© JUN 2026 | IRE Journals | Volume 9 Issue 12 | ISSN: 2456-8880
DOI: https://doi.org/10.64388/IREV9I12-1718999

A Conceptual Framework for A Unified Rotational and Structural Cipher System

S. RAVICHANDRAN

Abstract- ***This paper presents a conceptual framework for a multi-layer cipher system that combines rotational substitution, alphanumeric transformation, situational signaling, reverse encoding, and adaptive key management. The proposed system originates from an exploratory study aimed at understanding how multiple simple encoding mechanisms can be combined to produce a more structured communication security framework. The framework consists of four principal components: (1) letter encryption and decryption using rotational keys, (2) numerical encryption with adaptive representations, (3) situational cipher symbols for communicating predefined conditions, and (4) key scheduling and rotation strategies including alternate key families and secret constants. The study does not claim cryptographic equivalence with modern standards such as AES or RSA. Instead, it proposes an experimental architecture for secure communication research and educational investigation. The framework is intended to stimulate discussion, criticism, and further analysis by researchers interested in classical and hybrid cryptographic approaches.***

Keywords: Rotational Cipher, Multi-layer Encryption, Structural Cipher, Situational Cipher, Key Rotation, Secret Constant, Communication Security.

I. INTRODUCTION

Secure communication has been a central objective throughout the history of cryptography. From classical substitution ciphers to modern mathematical cryptosystems, researchers have continuously attempted to improve confidentiality and resistance against unauthorized access.

This paper presents an exploratory cipher framework developed through iterative discussions and experimentation. The framework attempts to integrate:

- Alphabetical substitution
- Numerical encoding
- Reverse transformation
- Situational signaling
- Rotating keys
- Alternate key families
- Organizational key management

The primary objective is not to replace modern cryptographic systems but to investigate whether multiple lightweight encoding mechanisms can be unified into a single conceptual architecture.

II. LETTER ENCRYPTION AND DECRYPTION

The first layer of the framework employs a rotational substitution system.
Example:

Day 1
A → T
B → U
C → V
D → W
E → X

Day 2
A → S
B → T
C → U
D → V

The substitution mapping changes according to the selected key schedule.

The rotational sequence begins with a shift corresponding to 20 and decreases sequentially. When the sequence reaches a predefined lower bound, it wraps around and continues from 21, 22, 23, and so on until the completion of the cycle.

III. REVERSE ENCODING LAYER

© JUN 2026 | IRE Journals | Volume 9 Issue 12 | ISSN: 2456-8880
DOI: https://doi.org/10.64388/IREV9I12-1718999

To increase concealment, messages may optionally be reversed before encryption.
Example:
Original Message: ANAND
Reverse: DNANA
After applying the rotational cipher:
UGSEDS
The reverse operation may also be performed after encryption, depending on operational requirements.

IV. NUMERICAL ENCRYPTION

Example for Day 1:

1 → 210
2 → 220
3 → 230
4 → 240
0 → 000

Example:
2026
Encoded Form:
220000220260
The encoded message may optionally be reversed before transmission.

V. SITUATIONAL CIPHER

Apart from ordinary text, the framework defines a symbolic cipher for communicating operational conditions.

Day 1
X = Danger
XY = High Danger
XYZ = Out of Control

Day 2
A = Danger
AB = High Danger
ABC = Out of Control

The symbols rotate according to the selected key schedule.

VI. KEY ROTATION

The framework employs multiple key rotation strategies.

Possible key selectors include:
1. Day Number
2. Hour of Transmission
3. Sentence Count
4. Sentence Count + Day Number
5. Secret Constant

The selected key determines the substitution table used for encryption and decryption.

VII. SECRET CONSTANTS

A secret constant may be introduced as an additional parameter known only to authorized participants.

The secret constant:
- Is determined by the organization
- Is securely distributed
- Remains hidden from unauthorized users
- Participates in key selection

The objective is to introduce additional unpredictability into the encryption process.

VIII. ALTERNATE KEY FAMILIES

The system supports multiple independent key families.

Key Family A
A → 20
B → 21
C → 22
Key Family B
A → 27
B → 28
C → 29
Key Family C
A → 35
B → 36
C → 37

If one key family is suspected to be compromised, the organization may switch to an alternate family.

IX. KEY ARCHIVAL AND ORGANIZATIONAL MANAGEMENT

The framework assumes that:

- Encryption rules are determined by the organization.
- Authorized users possess complete operational knowledge.
- Historical keys are archived securely.
- Alternate key families are maintained as backups.
- Key replacement procedures are predefined.

Thus, the framework combines cipher mechanisms with organizational security practices.

X. SECURITY DISCUSSION

Strengths

- Multi-layer architecture
- Rotational substitution
- Alternate key families
- Situational signaling
- Reverse transformation
- Organizational key management
- Secret constants

Limitations

- Lack of formal mathematical proof
- Predictable rotation patterns
- Unknown resistance against statistical cryptanalysis
- No formal resistance against known-plaintext or chosen-plaintext attacks
- Requires further evaluation and computer simulation

XI. FUTURE WORK

Future research may explore:

- Randomized key schedules
- Non-linear substitutions
- Entropy analysis
- Statistical cryptanalysis
- Computer implementation
- Comparative studies with classical ciphers
- Formal mathematical security proofs

XII. CONCLUSION

This paper presents a conceptual framework for a Unified Rotational and Structural Cipher System.
The framework combines letter encryption, numerical encoding, situational signaling, reverse transformations, rotating keys, alternate key families, and organizational key management into a single architecture.

The present work is exploratory in nature and is intended to stimulate further discussion and research. Future investigations may determine the practical applicability and security characteristics of the proposed framework.