Project-Based Learning for Teaching "Diffie-Hellman Algorithm, Elgamal Variant"

2022 29th International Conference on Systems, Signals and Image Processing (IWSSIP) | 978-1-6654-9578-3/22/$31.00 ©2022 IEEE | DOI: 10.1109/IWSSIP55020.2022.9854393

Adriana Borodzhieva
Department of Telecommunications
University of Ruse "Angel Kanchev"
Ruse, Bulgaria
aborodzhieva@uni-ruse.bg

***Abstract*—The paper presents the application of the flipped classroom and project-based learning approaches used in the course "Telecommunication Security" intended for students from the specialty "Internet and Mobile Communications" at the University of Ruse when teaching the topic "Diffie-Hellman Algorithm, Elgamal Variant". Project-based learning, one of the tendencies of Education 4.0, develops and improves the main 21st-century skills.**

Keywords—project-based learning; flipped classroom; cryptosystems; Diffie-Hellman algorithm, Elgamal variant.

I. INTRODUCTION

Over the last few years, the terms "Industry 4.0" and "Education 4.0" are increasingly used in our daily lives. Undoubtedly, Education 4.0 contributes to the necessities for state-of-the-art integration of people and technologies on a global scale. In order to assist the execution of Education 4.0, the world's leading universities use modern communication and computer technologies to develop, acquire and improve educational resources, which makes better the engagement and learning of students. The combination of information and communications technology (ICT) and technological modern utensils in universities, including our university, is a defiance of the educational systems of the new era, striving to use the principles of Education 4.0 [1].

In traditional learning, the promotion of dissimilar thinking and creativity is restricted, which, in turn, discourages learners from developing and applying their creativity and dissimilar thinking in academia [2]. An alternative to traditional learning, respectively an innovative method of teaching, is project-based learning (PBL), which might be used as defiance for learners to find creative solutions to real-world problems to attract students' interest and increase and develop their knowledge, skills, and competencies [2].

The paper describes the application of the flipped classroom [3] and the project-based learning [4] approaches in the course "Telecommunication Security" intended for bachelors in the seventh semester from the specialty "Internet and Mobile Communications" at the University of Ruse for presenting the topic "Diffie-Hellman Algorithm, Elgamal Variant". Using these two pedagogical approaches definitely develops and improves the main 21st-century skills, for example, numeracy, and literacy, including ICT literacy, logical, critical, and analytical thinking, initiative, creativity, problem-solving, communication skills, etc.

II. PROJECT-BASED LEARNING IN THE "TELECOMMUNICATION SECURITY" COURSE DUE TO THE COVID-19 PANDEMIC

The course "Telecommunication Security" is studied as mandatory by undergraduate students majoring in "Internet and Mobile Communications" at our University in the seventh semester. The course deals with the main themes in the field of cryptography (used for transforming data from plaintext/ciphertext to ciphertext/plaintext, spanning from classical cryptographic ciphers to asymmetric encryption systems built on complex mathematical problems) and security (technique for protecting information from stealing and hardware or software failures) [3].

The lecturers have used active teaching methods for more than 10 years (since the academic 2010-2011 year). For each topic, students had to solve individual tasks manually in a blank form for the exercise located in the e-learning platform (ELSE) of our University, using guidelines and additional help, if necessary, from the teacher and/or classmates and give the teacher at the end of the exercise. Students are motivated to learn and the level of perception of the material is increased when using active teaching methods. In the last three academic years (2019-2020, 2020-2021, and 2021-2022) in the crisis of Covid-19, the teachers in the course "Telecommunication Security" began to use a combination of two pedagogical approaches – the flipped classroom (FC) and the project-based learning (PBL).

In the paragraph above this one the term "flipped classroom" is defined (Fig. 1, at the top) and similarities and differences between traditional and flipped classrooms are presented below in Fig. 1. The activities of teachers and students "at home" and "at school" (university) using the flipped classroom approach are presented in Fig. 1.

In the flipped classroom [3], at home:1) the lecturers created some videos and/or PowerPoint presentations on the material studied (Fig. 2) and shared them with students by e-mail, in ELSE, or in a Facebook group; 2) the students watched the videos and presentations and prepared some questions for discussions with the teacher.

At school: 1) the students asked questions and participated in the learning activities; 2) the lecturers answered students' questions and facilitated discussions [3].

Written instructions for students in the laboratory at a visible location are provided.

