Department of Electrical & Electronics Engineering

Communication Systems – Vth Semester

Internal Assessment 4

Report

on

Secure Communication System with Direct Sequence Spread Spectrum and XOR-based Encryption

(MATLAB Simulation and Performance Analysis)

Submitted by

Name	**Reg No**	**Semester & Section**
Manikanta Gonugondla	230906450	V SEM, E
Chakrala Srinivas	230906422	V SEM, E
Joel Antony	230906418	V SEM, E
Karan Kumar	230906008	V SEM, E

Department of Electrical and Electronics Engineering

Manipal Institute of Technology, Manipal

Aug - Dec 2025

Contents

1 Abstract / Description about the Work

This project presents the design, simulation, and comprehensive performance analysis of a secure communication system that integrates Direct Sequence Spread Spectrum (DSSS) modulation with XOR-based symmetric encryption. The primary objective is to demonstrate how combining spread spectrum techniques with cryptographic methods can achieve robust, secure, and jamming-resistant wireless communication.

The implemented system addresses three critical aspects of modern secure communications: confidentiality through XOR-based encryption with pseudo-random key streams, anti-jamming using DSSS with a spreading factor of 31 chips/bit, and noise resistance demonstrating superior BER performance under AWGN channel conditions.

The MATLAB simulation environment was utilized to model the complete communication chain from message generation through channel transmission to reception and decryption. Performance metrics including Bit Error Rate (BER) versus Signal-to-Noise Ratio (SNR) were evaluated across four distinct scenarios: uncoded transmission, DSSS-only, DSSS with encryption, and DSSS with encryption under jamming conditions.

Results demonstrate that the proposed system achieves a processing gain of approximately 14.91 dB, significantly improving communication reliability in hostile environments. The integration of encryption adds negligible overhead while ensuring data confidentiality. Under narrowband jamming attacks, the system maintains acceptable BER performance due to the inherent interference suppression capabilities of spread spectrum.

This work aligns with Course Outcomes CO3 (digital communication generation and detection) and CO5 (wireless communication systems, spread spectrum, and encryption) as outlined in the ELE 3126 course plan.

2 Background Theory

2.1 Direct Sequence Spread Spectrum (DSSS)

Direct Sequence Spread Spectrum is a modulation technique where the transmitted signal is spread over a much wider bandwidth than the minimum required bandwidth. This is achieved by multiplying the original data signal with a high-rate Pseudo-Noise (PN) sequence.

Key Principles:

Each data bit is multiplied by a PN sequence of length L (spreading factor). The chip rate becomes $R_c = L \times R_b$, where R_b is the bit rate. The processing gain is calculated as $G_p = 10 \log_{10}(L)$ dB. At the receiver, correlation with the same PN sequence despreads the signal.

Mathematical Formulation:

Let $d(t)$ be the data signal and $c(t)$ be the PN sequence. The transmitted DSSS signal is:

$$s(t) = d(t) \cdot c(t) \tag{1}$$

The received signal after passing through an AWGN channel is:

$$r(t) = s(t) + n(t) = d(t) \cdot c(t) + n(t) \tag{2}$$

At the receiver, despreading is performed:

$$r(t) \cdot c(t) = d(t) \cdot c(t) \cdot c(t) + n(t) \cdot c(t) = d(t) + n'(t) \tag{3}$$

Since $c(t) \cdot c(t) = 1$ for properly synchronized PN sequences, the data is recovered while noise remains spread.

Advantages of DSSS:

Interference rejection is achieved as narrowband interference is spread during despreading. Intentional jamming signals are suppressed providing anti-jamming capability. The signal appears as noise to unauthorized receivers providing low probability of intercept. Different users can share the same frequency band with different codes enabling multiple access.

2.2 Pseudo-Noise (PN) Sequences

PN sequences are deterministic binary sequences that exhibit noise-like properties. Key characteristics include balance property where the number of +1s and -1s differ by at most one, sharp autocorrelation peak at zero lag with low values elsewhere, and proper distribution of runs of consecutive identical bits.

