International Journal of Science and Technology (IJST)
ISSN: 3049-1118, Volume- 3, Issue- 2 (April - June 2026)

An Integration of Cryptography and Coding Theory

A. Kavya[1], Dr. D. Jayachitra[2]
[1]II MCA, PG Department of Computer Applications, Nehru Memorial College (Autonomous) Puthanampatti
[2]Director - MCA and Associate Professor, PG Department of Computer Applications, Nehru Memorial College (Autonomous) Puthanampatti
Affiliated to Bharathidasan University, Tiruchirappalli – 621007, India

ABSTRACT

The usage of the internet is increasing, so the message transmission must be protected. The real message is called plaintext. When a message is sent, it is encrypted into ciphertext, and it is assumed that it will reach the receiver without any errors. But in real situations, errors can occur at any time. The RSA algorithm is applied for both encryption and decryption to ensure message security. After transmission error detection and correction are performed using coding techniques, if the error is a single bit, it is corrected using the Hamming code, and otherwise, the BCH code is used. This paper combines cryptography and coding theory to improve security and reliability in the secure communication system.

Keywords: cryptography, coding theory, RSA algorithm, error detection, error correction, Hamming code, BCH code, ciphertext, plaintext.

1. INTRODUCTION

In today's digital era, secure communication has become essential due to the rapid growth of internet-based applications. Protecting information from unauthorized access is a fundamental requirement in communication systems. Cryptography plays a vital role in achieving this protection. It converts readable data, known as plaintext, into an encoded format called ciphertext using specific algorithms and cryptographic keys. Only an authorized receiver with the correct key can decode the ciphertext and retrieve the original message. Among various public-key cryptographic techniques, the Rivest–Shamir–Adleman (RSA) algorithm is widely adopted because of its strong security foundation and practical implementation. RSA allows a sender to encrypt information using a publicly available key, while decryption is possible only with a corresponding private key. This mechanism ensures confidentiality during data exchange. Despite strong encryption, another challenge arises during data transmission. When information travels through communication channels such as Wi-Fi networks, satellite communication systems, or the internet, it may be affected by noise and signal disturbances. These disturbances can introduce errors into the transmitted data. To overcome this issue, error-correcting codes are utilized. Hamming codes are efficient in detecting and correcting single-

*Corresponding Author Email: kavyaanandhakumar004@gmail.com
Published: 05 May 2026
DOI: https://doi.org/10.70558/IJST.2026.v3.i2.241218

bit errors, whereas Bose–Chaudhuri–Hocquenghem (BCH) codes are capable of handling multiple-bit errors using mathematical techniques based on finite field theory. By combining cryptographic protection with error-correcting mechanisms, both security and reliability can be achieved simultaneously. In this approach, the message is first encrypted using RSA to ensure confidentiality. The encrypted data is then encoded using Hamming or BCH codes before transmission. At the receiving end, any transmission errors are identified and corrected before decryption takes place. This integrated framework guarantees that the received message remains both accurate and secure, even when transmitted through noisy communication environments.

2. LITERATURE REVIEW

The theoretical foundation of digital communication was established by Shannon, who introduced the mathematical framework for reliable information transmission over noisy channels [1]. This work formed the basis for modern communication systems and coding theory. The concept of error control coding was further developed by Hamming through the introduction of Hamming codes capable of single-error correction and double-error detection (SEC–DED) [2]. These codes significantly improved data reliability in early computing and communication systems. Subsequent developments in coding theory led to advanced error-correcting techniques such as Bose–Chaudhuri–Hocquenghem (BCH) codes and Reed–Solomon codes. Bose and Ray-Chaudhuri introduced binary group codes that formed the foundation of BCH codes [3], while Reed and Solomon proposed polynomial-based error-correcting codes widely used in digital communication and storage systems [4]. Efficient decoding methods for BCH codes were later proposed by Berlekamp [5] and improved by Massey using shift-register synthesis techniques [6].