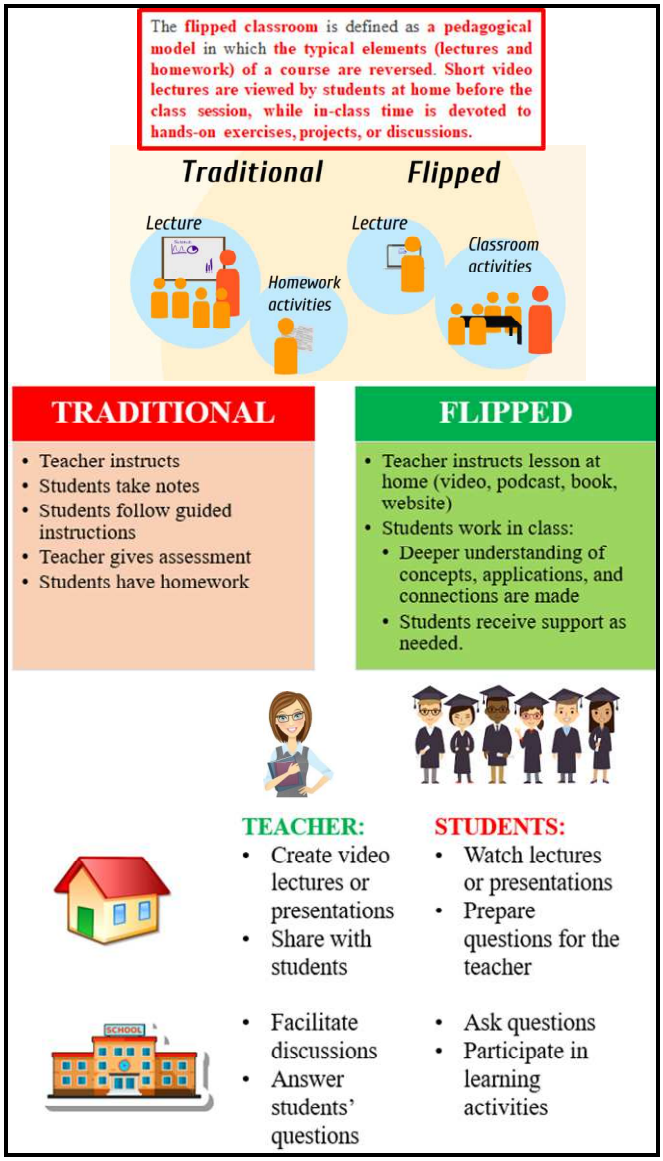


Fig. 1. Traditional vs flipped classrooms and "home" and "school" activities of teachers and students during the flipped classroom approach

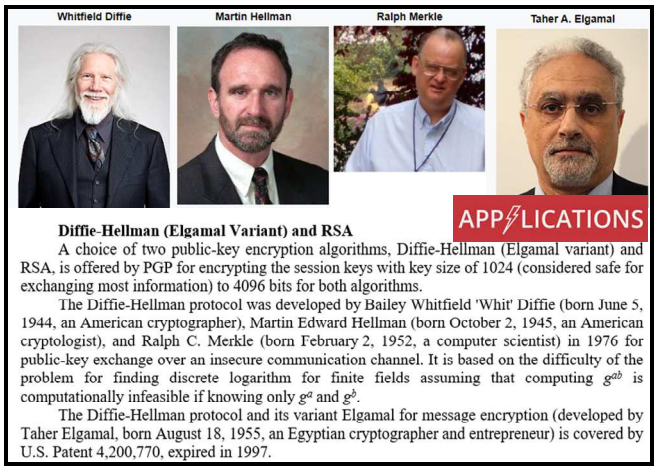
When introducing the PBL concept in the last three academic years, the teachers in the course decided to entrust students with the computer-based implementations of various cryptographic algorithms, such as the knapsack problem (relatively easy and applied in many fields and crypto-systems, presented in more detail in [5]), the Diffie-Hellman algorithm, Elgamal variant, etc. A preliminary acquaintance of the students with the topic "Diffie-Hellman Algorithm, Elgamal Variant" [6, 7, 8] was required. Some applications (for example, in Pretty Good Privacy, PGP), principles of operation, and examples of encrypting and decrypting messages are presented briefly in Fig. 2. For implementing the algorithm, students had to use various software tools, for example, MATLAB [9, 10], MS Excel [11], Logisim [12], ISE Project Navigator [13], etc., if applicable.