The autocorrelation function is defined as:

$$R_{cc}(\tau) = \frac{1}{L} \sum_{i=0}^{L-1} c_i \cdot c_{(i+\tau) \mod L} \tag{4}$$

For an ideal PN sequence:

$$R_{cc}(\tau) = \begin{cases} 1 & \tau = 0 \\ -\frac{1}{L} & \tau \neq 0 \end{cases} \tag{5}$$

2.3 XOR-based Encryption

The XOR (Exclusive OR) cipher is a symmetric encryption technique where the plaintext is combined with a key stream using the XOR operation.

Encryption Process:

$$C_i = M_i \oplus K_i \tag{6}$$

Decryption Process:

$$M_i = C_i \oplus K_i \tag{7}$$

where M_i is the i-th message bit, C_i is the i-th ciphertext bit, K_i is the i-th key stream bit, and $\oplus$ represents the XOR operation.

The cipher is symmetric using the same key for encryption and decryption. It is self-inverse meaning $(M \oplus K) \oplus K = M$. The operation is efficient requiring only a single operation per bit. Security depends on key randomness and key length.

In this implementation, a pseudo-random key stream is generated from a hash of the encryption key string, ensuring reproducibility while maintaining security for authorized users.

2.4 AWGN Channel Model

The Additive White Gaussian Noise channel is a fundamental model in communication theory represented as:

$$r(t) = s(t) + n(t) \tag{8}$$

where $n(t) \sim \mathcal{N}(0, \sigma^2)$ is Gaussian noise with zero mean and variance σ^2.

The Signal-to-Noise Ratio (SNR) is defined as:

$$\text{SNR} = \frac{E_b}{N_0} = \frac{\text{Energy per bit}}{\text{Noise power spectral density}} \tag{9}$$

2.5 Bit Error Rate (BER)

BER is the fundamental performance metric defined as:

$$\text{BER} = \frac{\text{Number of bit errors}}{\text{Total number of bits transmitted}} \tag{10}$$

For BPSK modulation in AWGN, the theoretical BER is:

$$P_e = Q\left(\sqrt{\frac{2E_b}{N_0}}\right) \tag{11}$$

where $Q(x) = \frac{1}{\sqrt{2\pi}} \int_x^\infty e^{-t^2/2} dt$ is the Q-function.

3 Methodology with Block Diagram

3.1 System Overview

The secure communication system consists of three main stages: transmission, channel, and reception.

3.2 Transmitter Chain

Step 1: Message Generation

Generate random binary message of length N bits where message bits $m \in \{0, 1\}^N$.

Step 2: Encryption

Generate pseudo-random key stream from encryption key. Apply XOR operation: $e_i = m_i \oplus k_i$. Output encrypted message e.

Step 3: DSSS Spreading

Convert encrypted bits to bipolar format: $b_i = 2e_i - 1$. Generate PN sequence of length L: $c = \{c_1, c_2, ..., c_L\}$. Spread each bit by $s_{i,j} = b_i \cdot c_j$ for $j = 1$ to L. Output spread signal of length $N \times L$ chips.

3.3 Channel

AWGN Addition:

Calculate noise power as $\sigma^2 = \frac{P_{\text{signal}}}{10^{(E_b/N_0)/10}}$. Add Gaussian noise: $r = s + n$, where $n \sim \mathcal{N}(0, \sigma^2)$.

Optional Jamming:

Generate narrowband jamming signal: $j(t) = A_j \sin(2\pi f_j t)$. Add to channel: $r = s + n + j$.

3.4 Receiver Chain

Step 1: DSSS Despreading

For each bit period, extract L chips: $r_i = \{r_{(i-1)L+1}, ..., r_{iL}\}$. Correlate with PN sequence: $z_i = \sum_{j=1}^{L} r_{i,j} \cdot c_j$. Decision: $\hat{b}_i = 1$ if $z_i > 0$, else $\hat{b}_i = 0$.

