Proceedings of 5th International Conference CNDGS'2026
ISSN 2669-2023 (print) / ISSN 2538-8959 (on-line) **/ https://doi.org/10.47459/cndcgs.2026.160**

Number Theory and Mathematical Foundations of Cybersecurity Education in the Training of Future National Defence Specialists

Radovan POTŮČEK[1]*

Department of Mathematics and Physics, Faculty of Military Technology, University of Defence, Kounicova 65, 662 10 Brno, Czech Republic

Correspondence: radovan.potucek@unob.cz*

Abstract

This paper presents an expanded discussion of the mathematical curriculum within the Cybersecurity specialization at the Faculty of Military Technology, University of Defence, with particular emphasis on discrete mathematics and number theory. Building on earlier work describing experiences in teaching Mathematics I–III and Graph Theory, we focus on selected number-theoretic topics and their concrete applications in cybersecurity- and cryptography-oriented courses. Through representative examples solved by students in discrete mathematics courses, we illustrate how concepts such as modular arithmetic, finite fields, and algebraic structures support the understanding of cryptographic algorithms and protocols. The paper further reflects on the role of mathematically grounded education in preparing future cybersecurity specialists for national defence tasks in the context of contemporary geopolitical challenges.

KEY WORDS: *discrete mathematics, cybersecurity education, number theory, cryptography, finite fields, algebraic structures, national defence*

Citation: Potůček, R. Number Theory and Mathematical Foundations of Cybersecurity Education in the Training of Future National Defence Specialists. In Proceedings of the Challenges to National Defence in Contemporary Geopolitical Situation, Brno, Czech Republic, 7-10 September 2026. ISSN 2538-8959, https://doi.org/10.47459/cndcgs.2026.160

1. Introduction

In the current geopolitical climate, threats in cyberspace are becoming increasingly sophisticated, persistent, and difficult to detect. Defence institutions therefore require cybersecurity specialists who combine practical skills with a solid theoretical background. Discrete mathematics, as systematically developed in standard textbooks [1–4] plays a central role in the understanding, analysis, and design of modern cybersecurity mechanisms, particularly in the areas of cryptography, secure communication, and algorithmic security [5–8].

In my earlier article [9], entitled *Experience Teaching Mathematics at the University of Defence in the Study Field of Cybersecurity*, I presented the structure and content of the courses Mathematics I–III and Graph Theory, together with sample examination tasks and an analysis of students' results over a five-year period. That work provided valuable insight into student performance, topic areas that tend to be challenging, and recurring patterns of success and difficulty.

The present paper builds on these findings by focusing more explicitly on the role of number theory and related discrete-mathematical topics in specialized cybersecurity courses. The aim is to demonstrate how selected mathematical concepts can be pedagogically linked to cryptography-oriented subjects, thereby strengthening students' theoretical preparedness for practical tasks in national defence [10–12] and cybersecurity [13–15].

2. Structure of Mathematical Courses in the Cybersecurity Curriculum at the University of Defence

This section provides an overview of the structure and content of the core mathematical courses within the Cybersecurity curriculum at the University of Defence. The aim is to outline how discrete mathematics, linear algebra, number theory, logic, and graph theory are distributed across individual subjects and how these topics gradually build the mathematical foundations required for advanced cybersecurity and cryptography-oriented courses [13–15].

Peer-review under responsibility of General Jonas Žemaitis Miltitary Academy of Lithuania and University of Defence, Czech Republic

2.1 Mathematics I

The course Mathematics I is allocated 90 teaching hours, corresponding to 45 learning units. It consists of 22 lectures and 23 exercise sessions, including two laboratory classes conducted in a computer classroom. The laboratory exercises make use of the computer algebra system Maple, which is also employed in subsequent mathematics courses.

The main topics covered in Mathematics I include mathematical logic and introductory proof techniques, set theory, binary relations, mappings, partially ordered sets, basic combinatorics, fields and vector spaces, matrices and matrix operations, systems of linear equations, vector subspaces, bases and dimensions of vector spaces, and linear mappings.

