Національний технічний університет України
«КИЇВСЬКИЙ ПОЛІТЕХНІЧНИЙ ІНСТИТУТ
імені ІГОРЯ СІКОРСЬКОГО»

Computer Systems Software Department

ALGORITHMIC AND SOFTWARE METHODS OF INFORMATION PROTECTION

Working program of the academic discipline (Syllabus)

Details of the academic discipline	
Level of Higher Education	***Second (Master's)***
Field of Study	*12 Information Technologies*
Specialty	*121 Software Engineering*
Education Program	*Software Engineering of Multimedia and Information Retrieval Systems*
Type of Course	*Selective*
Mode of Studies	*full-time*
Year of studies, semester	*1st year, spring semester*
ECTS workload	*Lectures: 36 hours, laboratory classes: 18 hours, independent work: 66 hours.*
Testing and assessment	*Assessment, modular control work, calendar control*
Course Schedule	*According to the schedule for the spring semester of the current academic year (rozklad.kpi.ua)*
Language of Instruction	*English*
Course Instructors	Lecturer: *Ph.D., Associate Professor, Onai Mykola* Computer workshop and laboratory classes: *Ph.D., Associate Professor, Onai Mykola*

Outline of the Course

1. Course description, goals, objectives, and learning outcomes

The study of the discipline "Algorithmic and Software Methods of Information Protection" allows students to develop the competencies necessary for solving practical problems of professional activity related to the analysis and use of cryptographic information protection systems.

The discipline "Algorithmic and Software Methods of Information Protection" ensures the successful completion of the bachelor's qualification work and the assimilation of knowledge and the performance of individual tasks, during the continuation of postgraduate studies in various natural and scientific disciplines.

The purpose of studying the discipline "Algorithmic and Software Methods of Information Protection" is the formation of students' ability to analyze cryptographic systems; choose a cryptographic algorithm according to the formulated task; ensure the operation of modern cryptosystems; debug and develop software for cryptographic protection.

***The subject of** the discipline "Algorithmic and Software Methods of Information Protection" is methods of building information protection systems.*

After mastering the discipline "Algorithmic and Software Methods of Information Protection", the learning outcomes are:

knowledge:

- *methods of protection against unauthorized reading, control of information integrity, authentication, protection of documents and securities against forgery;*

- *methods of performing operations in a finite field of the form GF(p) and its extension GF(pm), as well as on an elliptic curve;*
- *key distribution algorithms, digital signature formation, data encryption;*
- *principles of development of symmetric and asymmetric cryptographic algorithms;*
- *methods of using modern cryptographic algorithms;*
- *peculiarities of using cryptographic algorithms built on an elliptic curve*

skill:

- *analyze the results of the work of known cryptographic protocols;*
- *evaluate the stability of cryptographic algorithms;*
- *generalize the obtained experimental results*

experience:

- *development of software tools for encryption, data decryption and creation of an electronic digital signature;*
- *creation of elliptic cryptography software;*
- *application of cryptographic standards in software development.*

The discipline "Algorithmic and Software Methods of Information Protection" strengthens the formation of PC07 and PLO10.

2. Prerequisites and post-requisites of the course (the place of the course in the structural-logical scheme of studies in accordance with educational program)

The successful study of the discipline "Algorithmic and Software Methods of Information Protection" is preceded by the study of the discipline "Algorithmic support of multimedia and information-search systems" of the bachelor's training plan in the specialty 121 Software engineering.

The theoretical knowledge and practical skills obtained as a result of mastering the discipline "Algorithmic and Software Methods of Information Protection" can be useful for the completion of the bachelor's final qualification work.

