Journal of Theoretical and Applied Information Technology
15th May 2022. Vol.100. No 9
© 2022 Little Lion Scientific

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

DEVELOPMENT OF DUAL-BAND ENCRYPTION FOR WLAN SECURITY

SAED THUNEIBAT

Department of Electrical Engineering, Al-Balqa Applied University, Jordan

E-mail: saed1970@bau.edu.jo

ABSTRACT

Nowadays there is a large amount of information that needs to be communicated securely such as military and governmental issues over WLAN for example AD HOC network. In this paper, we propose the dual-frequency band cryptography with frequency hopping technique. By implementing the proposed method, we can create a system that can be protected from harmful intentions. While numerous WLAN security techniques have been presented in previous research, to our knowledge, no similar simple and effective methodology for WLAN encryption has been previously proposed. Our invention is the creation of a new methodology based on the transmitting data and keys separately by dual-frequency band. Simulation results validate the advantage of the proposed dual-band encryption for WLAN security.

Keywords- *AES, Dual-Frequency Band, WLAN, Cryptography, Symmetric technique.*

1. INTRODUCTION

Generally, security of information, systems and networks based on encryption with Symmetric, Asymmetric, Digital Signature and Hash value techniques. Symmetric encryption implements one secret key for encryption and decryption and is suitable for securing a large amount of data and big files. The problem in this strategy is in key sharing, which must be secure too.

The Asymmetric approach uses public and private keys calculated with difficult math operation, mainly by division by modulus. This technique is not suitable for big file encryption but can be used for key sharing in Symmetric approach demonstrated in Diffie-Hellman key exchange protocol.

Digital Signature is similar to Asymmetric with the difference in using keys and suitable for short messages and can provide a variety of security services such as Authentication and nonrepudiation. Data integrity is usually provided by Hash value technique.

We concentrate our attention on Symmetric technique for securing large amount of data and big files such as weekly or monthly reports in a bank.

The problem of sharing keys, we solved by double band transmission, one for data, the other for keys.

In this paper, we assure transmitting data between two entities within WLAN safely and without interception by an unauthorized individual. The idea of the research is to transmit encrypted data on high frequency band and to transmit the key on lower frequency band, which means we will send data and key in separate bands. The reason we use different frequency band is that it is hard to have single device that receives such very wide frequency range because it must have large number of antennas with different lengths. Table 1, below explains and defines the proposed communication techniques. Note that these frequencies belong to the ISM band and may be used for WLAN according to IEEE.802.11 free.

The aim of this paper is the development of dual-band encryption for WLAN security and perform a simulation methodology for validating and proving the implementation of this technique for securing data exchange in WLAN, for example a bank network.

Table 1. Proposed Communication Techniques.

Technique	Digital Modulation	Line Coding	Encryption Technique	Band, MHz
data Transmission	DPSK	D-Man	DSSS	2400--2835
Key transmission	BFSK	NRZ	AES	902-928

Literature review shows that a lot of research papers have been published about WLAN security. In [1], the current state of WLAN security is survived. Wireless nature of the communication leaves the communicated information and communicating devices, vulnerable to threats and attacks. The works [2, 3] consider the 4-way handshake flaws design, it is proved that both Wi-Fi Protected Access (WPA) and WPA2- based products are affected by attacks. Several critical vulnerabilities in 802.11 standard security protocols such Wired Equivalent Privacy (WEP), WPA, WPA-TKIP and WPA2 have been presented and discussed in [4, 5, 6].

The most promising security protocol in WLAN is WPA3, which is planned to invent in this year, it is the advanced and improved version of WPA and WPA2. Despite the improvement of WPA and WPA2, both have a common security risk, expressed in the Password Crack. In [7], authors mentioned the ability of an attacker to crack passwords within 2-4 hours.

Dual-band encryption technique implements the AES based Symmetric technique for securing large amount of data and big files such as weekly or monthly reports in a bank, in the same time it implements the wireless communication free bands for sharing keys. This technique is simple and effective in solving the problem of keys sharing.

In additive to these methods, the proposed method based on DSSS and DPSK for extra privacy.