2.2 Mathematics II

Mathematics II is likewise allocated 90 teaching hours, comprising 22 lectures and 23 exercise sessions, including three laboratory classes. The course deepens students' knowledge of linear algebra and introduces key topics from number theory and abstract algebra that are essential for cryptography. These include determinants and inverse matrices, eigenvalues and eigenvectors, diagonalization and matrix functions, divisibility, the Euclidean algorithm, Bézout's identity, prime numbers, congruences and systems of linear congruences, Euler's totient function, Fermat's little theorem, Euler's theorem, groups, rings, polynomial rings, Galois fields, lattices, and Boolean algebras.

2.3 Mathematics III

Mathematics III again comprises 90 teaching hours, divided into 22 lectures and 23 exercise sessions, including two laboratory classes. The course focuses primarily on logic, automata theory, and formal methods, while also covering selected topics from mathematical analysis when needed for continuity with previous study. Key topics include propositional and predicate logic, normal forms and their minimization, Karnaugh maps, deductive systems, automata and formal languages, recursion, basic computability theory, as well as selected topics from calculus, sequences, series, and generating functions.

2.4 Graph Theory

Graph Theory has been taught at the Faculty of Military Technology since the mid-1990s, initially within doctoral studies and later, from the academic year 2019/2020, as a core subject of the Cybersecurity master's programme. The course comprises 60 teaching hours (15 lectures and 15 exercise sessions), including three laboratory classes, and is completed with a classified credit rather than a semester examination. The course covers fundamental concepts of graph theory and key graph algorithms, including trees, connectivity, matchings, graph colourings, planar graphs, flows in networks, and selected applications relevant to cybersecurity and algorithmic problem solving.

3. Applications of Number Theory to Cryptography

The central role of number theory in modern cryptography is well documented in the literature [16–19] and forms an essential part of the mathematical background of cybersecurity specialists. In this section, we present selected applications of number-theoretic concepts that are introduced in the mathematics courses and later utilized in cryptography-oriented subjects, with emphasis on their didactic role and practical relevance.

3.1 Modular Arithmetic and Public-Key Cryptography

Modular arithmetic forms one of the fundamental mathematical tools used in modern public-key cryptography. Within the cybersecurity curriculum, students encounter congruence relations and modular computations primarily in the context of number theory topics introduced in Mathematics II. These concepts provide the necessary background for understanding the basic principles of widely used cryptographic schemes.

In particular, congruences modulo a positive integer n, Euler's totient function, Fermat's little theorem, and Euler's theorem are presented not as abstract theoretical results, but as practical instruments for secure communication. Their role becomes evident when explaining the mathematical foundations of public-key cryptosystems such as RSA. While students are not required to master formal proofs, emphasis is placed on understanding why modular exponentiation behaves differently from standard arithmetic operations and why certain computations are easy to perform while their inverse problems are computationally hard.

This approach helps students grasp the key idea underlying public-key cryptography: security is not based on secrecy of the algorithm, but on the computational difficulty of specific number-theoretic problems. By linking modular arithmetic directly to cryptographic applications, students develop an intuitive understanding of how abstract mathematical concepts translate into practical security mechanisms.

We now present several typical problems involving modular arithmetic, the use of Euler's theorem, and an illustration of the RSA encryption system, which students encounter in the course *Mathematics II*.

Example 1. Prove that the number $200^{200} - 1$ is divisible by 13.

Solution. We solve the problem in two ways:
(a) by a logical argument without using congruences,
(b) by using congruences.

(a) The problem cannot be solved directly using a scientific calculator, since the number

$$200^{200} \approx 1.6069 \times 10^{460}$$

has 460 digits and therefore cannot be displayed. We therefore use the following reasoning.
Writing the base 200 in terms of 13, we obtain

$$200^{200} - 1 = (13 \cdot 15 + 5)^{200} - 1.$$

This number has the same remainder modulo 13 as $5^{200} - 1$. Indeed, using the binomial expansion of $(13 \cdot 15 + 5)^{200}$, all terms are divisible by 13 except the last one, which is 5^{200}.

