FRI-ONLINE-1-CCT1-05

TEACHING CRYPTOGRAFY AND DATA SECURITY: SIMPLIFIED DES ALGORITHM[5]

Assist. Prof. Emilia Golemanova, PhD
Department of Computer Systems and Technologies,
"Angel Kanchev" University of Ruse
Tel.: 082-888-681
E-mail: EGolemanova@uni-ruse.bg

Assist. Prof. Tzanko Golemanov, PhD
Department of Computer Systems and Technologies,
"Angel Kanchev" University of Ruse
Tel.: 082-888-681
E-mail: EGolemanova@uni-ruse.bg

Abstract: *Although a lot of symmetric ciphers have been developed since the Data Encryption Standard (DES) was introduced, and although it is replaced by the Advanced Encryption Standard (AES), teaching DES plays a substantial part in every Cryptography and Data Security course, because the study of DES provides an understanding of the fundamental principles used in symmetric block ciphers at all. Due to the complex structure of the full DES, for teaching purposes a simplified version is usually used. It allows the student to perform encryption and decryption by hand and gain a good understanding of the working of the algorithm details. The paper describes the approach used in teaching of the Simplified DES (S-DES) at Computer Systems and Technologies department of Ruse University and the especially developed educational tool for learning and testing purposes.*

Keywords: *cryptography, block ciphers, DES, S-DES, teaching tool*

ВЪВЕДЕНИЕ

Въпреки че, след въвеждането на *Data Encryption Standard (DES)* през 1977 (National Bureau of Standards, 1977), са разработени много други симетрични шифри и въпреки че той е заменен от *Advanced Encryption Standard (AES)* през 2001 г (United States National Institute of Standards and Technology, 2001)., преподаването на DES играе съществена роля във всеки курс по „Криптография и защита на данните", тъй като изучаването му осигурява разбиране на основните принципи, използвани в съвременните симетрични блокови шифри като цяло. Поради сложната структура на DES и големината на входните данни, за учебни цели обикновено се използва опростена версия (Stallings, 2017). Тя позволява на обучавания да извърши криптиране и декриптиране на ръка и да придобие детайлна представа за работата на алгоритъма.

Макар и опростена версия на DES, преподаването на S-DES е предизвикателство и за обучаващия. Преподавателят се нуждае от удобен симулатор, чрез който да обясни алгоритъма за конкретен пример. Освен това добре е да разполага със софтуер, автоматизиращ процеса на самопроверка и тестване. За съжаление, повечето от използваните автоматизирани средства за обучение по S-DES са по-скоро калкулатори (Simplified DES (S-DES) Calculator, 2021) (Simplified DES (S-DES) Calculator, 2021), представящи само окончателния резултат от работата на алгоритъма, а не отделните стъпки. Други, които пък предлагат постъпково изпълнение са мобилни приложения (Mountogiannakis, 2021), имащи следните две ограничения - ограничено екранно пространство и визуализация на текстово, а не графично решение, какъвто е основният подход при дефинирането на S-DES.

[5] Докладът е представен на заседание на секция 3.2 на 29 октомври 2021 с оригинално заглавие на български език: ОБУЧЕНИЕ ПО КРИПТОГРАФИЯ И ЗАЩИТА НА ДАННИТЕ: ОПРОСТЕН DES

Представеният доклад описва подхода, използван при преподаването на опростения DES (S-DES) в катедра „Компютърни системи и технологии“ на Русенския университет и специално разработения инструмент за целите на обучението и тестването.