2. COMMUNICATION SYSTEM DESCRIPOTION

The proposed system in this paper is described in figure 1. The block diagram of the proposed system.

Figure 2 shows the system functions in detail.

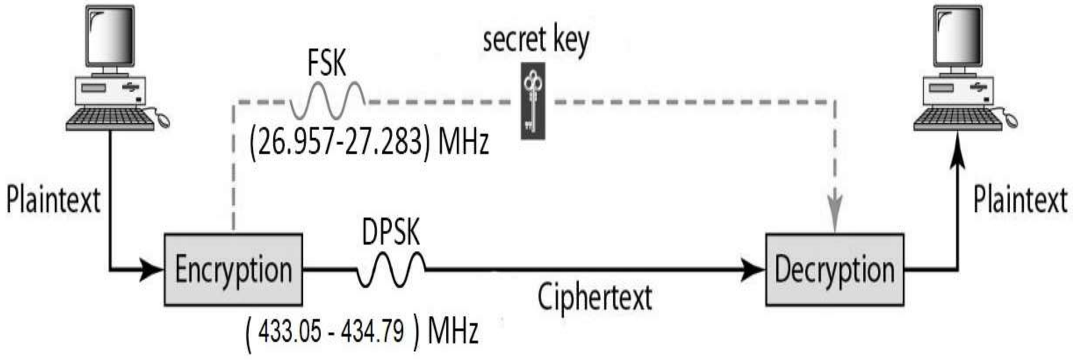


Figure 1: Block Diagram Of The System

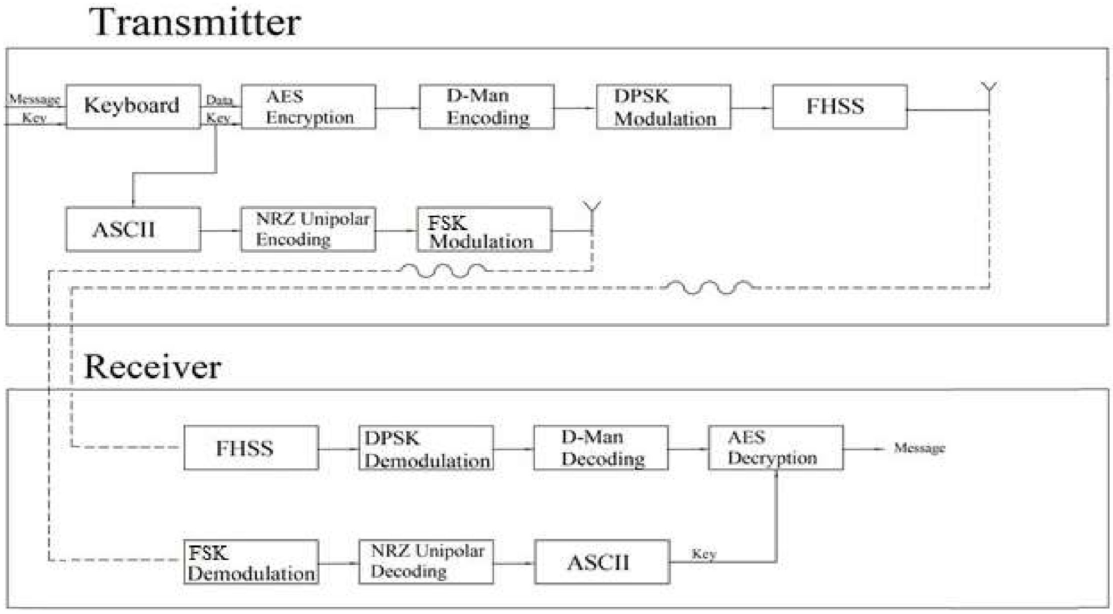


Figure 2: Detailed block diagram of the system

3. SIMULATION AND TESTING

Under my superposition, my students: Ehsan Shqairat and Mohammad Al-Ahmad have developed a Python-based simulation system in their graduation project at AL-Huson university college, BAU, Jordan.

In this section, we introduce simulation results and program run outputs. We chose Python programming language for simulating the proposed system.