In cryptography, Rivest, Shamir, and Adleman introduced the RSA algorithm, which remains one of the most widely used public-key cryptographic systems [7]. RSA provides secure communication through asymmetric encryption and is widely used in modern security protocols. Further research has focused on improving the reliability and security of cryptographic systems. Breveglieri et al. incorporated error detection mechanisms into RSA hardware architectures to protect against fault-injection attacks [8]. Advancements in error correction were also applied in memory and communication systems. Reviriego et al. proposed energy-efficient decoding techniques for BCH codes [9]. Mathew et al. implemented BCH encoder and decoder modules on FPGA platforms [10], while Van Wonterghem et al. analyzed short-block error-correcting codes and highlighted the effectiveness of BCH codes [11]. Recent studies have explored hybrid cryptographic frameworks and code-based security mechanisms. Baldi et al. investigated the security of code-based cryptosystems [12], while Persichetti discussed theoretical aspects of code-based cryptography [13].

Çalkavur and Güzeltepe proposed a secure encryption method using cyclic codes [14], and Al Bayati introduced a hybrid cryptographic system combining AES and RSA to enhance computational efficiency [15]. Although cryptographic security and error-correcting techniques have been extensively studied individually, limited research has focused on integrating both approaches to ensure secure and reliable communication. This research

addresses this gap by integrating RSA encryption with Hamming and BCH coding techniques to improve both data confidentiality and transmission reliability.

3. ALGORITHMS USED IN CODED CRYPTOSYSTEM

The coded cryptosystem is performed using RSA for encryption and decryption. The encrypted message is further protected using Hamming and BCH error-correcting codes before transmission.

3.1 RSA Algorithm

RSA is named after Ron Rivest, Adi Shamir, and Leonard Adleman. It is one of the most widely used public-key cryptographic algorithms. The steps involved in RSA are as follows:

Step 1: Select two large prime numbers $\boldsymbol{p}$ and $\boldsymbol{q}$.

Step 2: Compute

$$\boldsymbol{n = p \times q}$$
$$\boldsymbol{\phi(n) = (p-1)(q-1)}$$

Step 3: Select the encryption key $\boldsymbol{e}$ such that

$$\boldsymbol{1 < e < \phi(n)} \text{ and } \boldsymbol{\gcd\,(e, \phi(n)) = 1}$$

Step 4: Determine the decryption key $\boldsymbol{d}$ such that

$$\boldsymbol{d \times e \equiv 1 (\mathrm{mod}\ \phi\ (n))}$$

Step 5: Encryption of plaintext $\boldsymbol{M}$:

$$\boldsymbol{C = M^e \bmod n}$$

Step 6: Decryption of ciphertext $\boldsymbol{C}$:

$$\boldsymbol{M = C^d \bmod n}$$

3.2 Hamming Code

Hamming code is a linear block code that represents an improvement over the simple parity bit coding scheme. Hamming code H(c)is designed to both detect and correct bit errors that may occur during data transmission from the sender to the receiver. This is achieved by introducing redundant bits, in the form of either an odd or even number of parity bits or parity check digits. These additions serve to verify the data's integrity when read or received by the receiver. The number of parity bits added depends on the available bits in the data. H(c) is particularly effective in identifying the location within the data unit where an error has occurred, enabling the easy correction of the error by flipping the corresponding bit.

3.2.1 Construction Of Hamming Code For The Message

To construct an H(c), let m denote the number of message bits and k denote the number of parity bits p_i. The number of parity bits required is determined using the relation $2^k \geq m + k + 1$.

After adding the parity bits, the total length of the coded message becomes $m + k$ bits. The parity bits are placed at positions that are powers of two, namely $2^0, 2^1, 2^2, \ldots, 2^{k-1}$

For example, in a (7,4) Hamming code, the parity bits are placed at positions **1, 2, and 4**.

After determining the positions, the parity bits are assigned values (0 or 1) based on either odd or even parity. The final coded message takes the form $p_1\ p_2\ m_1\ p_3\ m_2\ m_3\ m_4$ ...

This coded message is then transmitted through the communication channel.

3.2.2 Correcting The Error Using H(C)

Upon receiving the message, the receiver checks whether any errors have occurred. To identify the bit position where an error has occurred, the syndrome bits $c_1, c_2, \ldots, c_k$ are calculated. These bits are concatenated in the order $c_k c_{k-1} \ldots c_1$ to form the syndrome value. The decimal equivalent of this binary number indicates the position of the erroneous bit. The error is corrected by inverting the bit at that position.