We again express the base in terms of 13 and obtain

$$5^{200} - 1 = 25^{100} - 1 = (13 \cdot 2 - 1)^{100} - 1.$$

This number has the same remainder modulo 13 as

$$(-1)^{100} - 1 = 0.$$

Thus, the remainder of $200^{200} - 1$ upon division by 13 is equal to 0, and hence the number is divisible by 13.
(b) The problem can be solved easily using congruences. Since

$$200^2 = 40\,000 \quad \text{and} \quad 40\,000 = 13 \cdot 3077 - 1 \equiv -1 (\text{mod } 13),$$

we use the basic property of congruences stating that for any $n \in \mathbb{N}$,

$$a \equiv b (\text{mod } m) \;\Rightarrow\; a^n \equiv b^n (\text{mod } m).$$

It follows that

$$200^{200} \equiv (-1)^{100} = 1 (\text{mod } 13).$$

Hence,

$$200^{200} - 1 \equiv 0 (\text{mod } 13),$$

which proves that $13 \mid (200^{200} - 1)$.

Example 2. Find all solutions of the linear congruence

$$13x \equiv 14 (\text{mod } 15).$$

Solution. The given linear congruence of the form $ax \equiv b (\text{mod } m)$is solvable because

$$\gcd(a, m) \mid b,$$

since

$$\gcd(13,15) = 1 \text{ and } 1 \mid 14.$$

We look for solutions among the integers $0,1, \ldots ,14$. Subtracting the congruence

$$13x \equiv 14 (\text{mod } 15)$$

from the trivial congruence

$$15x \equiv 0 (\text{mod } 15),$$

we obtain

$$2x \equiv -14 (\text{mod } 15).$$

After adding the modulus 15 to the right-hand side, we get

$$2x \equiv 1 (\text{mod } 15).$$

Multiplying this congruence by 6 yields

$$12x \equiv 6 (\text{mod } 15).$$

Subtracting this congruence from the original one $13x \equiv 14 (\text{mod } 15)$, we obtain

$$x \equiv 8 (\text{mod } 15).$$

Thus, the solution of the given congruence is

$$x = 8 + 15k, \qquad k \in \mathbb{Z}.$$

The correctness of the solution can be easily verified by substitution:

$$13(8 + 15k) = 104 + 195k = (6 \cdot 15 + 14) + (13k \cdot 15) \equiv 14 (\text{mod } 15).$$

These examples illustrate how modular arithmetic and basic properties of congruences provide efficient tools for solving problems involving large numbers, which frequently arise in cryptographic applications.

Example 3. Compute the remainder of the number 13^{12098} upon division by 1960.

Solution. We first determine the prime factorization of 1960, which is

$$1960 = 2^3 \cdot 5 \cdot 7^2.$$

Since $\gcd(1960,13) = 1$, Euler's totient function is given by

$$\varphi(1960) = 1960 \left(1-\frac{1}{2}\right)\left(1-\frac{1}{5}\right)\left(1-\frac{1}{7}\right) = 1960 \cdot \frac{1}{2} \cdot \frac{4}{5} \cdot \frac{6}{7} = 672.$$

By Euler's theorem $a^{\varphi(m)} \equiv 1 (\text{mod } m)$, we obtain

$$13^{672} \equiv 1 (\text{mod } 1960).$$

We express the exponent 12098 in terms of 672 as

$$12098 = 672 \cdot 18 + 2.$$

Since

$$13^{12098} = 13^{672 \cdot 18+2} = (13^{672})^{18} \cdot 13^2,$$

it follows that

$$13^{12098} \equiv 13^2 \equiv 169 (\text{mod } 1960).$$

Hence, the required remainder is 169.

Example 4. An illustrative example of the RSA encryption system. Encrypt and then decrypt the message *UO* using the RSA scheme.

Solution. We choose small prime numbers for illustrative purposes; in practice, primes of much larger size are used. The solution proceeds in six steps. Letters are encoded as numbers as follows:

$$\text{A} \sim 01, \ldots, \text{O} \sim 15, \ldots, \text{U} \sim 21, \ldots, \text{Z} \sim 26.$$

Thus, the message *UO* corresponds to the numerical code $m = 2115$.