3.1 Software Specifications

The main function of our software is to simulate the system described in figures 1 and 2, which is to encrypt data using AES-128 then sending the encrypted data and the key separately using different frequency bands and modulation techniques. Then collect the key to decrypt the data at the receiver end. It also guarantees that the key size will not be longer or shorter than 128 bits (16 Bytes) for AES-128 to work correctly.

3.2 Software Design and Implementation

In figure 3, by flowchart, we describe the operations of the software transmitter.

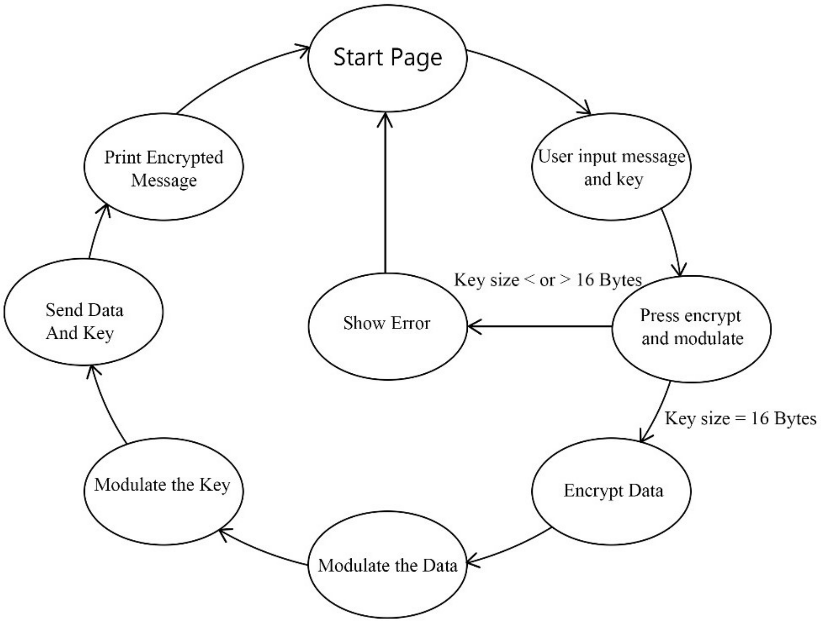


Figure 3: Transmitter Flowchart

At the start page, the user enters the message (plaintext) and the key and presses the button (Encrypt and Modulate). First, the software checks the key size, if it is less or more than 16 bytes an error message will be shown, if it is 16 bytes, then the software calls the encryption function to encrypt the data. After encryption, the software calls the modulation function for the data and the key each one with its own technique. The software sends the data and the key in separate channels simulated by adding random noise and using global variables.

The software also shows the encrypted form of the message (ciphertext).

In the next flowchart, in figure 4, we describe the operations of the receiver software.

