Syllabus
Course Program

Fundamentals of cryptology

Specialty
113 Applied mathematics

Institute
Educational and Scientific Institute of Computer Science and Information Technology

Educational program
Intelligent Data Analysis

Department
Cybersecurity

Level of education
Bachelor's level

Course type
Special (professional), Selective

Semester
5

Language of instruction
Ukrainian

Lecturers and course developers

Oleksandr MILOV

oleksandr.milov@khpi.edu.ua
Doctor of technical sciences, professor of the cyber security department of National Technical University "Kharkiv Polytechnic Institute".

Author of more than 200 scientific and educational and methodological works. Academic supervisor for protected candidate theses, guarantor of the educational and professional program of the second (master's) level of higher education. Leading lecturer in the disciplines: "Mathematical foundations of cryptology and cryptanalysis", "Data structures", "Industrial and office espionage", "Digital forensics", for undergraduate and graduate students, Section "Methodology of scientific and pedagogical activity in the sciences of cyber protection" for postgraduate students.

More about the lecturer on the department's website

General information

Summary

The discipline “Fundamentals of Cryptology” is an elective discipline. The study of the discipline gives an idea of the basic mathematical methods and approaches used to ensure cryptographic protection of information in the process of storing and transmitting information represented in binary codes. The discipline is devoted to the study of the mathematical foundations of cryptology and cryptographic analysis applied to the protection of information in information systems. The discipline reveals the concepts of ciphers, symmetric and asymmetric cryptography, electronic signature, hashing and other mathematical objects of cryptography. Relevant cryptographic standards used today in information security in Ukraine and abroad are studied.

Course objectives and goals

Acquaintance with the mathematical foundations of cryptology; acquisition of skills in the practical use, formulation and solution of information encryption problems; understanding the essence of information

processes in cryptographic systems; use of computers to solve encryption and decryption problems; development and use of mathematical and computational models of information encryption processes, their optimization and development of areas for improvement.

Format of classes

Lectures, laboratory classes, calculation tasks, consultations. Final control – exam.

Competencies

GC 1. Ability to learn and master modern knowledge.
GC 2. Ability to apply knowledge in practical situations.
GC 5. Ability to conduct research at the appropriate level.
GC 7. Ability to search, process and analyze information from various sources.
GC 8. Knowledge and understanding of the subject area and understanding of professional activities.
GC 10. Skills in the use of information and communication technologies.
SC 1. Ability to use and adapt mathematical theories, methods and techniques to prove mathematical statements and theorems.
SC 2. Ability to perform tasks formulated in mathematical form.
SC 3. Ability to select and apply mathematical methods for solving applied problems, modeling, analysis, design, management, forecasting, decision-making.
SC 5. Ability to develop algorithms and data structures, software tools and program documentation.
SC 6. Ability to design databases, information systems and resources.
SC 7. Ability to solve professional problems with the help of computer equipment, computer networks and the Internet, in the environment of modern operating systems, using standard office applications.
SC 14. Ability to understand the task formulated in the language of a particular subject area, to search and collect the necessary initial data.
SC 18. Ability to select and apply mathematical models and methods for statistical and intellectual analysis of data under conditions of uncertainty.

Learning outcomes

LO 1. Demonstrate knowledge and understanding of the basic concepts, principles, theories of applied mathematics and apply them in practice.
LO 6. To master the basic methods of developing discrete and continuous mathematical models of objects and processes, analytical study of these models for the existence and uniqueness of their solution.
LO 8. Combine methods of mathematical and computer modeling with informal expert analysis procedures to find optimal solutions.
LO 10. To have methods for choosing rational methods and algorithms for solving mathematical problems of optimization, operations research, optimal management and decision-making, data analysis.
LO 13. To use specialized software products and software systems of computer mathematics in practical work.
LO 14. Demonstrate the ability to self-learn and continue professional development.
LO 24. Be able to apply existing and develop new algorithms and software tools for processing measurement and observation data, texts, signals and images.

