**American Journal of Botany and Bioengineering**
https://biojournals.us/index.php/AJBB
**ISSN: 2997-9331**

# Designing a Secure System using Encrypted Radio Waves

**Noorulhda Mohamed Shaewit Jabr, Batool Mahdi Anad Yasser,**
**Abdullah Naeem Habeeb Shandoo, Atheer Haitham Hasson Dawood**
University of kut College of engineering Department of Laser and Engineering Optoelectronics

**Received:** 2025 19, Aug
**Accepted:** 2025 28, Sep
**Published:** 2025 08, Oct



**Annotation:** Designing a secure system based on encrypted radio waves aims to safeguard data transmission through advanced encryption techniques that prevent signal interception or manipulation during transit. This system incorporates various technologies, such as dynamic encryption protocols, frequency control, and identity verification systems, to ensure that transmitted and received signals are fully protected.

This research focuses on integrating radio encryption with intrusion detection systems and ensuring vulnerability analysis to develop comprehensive solutions that confidentiality, integrity, and availability in all operations relying on radio waves.

## 1.1 Introduction

Electromagnetic waves are formed by the interaction of electric and magnetic fields and can propagate through a vacuum. These waves include various types such as X-rays, optical rays, microwaves, radio waves, and ultraviolet rays. They are fundamental to modern physics and have important applications in technology, life sciences, and medicine.

In the 19th century, significant progress was made in the study of electromagnetic induction and waves. Michael Faraday discovered that a changing magnetic field produces a changing electric field. Later, James Clerk Maxwell formulated equations that described how time-varying electric and magnetic fields generate each other, predicting the existence of electromagnetic waves that travel at the speed of light. Maxwell concluded that visible light is a form of electromagnetic wave. His predictions were confirmed by Heinrich Hertz, who was the first to generate and detect electromagnetic waves, paving the way for the era of wireless communication, including radio, radar, and television.

### 1.2 Historical Development :

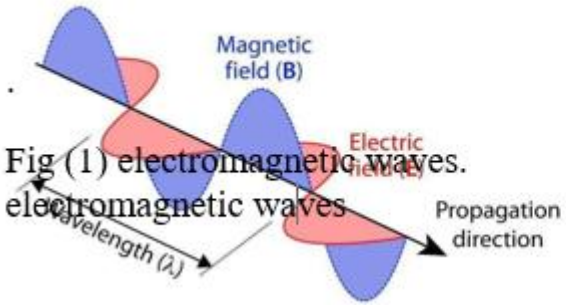
The discovery of electromagnetic induction was made independently by Michael Faraday and Joseph Henry. Although Faraday published his findings first in 1831, Henry had already been working on similar concepts, including self-induction and the use of spiral conductors.

Faraday's extensive experimental work laid the foundation for modern electromagnetism, despite his limited use of mathematics. His key experiments involved inducing electric currents using magnetic fields, leading to the discovery of electromagnetic induction, mutual induction, and key laws governing induced currents.

Faraday introduced the concept of magnetic lines of force, helping to visualize magnetic fields. He also proposed a molecular theory of electricity and discovered diamagnetism and paramagnetism. His discoveries influenced major developments in electrical engineering, including the dynamo, electric motors, and electric lighting.

Following Faraday, other scientists made significant contributions. Heinrich Lenz formulated Lenz's Law. Nicholas Callan designed the first induction coil, while Romkorff improved its efficiency. Joseph Henry developed powerful electromagnets. In 1864, James Clerk Maxwell presented his electromagnetic theory of light, showing that light is an electromagnetic wave, traveling at the same speed as light in a vacuum. Maxwell's equations unified electricity, magnetism, and optics into a single theoretical framework, revolutionizing the field.

Electromagnetic waves, as defined, do not need a medium for transmission and are produced by the vibration of electric and magnetic fields, forming the basis for many modern technologies.



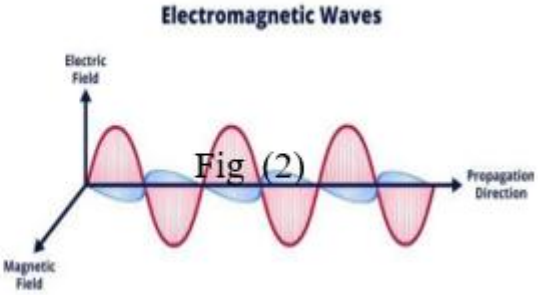




Fig (1) electromagnetic waves. Fig (2) electromagnetic waves

One wave is measured from top to top, or from bottom to bottom is called a cycle, as for the number of cycles that occur during one second is called the "wave frequency" and the wave frequency is measured in Hertz, the shorter the wavelength, the higher the frequency, the higher the energy of the electromagnetic wave, it is worth noting that electromagnetic waves are used in many fields and daily and practical applications, such as: cell phone communication, Wi-Fi network (WiFi), radio broadcasting, cancer treatment, medical imaging, cooking, and others

### 1.3 General characteristics of electromagnetic waves :

1. Transverse Nature: The electric and magnetic fields oscillate at right angles to each other and to the direction of wave propagation.
2. No Medium Required: They can travel through a vacuum without needing a material medium.
3. Speed in Vacuum: Electromagnetic waves move at the speed of light in a vacuum (~299,792,458 m/s).
4. Wide Range of Wavelengths and Frequencies: They form a continuous spectrum from long-wavelength, low-frequency radio waves to short-wavelength, high-frequency gamma rays.
5. Energy Transport: These waves carry energy and momentum, which can be transferred to objects.

