

Teaching Strategies of Discrete Mathematics in Cryptography Education

Yuying Ou*, Wenbin Zhang

Guangzhou Huashang College, Guangzhou 511300, Guangdong, China.

How to cite this paper: Yuying Ou, Wenbin Zhang. (2025) Teaching Strategies of Discrete Mathematics in Cryptography Education. *Journal of Applied Mathematics and Computation*, 9(2), 144-149. DOI: 10.26855/jamc.2025.06.006

Received: April 26, 2025

Accepted: May 22, 2025

Published: June 19, 2025

***Corresponding author:** Yuying Ou, Guangzhou Huashang College, Guangzhou 511300, Guangdong, China.

Abstract

In the digital age, discrete mathematics is reshaping the ecosystem of cryptography education. This paper integrates discrete mathematics into the teaching of cryptography, cultivates students' multi-dimensional thinking and problem decomposition ability, and infuses the soul into algorithm construction. Innovatively propose an integrated teaching strategy, break through traditional boundaries, incorporate cutting-edge technologies such as case-based and project-based learning, and build immersive scenarios. Introducing a project-driven teaching method helps students understand the core principles of knowledge through the practical application of cracking real cryptographic security protocols. This approach will enable students to excel in the field of cryptography and contribute innovative insights.

Keywords

Discrete mathematics; Cryptography; Integrated teaching

1. Introduction

With the rapid development of information technology, the demand for professional talent in the field of cryptography is increasing day by day. And discrete mathematics, as the theoretical cornerstone of these fields, its educational role is becoming more and more prominent. Mathematics originates from practice and converges in practice. Discrete mathematics is a mathematics course and should be like this as well [1]. From point to surface and step by step, the quality goals, ability goals and knowledge application goals are quantitatively incorporated into the assessment system, with the aim of enabling students to acquire good scientific thinking qualities, essential logical reasoning and abstract thinking abilities, systematic discrete mathematics modeling and multi-disciplinary penetration, and other cross-integrated teaching goals that apply what they have learned [2].

In cryptography, knowledge such as algebraic system theory, number theory, and logical operations of discrete mathematics is the core for constructing various encryption algorithms. For example, the security of the RSA algorithm is based on the mathematical problem of factoring large integers, while elliptic curve cryptography relies on the discrete logarithm problem. Furthermore, combinatorial mathematics in discrete mathematics provides theoretical support for key generation and management in cryptography, and graph theory also has important applications in cryptanalysis and data structure design.

However, the discrete mathematics course is confronted with many challenges in teaching practice. The main core teaching contents of discrete mathematics include four major parts: mathematical logic, set theory, algebraic systems, and graph theory [3]. The content is highly abstract and involves multiple complex branches of mathematics, making it often difficult for students to understand and master. Meanwhile, the traditional teaching mode is difficult to stimulate students' interest in learning, which affects the teaching effect. Therefore, it is particularly important to explore innovative teaching strategies to improve the teaching quality of discrete mathematics.

This article will deeply explore the cornerstone role of discrete mathematics in cryptography education, analyze the existing problems in current teaching, center on students, focus on the achievement of learning outcomes, and promote the all-round development of students in terms of knowledge, ability and quality by setting clear learning goals, designing effective teaching activities and constructing a diversified evaluation system [4]. Combined with the cutting-edge teaching concepts, a series of innovative teaching strategies are proposed, aiming to provide useful references and inspirations for the educational reform of discrete mathematics and assist in cultivating cryptography professionals who can meet the demands of the new era.

2. The Idea of Integrated Teaching

2.1 The integration of discrete mathematics and cryptography courses

The integration of cryptography courses and discrete mathematics is mainly reflected in the following aspects:

Algebraic structures: The algebraic system theory in discrete mathematics provides cryptography with the concepts and theories of algebraic structures such as groups, rings, and fields, which play a crucial role in the design of encryption algorithms and digital signature algorithms. For example, elliptic curve cryptography is based on the algebraic properties of elliptic curve groups to achieve secure key exchange and encryption operations.

The foundation of number theory: The knowledge of number theory in discrete mathematics provides a basis for many algorithms in cryptography, such as modular operations, prime number detection, and factorization of large integers. These number theory concepts have important applications in classic cryptographic algorithms such as the RSA algorithm and the Diffie-Hellman key exchange algorithm, providing theoretical support for students to understand the security and efficiency of cryptographic algorithms.

Logical operations: The application of logical operations in discrete mathematics in cryptography includes bit operations, Boolean functions, etc. These operations play a significant role in the design and analysis of symmetric encryption algorithms, hash functions, etc., helping students understand the internal mechanisms and security principles of cryptographic algorithms.

