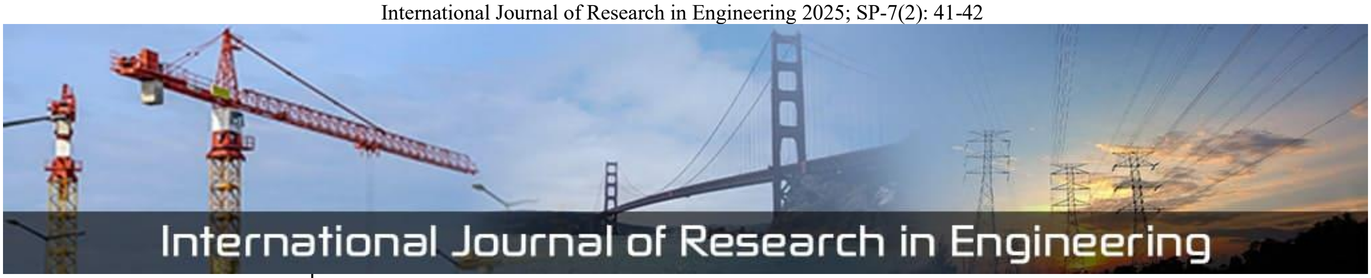

E-ISSN: 2664-8784
P-ISSN: 2664-8776
IJRE 2025; SP-7(2): 41-42
© 2025 IJRE
www.engineeringpaper.net
Received: 18-04-2025
Accepted: 20-05-2025

Prachi Mishra
Department of Mathematics
D.P.G Degree College,
Gurugram, Haryana, India

Two-Days National Conference on Multidisciplinary Approaches for Innovation and Sustainability: Global solution for contemporary Challenges-NCMIS (DPG Degree College: 17 th-18th 2025)

Significance of congruence in cryptographic process

Prachi Mishra

DOI: https://www.doi.org/10.33545/26648776.2025.v7.i2a.90

Abstract

Encryption and decryption are significant applications of cryptography, which allows data security by disrupting third-party access, and the key feature behind this is congruence, a modular arithmetic technique that codes text using a congruence function where alphabets in text get converted into numeral values according to their order in the alphabet and decodes back to the original text for the recipient. Computer science and number theory are two distinct disciplines that are combined in this study. The applicability of this approach to solve the linear congruences is demonstrated by a few sample instances.

This mathematical procedure has led to great usage in digital security, like website security, emails, confidential/sensitive data, online transactions, VPNs, and social platforms.

Keywords: Encryption, decryption, cryptography, congruence

Introduction

In the age of the internet and electronic commerce, the issue of privacy in electronic communication has become increasingly critical. With vast amounts of personal and sensitive information being transmitted and stored daily, organizations in both the public and commercial sectors face the challenge of safeguarding this data. This document explores the role of cryptography in securing electronic communications, detailing its mechanisms and the two primary systems of cryptography: private key and public key systems.

Understanding Cryptography

Cryptography is a vital field within Computer Science that focuses on making communications unintelligible to unauthorized parties. It employs processes such as encryption and decryption to protect sensitive information. By ensuring the confidentiality of data, cryptography not only safeguards personal information but also enhances the integrity and authenticity of the data being transmitted.

Private Key Cryptography

One of the two primary cryptographic systems is private key cryptography, also known as symmetric cryptography. In this system, both the sender and the receiver agree upon a secret key that is used for both encrypting and decrypting messages. The strength of this system lies in the secrecy of the key; if the key remains confidential, the communication can be considered secure. However, the challenge arises in the secure exchange of the key itself, as any interception could compromise the entire communication.

Encryption Example Using Modular Arithmetic

This document provides a detailed example of how to encrypt a word using a specific encryption function. The example illustrates the process step-by-step, demonstrating how to convert letters into numerical values, apply the encryption function, and then convert the results back into letters.

Encryption Process

To encrypt the word "WORK" using the encryption function $f(x) = (3x + 7) \bmod 26$, we first

Correspondence
Prachi Mishra
Department of Mathematics
D.P.G Degree College,
Gurugram, Haryana, India

need to assign numerical values to each letter based on their position in the alphabet, where A=0, B=1, C=2, Z=25.