1. The recipient chooses two distinct prime numbers, for example $p = 67$ and $q = 73$, and computes the public modulus
$$n = pq = 67 \cdot 73 = 4891.$$
2. The value of Euler's totient function is computed as
$$\varphi(4891) = \varphi(67 \cdot 73) = 66 \cdot 72 = 4752.$$
3. A number $E \in \mathbb{N}$, $1 < E < 4752$, such that $\gcd(E, 4752) = 1$is chosen, for example $E = 17$. This number is the public encryption exponent and is sent openly to the sender.
4. The recipient determines the private decryption exponent D such that
$$DE \equiv 1 (\text{mod } \varphi(n)),$$

that is,

$$17D \equiv 1 (\text{mod } 4752).$$

The modular inverse $D = 4193$ of 17 can be found, for instance, using an online calculator. The decryption exponent D is kept secret by the recipient.

5. The sender encrypts the numerical code $m = 2115$ by computing

$$b = m^E (\text{mod } n),$$

that is,

$$b = 2115^{17} (\text{mod } 4891) = 4854,$$

and sends the encrypted value b to the recipient.

6. The recipient recovers the original numerical code m by decrypting b via

$$m = b^D (\text{mod } n),$$

that is,

$$m = 4854^{4193} (\text{mod } 4891) = 2115.$$

Splitting the result into pairs $21 \mid 15$ yields the original message *UO*.

This simplified example demonstrates the core principles of public-key cryptography while remaining computationally accessible for students.

The presented examples demonstrate how fundamental results of number theory, such as Euler's theorem and modular inverses, form the mathematical backbone of public-key cryptographic systems.

3.2 Finite Fields and Symmetric Cryptography

Finite fields constitute another essential area of number theory with direct relevance to cybersecurity, particularly in symmetric cryptography. In the mathematics curriculum, finite fields are introduced in Mathematics II as algebraic structures extending modular arithmetic. Their importance becomes clear when students encounter encryption algorithms operating on binary data. Special attention is given to finite fields of the form $\mathbb{F}_p$ and $\mathbb{F}_{2^m}$, which naturally model arithmetic operations on digital data. Without delving into advanced algebraic theory, students are shown how addition and multiplication in finite fields differ from standard integer arithmetic and why these operations are well suited for cryptographic purposes.

A typical motivating example is the **Advanced Encryption Standard (AES)**, which has been used as the encryption standard in the United States since 2002 [20,21]. It is characterized by strong resistance to cryptanalytic attacks, and arithmetic in the finite field $\mathbb{F}(2^8)$ plays a central role in its design. A detailed analysis of the AES algorithm is beyond the scope of this paper; therefore, we present only illustrative examples of the mathematical operations employed in this encryption standard.

Example 5. XOR operator.

The XOR operator (exclusive disjunction), denoted by the symbol $\oplus$, takes the value 1 if and only if the two propositional variables have different truth values. The XOR operator can also be interpreted as addition modulo 2. For propositional variables p, q, the following logical equivalence holds:

$$p \oplus q \equiv (p \wedge \neg q) \vee (\neg p \wedge q) \; [\equiv \neg(p \leftrightarrow q)].$$

The truth table corresponding to the XOR operator is therefore

p	q	$p \oplus q$
0	0	0
0	1	1
1	0	1
1	1	0

In cryptography, the bitwise XOR function is frequently used. As an illustration, consider a simple XOR cipher, where a binary string and a key are given as inputs, and the XOR operator is applied to them. For example:

```
plaintext:  0101 1011 0110
key:        1011 0001 1101
```

```
XOR result: 1110 1010 1011
```

If we apply the XOR operator again to the XOR result (which represents the encrypted text) using the same key, we recover the original plaintext:

```
XOR result: 1110 1010 1011
key:        1011 0001 1101
plaintext:  0101 1011 0110
```

Interestingly, if we apply the XOR operator to the XOR result and the original plaintext, we obtain the original key:

```
XOR result: 1110 1010 1011
plaintext:  0101 1011 0110
key:        1011 0001 1101
```