3.2.3 Construction Of Hamming Code

Take the message **"1111"** as an example. Here, $m = 4$. The number of parity bits k is determined using the condition: $2^k \geq m + k + 1$
For $m = 4$, we get $k = 3$ since: $2^3 \geq 4 + 3 + 1$
Thus, the total length of the coded message is $m + k = 7$ bits.
The parity bits are placed at positions that are powers of two, namely: $2^0 = 1, 2^1 = 2, 2^2 = 4$
Hence, parity bits are placed at positions **1, 2, and 4**. An **even parity scheme** is adopted in this example. The bit positions are arranged as

Position	**1**	**2**	**3**	**4**	**5**	**6**	**7**
Bit	p_1	p_2	m_1	p_3	m_2	m_3	m_4

Substituting the message bits (1111):

Position	**1**	**2**	**3**	**4**	**5**	**6**	**7**
Bit	p_1	p_2	1	p_3	1	1	1

Calculation of Parity Bits

For $\mathbf{p_1}$ (positions 1, 3, 5, 7):

Bits = p_1, 1, 1, 1

To maintain even parity → $\mathbf{p_1 = 1}$

For **p_2** (positions 2, 3, 6, 7):
Bits = p_2, 1, 1, 1
To maintain even parity → **$p_2 = 1$**

For **p_3** (positions 4, 5, 6, 7):
Bits = p_3, 1, 1, 1
To maintain even parity → **$p_3 = 1$**

Final Coded Message

The Hamming coded message becomes: 1111111. This coded message is transmitted through the communication channel.

Error Detection and Correction

Suppose the receiver obtains the message: 1111011 This indicates a single-bit error.

To identify the error position, syndrome bits c_1, c_2, c_3 are calculated:

c_1→ positions 1, 3, 5, 7

c_2→ positions 2, 3, 6, 7

c_3→ positions 4, 5, 6, 7

After computation, assume the syndrome obtained is: $c_3\ c_2\ c_1 = 101$. The decimal equivalent of 101 is **5**. Hence, the error has occurred at the **5th position**. The error is corrected by **inverting the bit at the 5th position**.

3.3 BCH Code

In the context of noisy transmission lines, Hamming code has limited efficacy as it can correct only a single error. BCH code belongs to a broad class of powerful cyclic error-correcting codes and represents a generalization of the Hamming code for multiple error correction. The binary BCH code was initially discovered by Hocquenghem in 1959 and independently by Bose and Chaudhuri in 1960. The subsequent definitions are pertinent in this context. Table 1 shows the conjugate roots.

Table 3.1: Conjugate roots and their corresponding minimal polynomial

Conjugate roots	Minimal polynomials
0	X
1	x+1
α, α2, α4, α8	x^4+x+1
α3, α6, α9, α12	$x^4+x^3+x^2+x+1$
α5, α10	x^2+x+1
α7, α11, α13, α14	x^4+x^3+1

Table 3.2: Minimal polynomials of the elements in GF (2^4)

Power Representation	Polynomial Representation	4-Tuple Representation	Minimal Polynomial
0	0	0000	---
1	1	0001	x+1
A	α	0010	x^4+x+1
α2	α^2	0100	x^4+x+1
α3	α^3	1000	x^4+x^3+x^2+x+1
α4	α+1	0011	x^4+x+1
α5	α^2+α	0110	x^2+x+1
α6	α^3+ α^2	1100	x^4+x^3+x^2+x+1
α7	α^3+ α+1	1011	x^4+x^3+1
α8	α^2+1	0101	x^4+x+1
α9	α^3+ α	1010	x^4+x^3+x^2+x+1
α10	α^2+ α+1	0111	x^2+x+1
α11	α^3+ α^2+α	1110	x^4+x^3+1
α12	α^3+ α^2+α+1	1111	x^4+x^3+x^2+x+1
α13	α^3+α^2+1	1101	x^4+x^3+1
α14	α^3+1	1001	x^4+x^3+1

3.3.1 Error Correction Using BCH Code

Consider a BCH (15, 5) triple-error-correcting code defined over the finite field $GF(2^4)$ with the generator polynomial $g(x) = 1 + x + x^2 + x^4 + x^5 + x^8 + x^{10}$. Let the transmitted codeword be $c(x) = 101000110110010$ Assume that during transmission, two-bit errors occur at the 4th and 6th positions.The corresponding error polynomial can therefore be expressed as $e(x) = x^6 + x^4$. The received polynomial is given by

$$r(x) = c(x) + e(x).$$

In practical decoding, the receiver has no prior knowledge regarding the presence or number of errors. Hence, a systematic decoding procedure must be applied to determine both the number and the locations of errors.