ИЗЛОЖЕНИЕ

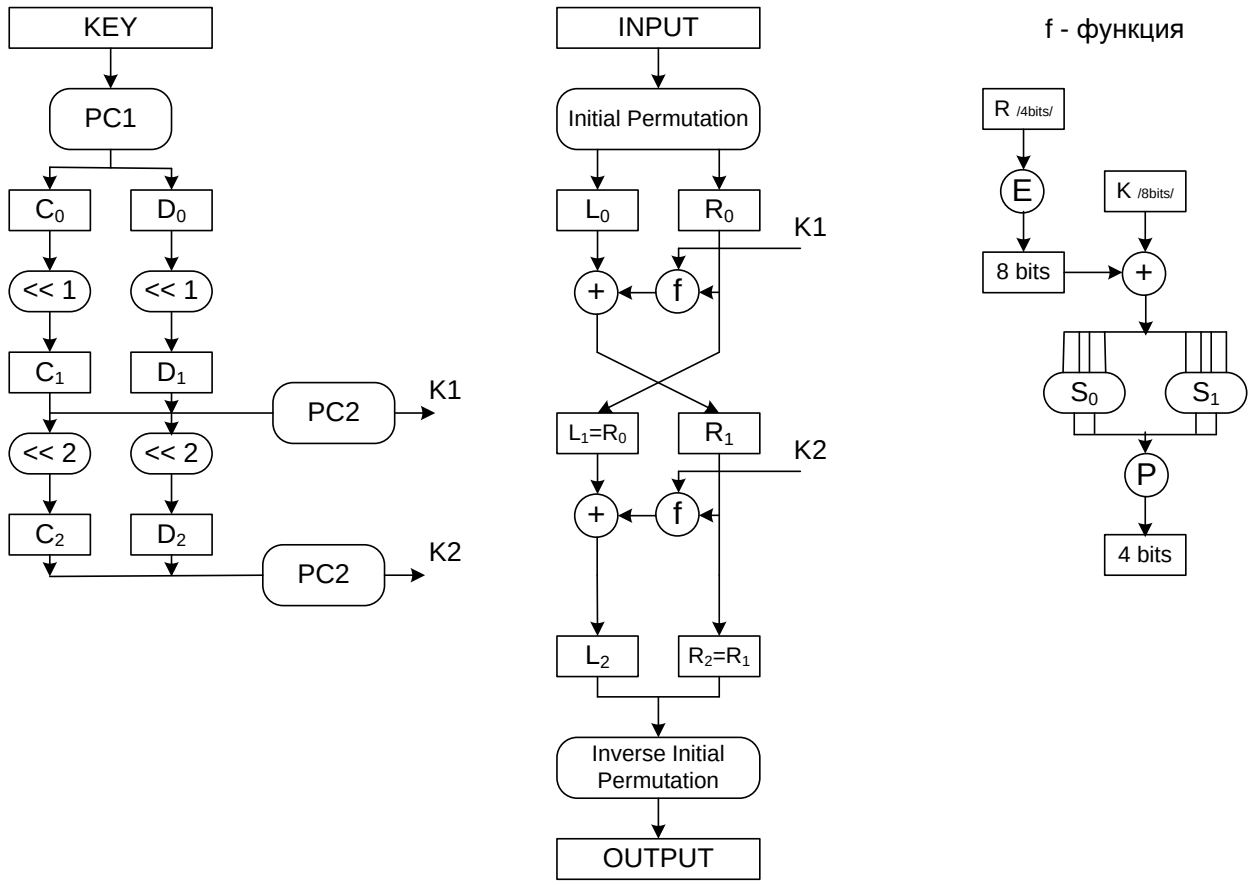
Опростен DES (S-DES)

Опростената версия на DES, използвана за учебни цели, има същата архитектура като тази на реалния шифър, но се различава по следните параметри:

Таблица 1. Разлика между DES и S-DES

Параметри	DES	S-DES
Размер на блока открит текст/ шифротекст	64	8
Първичен ключ	64	10
Рундов ключ	48	8
Брой рундове	16	2
Брой S-кутии	8	2
Вход/изход на S-кутия	6/4	4/2

Общата схема на S-DES, включваща криптиращия алгоритъм и генерирането на рундовите ключове, е представена на Фиг. 1.



Фиг. 1. Обща схема на S-DES

Стъпките, генериращи двата 8-битови рундови ключа (подключове) K1 и K2 са:

1. Преподреждане на първичния ключ K, използвайки фиксирана пермутационна схема PC1:

PC 1									
3	**5**	**2**	**7**	**4**	**10**	**1**	**9**	**8**	**6**

2. Разделяне на ключа на лява и дясна половина C_0 и D_0.
3. Кръгово изместване наляво с един бит на C_0 и D_0, получавайки C_1 и D_1.
4. Преподреждане заедно на двете половини C_1 и D_1, съобразно фиксирана пермутационна схема PC2, генерирайки първия рундов ключ K1.

