

## Case- Code Plan

**Keywords:** group, inverse, code, cryptography, secret messages

**Theorem:**  $(\mathbb{Z}_n, +), (U(n), \cdot)$  are groups.

### Teaching Aim:

With the development of AI, coding become important and useful. Using the theorem of code in this chapter, science is very important. Students should study hard and work hard. Everyone give his modest contribution to the strength of the motherland.

### Case Teaching methodology

Cryptography is the study of sending and receiving secret messages. The aim of cryptography is to send messages across a channel so that only the intended recipient of the message can read it. In addition, when a message is received, the recipient usually requires some assurance that the message is authentic. It has not been sent by someone who is trying to deceive the recipient.

Modern cryptography is heavily dependent on abstract algebra and number theory. The message to be sent is called the plaintext message. The disguised message is called the ciphertext. The plaintext and the ciphertext are both written in an alphabet, consisting of letters or characters. Characters can include not only the familiar alphabetic characters A, . . . , Z and a, . . . , z but also digits, punctuation marks, and blanks. A cryptosystem, or cipher, has two parts: encryption, the process of transforming a plaintext message to a ciphertext message, and decryption, the reverse transformation of changing a ciphertext message into a plaintext message. There are many different families of cryptosystems, each distinguished by a particular encryption algorithm. Cryptosystems in a specified cryptographic family are distinguished from one another by a parameter to the encryption function called a key. A classical cryptosystem has a single key, which must be kept secret, known only to the sender and the receiver of the message. If person A wishes to send secret messages to two different people B and C, and does

not wish to have B understand C's messages or vice versa, A must use two separate keys, so one cryptosystem is used for exchanging messages with B, and another is used for exchanging messages with C.

In the process of learning, we need to constantly summarize and consolidate the original knowledge with new knowledge. In the study of mathematics, we should have the spirit of bravely climbing the peak of science. We should realize that mathematics is the basis of all scientific knowledge, and only by laying a solid foundation, we can go further and higher. We should pursue excellence, original problems. We should take solving frontier problems as learning objectives, and prepare for the construction of the motherland at all time.