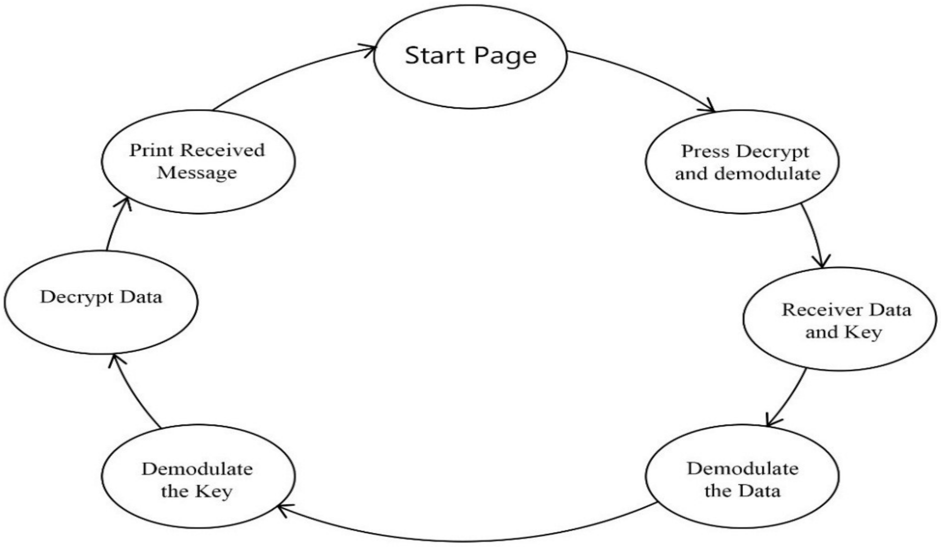


Figure 4: Receiver Flowchart

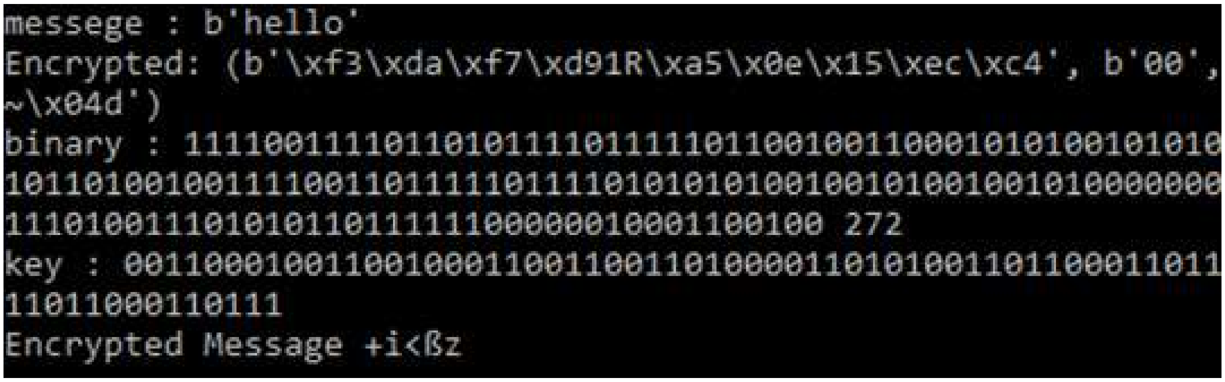
At the receiver page, the user presses the button (Demodulate and Decrypt). Instantly the software collects the noisy data and key signals via global variables. Then it calls the demodulation functions for the data and the key, and then calls the decryption function and decrypt data using the received key, then the decrypted message will be printed on the screen.

3.3 System Testing

In this section, we test each function individually, and then we introduce a full system testing. We introduce the code and implementation of the software.

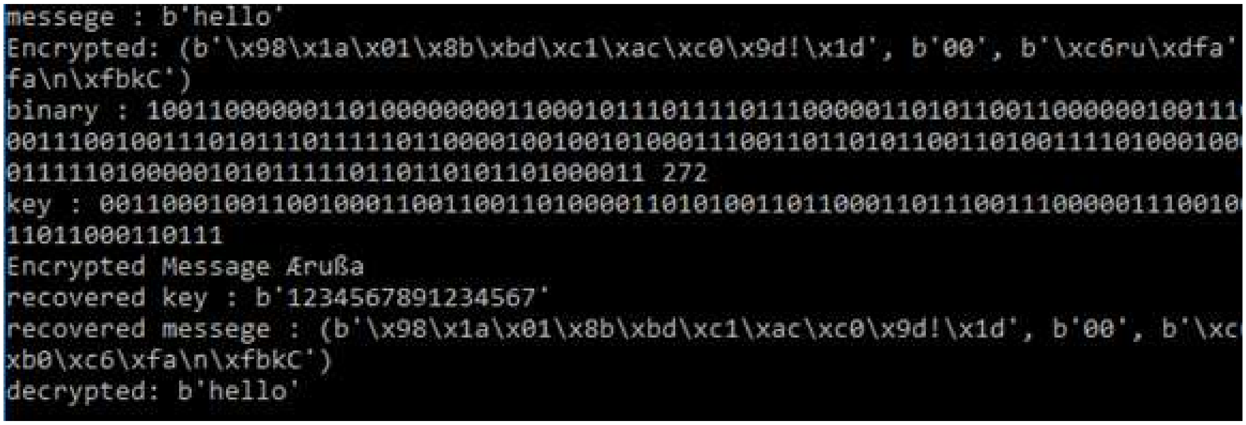
In figure 5, we see the user interface of the transmitter which contains three text boxes and two buttons, the upper text box for plaintext, the middle one for key and the lower one for ciphertext. We see the result of calling the encryption function, performed on "hello" as a message and "1234567891234567" as key.