PC 2							
6	**3**	**7**	**4**	**8**	**5**	**10**	**9**

5. Кръгово изместване наляво с два бита на C_1 и D_1, получавайки C_2 и D_2.
6. Преподреждане заедно на двете половини C_2 и D_2, съобразно фиксирана пермутационна схема PC2, генерирайки втория рундов ключ K2.

K1 и K2 се използват като входове на криптиращата/декриптираща схема.

Стъпките за криптиране са:

1. Прилагане на фиксирана начална пермутация

Initial Permutation							
2	**6**	**3**	**1**	**4**	**8**	**5**	**7**

2. Разделяне на резултата на две половини L_0 и R_0

3. Прилагане на функцията на Фейстел f върху дясната половина R_0:

3.1. Прилагане на фиксирана „разширяваща“ пермутация E

E							
4	**1**	**2**	**3**	**2**	**3**	**4**	**1**

3.2. XOR на резултата и подключа K1

3.3. Резултатът се разделя на два блока от по 4 бита, като първият се преобразува от S-кутията (таблицата) S_0, а вторият – от S_2, съобразно схемата:

- Първият и последният бит определят реда на таблицата, а вторият и третият – колоната.
- Резултатът е съдържанието на клетката от съответната таблица, съответстваща на определения ред и колона.

S_0				
	Column			
Row	**0**	**1**	**2**	**3**
0	1	0	3	2
1	3	2	1	0
2	0	2	1	3
3	3	1	0	3

S_1				
	Column			
Row	**0**	**1**	**2**	**3**
0	0	1	2	3
1	2	0	1	3
2	3	0	1	0
3	2	1	0	3

3.4. Преподреждане на получения резултат, съобразно фиксирана пермутационна схема P.

4. XOR на получения резултат с L_0

5. Резултатът от стъпка 4 е новата дясна половина R_1, а оригиналната дясна половина R_0 е новата лява половина L_1. Следва преход към втори рунд.

6. Прилагане на функцията на Фейстел f върху дясната половина R_1:

6.1. Прилагане на фиксирана „разширяваща“ пермутация E

6.2. XOR на резултата и подключа K2

6.3. Резултатът се разделя на два блока от по 4 бита, като първият се преобразува от S-кутията (таблицата) S_0, а вторият – от S_2, съобразно схемата:

- Първият и последният бит определят реда на таблицата, а вторият и третият – колоната.
- Резултатът е съдържанието на клетката от съответната таблица, съответстваща на определения ред и колона.

6.4. Преподреждане на 4-битовия резултат, съобразно фиксирана пермутационна схема P:

P			
2	**4**	**3**	**1**

7. XOR на получения резултат с L_1

8. Резултатът от стъпка 7 е новата лява половина L_2, а оригиналната дясна половина R_1 е новата дясна половина R_2.

9. Върху резултата L_2 R_2 се прилага фиксирана пермутация, която е обратната на началната пермутация от стъпка 1.

Inverse Initial Permutation							
4	**1**	**3**	**5**	**7**	**2**	**8**	**6**

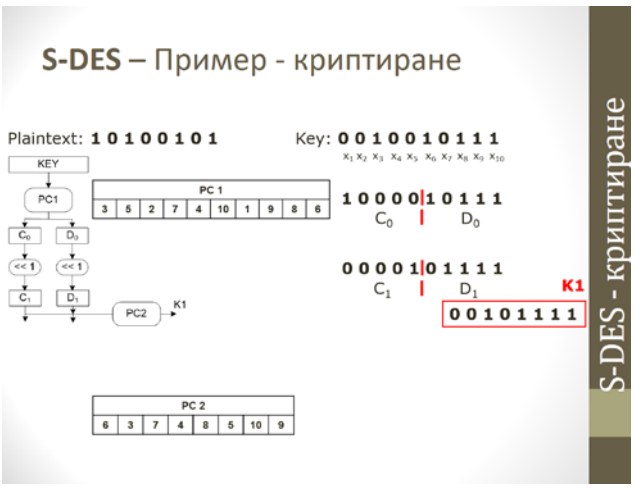
S-DES: обучение

Методическият подход, използван при преподаването на DES включва:

- използване на мултимедийна презентация за представяне на DES-алгоритъма;
- използване на мултимедийна презентация за представяне на S-DES-алгоритъма;
- използване на инструмент за самообучение по S-DES-алгоритъма;
- използване на инструмент за тестване на знанията върху S-DES-алгоритъма.