Example 6. Modular addition in a finite field. Modular addition of two elements in the finite field $\mathbb{F}(2^8)$ is performed by adding the coefficients corresponding to the same powers of the polynomial representation of the elements. The addition is carried out using the XOR operation, that is, modulo 2, where

$$0 \oplus 0 = 0, \;\; 0 \oplus 1 = 1 \oplus 0 = 1, \;\; 1 \oplus 1 = 0.$$

Alternatively, addition in the finite field can be described as bitwise addition modulo 2 of the corresponding bits of a byte, that is, a sequence of 8 bits. For two bytes

$$\{a_7a_6a_5a_4a_3a_2a_1a_0\} \quad \text{and} \quad \{b_7b_6b_5b_4b_3b_2b_1b_0\},$$

their sum is

$$\{c_7c_6c_5c_4c_3c_2c_1c_0\},$$

where each $c_i = a_i \oplus b_i$.

For example, the following representations are equivalent:

- **Polynomial representation:**

$$(x^6 + x^4 + x^2 + x + 1) + (x^7 + x + 1) = x^7 + x^6 + x^4 + x^2$$

- **Binary representation:**

$$\{01010111\} + \{10000011\} = \{11010100\}$$

- **Hexadecimal representation:**

$$\{57\} + \{83\} = \{d4\}$$

Example 7. Modular multiplication in a finite field. In the polynomial representation, modular multiplication in the finite field $\mathbb{F}(2^8)$ corresponds to polynomial multiplication modulo an irreducible polynomial of degree 8. A polynomial is irreducible if it is non-constant and its only divisors are 1 and the polynomial itself. An example of such an irreducible polynomial is

$$m(x) = x^8 + x^4 + x^3 + x + 1.$$

Since

$$(x^6 + x^4 + x^2 + x + 1)(x^7 + x + 1) = x^{13} + x^{11} + x^9 + x^8 + x^6 + x^5 + x^4 + x^3 + 1,$$

the result of multiplying these two polynomials in $\mathbb{F}(2^8)$ is obtained by reducing the polynomial

$$x^{13} + x^{11} + x^9 + x^8 + x^6 + x^5 + x^4 + x^3 + 1$$

modulo $m(x) = x^8 + x^4 + x^3 + x + 1$, with coefficients computed over the field $\mathbb{Z}_2$.

In this case, the result of the modular multiplication is the polynomial

$$x^7 + x^6 + 1.$$

Modular reduction by the polynomial $m(x)$thus ensures that the result is a binary polynomial of degree less than 8 and can therefore be represented as a byte.

These examples show how arithmetic operations in finite fields, implemented at the level of bits and bytes, play a crucial role in modern symmetric encryption standards such as AES.

3.3 Algebraic Structures and Cryptographic Security

Beyond modular arithmetic and finite fields, selected algebraic structures such as groups and cyclic groups are introduced as part of the mathematical foundation of cryptography. These topics provide the conceptual background for understanding several cryptographic protocols used in secure communication and authentication. In the cybersecurity program, students are introduced to the basic properties of groups and the notion of cyclicity primarily through concrete examples rather than through an abstract axiomatic development. This level of understanding is sufficient for explaining the principles underlying cryptographic constructions.

The pedagogical emphasis lies on the distinction between efficiently computable operations and computationally infeasible inverse problems. By illustrating how group operations can be performed quickly while reversing them remains hard for large parameters, students gain insight into why algebraic structures play a crucial role in modern cryptographic security. This knowledge supports their ability to critically assess cryptographic systems and understand their limitations in practical cybersecurity applications.

We now present three typical examples from group theory and the theory of cyclic groups that students solve during exercise sessions.

Example 8. Show that two following groups – the multiplicative group $(\{1, -1, \mathrm{i}, -\mathrm{i}\}, \cdot)$ and the additive group of residue classes $(\mathbb{Z}_4, \oplus)$ – are isomorphic.

Solution. Recall that two groups are isomorphic if there exists a bijection between their elements that preserves the group operation. By comparing the results of the group operations in the Cayley tables of the two groups, we verify that the groups are isomorphic.