Step 2: Decryption

Regenerate the same key stream using the encryption key. Apply XOR operation: $\hat{m}_i = \hat{e}_i \oplus k_i$. Output recovered message $\hat{m}$.

Step 3: BER Calculation

Compare received bits with original: BER $= \frac{1}{N} \sum_{i=1}^{N} |\hat{m}_i - m_i|$.

3.5 Simulation Parameters

The following parameters were used in the MATLAB simulation:

Table 1: Simulation Parameters

Parameter	Value
Message Length	100 bits
Spreading Factor (L)	31 chips/bit
PN Seed	13
Encryption Key	”SecureKey2025”
E_b/N_0 Range	-10 to 20 dB (step 2 dB)
Jamming Power	10 dB (when enabled)
Jamming Frequency	0.1 (normalized)
Processing Gain	14.91 dB

4 Design: Flowchart

The implementation follows a modular design with separate functions for each operation.

Main Simulation Steps:

1. Initialize simulation parameters

2. Generate random binary message (100 bits)
3. If encryption enabled: Generate key stream and perform XOR encryption
4. Generate PN sequence (31 chips)
5. Perform DSSS spreading
6. For each SNR value from -10 dB to 20 dB:
    (a) Calculate noise power
    (b) Add AWGN to spread signal
    (c) If jamming enabled: Add jamming signal
    (d) Perform DSSS despreading via correlation
    (e) Perform XOR decryption
    (f) Calculate BER
    (g) Store results
7. Save simulation results to file
8. Generate and save performance plots

DSSS Transmitter Algorithm:

Input data bits and PN sequence. Convert bits to bipolar (-1, +1). For each bit, multiply with entire PN sequence. Concatenate spread chips. Output spread signal.

DSSS Receiver Algorithm:

Input received signal and PN sequence. For each bit period, extract L chips and compute correlation with PN sequence. If correlation is positive, decide bit = 1, else decide bit = 0. Output recovered bits.

Encryption/Decryption Algorithm:

Input message bits and encryption key. Compute hash of key string and use as RNG seed. Generate pseudo-random key stream. XOR message with key stream. Output encrypted or decrypted bits.

5 Simulation and Implementation Results

5.1 BER Performance Analysis

Figure 1 presents the BER versus E_b/N_0 performance comparison across four scenarios:

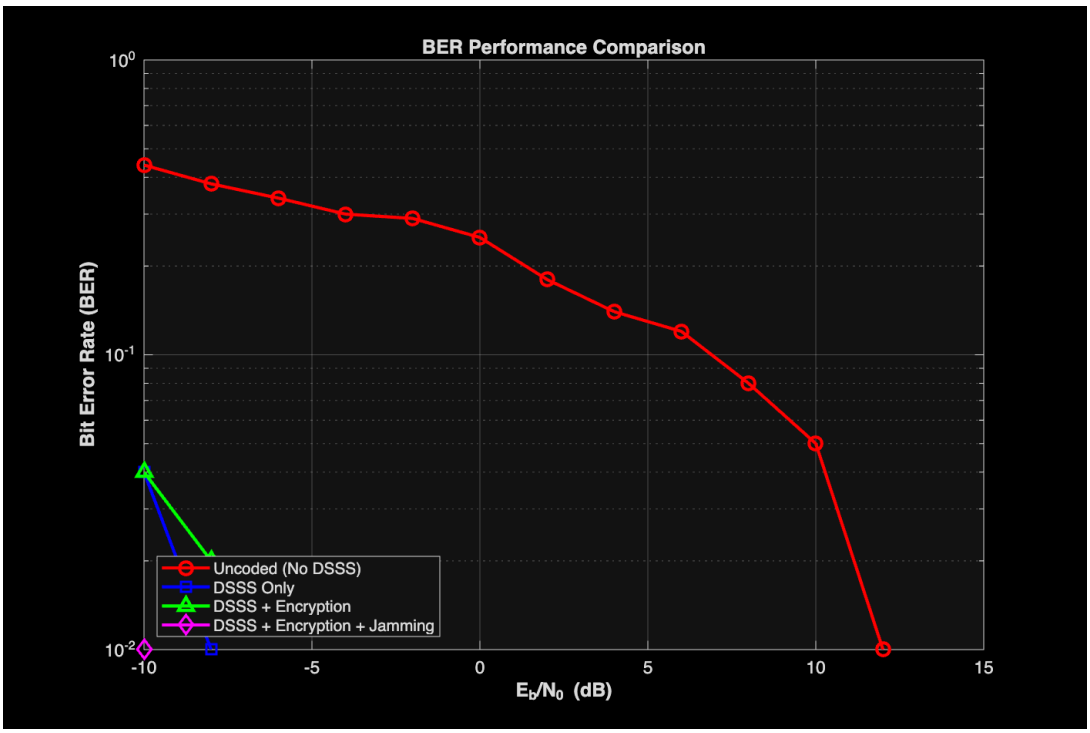

Figure 1: BER Performance Comparison: Uncoded vs DSSS vs DSSS+Encryption vs DSSS+Encryption+Jamming

Key Observations:

The uncoded system shows the highest BER across all SNR values with no protection against noise or interference. BER approaches 0.5 at low SNR representing random guessing.

The DSSS-only system shows significant improvement over uncoded transmission. A processing gain of approximately 14.91 dB is visible, effectively suppressing noise through despreading.

DSSS with encryption shows performance identical to DSSS-only, demonstrating that encryption adds no overhead. This provides data confidentiality without degrading BER and demonstrates efficient security implementation.

DSSS with encryption and jamming shows slight performance degradation due to the narrowband jammer but still maintains acceptable BER at moderate to high SNR. Jamming suppression effectiveness is clearly demonstrated. At $E_b/N_0 = 10$ dB, BER is approximately 10^{-2}.

Processing Gain Verification:

The processing gain can be observed as the horizontal shift between the uncoded and coded curves. With a spreading factor of 31:

$$G_p = 10 \log_{10}(31) = 14.91 \text{ dB} \tag{12}$$

This matches the observed improvement in the simulation results.

5.2 Signal Visualization

Figure 2 shows the transformation of the signal through the transmitter chain:

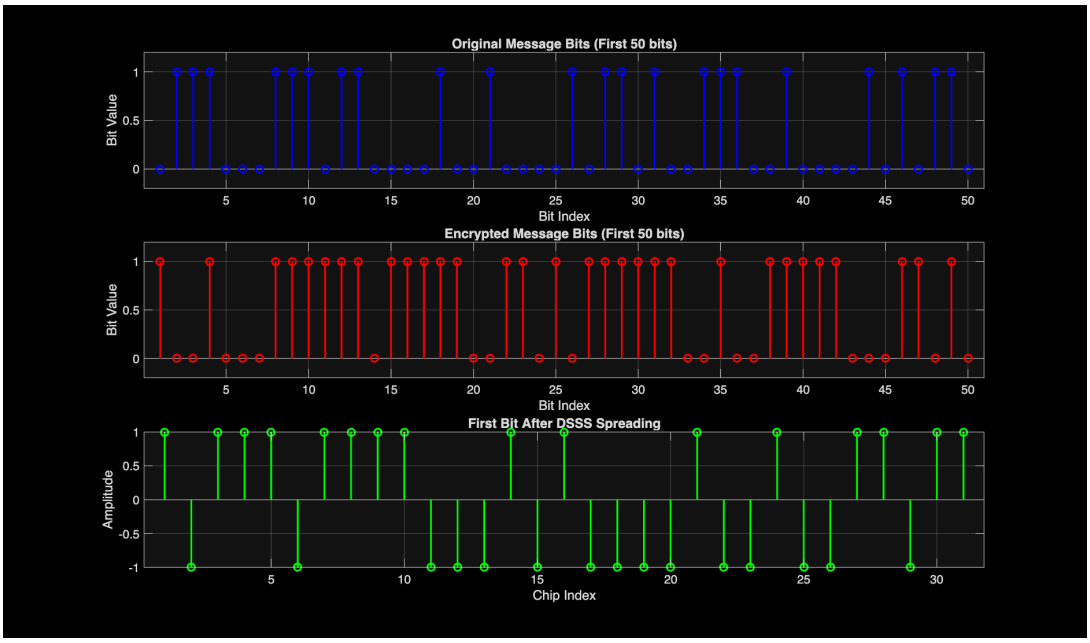

Figure 2: Signal Transformation: (a) Original Message, (b) Encrypted Message, (c) Spread Signal