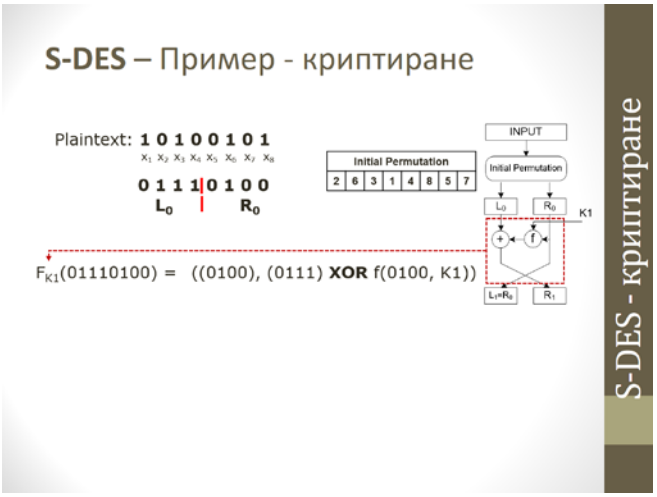
Мултимедийните презентации са удобен и атрактивен способ за представяне на информация. Съчетавайки в себе си динамика, звук, изображения, видео, анимация, те значително повишават възприемането на информацията, правейки ги и ефективен инструмент за обучение.

Разработените мултимедийни презентации, използват анимирани схеми, които нагледно изобразяват постъпковото изпълнение на DES и S-DES алгоритмите. На Фиг. 2 е представен един конкретен момент от изпълнението на S-DES – алгоритъма – генерирането на рундовия ключ K1 за разглеждания пример.

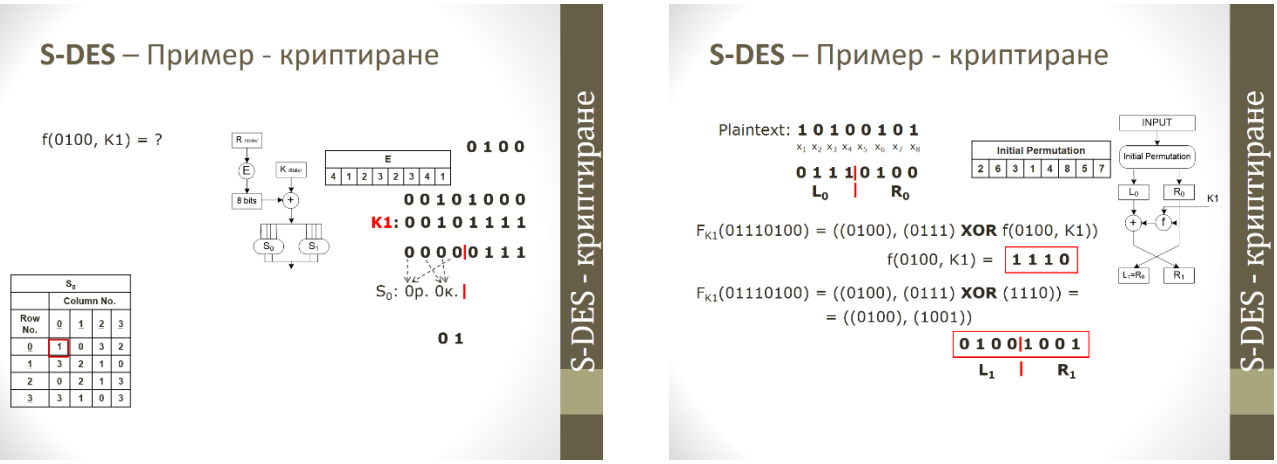


Фиг. 2. Генериране на първия рундов ключ

По-голяма трудност студентите изпитват при разбирането на работата на самия шифър при вече генерирани рундови ключове. За целта се използва подход с изчисляване на рундовите функции на двата последователни рунда. Всяка рундова функция се представя като функция, приложена върху лявата половина и дясната половина на обработвания блок и генерираща техните нови стойности, съобразно схемата на съответния рунд. Фигура 3 илюстрира описанието на рундовата функция за първи рунд, а Фиг. 4 - два момента от изчисляването й.