6. Obeys Wave Equation: They satisfy Maxwell's equations and follow the wave equation.
7. Polarization: Electromagnetic waves can be polarized due to their transverse nature.
8. Wave Behavior: They exhibit reflection, refraction, diffraction, and interference.
9. Interference: When overlapping, they can form constructive or destructive interference patterns.

### 1.4 SOURCES OF ELECTROMAGNETIC WAVES:

Electromagnetic waves are generated by the movement of charged particles and can come from both natural and artificial sources. Here are the main sources of electromagnetic waves

Natural Sources

1. The Sun – The primary source of electromagnetic radiation, including visible light, ultraviolet (UV) rays, and infrared radiation. 2.Lightning – Produces radio waves and other electromagnetic emissions.
2. Stars and Cosmic Bodies – Emit radio waves, X-rays, and gamma rays detected by telescopes.
3. Radioactive Decay – Certain radioactive materials emit gamma rays naturally.
4. Auroras (Northern and Southern Lights) – Caused by charged particles from the Sun interacting with Earth's magnetic field.

## Chapter two Radio waves

### 1.1 Introduction

Radio waves are a type of electromagnetic radiation with long wavelengths and low frequencies, typically ranging from 30 Hz to 300 GHz. Their properties allow them to travel long distances, penetrate obstacles, and carry information, making them vital for communication.

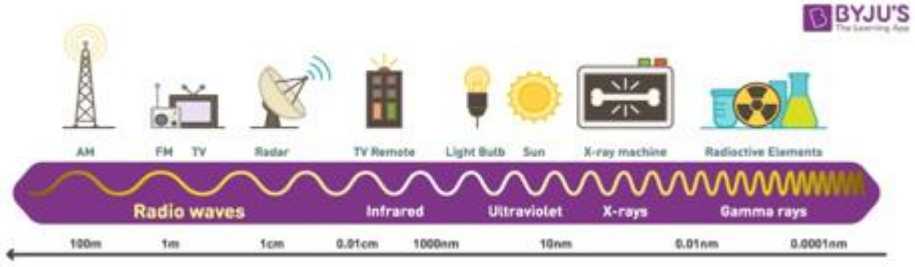
Key characteristics include their frequency, wavelength, and ability to propagate through various media. In communication systems, radio waves are modulated—via amplitude, frequency, or phase—to transmit information. Common methods include AM, FM, PM, and FSK.

Radio waves are widely used in broadcasting, mobile communication, Wi-Fi, Bluetooth, GPS, radar, and satellite systems. They offer advantages such as long-range transmission and wall penetration but can face challenges like interference and signal degradation.

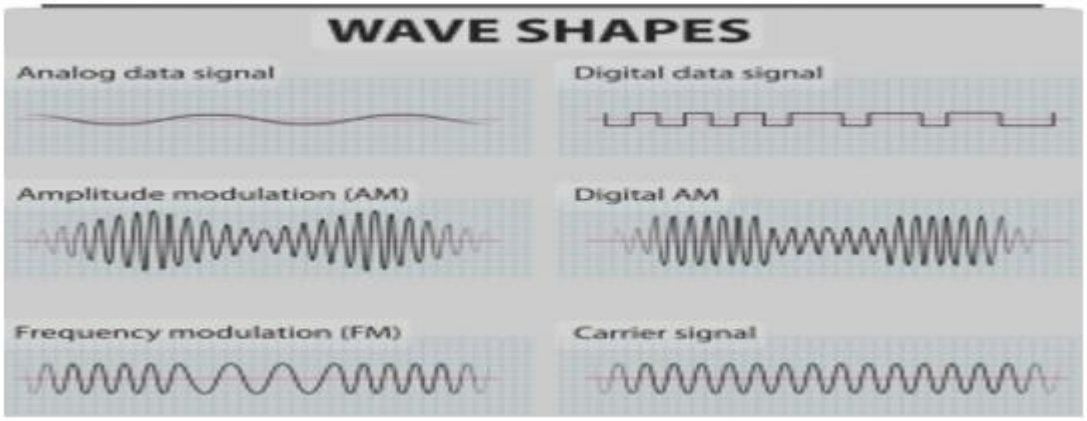
In conclusion, radio waves are essential in modern technology, supporting various communication systems and continuing to evolve with advancements in science and engineering.