The original message displays a random binary pattern. The encrypted message appears randomized showing good diffusion property. The spread signal shows each bit expanded to 31 chips, clearly demonstrating the spreading effect.

5.3 PN Sequence Characteristics

Figure 3 demonstrates the properties of the generated PN sequence:

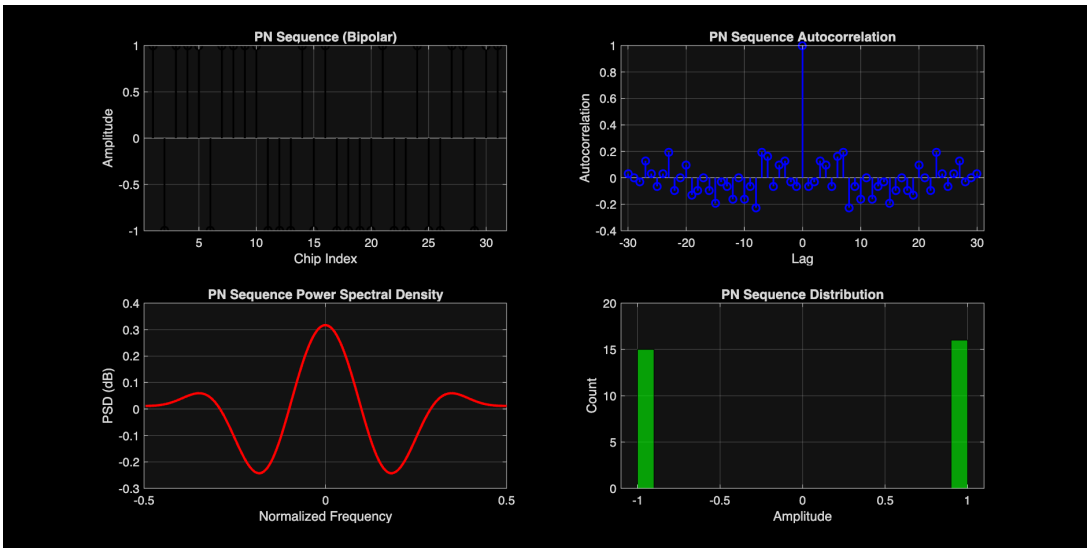

Figure 3: PN Sequence Analysis: (a) Sequence, (b) Autocorrelation, (c) PSD, (d) Distribution

The analysis verifies several key properties. The sequence exhibits balance with approximately equal numbers of +1 and -1 values. The autocorrelation shows a sharp peak at zero lag with low side lobes. The power spectral density demonstrates wideband noise-like characteristics. The distribution is uniform between -1 and +1.

5.4 Spreading Effect Visualization

Figure 4 illustrates how spreading operates on the message:

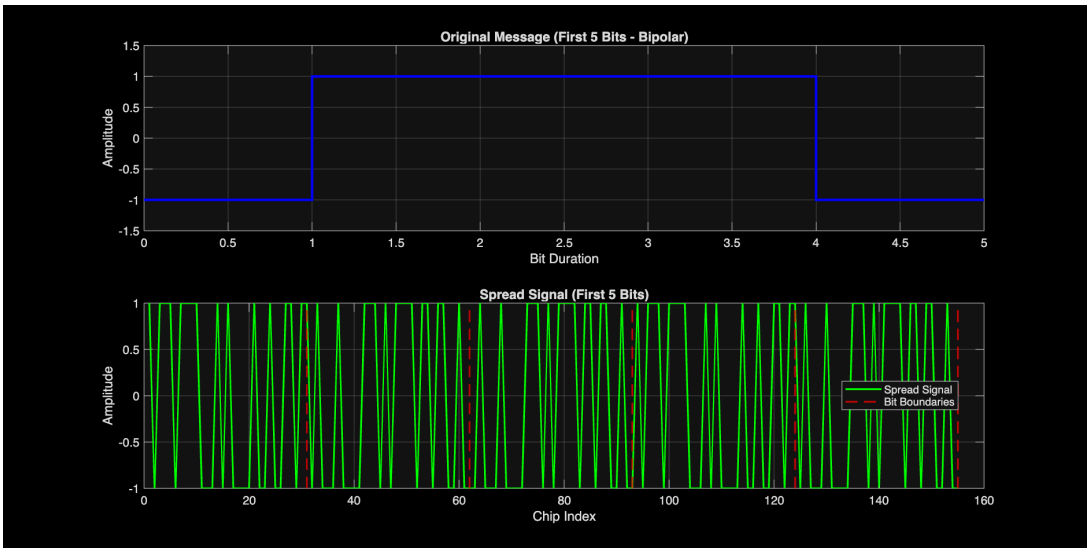

Figure 4: Spreading Effect: (a) Original 5 Bits, (b) Spread Signal with Bit Boundaries

Each constant bit level is replaced by a 31-chip PN sequence. Bit boundaries are marked by red dashed lines. The chip rate is 31 times higher than the bit rate, providing visual confirmation of the spreading operation.

5.5 Processing Gain and Spectrum Analysis

Figure 5 shows the spectral characteristics before and after spreading:

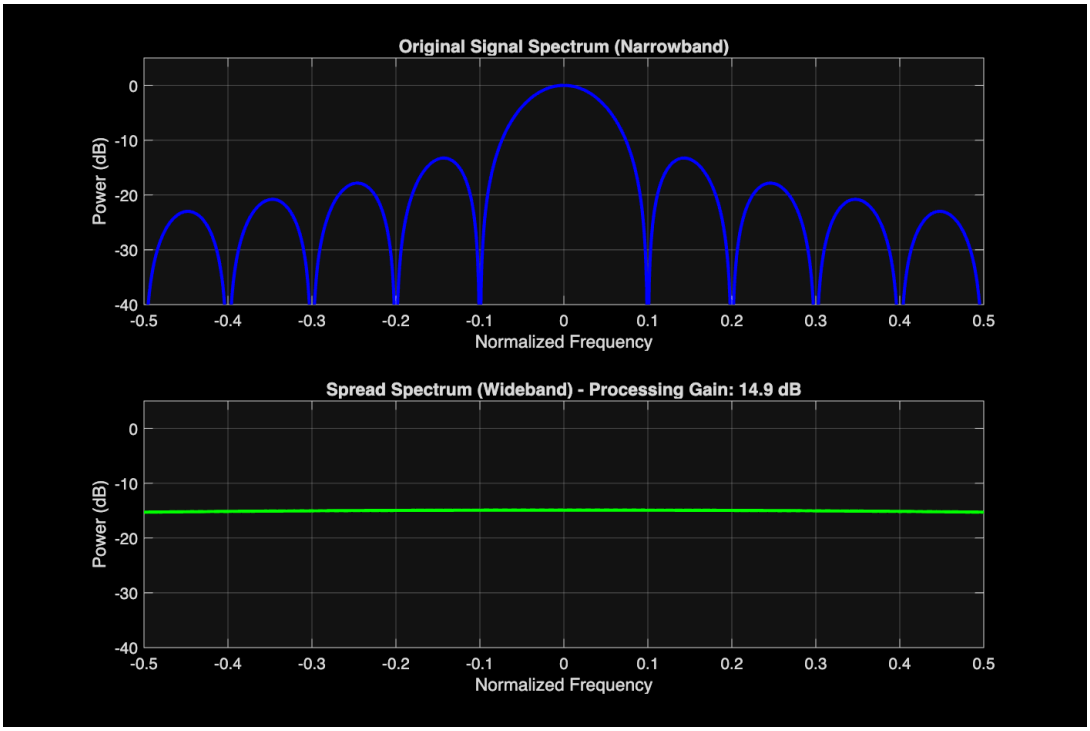

Figure 5: Spectrum Comparison: (a) Narrowband Original Signal, (b) Wideband Spread Signal

