми и структури от данни и програмиране. Учебният материал по дисциплината в Хб клас е разделен в четири основни теми: Бази от данни, Компщтърни презентации, Компютърни мрежи и интегриране на дейности. За първият учебен срок е предвидено по-обстойно запознаване с релационните бази данни, етапите на разработка и принципите на проектирането им. От учениците се изисква да придобият и усвоят основни умения при създаването на таблици в среда MS Access, да умеят да създават заявки за изчисления, с прости условия, със съставни условия, с предикати IN, BETWEEN, LIKE, с изчислени полета (изрази), параметрични, обобщаващи заявки (с групови функции), кръстосани заявки (таблични) и заявки за обновяване и изтриване. Релациите да съдържат и от трита типа взаимовръзки: 1:1, 1:M и M:N. Изискванията към формулярите да са : формуляри за разглеждане, формуляри за добавяне, формуляр с подформуляр, свързани формуляри, формуляр меню. Във самите тях да се съдържат различните видове контроли – label, text box, line, combo box, list box, button и др. Да умеят да създават отчети с групиране по поле. Отчетите трябва да съдържат номер на страница и дата. Макроси да отварят различни видове обекти. В учебната програма и на двете дисциплини се предвижда в началото и края на учебната година, както и след всеки тематичен раздел да се отделят специални уроци за осъществяване на входяща, междинна и изходяща диагностика. Именно след работа с линейни алгоритми и масиви е предвидена проверка и контрол на знанията на учениците. Същото е предвидено и след работа с всеки обект от MS Access е предвидена проверка и контрол на знанията на учениците. Получените данни от диагностиката на входно ниво, анализирани и сравнени, дават необходимата информация за компетентно и ефективно организиране на учебния процес. Изходящата диагностика дава възможност да се съпоставят резултатите от учебно-възпитателната работа по информатика и информационни технологии в края на учебната година с посочените в Държавните образователни стандарти изискванияза знанията и уменията. Тя разкрива постиженията и недостатъците в

подготовката на учениците, показва ефективността от работата на учителя. Често за входни, междинни и изходните нива учителите избират един от класическите методи, а именно – тест. Такава форма за контрол е предвидена и по информатика и информационни технологии. Подготвени са различни по структура тестве (с отворени и затворени въпроси). Уточнени са предварително критериите за оценяване. Отговорите на тестовете (примерен вариант) са съхранени в текстови файлове(фиг1.). Защитата на ключовете на тестовете е от особенна значимост за правилното и обективно оценяване на постигнатите умения и знания на учениците. За ефективното му осъществяване е целесъобразно да се използват различни криптографски алгоритми. Алгоритъмът, който използваме е реализиран с помощта на PHP – скриптов език с отворен код. Преди прилагането на алгоритъма за криптиране, той е подлойен на редица статистически тестове, за да се докаже криптографската му сигурност. Използван е NIST Test suite, който включва множество от функционални тестове. След изпълнението на алгоритъма (1) има възможност да се визуализира графично и таблично първоначалното съдържание на символите. (фиг.2). На фиг. 3 са представени таблично и графично символите след криптирането им, а на фиг. 4. текстовият файл след криптирането му.

```
1а, 2б, 3а, 4в, 5г, 6а, 7б, 8б, 9в, 10в, 11а, 12б, 13в, 14б, 15а, 16а, 17а, 18б, 19а, 20а, 21а, 22б, 23в, 24в,
```

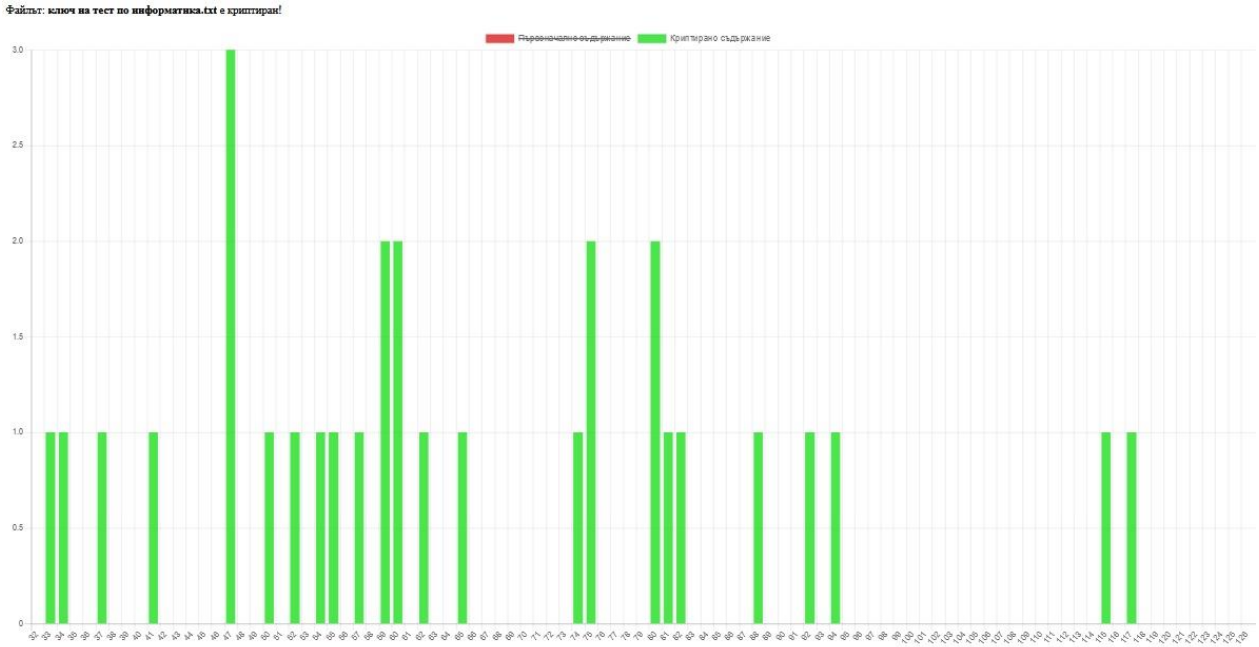
Фиг.1. Примерен вариант на отговори на тестове.