### 1.2 Definition of radio waves:

Radio waves are a type of electromagnetic radiation with long wavelengths (1 mm to 100 km) and low frequencies (30 Hz to 300 GHz). Generated by the motion of electric charges, they can travel through air, space, and certain solid materials. Unlike sound waves, they don't require a medium and can propagate through the vacuum of space.



Their ability to travel long distances, penetrate obstacles, and carry information makes them essential for wireless communication, including radio, TV, mobile phones, Wi-Fi, GPS, radar, and satellite systems. Radio waves are produced by oscillating electric currents in antennas, and their frequency determines their application—lower frequencies for long-range, and higher frequencies for high-speed data over short distances.




They are also used in radar systems for object detection and in medical imaging (e.g., MRI). The behavior and propagation of radio waves depend on factors like frequency, antenna design, and environmental conditions. Continuous research is improving their effectiveness, ensuring radio waves remain vital in advancing modern technology and global connectivity.

### 1.3 Physical Properties of Radio Waves

Radio waves, a form of electromagnetic radiation, possess several key physical properties:

1. Wavelength: Ranges from 1 millimeter to 100 kilometers. It is inversely proportional to frequency.
2. Frequency: Spans from 3 kHz to 300 GHz and is divided into bands like VLF, UHF, and EHF.
3. Speed: Travels at the speed of light (approximately 300,000 km/s) in a vacuum, slightly slower in other materials.
4. Energy: Has low photon energy, calculated using the formula $E = h \times f$.
5. Amplitude: Represents the wave's strength or power, influencing signal range and reception quality.
6. Polarization: Refers to the direction of the electric field oscillation—can be linear, circular, or elliptical.
7. Reflection and Refraction: Can bounce off surfaces and bend through different mediums.
8. Diffraction: Can bend around obstacles, enabling coverage beyond direct line-of-sight.
9. Attenuation: Loses strength over distance or when absorbed by obstacles, especially at higher frequencies.
10. Interference: Overlapping waves can cause constructive or destructive interference.

### 1.4 Radio Wave Applications and Wireless Communication

Radio waves are widely used across various fields due to their ability to travel long distances and penetrate materials. Major applications include:

1. Communication Systems:

- Broadcasting: Used in AM/FM radio and TV signals.

- Mobile Networks: Carry voice and data in cellular systems.
- Wi-Fi & Bluetooth: Enable short-range wireless internet and device connections.

2. Navigation and Location:

- GPS: Uses radio signals from satellites for accurate location tracking.
- Radar: Detects objects and measures their speed and distance, used in aviation, weather, and traffic control.

3. Medical and Industrial Uses:

- MRI: Employs radio waves for detailed internal body imaging.
- Remote Control Systems: Used in drones, garage doors, and RC toys. 4.Satellite Communication:
- Transmits TV signals and GPS data via satellites using radio waves.

Wireless Communication involves transmitting information without physical connections, using electromagnetic waves through air. It includes:

Key Components:

- Transmitter, Receiver, Medium (air), and Frequency Spectrum. Common Types:

1. Radio Communication: For broadcasts and two-way radios.
2. Microwave Communication: Used in point-to-point and satellite links.
3. Wi-Fi: Enables wireless networking in homes and public spaces.
4. Mobile Networks (2G–5G): Provide mobile voice, data, and multimedia.
5. Bluetooth: Short-range connections for personal devices. 6.Infrared: Short-range control systems like TV remotes.
6. Satellite Communication: Global coverage for GPS, TV, and military.

Advantages:

- Flexibility, scalability, mobility. Challenges:
- Interference, limited bandwidth, security issues, and power consumption.

## Chapter three Cryptography

### 1.1 Introduction

Cryptography is the science and art of securing communication by converting readable data (plaintext) into an unreadable format (ciphertext) and vice versa, ensuring confidentiality, integrity, and authenticity of the data. It plays a critical role in protecting sensitive information from unauthorized access, tampering, or interception, particularly in the digital world.

Key Concepts in Cryptography:

1. Cryptography: There are two main types of Cryptography:

- Symmetric Cryptography: The same key is used for both Cryptography and decryption (e.g., AES, DES).
- Asymmetric Cryptography: Uses a pair of keys—one for Cryptography (public key) and another for decryption (private key) (e.g., RSA, ECC).