3. The Specific Implementation Strategies of Integrating Ideas

3.1 Interdisciplinary instructional design

In terms of curriculum design, the relevant knowledge points of discrete mathematics can be organically integrated into the curriculum system of cryptography. Especially with discrete mathematics problems as the background, practical problems with sufficient breadth and depth can be constructed [5]. For instance, as shown in the following three questions and their solutions, in the course of cryptography, when explaining the public key cryptosystem, the number theory foundation and algebraic structure in discrete mathematics can be elaborated in depth. The relevant theoretical system should be integrated into the case series teaching from the simple to the complex [6]. Through this interdisciplinary instructional design, students can naturally understand and apply the knowledge of discrete mathematics while learning cryptography, thereby improving the learning effect.

Question 1: Suppose we want to conduct secure communication on the Internet and encrypt information using the RSA public key cryptosystem. Select two prime numbers $p = 3$ and $q = 11$, public key index $e = 3$.

- (1) Calculate the corresponding private key d .
- (2) Encrypt the plaintext with $m = 5$ and then send it.
- (3) After receiving the ciphertext, decrypt it with the private key to verify whether the plaintext can be recovered.

Answer:

- (1) Calculate the private key d :

First and foremost calculate modulus $n = p \times q = 3 \times 11 = 33$, Calculate the Euler function $\varphi(n) = (p - 1)(q - 1) = (3 - 1)(11 - 1) = 2 \times 10 = 20$.

Known public key index $e = 3$, The private key d is a positive integer that satisfies $e \times d \equiv 1 \pmod{\varphi(n)}$.

That is, to find $3d \equiv 1 \pmod{20}$. By trying or extending the Euclidean algorithm, $d = 7$ can be found, since $3 \times 7 = 21 \equiv 1 \pmod{20}$.

(2) Encrypted plaintext $m = 5$:

Calculate ciphertext $c = m^e \bmod n = 5^3 \bmod 33 = 125 \bmod 33 = 26$.

(3) Decrypt the ciphertext $c = 26$:

Use the private key d to calculate the plaintext:

$m' = c^d \bmod n = 26^7 \bmod 33$.

Calculate step by step first:

$26^2 = 676 \equiv 676 - 20 \times 33 = 676 - 660 = 16 \bmod 33$;

$26^4 = (26^2)^2 \equiv 16^2 = 256 \equiv 256 - 7 \times 33 = 256 - 231 = 25 \bmod 33$;

$26^6 = 26^4 \times 26^2 \equiv 25 \times 16 = 400 \equiv 400 - 12 \times 33 = 400 - 396 = 4 \bmod 33$;

$26^7 = 26^6 \times 26 \equiv 4 \times 26 = 104 \equiv 104 - 3 \times 33 = 104 - 99 = 5 \bmod 33$.

Hence the decryption results in the plaintext $m' = 5$, which is consistent with the original plaintext $m = 5$, and the verification is successful.

Question 2: Caesar cipher is a substitution encryption technique. Each letter is replaced by the last letter of the alphabet; for example, each letter is moved back by three places. Now, encrypt the plaintext “meet me after dark” using the Caesar cipher to find the ciphertext.

Answer:

First, convert the plaintext message to capital letters and remove the Spaces: “MEET ME AFTER DARK”.

Then, consider the alphabet as A system modulo 26 (A corresponds to 0, B corresponds to 1,...) Z corresponds to 25.

For each letter, move it backward by 3 places:

Table 1. System of Model 26

A→0	B→1	C→2	D→3	E→4	F→5	G→6
H→7	I→8	J→9	K→10	L→11	M→12	N→13
O→14	P→15	Q→16	R→17	S→18	T→19	U→20
V→21	W→22	X→23	Y→24	Z→25		

It can be calculated based on Table 1 above that the ciphertext is “PHHW PH DIWHU GDUN”.

Question 3: An affine cipher is a type of cipher replaced by a single table, which uses a linear function to encrypt letters. The encryption formula is: $E(x) = (ax + b) \bmod 26$, where a and 26 are coprime and b is an integer. Given that $a = 5$ and $b = 7$, encrypt the plaintext “HELLO” and obtain the corresponding decryption key.

Answer:

Convert plaintext to uppercase: “HELLO”.

The corresponding numbers of the alphabet: H(7), E(4), L(11), L(11), O(14).

Encryption process:

$E(H) = (5 \times 7 + 7) \bmod 26 = 42 \bmod 26 = 16 \rightarrow Q$

$E(E) = (5 \times 4 + 7) \bmod 26 = 27 \bmod 26 = 1 \rightarrow B$

$E(L) = (5 \times 11 + 7) \bmod 26 = 62 \bmod 26 = 8 \rightarrow I$

$E(L) = (5 \times 11 + 7) \bmod 26 = 8 \rightarrow I$

$E(O) = (5 \times 14 + 7) \bmod 26 = 77 \bmod 26 = 1 \rightarrow B$

Ciphertext is “QBIIB”.