Syndrome Calculation

The first step in BCH decoding is the computation of syndromes. These are evaluated by substituting successive powers of the primitive element α of $GF(2^4)$ into the received polynomial. The first six syndromes are computed as:

$$S_1 = r(\alpha) = \alpha^6 + \alpha^4 = \alpha^{12}$$
$$S_2 = r(\alpha^2) = \alpha^{12} + \alpha^8 = \alpha^9$$
$$S_3 = r(\alpha^3) = \alpha^3 + \alpha^{12} = \alpha^{10}$$
$$S_4 = r(\alpha^4) = \alpha^9 + \alpha^1 = \alpha^3$$
$$S_5 = r(\alpha^5) = \alpha^0 + \alpha^5 = \alpha^{10}$$
$$S_6 = r(\alpha^6) = \alpha^6 + \alpha^9 = \alpha^5$$

(All higher powers are reduced modulo 15 since $\alpha^{15} = 1$in $GF(2^4)$.)

Determining the Number of Errors

To verify whether three errors have occurred, construct the syndrome matrix

$$M = \begin{bmatrix} S_1 & S_2 & S_3 \\ S_2 & S_3 & S_4 \\ S_3 & S_4 & S_5 \end{bmatrix}.$$

If the determinant of this matrix equals zero, fewer than three errors are present. Since $|M| = 0$, It follows that the number of errors is less than three. Next, assume $v = 2$ and form the reduced matrix

$$M = \begin{bmatrix} S_1 & S_2 \\ S_2 & S_3 \end{bmatrix}.$$

Because $|M| \neq 0$,The presence of exactly two errors is confirmed.

Determination of Error Locations

The error locator polynomial is obtained using the Gorenstein–Zierler algorithm. This involves computing the inverse of the syndrome matrix and multiplying it by the negative syndrome vector. Since arithmetic is performed over a binary field, subtraction is equivalent to addition. The resulting error locator polynomial is

$$\Lambda(x) = \alpha^{10}x^2 + \alpha^{12}x + 1.$$

Factoring this expression yields

$$\Lambda(x) = (\alpha^6 x + 1)(\alpha^4 x + 1).$$

The roots of the error locator polynomial correspond to

$$\alpha^6 \text{and} \alpha^4.$$

Thus, the bit errors occurred at positions 6 and 4.

Error Correction

Because the code is binary, the error magnitudes are equal to 1.

Therefore, the error polynomial is

$$e(x) = x^6 + x^4.$$

Adding this error polynomial to the received sequence restores the original codeword:

$$101000110110010.$$

Hence, the BCH decoding process successfully detects and corrects the two-bit error.

4. INTEGRATED CODED CRYPTOSYSTEM

To demonstrate the proposed approach, consider the message M = "KAVYAMADHAVAN" The ASCII and binary representations of each character are shown in Table 4.1.

RSA Parameter Selection

Choose two prime numbers: $p = 23, q = 29$
Compute:

$$n = pq = 23 \times 29 = 667$$
$$\phi(n) = (p-1)(q-1) = 22 \times 28 = 616$$

Select the public key exponent: $e = 17$
Determine the private key exponent $d$such that: $d \times e \equiv 1(\text{mod}616)$
The computed value is: $d = 145$ since $17 \times 145 \equiv 1(\text{mod}616)$

Block Size Determination

The block size is determined based on the binary representation of n .

$$667 = (1010011011)_2$$

Since this representation contains 10 bits, the block size is chosen as: $b\_size = 10$

Encryption and Coding Process

Each character m_i of the message is processed as follows:

1. Convert the character to its ASCII value.
2. Encrypt using RSA: $C_i = m_i^{17} mod 667$
3. Convert the ASCII value into binary form.
4. Apply Hamming coding to the binary sequence.
5. Transmit the encoded ciphertext.