In figure 6, we see the user interface of the receiver which contains one text box for the decrypted message and two buttons. After using encryption function for the message "hello" and the key "1234567891234567" and receiving the encrypted message we call the decryption function we got the result shown in figure 6.



```
messege : b'hello'
Encrypted: (b'\xf3\xda\xf7\xd91R\xa5\x0e\x15\xec\xc4', b'00',
~\x04d')
binary : 1111001111011010111101111101100100110001010100101010
1011010010011110011011111011110101010100100101001001010000000
111010011101010110111111000000010001100100 272
key : 0011000100110010001100110011010000110101001101100011011
11011000110111
Encrypted Message +i<ßz
```

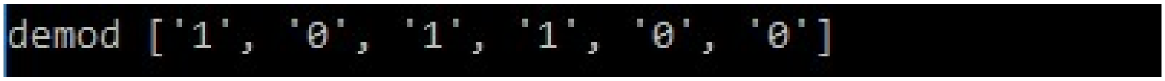
Figure 5: AES Encryption Testing



```
messege : b'hello'
Encrypted: (b'\x98\x1a\x01\x8b\xbd\xc1\xac\xc0\x9d!\x1d', b'00', b'\xc6ru\xdfa'
fa\n\xfbkC')
binary : 1001100000001101000000000110001011101111011100000110101100110000000100111
0011100100111010111011111011000010010010100011100110110101100110100111101000100
011111010000010101111110110110101101000011 272
key : 00110001001100100011001100110100001101010011011000110111001110000001110010
11011000110111
Encrypted Message Ærußa
recovered key : b'1234567891234567'
recovered messege : (b'\x98\x1a\x01\x8b\xbd\xc1\xac\xc0\x9d!\x1d', b'00', b'\xc
xb0\xc6\xfa\n\xfbkC')
decrypted: b'hello'
```

Figure 6: AES Decryption Testing

Figure 7 shows the output signals of D-Man line coding, DPSK modulation and noisy DPSK modulation after setting "101100" bits stream as an input.



```
demod ['1', '0', '1', '1', '0', '0']
```