Determination of the decryption key:

It is necessary to find the inverse of a , that is, to find a^{-1} such that $a \times a^{-1} \equiv 1 \bmod 26$.

Because $a = 5$, by attempting or extending the Euclidean algorithm, it is found that:

$$5 \times 21 = 105 \equiv 105 - 4 \times 26 = 105 - 104 = 1 \pmod{26},$$

Hence, $a^{-1} = 21$.

The decryption formula is $D(y) = 21(y - 7) \pmod{26}$.

The above three examples respectively demonstrate the application of discrete mathematics in different cryptosystems. Problem one involves knowledge such as modular operations, Euler's theorem, and the principle of the RSA encryption algorithm. Problem two is a Caesar cipher, involving simple modular operations, while Problem three, an affine cipher, uses linear functions and modular inversion operations. These steps demonstrate how to apply relevant discrete mathematics knowledge to perform encryption and decryption operations in cryptography.

3.2 Case-based teaching

The case-driven teaching method is adopted. Actual cryptography application scenarios are selected as teaching cases to guide students to apply the knowledge of discrete mathematics to solve practical problems. New exercises ranging from routine to challenging questions to enhance learning [7]. For instance, in the case of cryptography, students can be asked to design a digital signature scheme based on the discrete logarithm problem. Through practical operation and analysis, their understanding of the application of discrete mathematics knowledge in cryptography can be deepened. The following is a digital signature scheme based on the discrete logarithm problem. Case 1 is shown as follows:

Given a prime number p , a generator g (satisfying that the order of g is $p - 1$), and a certain power of g , $y = g^x \pmod{p}$, given y , g , and p , it is very difficult to calculate the exponent x . This difficult problem is the basis of many cryptographic schemes, including digital signatures.

Then, the following is the design of three steps for the digital signature scheme:

(1) Parameter initialization

Choose a large prime number p , for example, $p = 23$. In practical applications, the size of p is usually much larger than in this example to ensure security.

Select a generator G . Here, take $g = 5$ (its order under modulo 23 is 22, because $5^1 \pmod{23} = 5$, $5^2 \pmod{23} = 10$, $5^{22} \pmod{23} = 1$).

User A selects a private key x , for example, $x = 3$, and calculates the corresponding public key.

$$y = g^x \pmod{p} = 5^3 \pmod{23} = 10.$$

(2) Signature generation process

Suppose User A wants to sign the message m . First and foremost, perform hash processing on the message m . In practice, secure hash functions such as SHA-256 will be used. User A selects a random number k (k must be coprime with $p - 1$), for example, $k = 5$.

Calculate $r = g^k \pmod{p}$.

$$5^2 \pmod{23} = 25 \pmod{23} = 2, 5^4 = (5^2)^2 \pmod{23} = 2^2 \pmod{23} = 4,$$

$$5^5 = 5^4 \times 5 \pmod{23} = 4 \times 5 = 20 \pmod{23} = 20.$$

Hence, $r = 20$.

Calculate $s = k^{-1}(H(m) - x \cdot r) \pmod{p - 1}$. Here, $H(m)$ is the hash value of the message m (for simplicity, it is assumed that the message digest after hash is $H(m) = 8$).

First, calculate the modular inverse of k , $k^{-1} \pmod{p - 1}$. Since $p - 1 = 22$, find the inverse of 5 modulo 22, that is, it satisfies $5 \times d = 1 \pmod{22}$. Solving for d gives $d=9$ (since $5 \times 9 = 45$, $45 \pmod{22} = 1$).

By extending the Euclidean algorithm can find out $k^{-1} = 9$.

Substitute the numerical values $H(m) - x \times r = 8 - 3 \times 20 = 8 - 60 = -52$.

Because $-52 \pmod{22} = -52 + 3 \times 22 = -52 + 66 = 14$,

Hence, $s = 9 \times 14 \pmod{22} = 126 \pmod{22} = 16$, as a result, $s = 16$.

The output digital signature is $(r, s) = (20, 16)$. User A sends $(m, (r, s))$ to the validator.

(3) Signature verification process

The verifier uses the public key y , parameters p , g , and the received $(m, (r, s))$ to verify whether the signature is valid:

1) Inspection scope:

Ensure that $1 \leq r \leq p - 1$ and $0 < s < p - 1$. Because $r = 20$ (satisfying $1 \leq 20 \leq 22$), $s = 16$ (satisfying $0 < 16 < 22$), through.

2) Calculate the left value a : $a = y^r \times r^s \bmod p$.

Because $y = 10, r = 20, s = 16, p = 23$.