2. Decryption
3. Hashing

4. Digital Signatures
5. Cryptographic Protocols

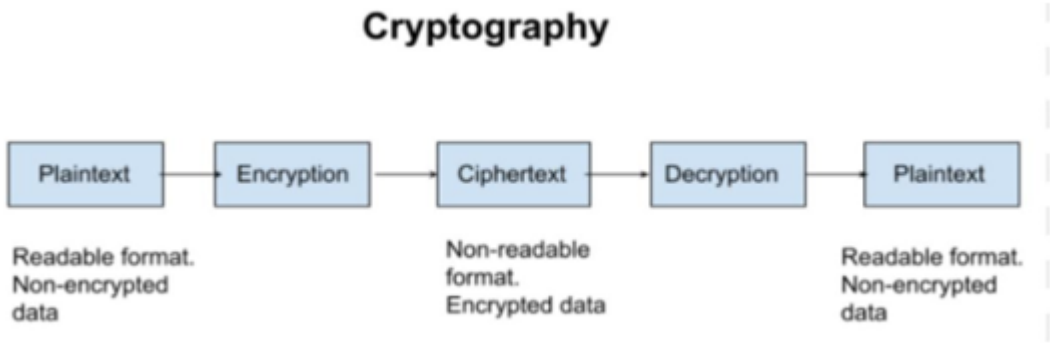
Key Goals of Cryptography:

- Confidentiality
- Integrity
- Authentication
- Non-repudiation

Cryptography has applications in many areas, including online banking, secure communications, digital identity verification, and more.

### 1.2 What is cryptography?

It is the study of mathematical techniques and their use in various aspects related to information security in order to achieve a set of goals.




Cryptography is used to maintain the confidentiality of information by converting it into random, incomprehensible codes, so the hacker (information pirate) will not be able to view its content even if he is able to obtain it. It is also used to ensure the integrity and integrity of information by controlling access to this information and limiting it to the authorized person only (who has a valid identity). In the event of a malfunction and the hacker is able to access and modify the information, we must be able to discover that this information has been modified and is not in its original state as it should be. This includes the goals of: non-denial, i.e. if we prove that the message (information) is correct and has not been tampered with and that it was actually issued by the person concerned, this person is bound by it and cannot deny it. For example, a customer asks the bank with which he deals electronically to transfer a large sum of money from his account to the account of another person, this customer cannot do so and place the responsibility on the bank as long as we can, using the science of Cryptography, prove the validity of this message and that it was issued by him personally.

### 1.3 Cryptographic applications:

1. Secure Communication: Cryptography secures internet data via protocols like HTTPS, SSL/TLS, and encrypts emails with tools like PGP and S/MIME to prevent interception.
2. Data Security & Privacy: Used in file, disk, and database encryption (e.g., BitLocker, FileVault) and in privacy technologies like anonymization and zero-knowledge proofs to protect sensitive data.
3. Authentication & Identity: Includes password hashing (SHA-256, bcrypt), digital signatures for verifying authenticity, and two-factor authentication to enhance login security.
4. Blockchain & Cryptocurrencies: Cryptography secures transactions, ensures blockchain integrity with hashing, and enables smart contracts that self-execute based on rules.

5. Digital Rights Management (DRM): Protects digital content (music, software, videos) from piracy by allowing only authorized access.
6. Banking & Finance: Encrypts data in ATMs, POS systems, and the SWIFT network, while digital wallets use tokens for secure mobile payments.
7. Government & Military: Secures classified information, supports secure e-voting, and protects satellite and remote communications.
8. Healthcare Security: Protects electronic health records and medical devices from unauthorized access and cyber threats.
9. Cloud Security: Encrypts cloud-stored data and controls access to ensure only authorized users can view sensitive information.
10. IoT Security: Encrypts data between connected devices, authenticates devices, and secures industrial and smart home systems.
11. Post-Quantum Cryptography: Develops future-proof algorithms to defend against potential threats from quantum computing.

### 1.4 Basic aspects of cryptography:

Cryptography includes multiple aspects (see Figure 3.1) and is divided into three main sections in terms of the use of keys and their type, as follows:

_A section related to the asymmetric key (public key): It includes three aspects: Cryptography, digital signature, and identity verification.

_Symmetric key section: It includes the following aspects: Cryptography (block Cryptography), (stream Cryptography), and reduction functions that are used to verify the authenticity of the message, digital signature, and pseudo-random numbers (bits), in addition to identity verification.

_A section that has no connection to keys: It includes the reduction functions, the permutation operation, and random numbers (bits).