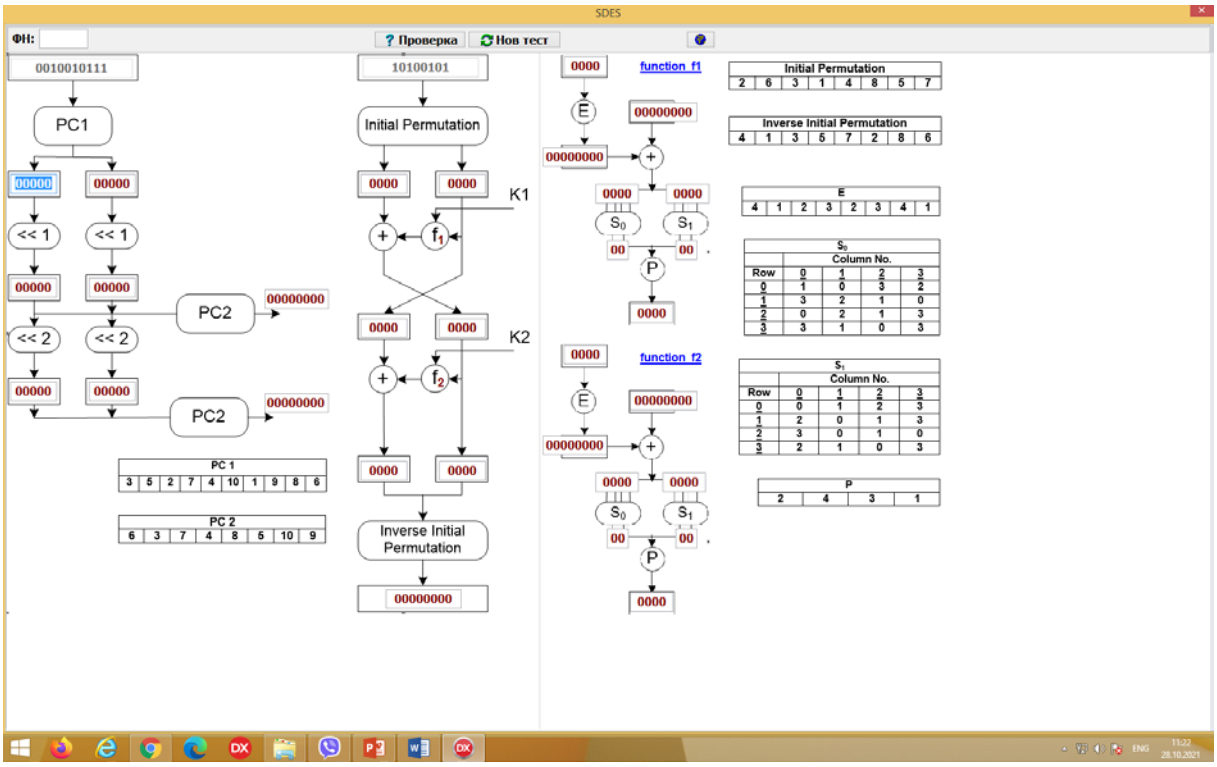
Фиг. 3. Представяне на рундовата функция за първи рунд



Фиг. 4. Два момента от изчисляването на рундовата функция за първи рунд

S-DES: самообучение

При самообучение и самопроверка на знанията студентите разполагат с инструментално средство, авторска разработка, което се използва както по време на практическите занятия, така и при самоподготовка. Предложеният софтуерен продукт **S-DES Tool** е разработен чрез Embarcadero® Delphi в средата на Embarcadero RAD Studio 10.3.3 Rio и има интерфейс (Фиг.6), съвпадащ с основната схема на S-DES, представена на Фиг. 1.