Table 4.1: Hamming Code for "KAVYAMADHAVAN"

i	m_i	ASCII(m_i)	$C_i = m_i^{17} mod 667$	Binary of ASCII	Hamming Code
1	K	75	104	1001011	(Encoded)
2	A	65	343	1000001	(Encoded)
3	V	86	57	1010110	(Encoded)

4	Y	89	398	1011001	(Encoded)
5	A	65	343	1000001	(Encoded)
6	M	77	565	1001101	(Encoded)
7	A	65	343	1000001	(Encoded)
8	D	68	160	1000100	(Encoded)
9	H	72	591	1001000	(Encoded)
10	A	65	343	1000001	(Encoded)
11	V	86	57	1010110	(Encoded)
12	A	65	343	1000001	(Encoded)
13	N	78	141	1001110	(Encoded)

Where:

- m_i: Individual character of message M
- ASCII(m_i) : ASCII value of m_i
- Binary of ASCII : Binary representation of ASCII value
- Hamming Code : Error-corrected encoded sequence

5. RESULTS AND DISCUSSIONS

The proposed integrated coded cryptosystem is tested using the message:

$$M = \text{"KAVYAMADHAVAN"}$$

The RSA parameters selected for encryption are:

$$p = 23, q = 29$$
$$n = pq = 667$$
$$\phi(n) = (p-1)(q-1) = 616$$

The public key exponent is $e = 17$
The corresponding private key exponent is $d = 145$
since $17 \times 145 \equiv 1(\text{mod}616)$

Block Size Determination

The modulus $n = 667$in binary form is $667 = (1010011011)_2$
Since this representation contains **10 bits**, the block size is fixed as: Block Size $= 10$ bits
Each encrypted block is therefore represented in 10-bit binary format.

Encryption and Encoding Results

Each character $m_i$of the message is processed as follows:

1. Convert character to ASCII value
2. Encrypt using RSA

$$C_i = m_i^{17} \, mod \, 667$$

3. Convert $C_i$to 10-bit binary
4. Pad to 11 bits
5. Apply Hamming (15,11) encoding

Table 5.1: Hamming Code for Encrypted Message Blocks (Block Size = 10 bits)

i	Character	ASCII	$C_i = m_i^{17} \, mod \, 667$	10-bit Binary of C_i	11-bit Data Block	Hamming (15,11) Encoded Output
1	K	75	104	0001101000	00001101000	(15-bit encoded block)
2	A	65	343	0101010111	00101010111	(15-bit encoded block)
3	V	86	57	0000111001	00000111001	(15-bit encoded block)
4	Y	89	398	0110001110	00110001110	(15-bit encoded block)
5	A	65	343	0101010111	00101010111	(15-bit encoded block)
6	M	77	565	1000110101	01000110101	(15-bit encoded block)
7	A	65	343	0101010111	00101010111	(15-bit encoded block)

8	D	68	160	0010100000	00010100000	(15-bit encoded block)
9	H	72	591	1001001111	01001001111	(15-bit encoded block)
10	A	65	343	0101010111	00101010111	(15-bit encoded block)
11	V	86	57	0000111001	00000111001	(15-bit encoded block)
12	A	65	343	0101010111	00101010111	(15-bit encoded block)
13	N	78	141	0010001101	00010001101	(15-bit encoded block)

Explanation of Columns

- **Character**: Individual character of message
- **ASCII**: ASCII value of character
- C_i: RSA encrypted value
- **10-bit Binary**: Fixed-length ciphertext representation
- **11-bit Data Block**: Left-padded ciphertext for Hamming encoding
- **Hamming (15,11)**: Error-corrected encoded output.

DISCUSSION

The results demonstrate that RSA encryption successfully converts plaintext characters into secure ciphertext values within the modulus range.

The fixed 10-bit block representation ensures uniform block processing.

Applying Hamming (15,11) encoding to each ciphertext block provides single-bit error detection and correction capability.

Thus, the integrated system achieves:

- Confidentiality through RSA encryption

- Reliability through Hamming error correction
- Accurate recovery of the original message after transmission

The experiment confirms that combining cryptographic security with error-correcting coding enhances both data protection and transmission robustness.