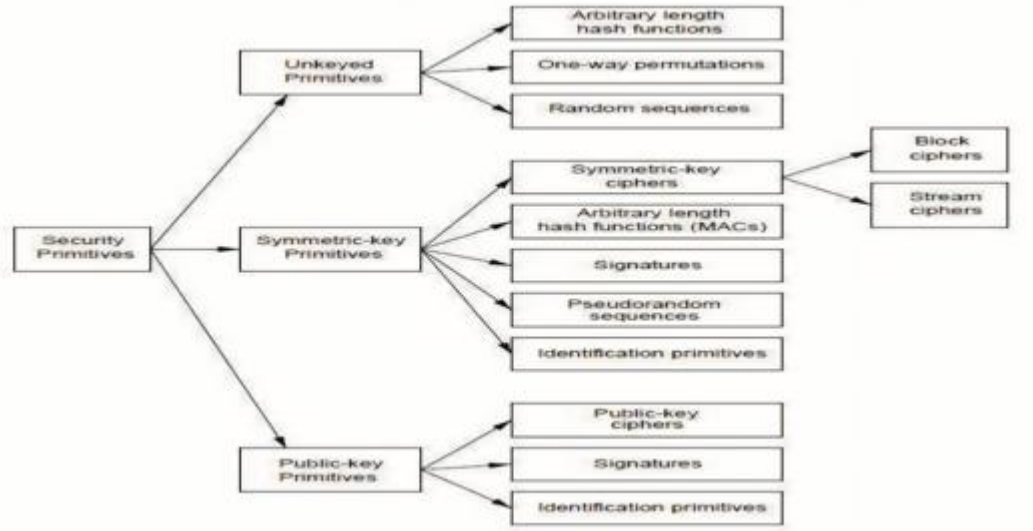



Figure (3.1): Basic aspects of cryptography.

### 1.5 Other important concepts:

- Substitution and permutation Cryptography: Substitution and permutation are classical cryptographic techniques used before the computer age. In substitution, letters in the original text are replaced with other letters based on a key. In permutation, the positions of letters are rearranged without changing the actual letters. These methods are often combined for

stronger encryption. Modern cryptographic algorithms still use these techniques, but with bits instead of letters, allowing encryption of any type of data. Typically, multiple rounds of substitution and permutation are applied for increased security.

- Plaintext: is the data (or message) to be encrypted using the Cryptography algorithm.
- Cryptography Algorithm: It is the algorithm that encrypts the original text using the (secret) key and the result is the encrypted text.
- Secret key: is a number (or string) of random bits used by the Cryptography algorithm to encrypt the original text. It must be kept secret because revealing it means revealing the secret of the information that was encrypted using it.
- Ciphertext: is the result of the Cryptography process, and is a random string of indirect letters (or bits) that results from entering the key and the original text into the Cryptography algorithm used.
- Decryption algorithm: Cryptography is a reverse process, i.e. a decryption algorithm must be used to decrypt and return the encrypted text to its original state; usually Cryptography algorithms are reversed, i.e. they are given the original text and the key (input) and this results in the encrypted text (output) and vice versa; enter the encrypted text and the same key and the same original text is returned.

### 1.6 Cryptographic goals:

There are four main goals behind the use of cryptography, which are as follows:

- Confidentiality or privacy: is a service used to save the information content of all Persons except those who have been authorized to view it.
- Data integration: it is a service used to save information from change (deletion, addition or modification) by unauthorized persons.
- Authentication: it is a service used to prove the identity of the data handling (authorized).
- Non-repudiation: it is a service used to prevent a person from denying doing an action, or proving an action he has done effectively, so he cannot deny it or evade it.encryption provides proof through its use in a digital signature, and a digital signature is a signature that uses encryption techniques and owns the public key, private key and digital certificate.

### 1.7 Cryptography and information security:

Security information relies heavily on the science of construction and the ciphers and algorithms that serve it, for a significant set of difficulties that must be endured to protect a lot of important information and officials (state secrets, targeted, commercial companies and government institutions and private accounts, e-commerce operations and many others) as this information can be a source or illegitimate when transmitted over the network; Among the least of these options that learning Cryptography can provide:

Privacy and confidentiality of information: i.e. maintaining the confidentiality of information so that it is only accessible to the authorized person who has a valid identity.

Data integrity and integrity: ensuring that information has not been modified (such as by adding, deleting or changing) by an unauthorized person or in an unknown manner.

Identity verification: verifying and confirming the identity of the person dealing with the information (whether a person, a program, a computer or other) and that he is actually the required person who has the appropriate authorization.

Message verification: proving the authenticity and authenticity of the message (information), i.e. that it has not been modified or tampered with by an unauthorized person or in an unknown manner.

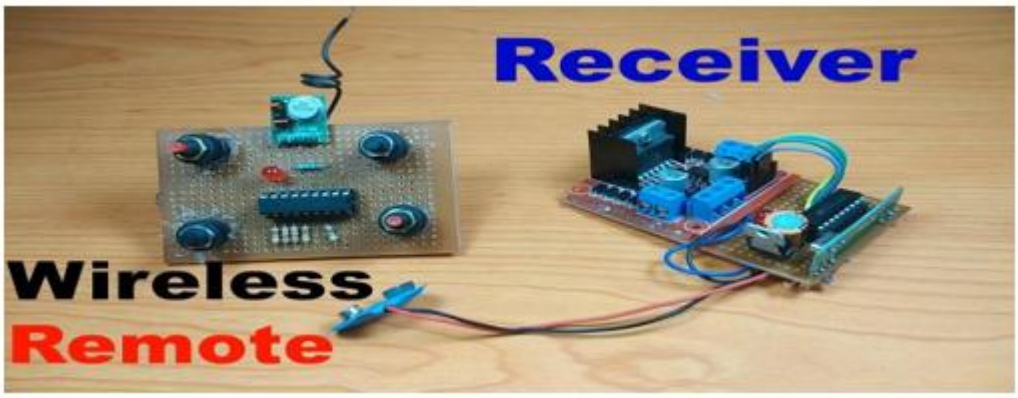
Non-repudiation: ensuring that the source of the message (information) does not deny it or claim that he is not responsible for it.