For the operation $\cdot$ in the multiplicative group $(\{1, -1, \mathrm{i}, -\mathrm{i}\}, \cdot)$, we have

$$1 \cdot 1 = (-1) \cdot (-1) = \mathrm{i} \cdot (-\mathrm{i}) = (-\mathrm{i}) \cdot \mathrm{i} = 1,$$
$$1 \cdot (-1) = (-1) \cdot 1 = \mathrm{i} \cdot \mathrm{i} = (-\mathrm{i}) \cdot (-\mathrm{i}) = -1,$$
$$1 \cdot \mathrm{i} = \mathrm{i} \cdot 1 = (-1) \cdot (-\mathrm{i}) = (-\mathrm{i}) \cdot (-1) = \mathrm{i},$$
$$1 \cdot (-\mathrm{i}) = (-\mathrm{i}) \cdot 1 = (-1) \cdot \mathrm{i} = \mathrm{i} \cdot (-1) = -\mathrm{i}.$$

Thus, we obtain the following Cayley table:

$\cdot$	1	i	-1	$-$i
1	1	i	-1	$-$i
i	i	-1	$-$i	1
-1	-1	$-$i	1	i
$-$i	$-$i	1	i	-1

The additive group of residue classes $(\mathbb{Z}_4, \oplus)$ has four elements, which are the numbers 0,1,2,3. For addition modulo 4, we have the relations

$$0 \oplus a = a \oplus 0 = a$$

for all $a \in \{0,1,2,3\}$, and furthermore

$$1 \oplus 2 = 2 \oplus 1 = 3, \quad 1 \oplus 3 = 3 \oplus 1 = 2 \oplus 2 = 0, \quad 2 \oplus 3 = 3 \oplus 2 = 1, \quad 1 \oplus 1 = 3 \oplus 3 = 2.$$

This yields the following Cayley table:

$\oplus$	0	1	2	3
0	0	1	2	3
1	1	2	3	0
2	2	3	0	1
3	3	0	1	2

There exists a bijection between the elements of the two groups given by

$$1 \leftrightarrow 0, \quad i \leftrightarrow 1, \quad -1 \leftrightarrow 2, \quad -i \leftrightarrow 3.$$

Hence, the groups are isomorphic.

Example 9. Show that the set $A = \{\mathrm{id}, \pi_3, \pi_4\}$ forms a commutative subgroup of the symmetric group $(S_3, \circ)$ with elements (i.e. with permutations)

$$\mathrm{id} = (1,2,3), \quad \pi_1 = (1,3,2), \quad \pi_2 = (2,1,3), \quad \pi_3 = (2,3,1), \quad \pi_4 = (3,1,2), \quad \pi_5 = (3,2,1).$$

Solution. From the following Cayley table of the group $(S_3, \circ)$,

$\circ$	id	π_1	π_2	π_3	π_4	π_5
id	id	π_1	π_2	π_3	π_4	π_5
π_1	π_1	id	π_4	π_5	π_2	π_3
π_2	π_2	π_3	id	π_1	π_5	π_4
π_3	π_3	π_2	π_5	π_4	id	π_1
π_4	π_4	π_5	π_1	id	π_3	π_2
π_5	π_5	π_4	π_3	π_2	π_1	id

it is evident that the set $A = \{\mathrm{id}, \pi_3, \pi_4\}$ forms a commutative subgroup of S_3, as illustrated by the corresponding subtable.

Example 10. Determine the generators of the groups:
(a) $(\mathbb{Z}_4, \oplus)$,
(b) $(\mathbb{Z}_9^*, \odot)$.

Solution. Recall that a group $(G, *)$ is called cyclic if there exists a generator of the group, that is, an element $a \in G$ that generates all elements of G using the operation $*$.