Calculate $10^{20} \bmod 23$:

$10^1 \bmod 23 = 10, 10^2 \bmod 23 = 8 \bmod 23, 10^4 \bmod 23 = 18 \bmod 23,$

$10^8 \bmod 23 = 2 \bmod 23, 10^{16} \bmod 23 = 4 \bmod 23, 10^{20} \bmod 23 = 3.$

Calculate $r^s = 20^{16} \bmod 23$. Similar:

$20^1 \bmod 23 = 20, 20^2 \bmod 23 = 9, 20^4 \bmod 23 = 12, 20^8 \bmod 23 = 6, 20^{16} \bmod 23 = 13.$

After that, $a = y^r \times r^s \bmod 23 = 3 \times 13 = 39 \bmod 23 = 16.$

3) Calculate the value b on the right side: $b = g^{H(m)} \bmod p$

Because $g = 5, H(m) = 8, p = 23$. Calculate $5^8 \bmod 23$:

$5^1 \bmod 23 = 5, 5^2 \bmod 23 = 2, 5^4 \bmod 23 = 4, 5^8 \bmod 23 = 16.$

Therefore $b = 16.$

4) Comparative verification:

If $a = b \bmod p$, then the signature is valid; Otherwise, it will be invalid. Because it is solved that $a = 16, b = 16$, and $16 \bmod 23 = 16$, hence $a = b \bmod 23$, the signature is valid.

In this digital signature scheme based on the discrete logarithm problem, through the actual calculation and verification process, it can be clearly seen that knowledge such as modular operations and the discrete logarithm problem in discrete mathematics is applied in cryptography. This practical operation and analysis help students deeply understand the important role that discrete mathematics plays in cryptography, such as the security and verification mechanism of digital signatures etc. If attackers want to forge signatures, they need to know the user's private key (x), which is equivalent to asking to solve the discrete logarithm problem. In this case, we demonstrated the generation and verification process of digital signatures through a simple example, enabling students to understand the practical application of the discrete logarithm problem in digital signatures. In practical applications, the selection of parameters (such as larger prime numbers (p)) will be made more cautiously to ensure higher security, and more complex hash functions will be used to handle messages.

This case enables students to conduct practical operations and analyses. Besides covering the basic knowledge of discrete mathematics, it provides readers with a broader perspective [8]. For example, by calculating the values in each step and understanding the guarantee of security provided by the discrete logarithm problem, the understanding of the application of discrete mathematics in cryptography can be deepened. Students can try to change the parameters, messages, or private keys, and re-sign and verify the process to further familiarize themselves with the entire mechanism.

4. Conclusion

This paper deeply explores the cornerstone role of discrete mathematics in cryptography education. By analyzing the integration of discrete mathematics in the discipline of cryptography, it reveals the importance of discrete mathematics in cultivating logical thinking, abstract thinking, and problem-solving abilities. Discrete mathematics provides core knowledge, such as algebraic system theory and number theory, for cryptography. The article proposes innovative teaching strategies, including interdisciplinary instructional design and case-based teaching, aiming to enhance the teaching effect of discrete mathematics and strengthen students' ability to apply knowledge in the field of cryptography. These strategies provide a new direction for the reform of discrete mathematics education, which is conducive to cultivating compound talents that meet the demands of the new era and promoting the digital transformation of education.

Funding

This paper is supported by the Guangzhou Huashang College 2024 Integrated Curriculum Project "Discrete Mathematics" (Project No.: HSRHKC2024126).

References

- [1] Zhijuan D. “Diversity” of discrete mathematics teaching research. *J Comput Educ.* 2021;(7):121-5.
- [2] Hailing W. Teaching Reform of Discrete Mathematics in Information Science Major in the Era of Big Data. *Comput Educ.* 2020;(7):66-9.
- [3] Dan S, Ying H, Zhengjun F, et al. Research and Practice of Smart Teaching Mode Based on Students’ Situation Data. *High Eng Educ Res.* 2022;(6):116-20.
- [4] Canglu Z, Xuexue Z. Exploration and Research on the Innovative Teaching Mode of Discrete Mathematics Course Based on Outcome-Oriented Approach. *Comput Knowl Technol.* 2021;21(3):118-20.
- [5] Wuhui C, Xiaocong Z. Teaching Exploration on the Integration of Programming Design and Discrete Mathematics Courses. *Comput Educ.* 2023;(3):76-80.
- [6] Zuowen T. Exploration of Practical Teaching of Discrete Mathematics Course “Case + Four-Level Experiment” under the Background of New Engineering. *Comput Educ.* 2024;(3):199-204.
- [7] Rosen KH. *Discrete Mathematics and Its Applications.* 8th ed. New York: McGraw-Hill Education; 2019.
- [8] Rosen KH, Michaels JG. *Modern Discrete Mathematics and Its Applications.* 3rd ed. Hoboken: Wiley; 2018.