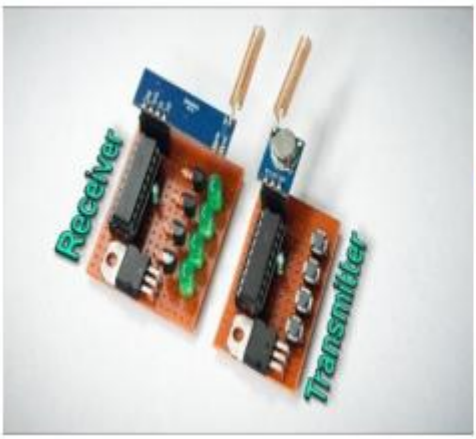
f the shared key is exposed or stolen, the entire communication is at risk, as the same key is used for both encryption and decryption.

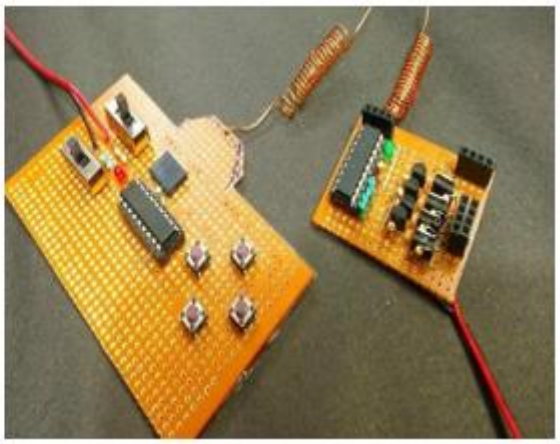
**Chapter four Result & Discussion And Conclusion**

A wireless protection system has been designed, **consisting**:

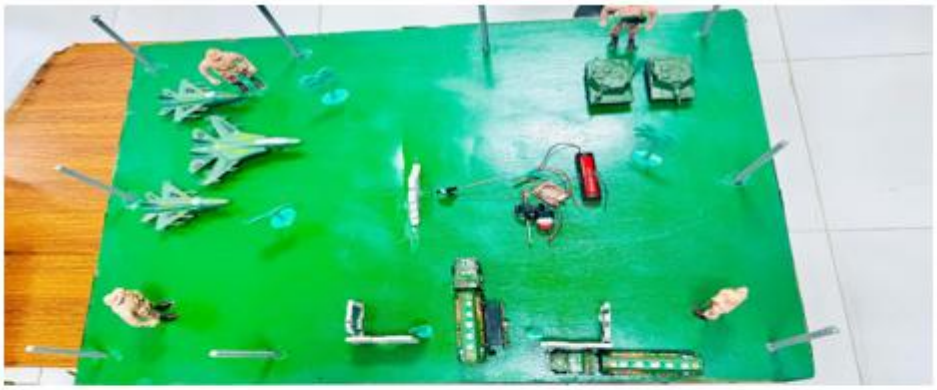
1. Wireless transmitter: A transmitter that sends an encrypted wireless signal when the transmission switch is pressed.
2. Receiver: A receiver that wirelessly receives the radio signal, amplifies it, and then sends it to the control system located at the entrance gate.
3. Power Supply: A power source that provides the necessary power to both the transmitter and receiver circuits separately.
4. Antenna: Connected to both the transmitter and receiver to enhance signal reception.
5. In this project, a wireless transmission circuit has been designed, as shown in figure, which can be carried by vehicles, machinery, or individuals. When approaching designated locations, the transmission switch is pressed to wirelessly send the encrypted signal to the receiving site. This transmitted signal will be received by the electronic reception system, as shown in figure, which will then trigger an alert or control the opening and closing of the entrance gate. A very important point to note here is that the transmission and reception frequencies must be the same to ensure proper communication between them.
6. Wireless Technologies: Various wireless technologies, such as Wi-Fi or Bluetooth, can be used to enhance the performance of the protection system.