Символи в първоначалното съдържание:

1 = 13	, = 10	2 = 8	, = 7	3 = 3	4 = 3	, = 6	5 = 2	, = 1	6 = 2	7 = 2	8 = 2	9 = 2	0 = 2	

Фиг.2 Символи в първоначално съдържание



Символи в първоначалното съдържание:

1 = 13	, = 10	2 = 8	, = 7	3 = 3	4 = 3	, = 6	5 = 2	, = 1	6 = 2	7 = 2	8 = 2	9 = 2	0 = 2	

Символи в криптираното съдържание:

= 2	' = 1	a = 1	= 1	J = 1	= 2	= 1	K = 2	= 1	= 3	y = 1	= 3	< = 2	= 2	= 1
P = 2	Hk = 1	= 1	o = 1	; = 2	" = 1	s = 1	' = 1	2 = 1	к = 1	> = 1	X = 1	= 1	= 1	4 = 1
/ = 3	= 1	Q = 1	= 1	= 2	p = 1	A = 1	= 1	! = 1	u = 1	= 1	= 1	= 1	= 2	= 1
R = 1	= 1	= 2	= 1	6 = 1	5 = 1	= 2	% = 1	J7 = 1	= 1	\ = 1	^ = 1	= 1	G = 1	7 = 1
z7 = 1	9 = 1	= 1	) = 1	= 1	H = 1	= 1	= 1							

Фиг.3. Символи в криптирано съдържание

$$u_{m+1} = u_m^2 - v_m^2 + au_m + bv_m \quad (1)$$
$$v_{m+1} = 2u_m v_m + cu_m + dv_m$$

където a=0,9, b=-0,6013, c=2.0, и d=0,50. [2]

Разкриването на съдържанието на данните е най-често срещаното преднамерено въздействие, което по същество води до нарушаване на анонимността на данновия обмен [3]. За декриптирането на файла се изисква да знаем ключът за декриптиране, който се генерира от друг алгоритъм. По този начин, можем да твърдим, че текстовите файлове, в които се съдържат отговори на тестове са максимално защитени в базата данни от нежелан достъп. Сигурността на информацията е понятие, което може да се опише със следните три основни характеристики: конфиденциалност или секретност, цялостност и точност, наличност[5].

```
011011/1101010100100111111101000/011000/0110000110110110010010l0/001011/1010100101001011100l0111/
010101/1110110011011101011111001/011001/0011110000011101100110011/000101/1110010101001000011010ll/
010100/1100110110111110100111011/100010/0111001111011001101000011/110010/0000110100101010000l0101/
011011/111110/0101100010111111010100111/110100/111011/0010111111100100111011100/011001/010101/
0000010100011111101110001/001110/001101/0111000001000001100000101/100001/010000/0111010100001101000111101/
001001/111100/1100000000101111100011100/001010/101111/0000000001010010000000001/010111/001011/
1011010000110110110000110/110101/011000/0010010111110001010010l0/110111/011011/1010010101011100010111l0/
000000/011000/1110001011110001010001l1/110111/010111/0100101111100010011100l1/110111/111001/
1110111111101110100010ll/010110/101001/0001001111010011100010010/010101/011001/0001111010001100110001000
```

Фиг.4. Криптиран файл съдържащ ключ на тест по информатика

3. ЗАКЛЮЧЕНИЕ

Чрез тестовете (най-използваните методи за педагогически изследвания) се проверява степента и качеството на усвоените знания и умения. Предимствата, които дава този метод на диагностика, са много, но най значимото, е че осигурява обективност на оценяването, защото се посочват ясни и еднозначни критерии за

оценяване и скали за измерване на резултатите. У обучаемите се сформират навици за системна работа през семестъра по овладяване на учебното съдържание по информатика и информационни технологии.

ИЗТОЧНИЦИ

[1] Станев Ст., С. Железов, Т.Великова, В. Неделчева, М. Иванова. К вопросу применения термина „Эффективность стегосистем“ в учебном курсе „Компютерная стеганография“. Трудове на международната научно-практическа конференция на НПУ „Драгоманов“, Киев, 2011, 310-311.
[2] Malchev, D., Ibryam, I. Applied Mathematical Sciences, Vol. 9, 2015, no. 78, 3847 – 3853, HIKARI Ltd, www.m-hikari.com, http://dx.doi.org/10.12988/ams.2015.52149
[3] Антонов П. Малчев, С. Криптография в компютърните комуникации, Варна 2000, стр.15.
[3] Ibryam, I, Mustafa, B., Mustafa, A, Creating an information system for a police office and cryptographic protection of its information, XV-th Jubilee INTERNATIONAL SIENTIFIC CONFERENCE December, Bansko, Bulgaria
[5] Синягина, Н. Мирчев, И., Дамянов, И., Христов, С. Защита на компютърната информация, Университетско издателство"Неофит Рилски", стр. 23, Благоевград, 2005