Complex approach in telecommunication engineering education: develop engineering skills by a team project

*Luminița Scripcariu**, and *Petre-Daniel Mătășaru*

Technical University "Gheorghe Asachi" of Iasi, Faculty of Electronics, Telecommunications and Information Technology, 11 Carol I Blvd., Iasi, Romania

Abstract. This paper provides an overview of the educational process of telecommunication engineering students by presenting the preparation of a team project focused on information security. Our educational approach combines basic knowledge such as mathematics with specialized engineering notions and various skills. The project theme is to design, implement and test an encryption algorithm. Students are provided with online courses, specific software programs and Internet access. They have to choose an encryption algorithm, to study its details and to write the script of the encryption algorithm in MATLAB program. The algorithm is implemented in C/C++ programming language and tested. Finally, a concurrent team tries to break the algorithm by finding the decryption key. It is an interactive approach which combines various education methods including gaming concepts. The covered topics provide students professional outcomes such as knowledge and use of specific mathematical tools and software environments (C/C++ programming languages, MATLAB), abilities to design, develop, implement and test software algorithms. The project also provides transversal outcomes such as ability to team work, skills of computer use and information technology and capability to take responsibilities. Creativity is also encouraged by extending the algorithm to other encryption key lengths than the usual ones.

1 Introduction

The project is proposed to students, from "Telecommunication Systems and Technologies" bachelor program, during the "Introduction to Communication" class, in order to apply the theoretical notions presented in the course unit, focused on information security and encryption algorithms.

The objective of this activity is to offer thorough knowledge of encryption techniques to the students and to develop their programming skills.

Students can choose between different encryption algorithms, both with public or private encryption key.

* Corresponding author: luminita.scripcariu@gmail.com

Usually the team is composed by three students and one of them is the team leader which coordinates all the activities of the project.

The team securely accesses bibliographical references through Moodle application, provided by the faculty servers (<http://edu.etti.tuiasi.ro>).

The basic mathematical notions about Galois Fields must be known. Students have programming skills from previous courses. Matlab operating skills are also required. The students are solving the project tasks during six hours. Finally, a student workshop is organized and each team presents the project to the others. Competitiveness is stimulated. Like in a gaming environment, a challenge is launched to the other teams, to find the secret decryption key.

In this way, the educational process has the main goal to develop different cross-disciplinary professional skills such as knowledge and use of specific mathematical tools and software environments (C/C++ programming languages, MATLAB), abilities to design, develop, implement and test software algorithms and to develop student's transversal skills like team working, creativity and sense of responsibility. Educational methods and techniques are adapted to students, with different levels of motivation and attitudes about learning and working [1].

2 Cross-disciplinary requirements

Encryption algorithms are intended to ensure information security [2]. Telecommunication engineers must have knowledge of **security techniques** used by communication systems and networks.

Different encryption algorithms can be used:

a. private-key algorithms: DES (Data Encryption Standard), TDES (Triple DES), AES (Advanced Encryption Standard) etc.

b. public-key algorithms: RSA (Rivest-Shamir-Adleman), El-Gamal etc.

The difficulty of implementing these algorithms consists in working with very large numbers and also in working with different data structures.

Understanding these algorithms is an essential requirement for the students as future specialists on telecommunication systems.

The **mathematical aspects** of the algorithm must be well known by students.

DES and TDES are binary block algorithms. Students must know Boolean algebra notions. The encryption key is a 64-bit sequence for DES and 128-bit sequence for TDES [3].

AES works on the Galois Field GF (256) with 8-bit input values, with 128, 192 or 256-bit keys [4]. In this case, the operations are made algebraically based on the Galois Field rules.

First the students read the standard and analyze the encryption algorithm, by studying all the steps.

It is important that the actual cryptography standards are freely available on the Internet [5].

Numerical data is used to exemplify the algorithm. Different input sequences are chosen and encrypted by hand in order to finally test the implemented algorithm. Numerical examples are essential for understanding how the algorithm works. In fact, it is confirmed the fact that some details are lost by reading only the theoretical description of a standard. For example, students do not always pay attention to the data type until a numerical value is required as an example.

After well-understanding the algorithm, students write the Matlab scripts of the encryption algorithm and the decryption one.

This activity requires **programming skills and knowledge of Matlab commands** [6]. This is a good opportunity for students to learn and use the Matlab tools which are required by various employers.

After writing the Matlab scripts, students test them with different input data.

This is a laborious process because different errors occur and students must solve all the problems before using the script. They must have patience and work systematically. In this time, the student working style is shaped.

The finality of the project consists in a software program, written using C/C++ language, which encrypts and decrypts a file. It is a difficult operation but working as a team is crucial and efficient. Some students could not complete this task in time without the help of the other colleagues. It is a good opportunity for each student to learn from the experience of the others.