(a) The generators of the group $(\mathbb{Z}_4, \oplus)$ are the elements 1 and 3, since modulo 4 we have

$$1 \oplus 1 = 2, \quad 1 \oplus 1 \oplus 1 = 3, \quad 1 \oplus 1 \oplus 1 \oplus 1 = 0, \quad 1 \oplus 1 \oplus 1 \oplus 1 \oplus 1 = 1,$$
$$3 \oplus 3 = 2, \quad 3 \oplus 3 \oplus 3 = 1, \quad 3 \oplus 3 \oplus 3 \oplus 3 = 0, \quad 3 \oplus 3 \oplus 3 \oplus 3 \oplus 3 = 3.$$

(b) The group $(\mathbb{Z}_9^*, \odot)$ consists of the elements of the set $\{1,2,\ldots,9\}$ that are coprime to 9. Since $\varphi(9) = 6$, we have

$$\mathbb{Z}_9^* = \{1,2,4,5,7,8\}.$$

The group $(\mathbb{Z}_9^*, \odot)$ is generated by the elements 2 and 5, because modulo 9,

$$2^2 = 4, \quad 2^3 = 8, \quad 2^4 = 4, \quad 2^5 = 5, \quad 2^6 = 1, \quad 2^7 = 2,$$
$$5^2 = 7, \quad 5^3 = 8, \quad 5^4 = 4, \quad 5^5 = 2, \quad 5^6 = 1, \quad 5^7 = 5.$$

Therefore, both groups $(\mathbb{Z}_4, \oplus)$ and $(\mathbb{Z}_9^*, \odot)$ are cyclic groups.

The examples emphasize how basic concepts of group theory and cyclic structures, introduced through concrete computations, support the understanding of algebraic principles underlying cryptographic constructions.

4. Conclusions

This paper has presented an overview of the role of discrete mathematics and number theory in the education of cybersecurity students at the University of Defence, with particular emphasis on their application in cryptography. By linking concrete mathematical topics from core courses to selected cryptographic algorithms and standards, we have shown how theoretical concepts support practical understanding in specialized cybersecurity training.

The presented examples demonstrate that even a non-axiomatic, example-driven introduction to modular arithmetic, finite fields, and algebraic structures is sufficient to explain the fundamental principles underlying modern cryptographic systems. Such an approach is particularly suitable for future engineers and cybersecurity specialists, who are primarily users of mathematical tools rather than professional mathematicians. At the same time, experience from teaching indicates that students often face difficulties with abstract algebraic reasoning, formal logic, and combinatorial thinking. These challenges can be effectively addressed using computational tools, visualizations, progressive problem sets, and closer coordination between mathematics and cybersecurity courses, ensuring that mathematical topics are introduced in a context directly relevant to their future professional practice.

In the current geopolitical context, cyberspace represents a critical domain of national defence. Well-trained cybersecurity specialists, equipped with a solid mathematical foundation, are essential for the design of secure systems, cryptographic resilience, and effective detection and response to cyber threats. From this perspective, the integration of discrete mathematics and number theory into cybersecurity education is not only an academic necessity, but also a strategic requirement for national defence.

Acknowledgements. The work presented in this paper has been supported by the Project for the Development of the Organization „DZRO Military autonomous and robotic systems“.