3. Content of the course

The discipline "Information Security Software" involves the study of the following topics:

Topic 1. Problems of cryptography

Topic 2. General principles of building symmetric cryptosystems

Topic 3. Modern symmetric cryptosystems

Topic 4. Elements of abstract algebra

Topic 5. Classical asymmetric ciphers

Topic 6. Cryptography on elliptic curves

Topic 7. Electronic digital signature

Modular control work

Test

4. Educational materials and resources

Basic literature:

1. *Tekhnolohii zakhystu informatsii [Elektronnyi resurs] : pidruchnyk dlia stud. spetsialnosti 122 «Kompiuterni nauky», spetsializatsii «Informatsiini tekhnolohii monitorynhu dovkillia»,*

«Heometrychne modeliuvannia v informatsiinykh systemakh» / Yu. A. Tarnavskyi; KPI im. Ihoria Sikorskoho. – Elektronni tekstovi dani (1 fail: 2,04 Mbait). – Kyiv : KPI im. Ihoria Sikorskoho, 2018. – 162 s.

2. *DSTU ISO/IEC 27001:2023 Informatsiina bezpeka, kiberbezpeka ta zakhyst konfidentsiinosti. Systemy keruvannia informatsiinoiu bezpekoiu. Vymohy (ISO/IEC 27001:2022, IDT)*
3. *DSTU 9041:2020 Informatsiini tekhnolohii. Kryptohrafichnyi zakhyst informatsii. Alhorytm shyfruvannia korotkykh povidomlen, shcho gruntuietsia na skruchenykh eliptychnykh kryvykh Edvardsa*
4. *Kiberbezpeka : suchasni tekhnolohii zakhystu. Navchalnyi posibnyk dlia studentiv vyshchykh navchalnykh zakladiv. / S. E. Ostapov, S. P. Yevseiev, O.H. Korol. – Lviv, 2020 . – 678 s*
5. *Derzhavnyi standart Ukrainy. Informatsiini tekhnolohii. Kryptohrafichnyi zakhyst informatsii. Tsyfrovyi pidpys, shcho gruntuietsia na eliptychnykh kryvykh. Formuvannia ta perevirka. DSTU 4145-2002*

Additional literature:

1. *Jean-Philippe Aumasson Serious Cryptography: A Practical Introduction to Modern Encryption, 2-nd Edition : No Starch Press, 2024*
2. *Michael E. Wihitman, Herbert J. Mattord Principles of Information Security, Sixth Edition, Kennesaw State University.*
3. *Wenbo Mao Modern Cryptography: Theory and Practice : Pearson P T R; 1st edition*
4. *Thomas R. Shemanske Modern Cryptography and Elliptic Curves: A Beginner's Guide : American Mathematical Society (July 31, 2017)*
5. *Niels Ferguson, Bruce Schneier, Tadayoshi Kohno Cryptography Engineering: Design Principles and Practical Applications Wiley*
6. *Seth James Nielson, Christopher K. Monson Practical Cryptography in Python: Learning Correct Cryptography by Example Apress; 1st ed. edition (September 27, 2019)*
7. *Lawrence C. Washington Elliptic Curves: Number Theory and Cryptography Chapman and Hall/CRC; 2nd edition*

Educational content

5. Methodology of mastering the discipline (educational component)

No.	Type of training session	Description of the training session
Topic 1. Problems of cryptography		
1	*Lecture 1. Problems of cryptography*	*Classification of cryptographic systems. Encryption key. Symmetric cryptosystem. Asymmetric cryptosystem. Differential, linear and interpolation cryptanalysis. Fields of application of cryptography. Imitation protection User identification. Password storage methods. Information integrity control. Authentication of information. Electronic digital signature.*
Topic 2. General principles of building symmetric cryptosystems		
2	*Lecture 2. General principles of building symmetric cryptosystems*	*Monoalphabetic substitution ciphers. Caesar's Cipher. Generalized Caesar Cipher. Playfire cipher. Hill's Cipher. Polyalphabetic substitution ciphers. Wigener cipher. Permutation ciphers.*