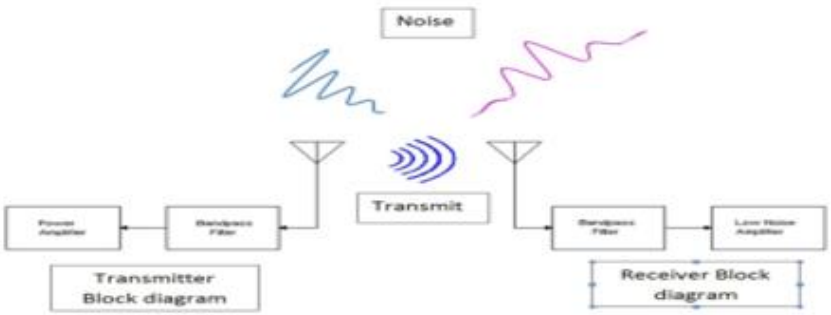



Microcontroller Integration: A microcontroller unit, such as Arduino or ESP8266, can also be added to the system to improve performance and functionality.



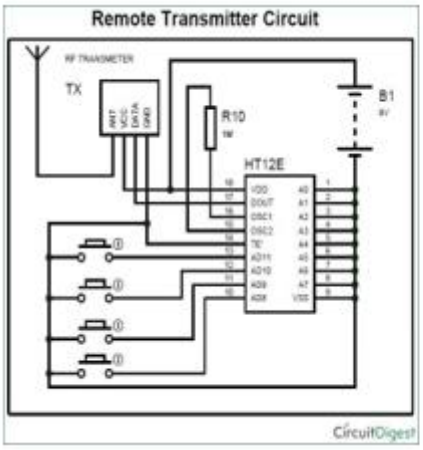
## Methods of protection:

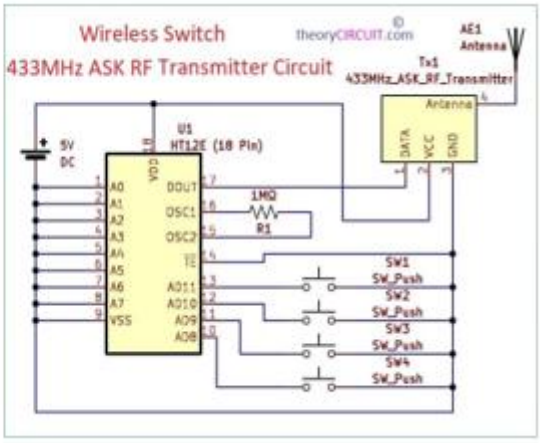
| Disadvantages | Advantages | Protection Method |
|---|---|---|
| - Vulnerable to high-powered jamming attacks. - Requires regular encryption key updates. | - High security through encryption. - Resistant to jamming by changing frequency. - Flexible installation and usage. | **Encrypted Radio Waves** |
| - Difficult to install and extend. - Prone to physical damage and wear. | - Difficult to breach through a wired network. - High signal stability. | **Wired Protection** |
| - Vulnerable to denial-of-service (DDoS) attacks. - Performance drops due to signal interference. | - Easy to set up and flexible. - Supports modern encryption methods (WPA3). | **Wi-Fi Protection** |
| - Limited range. - Susceptible to brute-force attacks. | - Low power consumption. - Easy to pair with other devices. | **Bluetooth Protection** |
| - High cost. - Performance affected by environmental factors (e.g., fog, rain). | - High precision in sensing. - Difficult to manipulate the signal. | **Laser Protection** |
| - High cost for installation and maintenance. - Privacy concerns. - Vulnerable to network or power failure. | - Continuous 24/7 monitoring. - Provides visual evidence for security incidents. - Can be integrated with other security systems. | **Camera-Based Protection** |



### 1.1 Electronic Circuit Components:

1. HT12E ICs, 2 pieces
2. Switch pushbuttons, 2 pieces
3. Power supply, 3.7 volts, 5 amps, 2 pieces
4. resistance 1mohm ¼ watts
5. Antennas, 2 pieces
6. Transistors, BC107, 2 pieces
7. Motor, 3 volts, 1 piece
8. Red LED, 1 piece
9. toggle switch, 1 piece
10. Wires and connectors
11. A wooden base measuring 80 x 80 cm containing replicas of military vehicles and guard soldiers.