References

1. **Lehman E., Leighton F. T., Meyer, A. R.** Mathematics for Computer Science, Samurai Media Limited, 2017, ISBN 978-9888407064, 988 pp. https://courses.csail.mit.edu/6.042/spring18/mcs.pdf
2. **Rosen K. H.** Discrete Mathematics and Its Applications, McGraw Hill Education, 8th Edition, 2019, ISBN 978-1-259-67651-2, 1118 pp.
3. **Rosen K. H.** Student's Solutions Guide for Discrete Mathematics and Its Applications, McGraw-Hill Education, ISBN 978-1259731693, 8th Edition, 2018, 584 pp.
4. **Reilly D.** Math for Security: From Graphs and Geometry to Spatial Analysis, No Starch Press, San Francisco, 2023, ISBN 978-1-7185-0257-4, 312 pp.
5. **Kelemen M., Szabo S., Vajdova I.** Cybersecurity in the Context of Criminal Law Protection of the State Security and Sectors of Critical Infrastructure. Challenges to National Defence in Contemporary Geopolitical Situation, 2018, pp. 100-104. https://doi.org/10.47459/cndcgs.2018.14
6. **Korecki Z., Adamkova B.** Human Factor Failure in Hybrid Warfare and its Impact on Airport Security. Challenges to National Defence in Contemporary Geopolitical Situation, 2020, pp. 129-144. https://doi.org/10.47459/cndcgs.2020.17
7. **Zagorodna N., Stadnyk M., Lypa B., Gavrylov M., Kozak R.** Network Attack Detection Using Machine Learning Methods. Challenges to National Defence in Contemporary Geopolitical Situation, 2022, pp. 55-61. https://doi.org/10.47459/cndcgs.2022.7
8. **Pakholchuk V., Horiacheva K.** Methodological Concepts of Appling AI into Military and Economic Capabilities Data Analysis. In Proceedings of the Challenges to National Defence in Contemporary Geopolitical Situation, Brno, Czech Republic, 11-13 September 2024. https://doi.org/10.3849/cndcgs.2024.25
9. **Potůček R**. Experience Teaching Mathematics at the University of Defence in the Study Field of Cybersecurity, WSEAS Transactions on Advances in Engineering Education, 2024, Vol. 21, p. 155-169. https://wseas.com/journals/education/2024/a365110-014(2024).pdf
10. **Lété B., Pernik P.** EU–NATO Cybersecurity and Defense Cooperation: From Common Threats to Common Solutions, Security and Defense Policy, 2017, No. 38, 9 pp. https://www.gmfus.org/sites/default/files/EU-NATO-Cybersecurity-and-Defense-Cooperation.pdf
11. **Paunescu D.-M.** NATO's Encounters in the Cyber Domain, Proceedings of the 17th International Scientific Conference Strategies XXI, 2021, Vol. 17, No. 1, p. 153-158. https://doi.org/10.53477/2668-2001-21-18 https://revista.unap.ro/index.php/XXI_FSA/article/download/1274/1237/4470
12. **U.S. Department of Defense** Cybersecurity – Resource and Reference Guide, Cleared for Open Publication: Feb 28, 2022, 59 pp. https://dodcio.defense.gov/Portals/0/Documents/Library/CSResourceReferenceGuide.pdf
13. **Cieslak E.** Understanding People and Technology. Professional Military Education and Challenges of Future Commanders Development. Challenges to National Defence in Contemporary Geopolitical Situation, 2018, pp. 134-141. https://doi.org/10.47459/cndcgs.2018.20
14. **Bekesiene S., Prusevicius G.** Simulators Usage Assessment for Higher Military Readiness. Challenges to National Defence in Contemporary Geopolitical Situation, 2020, pp. 114-124. https://doi.org/10.47459/cndcgs.2020.15
15. **Vagner M., Hasilova K.** Success/Leaving Rate of the Military Students. Challenges to National Defence in Contemporary Geopolitical Situation, 2022, pp. 76-81. https://doi.org/10.47459/cndcgs.2022.10
16. **Aumasson J.-P.** Serious cryptography, No Starch Press, San Francisco, 2018, ISBN 978-1-59327-826-7, 314 pp. https://www.kea.nu/files/textbooks/humblesec/seriouscrytography.pdf
17. **Zheng Z.** Modern Cryptography Volume 1, Springer Singapore, Open Access, 2022, ISBN 978-981-19-0919-1, 359 pp. https://link.springer.com/book/10.1007/978-981-19-0920-7
18. **Zheng Z.** Modern Cryptography Volume 2, Springer Singapore, Open Access, 2023, ISBN 978-981-19-7643-8, 202 pp. https://link.springer.com/book/10.1007/978-981-19-7644-5
19. **Bellare M., Rogaway P.** Introduction to Modern Cryptography, University of California at Davis 2005, 283 pp. https://web.cs.ucdavis.edu/~rogaway/classes/227/spring05/book/main.pdf
20. **Abdullah A. M.** Advanced Encryption Standard (AES) Algorithm to Encrypt and Decrypt Data. Cryptography and Network Security, 2017, Vol. 16, 12 p. 1-11. https://www.researchgate.net/publication/317615794_Advanced-Encryption_Standard_AES_Algorithm_to_Encrypt_and_Decrypt_Data
21. **Brown K. H.** Advanced Encryption Standard (AES), Report on the Development of the Advanced Encryption Standard. (AES). Journal of Research of NIST (NIST JRES), November 2001, updated May 2023, 46 pp. https://doi.org/10.6028/NIST.FIPS.197-upd1