At the beginning of the semester, different applications of the teacher were presented to students in advance. They were designed mainly to support the teacher in creating individual tasks for students during the workshops.

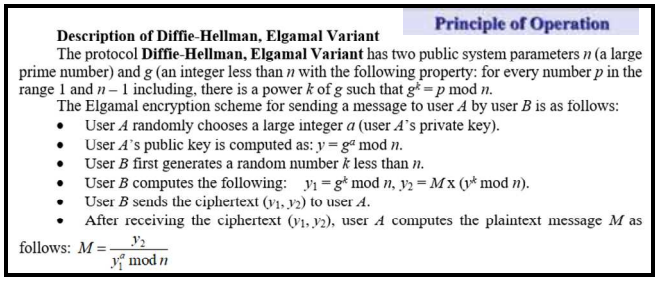
The applications were created with different software tools such as:

1) MATLAB (a platform for numeric computations and programming used by students, scientists, and engineers for data analysis, algorithms and models synthesis" [9]) and GUIDE (an extension in MATLAB intended for building tools with graphical user interfaces, GUIs [10]) – Fig. 3 (top-left), where implementations of classical ciphers are given, such as MATLAB implementations of bifid [14] and affine [15] ciphers (with GUI).

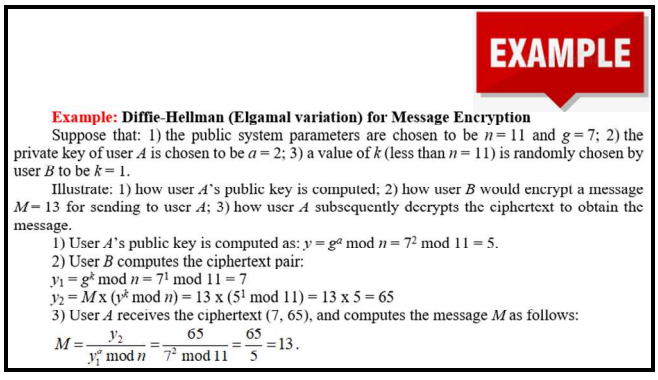
2) MS Excel [11], which makes the solution of a specific task easily and readable because of the tabular view of the calculations – Fig. 3 (top-right), where implementations of cryptographic ciphers and algorithms are given, for example, Hill ciphers [16], Shamir's Secret Sharing algorithm [17], RSA algorithm (coming from the surnames of Ron Rivest, Adi Shamir, and Leonard Adleman, who publicly described the algorithm in 1977) [18], cryptosystems built on Linear Feedback Shift Registers (LFSRs) [19, 20] or Non-Linear Feedback Shift Registers (NLFSRs) [21], Fibonacci or Galois LFSRs [22].



a)



b)



c)

Fig. 2. Diffie-Hellman algorithm, Elgamal variant – a) applications; b) description; c) example