Step 1: Assign Numerical Values

- W = 22
- = 14
- R = 17
- K = 10

Step 2: Apply the Encryption Function

Now, we will apply the function f(x) = (3x + 7) mod 26 to each numerical value:

- **For W (22):** [f (22) = (3times 22 + 7) mod 26 = (66 + 7) mod 26 = 73 mod 26 = 21]
- **For O (14):** [f (14) = (3times 14 + 7) mod 26 = (42 + 7) mod 26 = 49 mod 26 = 23]
- **For R (17):** [f (17) = (3times 17 + 7) mod 26 = (51 + 7) mod 26 = 58 mod 26 = 6]
- **For K (10):** [f (10) = (3 times 10 + 7) mod 26 = (30 + 7) mod 26 = 37 mod 26 = 11]

Step 3: Convert Back to Letters

Now, we convert the resulting numerical values back to letters:

- 21 corresponds to V
- 23 corresponds to X
- 6 corresponds to G
- 11 corresponds to L

Final Result

Thus, the encrypted form of the word "WORK" is "VXGL."

This example illustrates the process of encryption using a simple modular arithmetic function, showcasing how letters can be transformed into a different set of characters through mathematical operations. This process is called encryption.

Understanding Decryption

This part explores the concept of decryption by finding the inverse of an encrypted function

F (x) = (3x + 7) mod 26.

This is calculated by finding the modular inverse of 3 modulo 26, which is 9, and then applying it to the function which is named as Decryptive function

G (x) = (9x + 15) mod 26

We will illustrate how this function can be applied to decrypt a message, and we will also discuss the role of congruence in cryptography, highlighting its importance in ensuring the effectiveness and security of encryption schemes.

To decrypt a message using the inverse function (g(x) = (9x + 15) mod 26), we first need to apply the function to each letter of the encrypted text.

For example, to decrypt the text" VXGL" where "V' corresponds to the number 21. Using the decryption function, we calculate:

G (x) = (9(21) + 15) mod 26

Here, we substitute (x) with 21 (the numerical representation of "V")

G (21) = 9(21) + 15 = 189 + 15 = 204 mod 26

Calculating (204 mod 26) gives us a remainder of 22, which corresponds to the letter "W." This confirms that we have correctly decrypted the letter.

To decrypt the entire word "WORK," we would repeat this process for each letter, converting them to their respective numerical values, applying the function, and then converting back to letters.

Congruence plays a crucial role in cryptography by allowing mathematical operations to be performed within a finite set of integers. This is essential for the security of encryption schemes, as it ensures that operations remain predictable and manageable. By working within a limited range, cryptographic systems can effectively secure data against unauthorized access while maintaining the integrity of the information being transmitted.

Conclusion

In conclusion, understanding the decryption process and the role of congruence in cryptography is vital in the field of secure communications. The use of inverse functions, like (g(x)), exemplifies how mathematical principles underpin the security of encrypted messages, ensuring that only authorized parties can access the original information.

Applications in Cryptography

RSA: This popular public-key encryption technique mainly depends on congruence and modular arithmetic. It encrypts and decrypts communications using exponentiation modulo 'n' and large prime numbers.

Cipher: The word 'Cipher' means to write something in a secretive pattern which represent a set of letter. Congruence serves as a mathematical basis for encryption and decoding in a number of additional symmetric and asymmetric ciphers.

Hashing: A mapping is often called 'hashing'. Modular arithmetic and congruence are frequently used by hash functions, which map data to a specified range and generate a fixed-size output from an input.

References

1. Cuarto PM. Algebraic algorithm for solving linear congruences: its application to cryptography. Asia Pac J Educ Arts Sci. 2014;1(1):1-10.
2. Adams DG. Distinct solutions of linear congruences. Acta Arith. 2010;141(2):103-152.
3. Burger EB. Small solutions of linear congruence over number of fields. Rocky Mt J Math. 2006;26(3):875-888.
4. Frieze A, *et al.* Reconstructing truncated integer variables satisfying linear congruences. SIAM J Comput. 2006;17(2):262-280.
5. Cuarto PM. Algebraic algorithm for solving linear congruences: its application to cryptography. Asia Pacific Journal of Education, Arts and Sciences. 2014;1(1):34-37.