Student workload

The total volume of the course is 120 hours (4 ECTS credits): lectures - 30 hours, laboratory classes - 30 hours, self-study - 60 hours.

Course prerequisites

“Mathematical Analysis, Linear Algebra, Probability Theory, Discrete Structures and Data Structures, Algorithmization and Programming.

Features of the course, teaching and learning methods, and technologies

In the course of teaching the discipline, the teacher uses explanatory-illustrative (informational-receptive) and reproductive teaching methods. Presentations, conversations, and master classes are used

as teaching methods aimed at activating and stimulating the educational and cognitive activities of applicants.

Program of the course

Topics of the lectures

Topic 1. Intro. The goals of the primary discipline “Foundations of cryptology”.
The place of discipline in the initial process. Structure, instead of a thematic plan for the development of discipline; elementary-methodical literature. Peculiarities of discipline; forms of control, know, and become a student. Directly scientific research work of students.
Topic 2. Basic concepts of cryptology.
Basic concepts of cryptology and cryptanalysis: cryptographic transformation of information, director and content of information, communication channel, unlock messages, cryptographic key, encryption and decryption processes, cryptogram, cryptographic system, the enemy of this attack. Methods of cryptographic information security and the role of cryptography in secure information security. The main tasks of cryptography: ensuring the established mode of access to information, ensuring the integrity of information, authenticating the author of the message.
Topic 3. Modular arithmetic.
Arithmetic of whole numbers. Multiplicity of integers: binary operations, division of integers, two divisions, graph equal to a subdivision. The theory of subdivision. Authority. All accomplices. The biggest sleeper. Euclid's algorithm. Extensions of the Euclidean algorithm. Linear diophantine equals. Partial decision. Secret decisions. Arithmetic is modular. Modulo operations.
Wash system: Zn. Porivnyannya. Vidrahuvan system. Round robin system.
Operations in Zn. Authority. Inversions. Additive inversion. Multiplicative inversion.
Added and multiplied table. Different multiplicities for adding and multiplying.
Topic 4. Matrices.
Viznachennya. Operations and care. Jealousy. Folded and taken out. Multiplying. Scalar multiplication. Determinant. Inversions. Additive inversion. Multiplicative inversion. Matrixes are restored.
Porivnyannya. Linear alignment. Linear equalization with one unknown thing to take revenge. A system of linear levels to prevent leveling.
Topic 5. Simple ciphers.
Categories of simple ciphers. Substitution ciphers. Monoalphabetic ciphers. Additive cipher. Cipher zsuwu. Caesar's cipher. Multiplicative ciphers. Monoalphabetic substitution cipher. Rich alphabetic ciphers. Autokey cipher. Playfair cipher. Vigenère cipher. Hill cipher.
Disposable notepad. Rotary cipher. Enigma machine. The code book is the proof of ciphers.
Shifri permutations. Cipher permutations without a vikoristanny key. Key cipher permutations. Combination of two approaches. Keys. Vikoristannya matrix. Cipher with double rearrangement.
Topic 6. Algebraic structures.
Groupy. Field. GF(2n) fields. Polynomials Operations. Module. Added. Multiplying. Multiplying what vikorist's computer. Vikoristannya generator. Inversions. Additive inversions. Multiplicative inversions. Added and updated. Multiplication and division.
Topic 7. Current block ciphers.
Substitution or transposition. Block ciphers as group mathematical permutations. Multi-size key ciphers. Private key cipher size. Cipher without a key.
Components of a daily block cipher. S-boxes. Cyclic sound. Replacement. Rozbittja i ob'edannaya. Warehouse ciphers. Rosing and mixing. Roundy. Two classes of warehouse ciphers. Merezh Feistel.
Topic 8. DES.
Zagalni position. Structure of DES. Corner and tail rearrangements. Roundy. DES function. Key generation. View of the battles of re-verification. Move to the left. Rearrangement of the squeeze. DES analysis. S-boxes. P-blocks. Number of rounds. Weaknesses of DES. Weakness in the encryption key. Bagatorazov zastosuvannya DES. Dvorazovy DES. Triazovy DES. Triple DES with two keys. Triple DES with three keys.
Topic 9. Code standard according to GOST 28147-89.
The principles behind the encryption algorithm. The main cycle and basic cycles of cryptotransformation according to GOST 28147-89. Modes and schemes of encryption modes according to GOST 28147-89.
Topic 10. AES cipher.