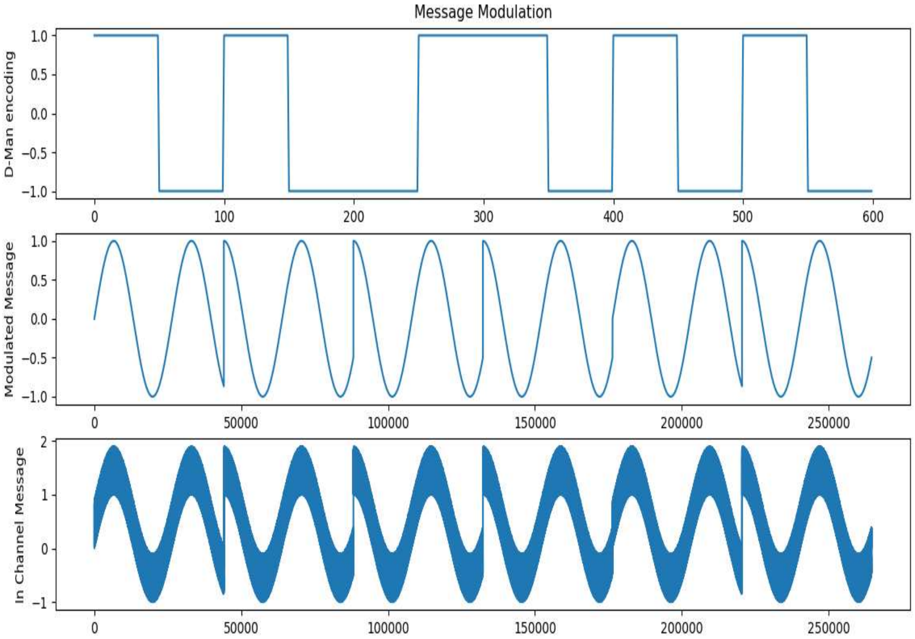
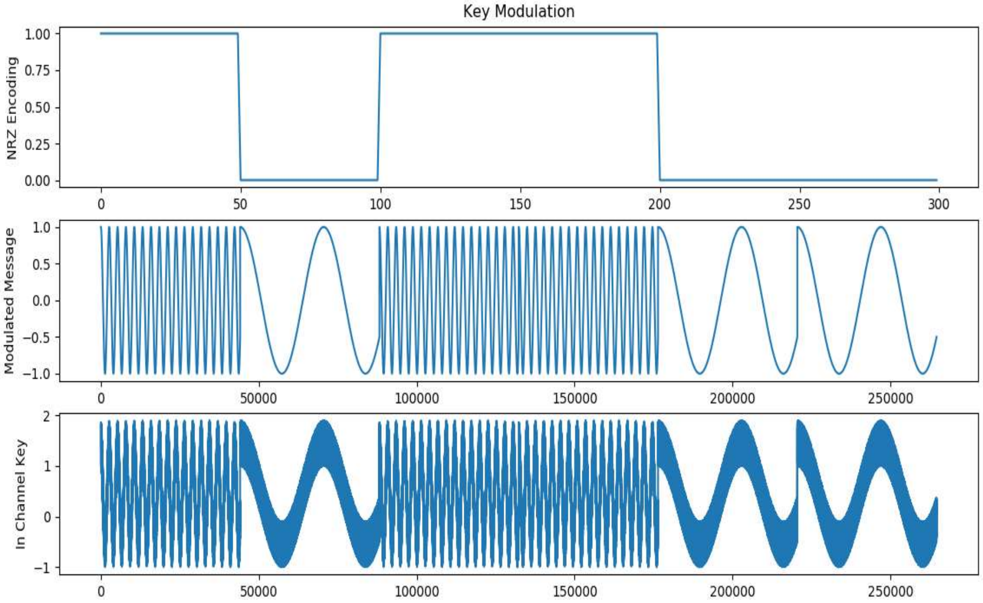
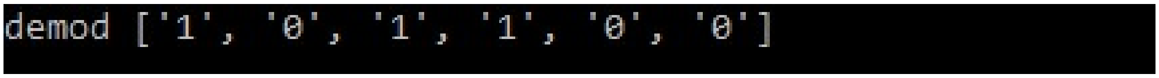


Figure 7: DPSK Modulation Testing

Figure 8 shows the output signals of NRZ line coding, FSK modulation and noisy FSK modulation after setting “101100” bits stream as an input.

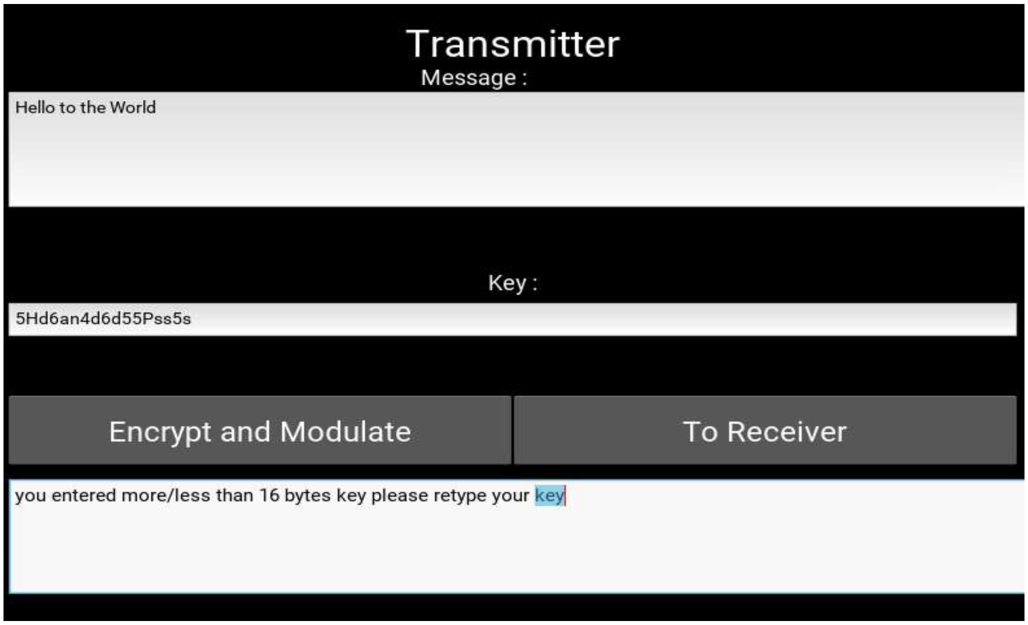




```
demod ['1', '0', '1', '1', '0', '0']
```