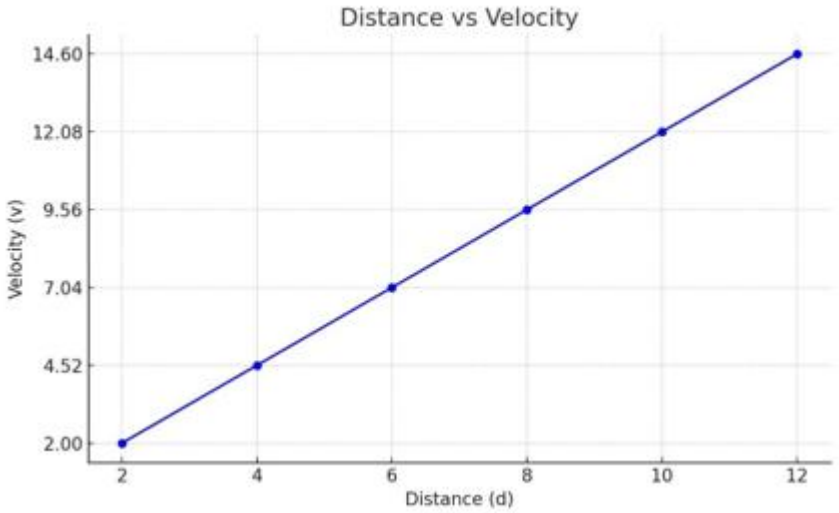



### Recommendations:

1. Install Surveillance Cameras: Install surveillance cameras alongside the radio system to operate when wireless signals are received.
2. Install Laser Monitoring: Install a laser-based transmission and reception system before the site entrance gate to enhance protection against unauthorized entry, send warning signals, and control the gate opening and closing system.
3. Daily Signal Encryption Change: The encrypted signal should be changed daily to ensure protection against hostile interception.

| D (Distance between sender and recipient)(meter) | V (volt) |
|---|---|
| 2 | 2 |
| 4 | 4.52 |
| 6 | 7.04 |
| 8 | 9.56 |
| 10 | 12.08 |
| 12 | 14.6 |




### 1.2 Result & Conclusion

In this experiment, we read the power of the received signal with an AVO meter and a Oscillascope after magnifying it by amplifier magnification circuits and at a distance of 2 meters between the sender and the recipient, and its value was 2 volts, and after a distance of 12 meters between the sender and the recipient, we got a signal of 14.6 millivolts

We notice here a loss in the received signal, and this applies according to inverse square law

Here we note the difference of the results with readings according to the inverse square law in the laboratory

This difference is caused by reflections by the walls of the laboratory and the metal devices located in it

And here, according to the law of the hole coefficient, it is assumed that the path losses n=2 for free space, n=3 for urban areas and n=4 for the city, as the number of n increases, the loss increases

Applying the inverse square law p2=1.16 MV for urban areas.

Losses here are losses in the power of the radio signal when transmitted through a certain transmission medium such as air, wires or optical fibers for light transmission and these losses are affected by several factors including frequency, type of medium, signal transmission distance, signal size and the quality of the equipment used in the transmitter .

We also note that at low radio frequencies, its ceiling is small relative to high radio frequencies

For example, in low wireless bands such as Wi-Fi and Bluetooth technology, losses are relatively limited, while the high frequency used in the fifth generation 5G losses increase significantly because 5G uses an automatic frequency.

Note/ we sent two frequencies loaded on a carrier wave of 27MHZ and 40MHZ the first frequency was 300Hz and the second 150Hz loaded on that carrier wave

We used the first frequency to turn on the BC developer to open the entrance gate and used the second frequency to turn on the remote signal lamp

**References:**

1. Smith, J. (2010). Electromagnetic Waves: Principles and Applications. New York: Wiley.
2. Wang, L., & Jones, R. (2015). Introduction to Electromagnetic Waves. Boston: Pearson.
3. Johnson, M. (2012). Electromagnetic Waves and Their Properties. London: Springer.

4. Brown, K. (2018). Electromagnetic Waves in Modern Technology. Chicago: University of Chicago Press.
5. Lee, S., & Kim, H. (2014). Electromagnetic Wave Theory. San Francisco: McGraw-Hill.
6. Chen, Y. (2016). Electromagnetic Waves and Antennas. Amsterdam: Elsevier.
7. Davis, P. (2013). Electromagnetic Waves: A Comprehensive Guide. Oxford: Oxford University Press.
8. Wilson, T. (2017). Electromagnetic Waves and Communication Systems. Cambridge: Cambridge University Press.
9. Wang, J., & Zhang, Y. (2018). Electromagnetic wave propagation in anisotropic media. Springer.
10. Balanis, C. A. (2016). Antenna theory: analysis and design. John Wiley & Sons.
11. Collin, R. E. (2001). Foundations for microwave engineering. McGraw-Hill Education.
12. Pozar, D. M. (2011). Microwave engineering. John Wiley & Sons.
13. Stutzman, W. L., & Thiele, G. A. (2012). Antenna theory and design. John Wiley & Sons.
14. Mailloux, R. J. (2014). Phased array antennas. John Wiley & Sons.
15. Kraus, J. D., & Marhefka, R. J. (2002). Antennas for all applications. McGraw-Hill Education.
16. Balanis, C. A. (2016). Advanced engineering electromagnetics. John Wiley & Sons.
17. Terman, F. E. (1955). Radio engineering. McGraw-Hill Education.
18. Menezes, Oorschot, and Vanstone, Handbook of Applied Cryptography, 5th Edition, CRC Press, 1997.
19. National Institute of Standards and Technology, FIPS PUB 140-2, SECURITY REQUIREMENTS FOR CRYPTOGRAPHIC MODULES, March 2002.
20. National Institute of Standards and Technology, FIPS PUB 180-4, Secure Hash Standard (SHS), March 2012.