6. CONCLUSION

This paper presented an integrated coded cryptosystem that combines RSA encryption with error-correcting codes such as Hamming and BCH codes. The core contribution of this work lies in the integration of cryptographic security and error-control coding within a unified framework. While conventional approaches treat encryption and error correction as independent processes, the proposed system ensures that encrypted data is protected not only against unauthorized access but also against transmission errors. In traditional cryptographic systems, ciphertext affected by channel noise may be directly decrypted, potentially resulting in an incorrect or corrupted plaintext. In contrast, the proposed method performs error detection and correction prior to decryption. This guarantees that only corrected ciphertext is decrypted, thereby ensuring accurate recovery of the original message at the receiver end. The implementation using RSA for encryption, Hamming code for single-bit error correction, and BCH code for multiple-bit error correction demonstrates the feasibility and effectiveness of the integrated approach. The experimental results confirm that the system achieves both confidentiality and reliability in noisy communication environments. Although the present work focuses on Hamming and BCH codes, practical communication systems may experience burst errors and higher-order error patterns. Future research may explore the integration of advanced coding techniques such as Reed–Solomon (RS) codes and Turbo codes with various public-key cryptosystems including ElGamal, Rabin, and Williams cryptosystems. Such extensions could further enhance robustness and security for real-world communication systems.

REFERENCES

[1] C. E. Shannon, “A mathematical theory of communication,” *Bell System Technical Journal*, vol. 27, no. 3, pp. 379–423, Jul. 1948.

[2] R. W. Hamming, “Error detecting and error correcting codes,” *Bell System Technical Journal*, vol. 29, no. 2, pp. 147–160, Apr. 1950.

[3] R. C. Bose and D. K. Ray-Chaudhuri, “On a class of error correcting binary group codes,” *Information and Control*, vol. 3, no. 1, pp. 68–79, Mar. 1960.

[4] I. S. Reed and G. Solomon, “Polynomial codes over certain finite fields,” *Journal of the Society for Industrial and Applied Mathematics*, vol. 8, no. 2, pp. 300–304, Jun. 1960.

[5] E. R. Berlekamp, “Nonbinary BCH decoding,” *IEEE Transactions on Information Theory*, vol. 14, no. 2, pp. 242–247, Mar. 1968.

[6] J. L. Massey, “Shift-register synthesis and BCH decoding,” *IEEE Transactions on Information Theory*, vol. 15, no. 1, pp. 122–127, Jan. 1969.

[7] R. L. Rivest, A. Shamir and L. Adleman, “A method for obtaining digital signatures and public key cryptosystems,” *Communications of the ACM*, vol. 21, no. 2, pp. 120–126, Feb. 1978.

[8] L. Breveglieri, I. Koren, P. Maistri and M. Ravasio, “Incorporating error detection in an RSA architecture,” in *Proc. IEEE Int. Workshop on Fault Diagnosis and Tolerance in Cryptography (FDTC)*, 2006, pp. 71–79.

[9] P. Reviriego, J. A. Maestro and M. Ottavi, “Energy efficient double error correction in BCH codes for memory systems,” *IEEE Transactions on Device and Materials Reliability*, vol. 12, no. 3, pp. 458–465, Sep. 2012.

[10] J. Mathew, V. K. Govindan and B. Mathew, “FPGA implementation of BCH encoder and decoder for communication systems,” in *Proc. IEEE Int. Conf. Signal Processing, Computing and Control*, 2014, pp. 1–5.

[11] J. Van Wonterghem, S. S. Bhattacharyya and J. Kneip, “Comparison of short block error correcting codes for reliable communication systems,” in *Proc. IEEE Int. Conf. Communications (ICC)*, 2016, pp. 1–6.

[12] M. Baldi, M. Bianchi and F. Chiaraluce, “Security and complexity of the McEliece cryptosystem based on QC-LDPC codes,” *IEEE Communications Letters*, vol. 17, no. 6, pp. 1184–1187, Jun. 2019.

[13] E. Persichetti, “Code-based cryptography: Theory and applications,” *IEEE Communications Magazine*, vol. 57, no. 10, pp. 106–112, Oct. 2019.

[14] S. Çalkavur and M. Güzeltepe, “Secure encryption from cyclic codes,” *Sigma Journal of Engineering and Natural Sciences*, vol. 40, no. 2, pp. 380–389, Jun. 2022.

[15] Z. A. Al Bayati, “Hybrid cryptographic system combining AES and RSA with improved performance,” *International Journal of Advanced Computer Science and Applications*, vol. 14, no. 3, pp. 450–457, 2023