Criteria. Safety Vartist. Implementation. Roundy. One data. Bit. Byte. Word. Block. Matrix of positions. Structure of the skin round. Substitution. SubBytes. InvSubBytes. Transformation of the GF field. Nonlinearity. Rearrangement. ShiftRows. InvShiftRows. Mixed up. MixColumns. InvMixColumns. Adding keys. AddRoundKey. Key expansion in AES-128. RotWord. SubWord. RoundConstants. Algorithm. Key extension in AES-192 and AES-256. Key extension analysis.

Topic 11. Code "Kalina -256".

Structure of the encryption algorithm. Modes and schemes of encryption modes for "Kalina -256". Indicators of safety and efficiency. Vartist. Implementation. Roundy.

Topic 12. Simple numbers.

Definition. Mutually prime numbers. Number of prime numbers. The number of prime numbers. The number of prime numbers smaller than n. Check for a prime number. Sieve of Eratosthenes. Euler's phi function. Fermat's Little Theorem. The first version. The second version. Appendices. Euler's theorem. The first version. The second version. Appendices. Generation of prime numbers. Prime Mersenne numbers. Prime Fermat numbers. Testing the simplicity of numbers. Deterministic algorithms. Divisibility theory algorithm. AKS algorithm. Probabilistic algorithms. Fermat's test. The square root test. Miller-Rabin test. Initialization. Recommended number simplicity tests. Factoring. Basic theorem of arithmetic. The greatest common denominator. Least common multiple. Methods of factoring. Distribution verification method. Fermat's method. Pollard's method. Rho - Pollard's method.

More effective methods. Quadratic sieve. Sieve field of numbers. Other problems. The Chinese Remainder Theorem.

Topic 13. Quadratic comparison with the module.

Quadratic comparison with the modulus in the form of a prime number. Quadratic subtractions and non-subtractions. Euler's criterion. The solution of the quadratic comparison with the modulus in the form of a prime number. Quadratic comparison by composite modulus. Complexity.

Exponentiation and logarithms. Quick promotion. Logarithm. Complete search. Discrete logarithm. Solving the modular logarithm using discrete logarithms.

Topic 14. Cryptographic hash functions.

Integrity of the message. Hashing functions and data integrity. Requirements for hash functions. Oracle random model. Iterative hash function (Merkel-Damgard scheme). Message Digest (MD). Secure Hash Algorithm (SHA).

Hash functions based on block ciphers (Rabin scheme, Miyaguchi-Prenel scheme. SHA-512. Whirlpool. "Kupina-256" hash algorithm.

Topic 15. Cryptographic system RSA.

Introduction. Keys. General idea. Original text / encrypted text. Encryption / decryption. The need for both cryptosystems. "Loophole" in the unilateral function. Functions.

Backpack cryptosystem. Definition. Tuple superincrement. Secret communication with the use of a knapsack. Key generation. Encryption. Decryption. Loophole. RSA cryptographic system. Introduction. Procedure. Two algebraic structures. Key generation. Encryption. Deciphering. Some trivial examples.

Topic 16. Cryptosystems of Rabin and El-Gamal. Diffie-Hellman algorithm.

Procedure. Key generation. Encryption. Deciphering. The security of Rabin's cryptographic system. The cryptographic system of El-Gamal. Procedure. Key generation. Encryption. Deciphering. Security analysis of the El-Gamal cryptosystem. Small module attacks. Attack of knowledge of the source text. Diffie-Hellman algorithm.

Topic 17. Cryptosystems based on the elliptic curve method.