Figure 8: FSK Modulation Testing

We introduce a full system Testing. Starting with figure 9 which shows a case when the user enters long key (more than 16 bytes).



Hello to the World

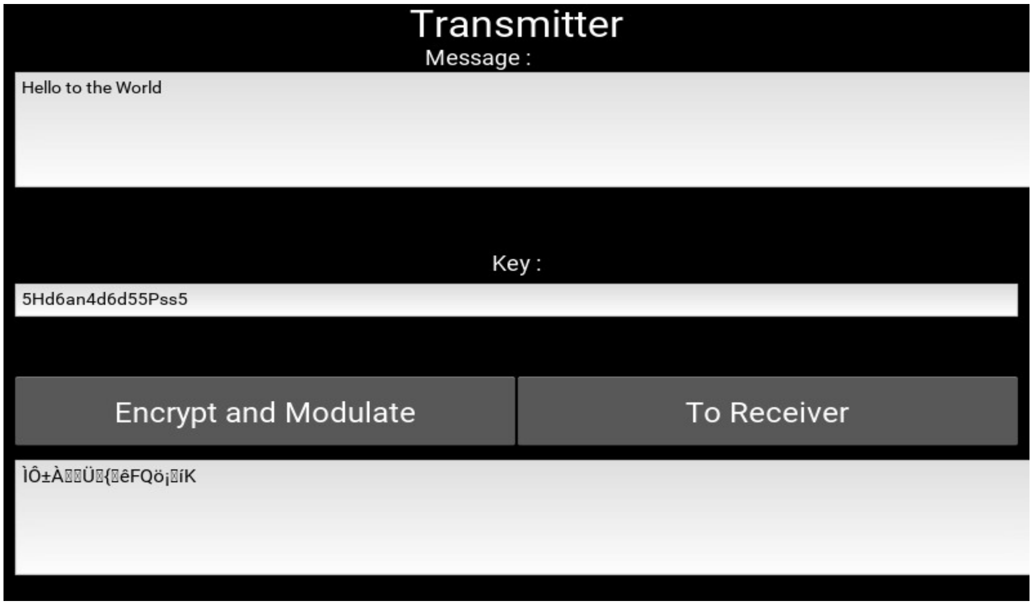
5Hd6an4d6d55Pss5s

you entered more/less than 16 bytes key please retype your key

Figure 9: Transmitter System Testing With More Than 16 Bytes Key

As shown in figure 9 the system prints error message when the user enters more than 16 Bytes key. The system will print the same message if the user enters less than 16 Bytes key.

Figure 10 shows an example of a full system testing for the transmitter showing the ciphertext after pressing “Encrypt and Modulate” and calling the AES encryption function, DPSK modulation function, FSK modulation function.