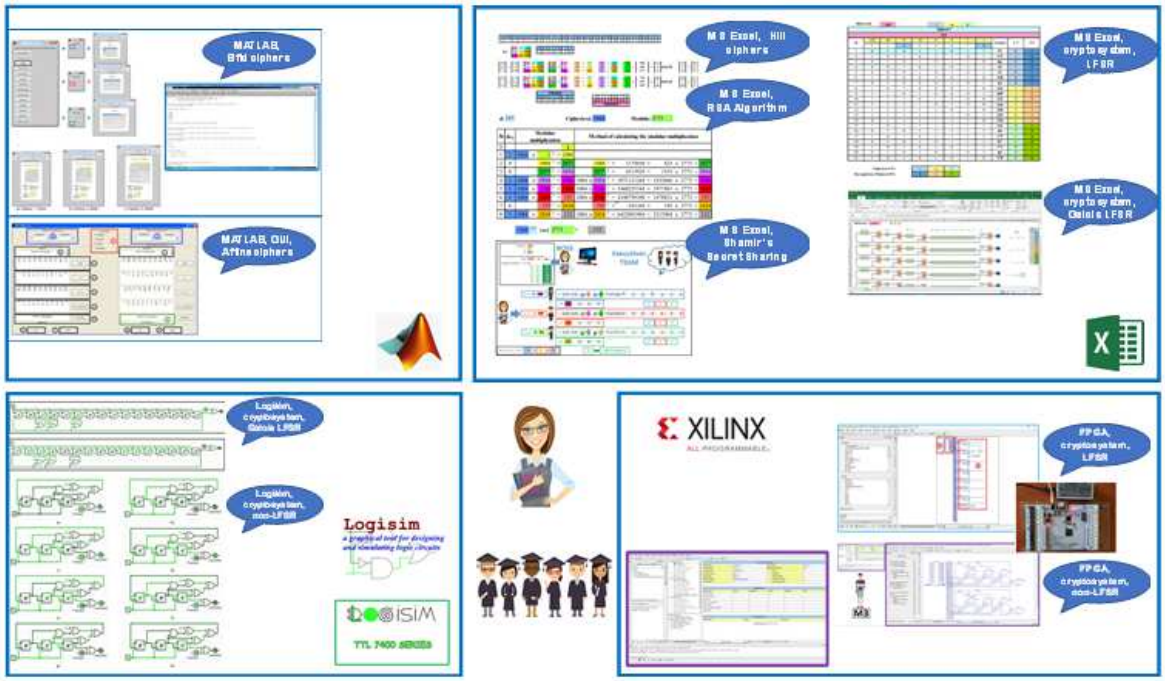


Fig. 3. Implementations in MATLAB, MS Excel, Logisim, and ISE Project Navigator (of Xilinx) of classical ciphers, cryptographic algorithms, and cryptosystems

3) Logisim [12] (for designing and simulating digital circuits) – Fig. 3 (bottom-left), where implementations of cryptosystems are given, for example, cryptosystems built on LFSRs [19, 20, 23] or NLFSRs [21], Fibonacci or Galois LFSRs [22].

4) ISE Project Navigator or ISE Design Suite 14.7 [13] for programming the devices on the lab-board based on Field Programmable Gate Arrays (FPGA), designed and used at our University [19, 20] – Fig. 3 (bottom-right), where implementations of cryptosystems are given, for example, cryptosystems built on LFSRs [19, 20, 23] or NLFSRs [21], Fibonacci or Galois LFSRs [22, 23].

Presenting some previous works of cryptographic algorithms and cryptosystems (Fig. 3) increased students' interest in the theoretical issues and stimulated them for implementing their projects. During the project implementation, students had to find a suitable solution to the problem using various software tools and present it to be evaluated by the teacher. As a result, students have gained confidence in applying what they have learned in class and putting this knowledge into practice.

During the classes (at school) the students had to develop a module in MS Excel, which allows checking whether the selected value of g is correct (Fig. 4 a) or incorrect (Fig. 4 b) as well as the formulas used (Fig. 4 c), depending on the description of the Diffie-Hellman algorithm, Elgamal variant (Fig. 2 b). The choice of the public parameter g must be according to the rule: g, an integer less than n, for each number $p \in [1; n-1]$, a power k of g exists such that $g^k = p \bmod n$.

Next, students had to create a module in MS Excel (but a possible option is also MATLAB to be used), which illustrates the encryption and decryption principles using the Diffie-Hellman algorithm, Elgamal variant, presenting the main stages and activities of the two participants in the communication process (Fig. 5). The application is based on the example presented in [6] (Fig. 2 c), namely: the public parameters $n = 11$ and $g = 7$, the private key $a = 2$ of user A, the random number $k = 1$ chosen by user B, the message for encryption $M = 13$. This example is used for tests of the reliability of the application. All the stages (activities) of users A and B are described in the application for better mastering the theory studied by students (Fig. 5). The application also contains a visualization of the exact formulas for calculating the public keys of users A and B, as well as the stages of encryption and decryption of messages. After testing the developed application using the example of Fig. 2 c, students tried different combinations of parameters n, g, a, k, such as (11,7,2,1), (23,7,5,3), (17,3,4,2), etc. formed as separate worksheets in MS Excel.

n	11
g	7

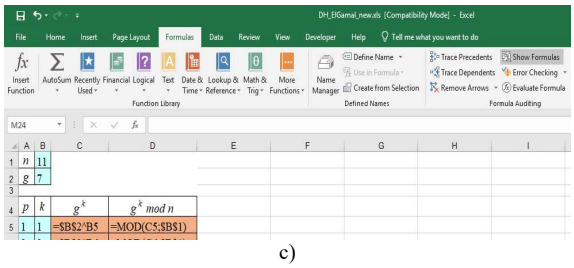
p	k	g^k	$g^k \bmod n$
1	1	7	7
2	2	49	5
3	3	343	2
4	4	2401	3
5	5	16807	10
6	6	117649	4
7	7	823543	6
8	8	5764801	9
9	9	40353607	8
10	10	282475249	1

a)

n	11
g	4

p	k	g^k	$g^k \bmod n$
1	1	4	4
2	2	16	5
3	3	64	9
4	4	256	3
5	5	1024	1
6	6	4096	4
7	7	16384	5
8	8	65536	9
9	9	262144	3
10	10	1048576	1

b)



c)