Topic 3. Modern symmetric cryptosystems		
3	*Lecture 3. The Feistel cipher*	*The Feistel cipher as a practical implementation of Shannon's ideas. Block cipher. Encryption round. Algorithm for calculating round subkeys.*
4	*Laboratory session 1*	*Develop a program in any programming language that will implement encryption and decryption of data using one of the algorithms: Caesar's cipher, Playfair's cipher, Lester Hill's cipher.*
5	*Lecture 4. Data Encryption Standard (DES)*	*NBS competition. Simplified DES. Round function. Permutation with expansion. S-matrix. Avalanche effect. Subkey generation scheme. Permutation with choice. DES operating modes. Multiple DES. Advanced DES.*
6	*Lecture 5. AES standard*	*NIST competition. Requirements for the new algorithm. Criteria for algorithm analysis. SP networks. "Square" structure. The Rijndael algorithm. Ways of presenting a block of plaintext and a key. Rijndael encryption steps. Swap bytes and represent data as elements of a GF(28) field. Mathematical component of column shuffling operation. Matrix representation of the column shuffling step. Formation of a round key from the main one. Peculiarities of construction of the decryption algorithm. Decryption algorithm with direct order of transformations.*
7	*Laboratory lesson 2*	*Develop a program in any programming language that will implement encryption and decryption of data using one of the algorithms: permutation cipher, Wigener cipher.*
8	*Lecture 6. The International Data Encryption Algorithm (IDEA) and the Blowfish cipher*	*Difference from Feistel's classic structure. MA structure. Features of generating subkeys in IDEA. The relationship between decryption subkeys and encryption subkeys. Basic mathematical operations in IDEA. Blowfish algorithm. Selection of the initial value of the P-array and the table of substitutions. Comparison of IDEA and Blowfish algorithms with other symmetric cryptosystems.*
9	*Lecture 7. The RC5 cipher and general approaches to building block and stream ciphers*	*Parameters for defining the RC5 algorithm. Ways of writing multibyte words. Features of the formation of round subkeys. RC5 operating modes. Stream encryption systems. Synchronous systems and systems with self-synchronization. Shift registers with linear feedback. A primitive polynomial. Examples of the use of stream ciphers in communication systems.*
10	*Laboratory lesson 3*	*Develop a program in any programming language that will implement data encryption and decryption using one of the following algorithms: triple DES (implement three modifications), extended DES (implement three modifications), International Data Encryption Algorithm (IDEA)*
15	*Modular control work. Part 1*	
Topic 4. Elements of abstract algebra		
11	*Lecture 8. Arithmetic in classes of modulo*	*Basic algebraic structures. Groupoid. Half group. Monoid. Group. Additive and multiplicative groups. Element order. The creative element of the group. Cyclic group. Algebraic structure of a ring. Concepts of*