Presenting the project is made by all the members of the team. The presentation itself is a challenge for students. Using a specific presentation program implies different competences on software operation and highlights their experience in promoting a project in front of a large audience. Communication skills are also developed by this activity.

The project requires many cross-disciplinary capabilities from mathematical, programming and technical areas, and educational methods are adapted to the students' needs [7].

3 Project Description

3.1 Project theme

The theme of the project is "Design, implement and test an encryption algorithm as Matlab scripts and as a C/C++ program". The project of a team working on AES algorithm is described as a relevant example in the following paragraphs.

3.2 Project tasks

The project tasks consist in:

- Reviewing the Galois Fields' properties.
- Studying AES standard and making a synthesis of it.
- Applying AES on numerical data as an exercise.
- Writing the Matlab scripts of AES encryption and decryption algorithms.
- Testing the Matlab scripts with numerical data.
- Implementing AES algorithms as a C/C++ programs with a friendly graphical user interface (GUI).

Each task requires special abilities and students are trained to complete these tasks as a team. Teacher is supervising the team and provides technical information at the request of students.

3.2.1 Reviewing Galois Fields properties

Galois Fields (GFs) are algebraic finite fields with internal operations of addition and multiplication [8].

Special rules must be followed in order to operate in these fields.

Students learn about Galois Fields as an introductory lecture and then they use it to implement an encryption algorithm.

Let us denote by m the number of bits used to express a symbol from GF and by $p(x)$ the m -degree primitive polynomial used to multiply numbers in GF (2^m). For example, AES algorithm uses GF (256) = {0, 1, 2 ... 255} and 8-bit values.

The elements of a GF can be expressed as decimal values, as binary sequences and as polynomials:

$$a = [a_0 \ a_1 \ a_2 \ \dots \ a_{m-1}] \quad (1)$$

$$a(x) = \sum_{i=0}^{m-1} a_i x^i \quad (2)$$

Conversion of decimal values into binary form and knowledge of Boolean algebra are prerequisites of this course unit and of this project.

The addition of two numbers from GF is made modulo-2 bit-by-bit:

$$s = a + b \Leftrightarrow s_i = a_i \oplus b_i, \text{ for } i = 0 \text{ to } m-1 \quad (3)$$

The multiplication of two elements is made using the polynomials associated to each number and the chosen primitive polynomial $p(x)$:

$$c(x) = \{a(x) \cdot b(x)\} \bmod p(x) \quad (4)$$

Numerical exercises are done by the team to become familiar to GF's algebra. Students have to pay attention to operate according to the rules specified by the GF and avoid of adding or multiplying numbers as usual decimal values. This is a good exercise of attention and concentration. It develops abstract understanding and exercise solving skills.

3.2.2 AES Synthesis

FIPS PUB 197 standard is studied by the team and the steps of the algorithm are described synthetically:

- Each data block is written as a sequence of 16, 24, 32 or 64 bytes that become the elements of the data-matrix having four rows. For example, the data matrix used by AES-128 is presented below:

$$S = \begin{bmatrix} s_{00} & s_{01} & s_{02} & s_{03} \\ s_{10} & s_{11} & s_{12} & s_{13} \\ s_{20} & s_{21} & s_{22} & s_{23} \\ s_{30} & s_{31} & s_{32} & s_{33} \end{bmatrix} \quad (5)$$

- Each byte is substituted according to the following affine transformation containing the bits from the binary form of the byte $[b_i \ b_{i+1} \ b_{i+2} \ b_{i+3} \ b_{i+4} \ b_{i+5} \ b_{i+6} \ b_{i+7}]$ and a constant byte $c = 0110.0011 = 0x.63$. This step is called *SubByte* and it is described by the following relation:

$$b'_i = b_i \oplus b_{(i+4) \bmod 8} \oplus b_{(i+5) \bmod 8} \oplus b_{(i+6) \bmod 8} \oplus b_{(i+7) \bmod 8} \oplus c_i \quad (6)$$

- Next step, called *ShiftRows*, consists of a permutation of the elements. Each row of the state-matrix is shifted with a different shift value: 0 for the first row, 1 for the second one, 2 for the third and 3 for the last:

$$S' = \begin{bmatrix} s_{00} & s_{01} & s_{02} & s_{03} \\ s_{13} & s_{10} & s_{11} & s_{12} \\ s_{22} & s_{23} & s_{20} & s_{21} \\ s_{31} & s_{32} & s_{33} & s_{30} \end{bmatrix} \quad (7)$$

- The so-called step of the algorithm *MixColumns* is a simple multiplication of each column of the data matrix with a given matrix A, according to the algebraic rules of GF.
- The final step, *AddRoundKey*, consists in adding the key matrix to the data matrix.