Fig. 4. MS Excel-based module for choosing the parameter g: a) correct choice; b) incorrect choice; c) formulas used in the module

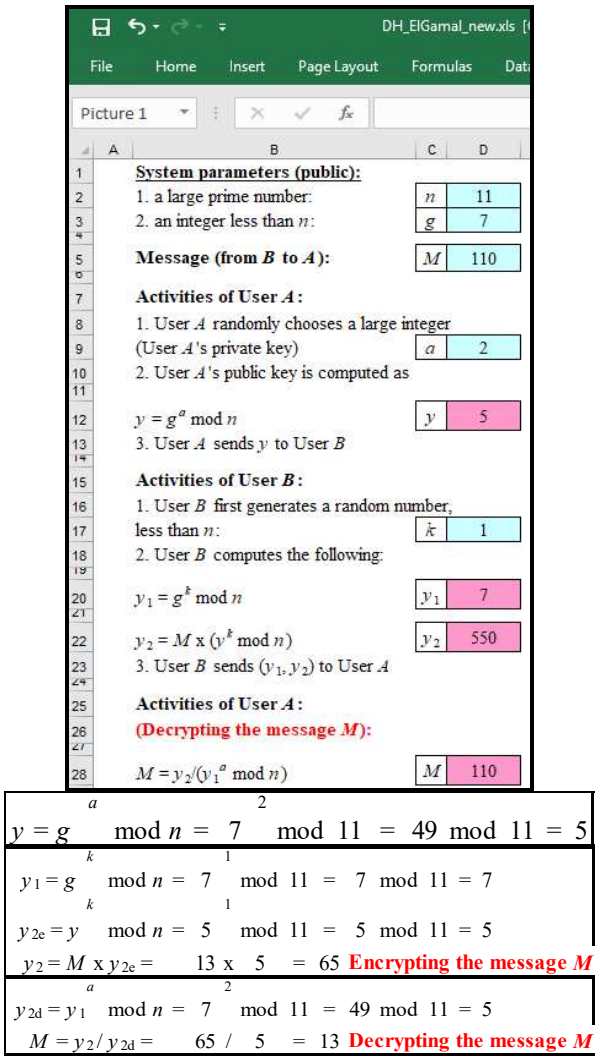


Fig. 5. MS Excel-based module for encryption and decryption using the Diffie-Hellman algorithm, Elgamal variant

Finally, a game was organized with students who could use the developed applications. They were assigned a series of ciphertexts of the type (y_1,y_2), and they had to decrypt the text. The plaintext for encryption "Diffie-Hellman" is chosen as an example. The conversion of the letters into numbers is done using ASCII code, the decimal representation of the symbols, as a result, the following sequence of numbers is obtained: 68, 105, 102, 102, 105, 101, 45, 72, 101, 108, 108, 109, 97, 110, based on the given example (Fig. 2). The following encrypted text is obtained (only the second numbers in the pairs (y_1,y_2)): 340, 525, 510, 510, 525, 505, 225, 360, 505, 540, 540, 545, 485, 550.

III. Conclusions

The paper describes results from the application of the flipped classroom and the project-based learning approaches used in the course "Telecommunication Security" studied by students in the "Internet and Mobile Communications" specialty in the seventh semester, at the University of Ruse, for teaching and learning the topic "Diffie-Hellman Algorithm, Elgamal Variant". Project-based learning develops and improves the main 21st-century skills, for example, numeracy and literacy, including ICT literacy, logical, critical, and analytical thinking, initiative, creativity, problem-solving and communication skills, etc.

References

[1] A. Silva, L. Docampo, S. Silva, M. Lorenzo-Moledo. "Challenges of the border educational centers of Portugal and Spain towards the 21st century skills", Teoria de la Educacion, Vol. 34, pp. 167 – 187, 2022, doi 10.14201/TERI.25682.

[2] B. Panapt, C. Pandit, "Project-based learning approach in under-graduate engineering course of cryptography and security in computer science", Journal of Engineering Education Transformations, Vol. 33, pp. 153 – 158, 2019, doi 10.16920/jeet/2019/v33i1/149006.