	remainders, Fermat's and Euler's Theorem	*divisibility and comparability by module. Divisor of zero. Congruence class. Subgroup. Lagrange's theorem. Canonical expansion of a number. Euler's function. The system of remainders is given. Euler's theorem. Fermat's theorem as a partial case of Euler's theorem. Primitive or primitive roots. Methods of finding primordial roots.*
12	*Laboratory session 4*	*Develop a program in any programming language that will implement encryption and decryption of data using one of the algorithms: RC5 cipher (use parameter values not less than 32/12/8), Rijndael cipher*
13	*Lecture 9. Algorithms for checking numbers for simplicity and arithmetic of long numbers*	*Tests of numbers for simplicity. A test using a full sweep. Luke-Lehmer test for Mersenne numbers. Fermat's test. Arithmetic of long integers. Karatsuba Multiplication. FFT multiplication. Peculiarities of performing the operation of finding the remainder modulo for long integers.*
Topic 5. Classical asymmetric ciphers		
14	*Lecture 10. Generation of random prime numbers and principles of construction of cryptosystems with a public key*	*Miller-Rabin test. Solovei-Strassen test. AKS test. One-sided function. Key distribution protocols.*
16	*Lecture 11. Key exchange according to the Diffie-Hellman scheme, the RSA algorithm and methods of number factorization*	*The main mathematical operation in the Diffie-Hellman scheme. Connection of the discrete logarithm problem with the Diffie-Hellman algorithm. Generalization of the Diffie-Hellman algorithm. Algorithm for creating RSA public and secret keys. Transmission of an encrypted message using the RSA algorithm. Connection of the RSA algorithm with the factorization problem. Selection of RSA algorithm parameters. Factorization of integers. Sorting out divisors. Pollard's ρ-method. Pollard-Strassen algorithm.*
17	*Laboratory lesson 5*	*Develop a program in any programming language that will implement data encryption and decryption using one of the algorithms or perform specified mathematical operations in finite algebraic structures: RSA encryption algorithm, RSA digital signature algorithm*
18	*Lecture 12. El-Gamal scheme and methods of finding a discrete logarithm*	*Selection of El-Gamal scheme keys. Open and secret parameters of the El-Gamal scheme. Encryption and decryption algorithm according to the El-Gamal method. Element index by module. Index existence condition. One-sided function. Discrete logarithmization. Shanks method.*
Topic 6. Cryptography on elliptic curves		
19	*Lecture 13. Definition of the elliptic curve concept*	*An elliptic curve in Weierstrass form. Elementary operations on points of an elliptic curve. Projective coordinate system. Singular elliptic curves.*
20	*Laboratory lesson 6*	*Develop a program in any programming language that will implement data encryption and decryption using one of the algorithms or perform given mathematical operations in finite algebraic structures: El-Gamal encryption algorithm, El-Gamal digital signature algorithm, algorithm for finding the inverse element of the GF field (pm) in polynomial representation, Shanks method and matching method*

21	*Lecture 14. Elliptic curves over finite fields GF(p) and GF(p^m)*	*Varieties of Galois fields. Multiplicative group of a finite field. The order of the multiplicative group of the remainder ring. Finding the multiplicative inverse element in the field GF(p). Peculiarities of performing operations on the elements of the field GF(p^m). Supersingular and non-supersingular elliptic curves. Elliptic curve point group.*
22	*Lecture 15. Elliptical analogue of key exchange according to the Diffie-Hellman scheme*	*The main mathematical operation in the Diffie-Hellman scheme on an elliptic curve. Multiplying a point on an elliptic curve by a number. Connection of the discrete logarithm problem on an elliptic curve with the Diffie-Hellman algorithm. Generalization of the Diffie-Hellman algorithm in elliptic cryptography.*
Topic 7. Electronic digital signature		
2 3	*Lecture 16. Digital signature standard (DSS), RSA algorithm and El-Gamal scheme in digital signature mode*	*Recommended prime number generation algorithms for DSA. Using DES in the DSA algorithm. Basic parameters of the digital signature scheme. A system for checking the implementation of the algorithm for compliance with the standard. Peculiarities of using the RSA algorithm for forming a digital signature. The algorithm for forming a digital signature using the El-Gamal scheme. Digital signature verification.*
2 4	*Lecture 17. Elliptical algorithms for forming an electronic digital signature*	*DSA algorithm on an elliptic curve. Features of ECDSA key generation. Digital signature calculation and verification algorithm. Elliptic curve requirements used in ECDSA algorithms. Elliptical analogues of RSA and El-Gamal algorithms in digital signature mode.*
2 5	*Laboratory session 7*	*Develop a program in any programming language that will implement encryption and decryption of data or creation of an electronic digital signature using one of the algorithms: ECDSA, EdDSA*
2 6	*Laboratory session 8*	*Develop a program in any programming language that will implement encryption and decryption of data or creation of an electronic digital signature using one of the algorithms: ECMQV, ECQV*
27	*Modular control work. Part 2*	

6. Independent work of a student/graduate student

The discipline "Algorithmic and Software Methods of Information Protection" is based on independent preparation for classroom classes on theoretical and practical topics.

