

Faculty: FACULTY OF TELECOMMUNICATIONS AND MANAGEMENT
Department: INFORMATION TECHNOLOGIES
Professional Field: 5.3 COMMUNICATION AND COMPUTER TECHNOLOGY
Specialty: SOFTWARE DESIGN
Educational-qualification degree: PROFESSIONAL BACHELOR

LEARNING COURSE DESCRIPTION

1. **Course title:** *FUNDAMENTALS OF CRYPTOGRAPHY*

2. **Course code:** P.17.027.1

3. **Type of the course:** *compulsory*

4. **Level:** Professional bachelor

5. **Year of study:** 2

6. **Semester:** 4

7. **Number of credits:** 4,5

8. **Name of the lecturer:** Assoc. Prof. Dr. Eng. Ivan Ivanov

9. **Course learning outcomes:**

The aim of the course is to give students basic (fundamental) knowledge in the field of cryptography in a systematized form.

Students who have completed their studies in the discipline must acquire:

Basic knowledge of the nature and specificity of cryptographic procedures and algorithms.

Practical skills for the technology of applying cryptographic algorithms at the bit level, as well as the possibilities for their implementation in various applications and end devices.

Competences: After completing the course, students must have mastered the working mechanisms and practical implementation of cryptographic algorithms.

10. **Teaching methods:**

The lectures are conducted by acquainting the students with the material provided in the curriculum. The lectures are illustrated with graphic and video material, with illustrative examples and tasks, which are presented through presentations with a multimedia projector.

The practical exercises are conducted in the laboratories of the department, equipped with modern computers and network devices, and each student works independently.

Before each practical session, students are informed about the need for preliminary training on the topic.

11. **Prerequisites:**

Knowledge acquired in the disciplines of Engineering Mathematics, Fundamentals of Security, Cyber Threats and Cyber Crises and Object Oriented Programming is essential.

12. **Course contents:**

The course examines current topics related to the history of cryptography, as well as the basic cryptographic procedures and schemes on which all modern algorithms are based. A classification of cryptographic algorithms has been made, as the more well-known in each direction have been examined - symmetric, asymmetric and streaming.

13. **Bibliography**

Basic literature:

1. Ivanov I. Fundamentals of Cryptography, VUTP Publishing House, 2021.
2. Stallings W., Cryptography and Network Security: Principles and Practice, 7th Edition, Pearson, March 5, 2016.
3. Schneier B. Applied Cryptography Protocols, Algorithms, and Source Code in C, Wiley, pp. 81-221, 2013.
4. Babash A. V., Baranova E. K. Cryptographic methods of protecting information. KNORUS. Moscow, 2016.

5. Forouzan B.A., Management of encryption keys and network security (2nd ed.), M.: NOU "Intuit", 2016.

Additional literature:

1. Ivanov I. Manual for laboratory exercises on information security and protection and administration and protection of communication and computer networks, ed. center-VU KTP, Sofia, 2013, ISBN: 978-954-9332-88-9.

2. Easttom C, Modern Cryptography: Applied Mathematics for Encryption and Information Security, McGraw-Hill Education, October 12, 2015.

3. Hoffstein J, Pipher J, Silverman J, An Introduction to Mathematical Cryptography 2nd Edition, Springer, September 11, 2014.

4. Mayvold E. Network security. National Open University "INTUIT", 2016.

5. Behrouz A.F., Mathematics of cryptography and theory of encryption (2nd ed.), M.: NOU "Intuit", 2016.

14. Assessment methods and criteria:

The evaluation of the discipline is formed through a point system, the maximum number of points that students can receive is 100 (see table 1). Knowledge, skills and competence are evaluated by conducting written control works to check the theoretical and practical assimilation of the learning material, the performance of the students during the practical exercises, as well as their ability to independently solve the tasks set in the practical exercises. The discipline ends with a written exam.

Table 1.

Number of points	Assessment According to the 6-point Scale System
0 – 20	Fail 2 (F)
20 – 39	Fail 2 (FX)
40 – 49	Satisfactory 3.00 (E)
50 – 59	Satisfactory 3.00 (D)
60 – 69	Good 4.00 (C)
70 – 84	Very good 5.00 (B)
85 – 100	Excellent 6.00 (A)

15. Language of instruction: *Bulgarian/English*