[3] A. Bicer, Y. Lee, R. Capraro, M. Capraro, L. Barroso, M. Rugh, "Examining the effects of STEM PBL on students' divergent thinking attitudes related to creative problem solving", FIE, 2019, doi 10.1109/FIE43999.2019.9028431.

[4] C.-C. Lo, M.-H. Hsieh, H.-H. Lin, H.-H. Hung, "Influences of flipped teaching in electronics courses on students' learning effectiveness and strategies", International Journal of Environmental Research and Public Health 18(18),9748, 2021.

[5] A. Borodzhieva, "Project-Based Learning for Teaching the Knapsack Problem in the Course "Telecommunication Security"". 2022 21st International Symposium INFOTEH-JAHORINA, Bosnia and Herzegovina, pp. 1-7, doi: 10.1109/INFOTEH53737.2022.9751273.

[6] B. Sklar, "Digital Communications. Fundamentals and Applications." 2nd Edition. Communications Engineering Services, California, 2001.

[7] C. Gupta, N.V.S. Reddy, "Enhancement of Security of Diffie-Hellman Key Exchange Protocol using RSA Cryptography", 2022, Journal of Physics: Conference Series, 2161(1),012014.

[8] M. Mohan, M. Kavithadevi, V. Prakash, "Improved ElGamal Cryptosystem for Secure Data Transfer in IoT Networks". Proceedings of the 4th International Conference on IoT in Social, Mobile, Analytics and Cloud, ISMAC 2020, pp. 295-302.

[9] MATLAB, https://www.mathworks.com (May 2022)

[10] Create apps with GUIs in MATLAB, https://www.mathworks.com/discovery/matlab-gui.html (May 2022).

[11] MS Excel, https://www.microsoft.com/bg-bg/microsoft-365/excel (May 2022)

[12] Logisim, www.cburch.com/logisim/ (May 2022).

[13] Xilinx, https://www.xilinx.com/content/xilinx/en/downloadNav/design-tools/v2012_4---14_7.htm (May 2022).

[14] A. Borodzhieva, "MATLAB-based software tool for implementation of bifid ciphers". CompSysTech'17, Ruse, 2017, pp. 326 – 333.

[15] A. Borodzhieva, P. Manoilov, "Training module with graphical user interface for encryption and decryption using affine ciphers applied in cryptosystems". SIITME 2014, Bucharest, Romania, pp. 281 – 286.

[16] A. Borodzhieva, "MS Excel-based application for encryption and decryption of english texts with the Hill cipher on the basis of 3×3-matrix". ET2016, Sozopol, Bulgaria, pp. 67-71.

[17] A. Borodzhieva, "MS Excel-based application for implementing the cryptographic algorithm Shamir's secret sharing". MIPRO 2020, Opatija, Croatia, Engineering Education, pp. 1611-1616, doi: 10.23919/MIPRO48935.2020.9245422.

[18] A. Borodzhieva, "Software implementation of a module for encryption and decryption using the RSA algorithm". ET2016, 2016, Sozopol, Bulgaria, pp. 63-66.

[19] A. Borodzhieva, "Modeling of cryptosystems based on linear feedback shift registers using spreadsheets". MIPRO 2019, Opatija, Croatia, Engineering Education, pp. 1713 – 1718.

[20] Borodzhieva, A., I. Stoev, V. Mutkov. FPGA implementation of cryptosystems based on linear feedback shift registers for educational purposes. 29th Annual Conference of the European Association for Education in Electrical and Information Engineering, 2019, Ruse, Bulgaria, pp. 306 – 309.

[21] A. Borodzhieva, I. Tsvetkova, S. Zaharieva, D. Dimitrov and V. Mutkov. "Active and interactive methods used in teaching and learning the topic "Cryptosystems Based on Nonlinear Feedback Shift Registers"". SIITME 2021, Timisoara, Romania, pp. 137-142, doi: 10.1109/SIITME53254.2021.9663418.

[22] A. Borodzhieva, "Computer-based education for teaching the topic "Galois linear feedback shift registers". SIITME 2020, Pitești, Romania, pp. 291-294, doi: 10.1109/SIITME50350.2020.9292268.

[23] A. Borodzhieva, "Computer-based tools applied in the course "Telecommunication Security"". eLSE 2020, Bucharest, Romania, Vol. 2, pp. 42 – 52, doi: 10.12753/2066-026X-20-091.