No. z/p	*The name of the topic submitted for independent processing*	*Number of hours*	*literature*
1	*Preparation for lectures*	*16*	*1-4*
2	*Preparation for a computer workshop*	*27*	*1-4*
3	*Preparation for modular control work. Part 1*	*9*	*1-4*
4	*Preparation for modular control work. Part 2*	*9*	*1-4*

5	*Preparation for the test*	*5*	*1-4*

Policy and Assessment

7. Policy of academic discipline (educational component)

Attending classes. *Absence from a classroom session does not involve the calculation of penalty points, since the student's final rating score is formed solely on the basis of the evaluation of study results. At the same time, discussion of the results of the thematic tasks, as well as presentation / public speaking and participation in discussions and additions at seminars will be evaluated during classroom classes. In order to actively participate in the work of the seminar, the student prepares for a specific seminar class in literature as recommended by the teacher. Participation in the work of the seminar also involves the preparation of reports and co-reports within all classes.*

Missed evaluation control measures. *Every student has the right to make up lessons missed for a valid reason (hospital, mobility, etc.) at the expense of independent work. More details at the link: https://kpi.ua/files/n3277.pdf .*

The procedure for contesting the results of assessment control measures. *A student may raise any issue relating to the assessment procedure and expect it to be dealt with in accordance with pre-defined procedures. Students have the right to challenge the results of control measures with arguments, explaining which criteria they disagree with according to the evaluation. Calendar control is carried out in order to improve the quality of students' education and monitor the student's fulfillment of the syllabus requirements.*

Academic integrity. *The policy and principles of academic integrity are defined in Chapter 3 of the Code of Honor of the National Technical University of Ukraine "Igor Sikorsky Kyiv Polytechnic Institute". More details: https://kpi.ua/code .*

Norms of ethical behavior. *Standards of ethical behavior of students and employees are defined in Chapter 2 of the Code of Honor of the National Technical University of Ukraine "Igor Sikorsky Kyiv Polytechnic Institute". More details: https://kpi.ua/code .*

Inclusive education. *The acquisition of knowledge and skills in the course of studying the discipline "Research activity in computer engineering" can be accessible to most people with special educational needs, except for students with serious visual impairments that do not allow them to perform tasks with the help of personal computers, laptops and/or other technical means.*

Studying in a foreign language. *In the course of the tasks, students may be recommended to refer to English-language sources. Assigning incentive and penalty points According to the Regulation on the system of evaluation of learning results, the sum of all incentive points cannot exceed 10% of the rating scale.*

All students must attend lectures and practical classes, where you need to actively work on learning the learning material. For objective reasons (for example - illness, international internship), training can take place in an online form individually upon agreement with the head of the course.

Deadlines and Rescheduling Policy:

Works that are submitted late without good reason will be assigned a lower grade. Rearranging modules takes place with the permission of the dean's office if there are good reasons (for example, sick leave).

Policy on academic integrity *:*

All written works are checked for plagiarism and accepted for defense with correct textual borrowings of no more than 20%. Write-offs during control work are prohibited (including using mobile devices).

8. Types of control and rating system of assessment of learning outcomes

During the semester, students perform 8 laboratory classes. The maximum number of points for each laboratory session: 6 points.

Points are awarded for:
- quality of laboratory work: 0-2 points;
- answer to theoretical questions during the defense of laboratory work: 0-2 points;
- timely presentation of work for defense: 0-2 points.

Performance evaluation criteria:
2 points – the work is done qualitatively, in full;
1 point - the work is completed in full, but contains minor errors;
0 points – the work is incomplete or contains significant errors.

Answer evaluation criteria:
2 points – the answer is complete, well-argued;
1 point – the answer is generally correct, but has flaws or minor errors;
0 points - there is no answer or the answer is incorrect.