The algorithm has a different number of rounds (10, 12 or 14), depending on the length of the key. A key schedule algorithm is applied to generate the sub-keys for these rounds.

Numerical examples of AES algorithm are calculated by students in order to fully understand the details of the algorithm which requires in-depth mathematical knowledge.

Making calculation with numerical data is an essential way for understand the algorithm, to be aware of the type of data used for each step of the algorithm (binary, decimal, octal etc.), to be aware of the size of the data block processed by the algorithm (8-bit word, 4-by-4 matrix, 4-by-1 column vector) or of how the algorithm operates (based on bitwise logical AND, exclusive-OR, multiplication of two arrays using the rules of addition and multiplication of the Galois Field with 8-bit elements etc.).

3.2.3 Implementing AES as Matlab scripts and C/C++ programs

To accomplish the task of writing the encryption and decryption scripts in Matlab program, students must have previous knowledge of this software program widely used in engineering. Matlab scripts are written for the encryption and the decryption algorithms.

Students must use their knowledge about the syntax used to write Matlab scripts or to access the Matlab manual [6]. Graphical User Interfaces (GUIs) are designed by the students based on their knowledge of how to make a GUI in Matlab program or accessing the documentation.

Then both algorithms are implemented using the C/C++ language as two independent applications. This is a difficult task which requires advanced programming abilities, a lot of time, a systematic thinking and an efficient human resource management. Strong leadership abilities are also required for at least one member of each team.

Tests are performed by students to validate their applications.

This task develops the programming skills of students and enforces the spirit of teamwork.

3.3 Project results

The selected team implements AES in Matlab and as C/C++ programs, with some easy-to-use GUIs.

The team writes the Matlab scripts for 128, 192, 256 and 512-bit key sequences. The last specified key length is suggested by the teacher and it is presented as an extension of the classical AES algorithm, sustaining the creativity and adaptability of students to execute special tasks.

The algorithms can be tested by the team itself and other colleagues, too, in order to identify possible weaknesses or non-functional aspects of the applications.

Testing the algorithms by others is an interesting and useful exercise for all students. All of them get used with the algorithms, applying it on a particular data set. They become aware of the details of the application and therefore, some changes are made after testing it,

in order to optimize different aspects. Testing becomes an intermediary step of the project itself.

The difficulty of the project has been overcome by the team spirit and by the perseverance of the students. By doing this project, students get used to tackle complex tasks and show that they are capable of making a complex project as a team.

3.4 Project Presentation

The presentation of projects is done in a large room, in front of the audience consisting in about 60 students and two teachers. A video-projector and a computer are available to expose the prepared presentation.

The team has 15 minutes to present the project and five minutes to answer the questions from the audience. Students must have a suitable outfit and control their emotions. They must speak clearly and fluently, without reading from different other helpful materials.

The audience can address questions to the team and the answers are evaluated among other aspects of the project.

The implementation of the algorithm is the contribution of the team and it was well appreciated by the audience during presentation.

The presentation of the project is a valuable experience for the students, useful for future job interviews in which they will participate.

4 Conclusions

This paper illustrates the efficient concept of engineering education by developing cross-disciplinary team projects. We illustrate the way of making a project on an information security theme, by a team of students enrolled in the third study year of the bachelor study program "Telecommunications Systems and Technologies". Students improved their professional and transversal skills working on a complex project and the results were above expectations. Educational methods are adapted to the students with different attitudes and learning needs. We consider that the educational objectives are accomplished and all the intended skills of the students are formed by doing a complex specialized project.

References

1. R.M. Felder, R. Brent, *Understanding Students Differences*, J. of Engineering Education (JEE) **94**, 1 (2005)
2. B. Schneier, *Applied cryptography, second edition* (NY: John Wiley & Sons, Inc., 1996)
3. *** FIPS PUB 46-3 (Federal Information Processing Standards, 1999)
4. *** FIPS PUB 197 (Federal Information Processing Standards, 2001)
5. E. Barker, *NIST Special Publication 800-175B, Guideline for Using Cryptographic Standards in the Federal Government: Cryptographic Mechanism* (NIST, 2016)
6. B.D. Hahn, D.T. Valentine, *Essential MATLAB for Engineers and Scientists, 4e*, (Academic Press, 2010)
7. W.Z. Khan, S. Al Zubaidy, *Engineering design approach in Marine Engineering: A bridge between Training Need Analysis (TNA) and Engineering Education*, Intern. J. Of Engineering And Science (IJES) **5**, 3 (2016)
8. L. Scripcariu, P.D. Mătăsar, *On the Substitution Method of the AES Algorithm, Proceed. of the Intern. Symposium on Signals, Circuits and Systems, ISSCS 2013*, Iași, Romania, **1** (2013).