Фиг. 6. **S-DES Tool** в режим „самообучение“

В режим „самообучение/самопроверка“ обучаемият има възможност:

- да избере език – български, английски, руски, което дава възможност за използването му и за обучение чуждестранни студенти;
- да проверява своя отговор на всяка стъпка от алгоритъма;
- да генерира нов тест.

Визуалното представяне на цялостния алгоритъм, както и на всички фиксирани пермутационни и субституционни схеми, подпомага разбирането на алгоритъма, а дори и отпадането на необходимостта от използването на „лист и химикал“ за решаването на конкретни операции и запазване на междинни резултати.

S-DES: тестване на знания при присъствено обучение

S-DES Tool може да се използва и в режим „тестване“. Разликата от режима „самообучение/самопроверка“ е, че обучаемият въвежда своя идентификатор (например факултетен номер) и подгрупа и има право само на една проверка, от която той трябва да прецени в кой момент да се възползва (след използването й, съответният бутон става неактивен). Резултатът от теста се пресмята автоматично като общ брой точки (който се визуализира) и се съхранява като цялостно решение в текстов файл.

S-DES: тестване на знания при дистанционно обучение

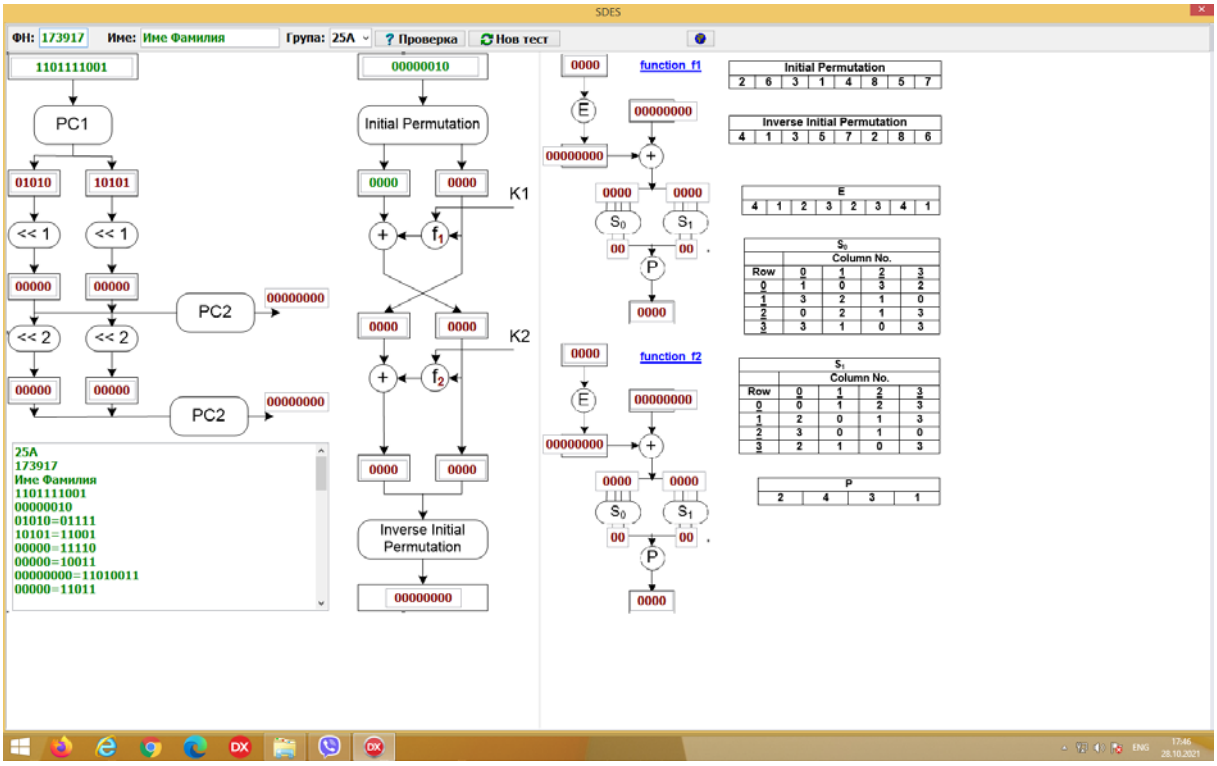
В условията на дистанционно обучение, където контролът върху манипулиране на резултатите от теста е занижен, е особено важно разработването на механизъм за гарантиране автентичността на крайните резултати.