Criteria for evaluating the timeliness of work submission for defense:
2 points – the work is presented for defense no later than the specified deadline;
0 points – the work is submitted for defense later than the specified deadline.

The maximum number of points for performing and defending laboratory work:
6 points × 8 lab. = 48 points.

*The assignment for **the modular test** consists of 3 questions - 2 theoretical and 1 practical. The answer to each theory question is worth 15 points, and the answer to a practical question is worth 20 points.*

Evaluation criteria for each theoretical test question:
14-15 points – the answer is correct, complete, well-argued;
11-13 points – the answer is correct, detailed, but not very well argued;
8-10 points - in general, the answer is correct, but has flaws;
5-7 points – there are minor errors in the answer;
1-4 points – there are significant errors in the answer;
0 points - there is no answer or the answer is incorrect.

Evaluation criteria for the practical test question:
19-22 points – the answer is correct, the calculations are completed in full;
14-18 points - the answer is correct, but not very well supported by calculations;
9-13 points - in general, the answer is correct, but has flaws;
5-8 points – there are minor errors in the answer;
1-4 points – there are significant errors in the answer;
0 points - there is no answer or the answer is incorrect.

The maximum number of points for a modular control work:
15 points × 2 theoretical questions + 22 points × 1 practical question = 52 points.

The rating scale for the discipline is equal to:
$R_c = R_{com.practice} + R_{interview} + R_{MKR} = 48$ points + 52 points = 100 points.

Calendar control: is carried out twice a semester as a monitoring of the current state of fulfillment of the syllabus requirements.
At the first certification (7th week), the student receives "passed" if his current rating is at least 50% of the maximum number of points (20 points) that the student can receive before the first certification.
At the second certification (13th week), the student receives "passed" if his current rating is at least 50% of the maximum number of points (35 points) that the student can receive before the second certification.

*Semester control: **assessment***

Conditions for admission to semester control:
With a semester rating (R_C) of at least 60 points and the enrollment of all computer practical work, the graduate student receives credit "automatically" according to the table (Table of correspondence of rating points to grades on the university scale). Otherwise, he has to complete the credit control work.

Completion and protection of a computer workshop is a necessary condition for admission to the performance of credit control work.

A graduate student can try to improve his grade by writing a graded test, and his semester marks will be canceled ("hard" grading system).

The composition and evaluation criteria of the assessment test:

***The test task** consists of 4 questions - 2 theoretical and 2 practical. The answer to each theoretical and practical question is evaluated by 25 points.*

Evaluation criteria for each theoretical test question:
24-25 points – the answer is correct, complete, well-argued;
21-23 points – the answer is correct, detailed, but not very well argued;
17-20 points - in general, the answer is correct, but has flaws;
12-16 points – there are minor errors in the answer;
1-11 points – there are significant errors in the answer;
0 points - there is no answer or the answer is incorrect.

Evaluation criteria for the practical test question:
24-25 points – the answer is correct, the calculations are completed in full;
21-23 points - the answer is correct, but not very well supported by calculations;
17-20 points - in general, the answer is correct, but has flaws;
12-16 points – there are minor errors in the answer;
1-11 points – there are significant errors in the answer;
0 points - there is no answer or the answer is incorrect.

The maximum number of points for a modular control work:
25 points × 2 theoretical questions + 25 points × 2 practical questions = 100 points.

Table of correspondence of rating points to grades on the university scale :

Scores	*Rating*
100-95	Perfectly
94-85	Very good
84-75	Fine
74-65	Satisfactorily
64-60	Enough
Less than 60	Unsatisfactorily
Admission conditions not met	Not allowed

9. Additional information on the discipline (educational component)

The list of questions submitted for semester control.

Work program of the academic discipline (syllabus):

Is designed by Ph.D., Assoc. Prof., Onai M.V.

Adopted by Computer Systems Software Department (protocol № 12, 11 February 2026)

Approved by the Methodical commission of the Faculty of Applied Mathematics (protocol № 7, 23 February 2026)