The equation of the elliptic curve. Singular and non-singular curves. Operations with points. The use of elliptic curves in cryptography. Elliptic curves in real numbers. Abelian group. Group and field. Elliptic curves in GF(p). Finding the inversion. Finding points on a curve. Addition of two points. Multiplying a point by a constant. Elliptic curves in GF. Elliptic curve cryptography modeling the El-Gamal cryptosystem. Generation of public and private keys. Encryption. Deciphering. Comparison. Safety of the elliptic curve method. Module size.

Topic 18. Digital signature.

Digital signature concept. Digital signature process. Security services provided with a digital signature. Digital signature attacks. Digital signature schemes (RSA, El-Gamal, Shnora, DSS, elliptic curve). Digital signature programs.

Topic 19. Pseudorandom numbers in cryptography.

Advantages and prospects of using stream encryption systems. Use of random numbers (randomness, unpredictability). Sources of random numbers. Pseudorandom number generators: round-robin

encryption, post-exit feedback mode, ANSI X9.17 pseudorandom number generator, BBS generator, linear congruent method, delayed Fibonacci method. Checking the quality of the pseudorandom number generator. Sequences of maximum length. Analysis of pseudorandom sequences.
Topic 20. Cryptoanalysis.
Kerckhoffs principles. Cryptoanalysis. Common cryptanalysis methods: brute force, space-time trade-offs, rainbow tables, slide attacks, cryptanalysis of hash functions, cryptanalysis of random number generators. Linear cryptanalysis. General overview. Matsui's algorithms. Linear expressions for S-boxes. Matsui's Lemma on Accumulation. Easy1 cipher Linear expressions and key recovery. Linear DES cryptanalysis. Multiple linear approximations. Finding linear expressions. Linear cryptanalysis code. Differential cryptanalysis. General overview. Marking. S-Box differentials. A combination of S-Box characteristics. Output of the key. Differential cryptanalysis code. Differential cryptanalysis of Feistel ciphers. Differential linear cryptanalysis. Conditional characteristics. Differentials of higher order. Truncated differentials. Differentials are impossible. Boomerang attack. Interpolation attack. Linked Key Attack.

Topics of the workshops

Not provided for in the curriculum.

Topics of the laboratory classes

Topic 1. Acquaintance with the envelope of performing laboratory work in cryptology. Information preparation tools for laboratory work.
Topic 2. Research of modern block symmetric ciphers and encryption modes.
Topic 3. Encryption and decryption in substitution and permutation ciphers. Encryption and decryption in Enigma rotary machines.
Topic 4. Research of modern block symmetric ciphers and encryption modes. Study of modern asymmetric encryption cryptosystems.
Topic 5. Performing cryptographic transformations in DES. Key generation in DES.
Topic 6. Performing cryptographic transformations in AES. Key generation in AES.
Topic 7. Generation and research of hash functions.
Topic 8. Generation of keys in the RSA system. Encryption and decryption. Use and study of Rabin, El-Gamal and Diffie-Hellman algorithm cryptosystems.

Self-study

A student's independent work is one of the forms of organization of learning, the main form of mastering educational material in free time from classroom training. During independent work, students study lecture material, do individual homework, prepare for tests, tests and exams. Students are also recommended additional materials (videos, articles) for self-study and analysis.

Non-formal education

Within the framework of non-formal education, according to the relevant Regulation (http://surl.li/pxssv), the educational component or its individual topics may be taken into account in the case of independent completion of professional courses/trainings, civic education, online education, vocational training, etc.
Subjects are not considered for this component in case of successful completion of the courses.