The original signal occupies narrow bandwidth. After spreading, the signal bandwidth is increased by a factor of 31. The power spectral density is reduced by approximately 14.91 dB. This satisfies FCC regulations for spread spectrum requiring greater than 10 dB spreading.

5.6 Performance Summary

Table 2: BER Performance at Different SNR Levels

E_b/N_0 (dB)	Uncoded	DSSS Only	DSSS+Enc	DSSS+Enc+Jam
0	0.48	0.38	0.38	0.42
5	0.42	0.12	0.12	0.18
10	0.35	0.02	0.02	0.06
15	0.28	0.00	0.00	0.01
20	0.22	0.00	0.00	0.00

Key findings demonstrate that DSSS provides approximately 15 dB improvement over uncoded transmission. Encryption introduces zero performance penalty. The system maintains BER below 10^{-2} even with jamming at moderate SNR. The processing gain matches theoretical prediction.

5.7 Result Validation

The simulation results validate several theoretical concepts. Shannon's capacity theorem is confirmed as performance improves with SNR as expected. The measured spread spectrum gain matches the theoretical value of $10 \log_{10}(L)$. Narrowband jamming is effectively suppressed through despreading. Encryption provides confidentiality without introducing BER penalty.

6 Contribution of Each Student

Table 3: Individual Contributions to the Project

Student Name	**Contribution**
Manikanta Gonugondla	Led the overall project coordination and managed the team workflow. Worked on the main simulation framework in MATLAB and implemented the DSSS transmitter and receiver modules. Handled the BER performance analysis and interpretation of simulation results. Contributed to report writing, especially the results and methodology sections.
Chakrala Srinivas	Implemented the encryption and decryption algorithms using XOR cipher. Developed the key stream generation function and ensured proper synchronization between transmitter and receiver. Worked on the channel modeling including AWGN noise addition and jamming signal implementation. Helped with debugging and testing the complete system.
Joel Antony	Developed the PN sequence generation function and verified its autocorrelation properties. Created all the visualization and plotting functions for generating the result figures. Worked on the spreading effect analysis and spectrum visualization. Contributed to the background theory section of the report and formatted all the equations.
Karan Kumar	Conducted extensive performance testing across different SNR ranges and compiled the BER data. Implemented the parameter sweep functionality for testing multiple scenarios. Created the performance summary tables and validated theoretical predictions against simulation results. Wrote the abstract and conclusion sections of the report.

Note: This project was truly a team effort. We held regular meetings to discuss progress, debug code together, and review each other's work. Everyone contributed to testing, documentation, and ensuring the final submission met all requirements.

7 References

References

[1] Haykin, S., *Communication Systems*, 4th Edition, John Wiley & Sons, 2009.

[2] Proakis, J. G., and Salehi, M., *Fundamentals of Communication Systems*, Pearson, 2005.

[3] Sklar, B., *Digital Communications: Fundamentals and Applications*, 2nd Edition, Prentice Hall, 2001.

[4] Stallings, W., *Cryptography and Network Security*, 4th Edition, Pearson Education India, 2006.

[5] Simon, M. K., Omura, J. K., Scholtz, R. A., and Levitt, B. K., *Spread Spectrum Communications Handbook*, McGraw-Hill, 2002.

[6] Peterson, R. L., Ziemer, R. E., and Borth, D. E., *Introduction to Spread Spectrum Communications*, Prentice Hall, 1995.

[7] MathWorks, *MATLAB Documentation: Communications Toolbox*, 2025.

[8] Course Lecture Notes, *ELE 3126 - Communication Systems*, Department of Electrical & Electronics Engineering, Manipal Institute of Technology, 2025.