Докладваният инструмент за обучение и тестване в режим на дистанционно обучение се използва от студента по подобен начин както и при присъствено обучение с тази разлика, че при генерирането на текстовия файл с резултатите, студентът има достъп до файла с цел по-късно той да бъде предоставен на преподавателя. За проверка целостността на информацията с резултатите от теста, **S-DES Tool** използва механизма на криптографските хеширащи функции. По този начин се **S-DES Tool** е защитен от:

- неправомерна корекция на резултатите от теста;
- решаването на няколко теста от един и същи потребител.

S-DES: обработка на тестовете

Разработеният софтуерен продукт може да се използва и в режим „преподавател“, за автоматична обработка на резултатите от проведените тестове както и за директен достъп до резултатите на даден студент. След успешна автентикация на преподавателя, той може да избере да визуализира резултатите на конкретен потребител като схема и като текстов файл (Фиг. 7) или да генерира Excel – файл, обобщаващ резултатите на всички тествани.



Фиг. 7. **S-DES Tool** в режим „преподавател“

ЗАКЛЮЧЕНИЕ

Разбирането на функционирането на DES е от ключово значение за разбирането на модела на съвременните симетрични шифри. Използването на опростен вариант на този иначе сложен алгоритъм и имащ големи параметри – 64-битов първичен ключ и 64-битов блок на откритя текст, е традиционен подход, използван при преподаването му. Използването на инструментални средства, улесняващи обучителния процес е с голямо търсене в съвременния свят.

Докладът представя подхода използван от авторите при преподаването на S-DES, както и специално разработено софтуерно средство **S-DES Tool,** подпомагащо както обучаемия, така

и преподавателя в различни етапи от процеса на обучение: обучение, самообучение и тестване в условия на присъствен или дистанционен учебен процес, както и автоматизирана обработка на резултатите от тестването. Предимство на представената разработка е защитата в няколко направления на целостността на резултатите от тестването, което в условията на дистанционно обучение е особено актуален въпрос.

В заключение, опитът от практическите занятия показва, че използваният методически подход на преподаване на S-DES и на разработеното обучително средство **S-DES Tool** увеличава доброто разбиране на оригиналната пълна версия на DES.

ACKNOWLEDGEMENTS

Този доклад се публикува с подкрепата на проект 21-ФЕЕА-01 „Интелигентни компютърни системи: изследване на тяхното развитие, приложение и управление“, финансиран от фонд „Научни изследвания“ на Русенски университет „Ангел Кънчев“.

REFERENCES

Mountogiannakis, A. G. (2021, 11). *S-DES Simulator*. Retrieved from Google Play: https://play.google.com/store/apps/details?id=com.sdesandroid&hl=en&gl=US

National Bureau of Standards, N. (1977). *Data Encryption Standard, FIPS-Pub.46.* Washington D.C.: National Bureau of Standards, U.S. Department of Commerce.

Simplified DES (S-DES) Calculator. (2021). Retrieved from Simplified DES (S-DES) Calculator: http://homepages.neiu.edu/~jakwon1/sdes.html

Simplified DES (S-DES) Calculator. (2021). Retrieved from Simplified DES (S-DES) Calculator: https://fauzanakmalh1.github.io/Simplified-DES-Calculator/

Stallings, W. (2017). *CRYPTOGRAPHY AND NETWORK SECURITY: PRINCIPLES AND PRACTICE* (Seventh Edition ed.). Pearson.

United States National Institute of Standards and Technology, N. (2001). .*Advanced Encryption Standard, Federal Information Processing Standards Publication 197.* United States National Institute of Standards and Technology (NIST).