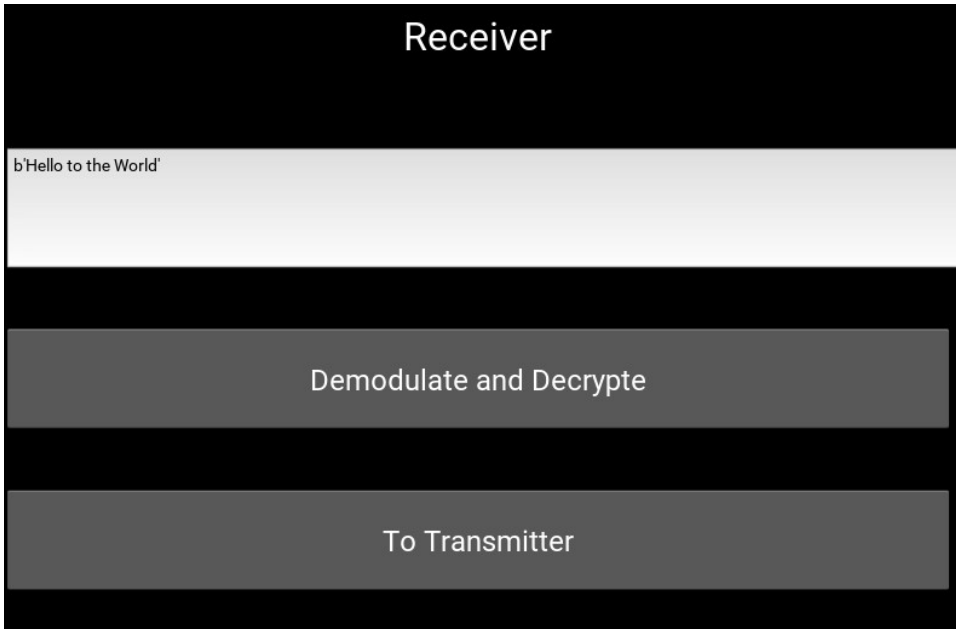
Hello to the World

5Hd6an4d6d55Pss5

ÌÔ±À▯▯Ü▯{▯êFQö¡▯íK

Figure 10: Transmitter System Testing

In Figure 11, we complete the example at the receiver, the figure shows the recovered message after pressing “Demodulate and Decrypt” which calls DPSK demodulation, FSK demodulation and AES decryption.



```
b'Hello to the World'
```

Figure 11: Receiver System Testing

4. CONCLUSION

The proposed security methodology for WLAN network is simulated and validated by the developed simulation Python software. Results obtained by several runs are presented in this paper and clearly showing the legality and authority of the proposed method.

From the results of simulation, figure 10, it is apparent that the message "Hello to the Word" using 16 Bytes key is transmitted as symbols without meaning. Only at desired receiver, the message is correctly accepted.

REFERENCES

[1] S. Lindroos, A. Hakkala, S. Virtanen. "A systematic methodology for continuous WLAN abundance and security analysis" *Computer Networks*, Volume 197, 9 October 2021, 108359, https://doi.org/10.1016/j.comnet.2021.108359

[2] K. G. Paterson, B. Poettering, and J. C. N. Schuldt. "Plaintext Recovery Attacks Against WPA/TKIP". *International Workshop on Fast Software Encryption*, April 2015, DOI:10.1007/978-3-662-46706-0_17

[3] M. Vanhoef, F. Piessens. "Key reinstallation attacks: Forcing nonce reuse in WPA2", in: *Proceedings of the 2017 ACM SIGSAC Conference on Computer and Communications Security*, CCS '17, ACM, New York, NY, USA, 2017, pp. 1313–1328.

[4] R. Moskowitz. "Weakness in passphrase choice in WPA interface", https://wifinetnews.com/archives/2003/11/weakness_in_passphrase_choice_in_ wpa_interface.html. (September 2020).

[5] M. Cermak, M. Svorencik, R. Lipovsky, O. Kubovic, KR00K. "Serious Vulnerability Deep Inside Your Wi-Fi Encryption", Tech. rep., ESET, 2020.

[6] T. Roth. "Breaking encryptions using GPU accelerated cloud instances", in: Black Hat Technical Security Conference, Las Vegas, NV, USA, pp. 1–9.

[7] S. Viehbock. "Brute forcing Wi-Fi Protected Setup" https://sviehb.files.wordpress.com/2011/12/viehboeck_wps.pdf