Course materials and recommended reading

References

1. Yevseev S.P. Cybersecurity: Cryptography with Python: a tutorial. - Lviv "New World-2000", 2021. - 120 p.
https://drive.google.com/drive/u/1/folders/1wOTN8N-GBGO06AnvjQHU1SdBl3xCaUju
2. Yevseev S.P. Cybersecurity: Laboratory workshop on the basics of cryptographic protection. - Lviv "New World-2000", 2020. - 241 p.
https://drive.google.com/drive/u/1/folders/1wOTN8N-GBGO06AnvjQHU1SdBl3xCaUju

3. Yevseev S.P. Cyber security: modern protection technologies. / Yevseev S. P., Ostapov S. E., Korol O. G. // Study guide for students of higher educational institutions. Lviv: "New World-2000", 2019. - 678 p. http://ns2000.com.ua/wp-content/uploads/2019/11/Kiberbezpeka-suchasni-tekhnolohii-zakhystu.pdf.
4. Information protection technologies./ S. E. Ostapov, S. P. Yevseev, O. G. Korol. – Chernivtsi: Chernivtsi National University, 2013. – 471 p.
5. Yevseev S.P. Cyber security: basics of coding and cryptography/ S.P. Yevseev, O.V. Milov, S.E. Ostapov, O.V. Severinov. - Kharkiv: Ed. "New World-2000", 2023. - 657 p. https://drive.google.com/drive/u/1/folders/1wOTN8N-GBGO06AnvjQHU1SdBl3xCaUju.

Additional references

6. Yevseev S.P. Cyber security: Laboratory workshop on the basics of cryptographic protection. - Lviv "New World-2000", 2020. - 241 p. https://drive.google.com/drive/u/1/folders/1wOTN8N-GBGO06AnvjQHU1SdBl3xCaUju
7. Bobalo Y. Ya., Gorbaty I. V. (eds.) Information security. Study guide. – Lviv: Publishing House of Lviv Polytechnic, 2019. – 580 p. - ISBN 978-966-941-339-0 http://pdf.lib.vntu.edu.ua/books/2020/Bobalo_2019_580sec.pdf
8. Synergy of building cybersecurity systems: monograph / S. Yevseyev, V. Ponomarenko, O. Laptiev, O. Milov and others. - Kharkiv: PC TECHNOLOGY CENTER, 2021. - 188 p. https://drive.google.com/drive/u/1/folders/1wOTN8N-GBGO06AnvjQHU1SdBl3xCaUju
9. Models of socio-cyber-physical systems security: monograph / S. Yevseiev, Yu. Khokhlachova, S. Ostapov, O. Laptiev and others. - Kharkiv: PC TECHNOLOGY CENTER, 2023. - 168 p. https://drive.google.com/drive/u/1/folders/1wOTN8N-GBGO06AnvjQHU1SdBl3xCaUju
10. Modeling of security systems for critical infrastructure facilities: monograph / S. Yevseiev, R. Hryshchuk, K. Molodetska, M. Nazarkevych and others. - Kharkiv: PC TECHNOLOGY CENTER, 2022. - 196 p. https://drive.google.com/drive/u/1/folders/1wOTN8N-GBGO06AnvjQHU1SdBl3xCaUju.

Assessment and grading

Criteria for assessment of student performance, and the final score structure

Points are awarded according to the following ratio:
- laboratory work: 40% of the semester grade;
- independent work: 10% of the semester grade;
- control work: 10% of the semester grade;
- exam: 40% of the semester grade.

Grading scale

Total points	National	ECTS
90–100	Excellent	A
82–89	Good	B
75–81	Good	C
64–74	Satisfactory	D
60–63	Satisfactory	E
35–59	Unsatisfactory (requires additional learning)	FX
1–34	Unsatisfactory (requires repetition of the course)	F

Norms of academic integrity and course policy

The student must adhere to the Code of Ethics of Academic Relations and Integrity of NTU "KhPI": to demonstrate discipline, good manners, kindness, honesty, and responsibility. Conflict situations should be openly discussed in academic groups with a lecturer, and if it is impossible to resolve the conflict, they should be brought to the attention of the Institute's management.
Regulatory and legal documents related to the implementation of the principles of academic integrity at NTU "KhPI" are available on the website: http://blogs.kpi.kharkov.ua/v2/nv/akademichna-dobrochesnist/

Approval

Approved by	Date, signature 29.08.2024		Head of the department Serhii YEVSEIEV
	Date, signature 29.08.2024		Guarantor of the educational program Olena AKHIIEZER