CHAPTER V

SYSTEM EVALUATION

5.1 INTRODUCTION

This chapter highlights the experiments and the evaluation that have been carried out to the TX and RX systems, it includes a step by step output for each execution phase for the project as shown in Figure 4.7. The chapter is organized as follows: section 5.2 shows preparation for and physical arrangement of the system. Section 5.3 shows the steps of the TX system and the output for each phase. Section 5.4 shows the steps of the RX system and the output of each phase. Section 5.5 is the conclusion of this chapter.

5.2 PREPARATION OF THE EXPERIMENT

The project contains two systems, An SDR TX system that will act as FM station, and an SDR RX system that will act as a WSN base station. The next sections will show the result for the phases that can be shown in figure 4.6 for the TX and RX systems. Figure 5.1 shows the two systems that contain a laptop connected to HackRF (acts as FM station) and a raspberry pi that is connected to an RTL-SDR dongle which acts as the WSN Base Station. The TX system is using GNURadio live 3.7.8 live distribution installed on USB thumb drive, while Raspberry Pi 2 is using Raspian that is installed on an SD card.

The TX systems have a cpu i7 2.13 GHZ clock speed, with a 4GB RAM, while Raspberry Pi 2 model B has an A 900MHz quad-core ARM Cortex-A7 CPU with 1GB of RAM. The next sections show a step by step process for the TX and the RX systems.

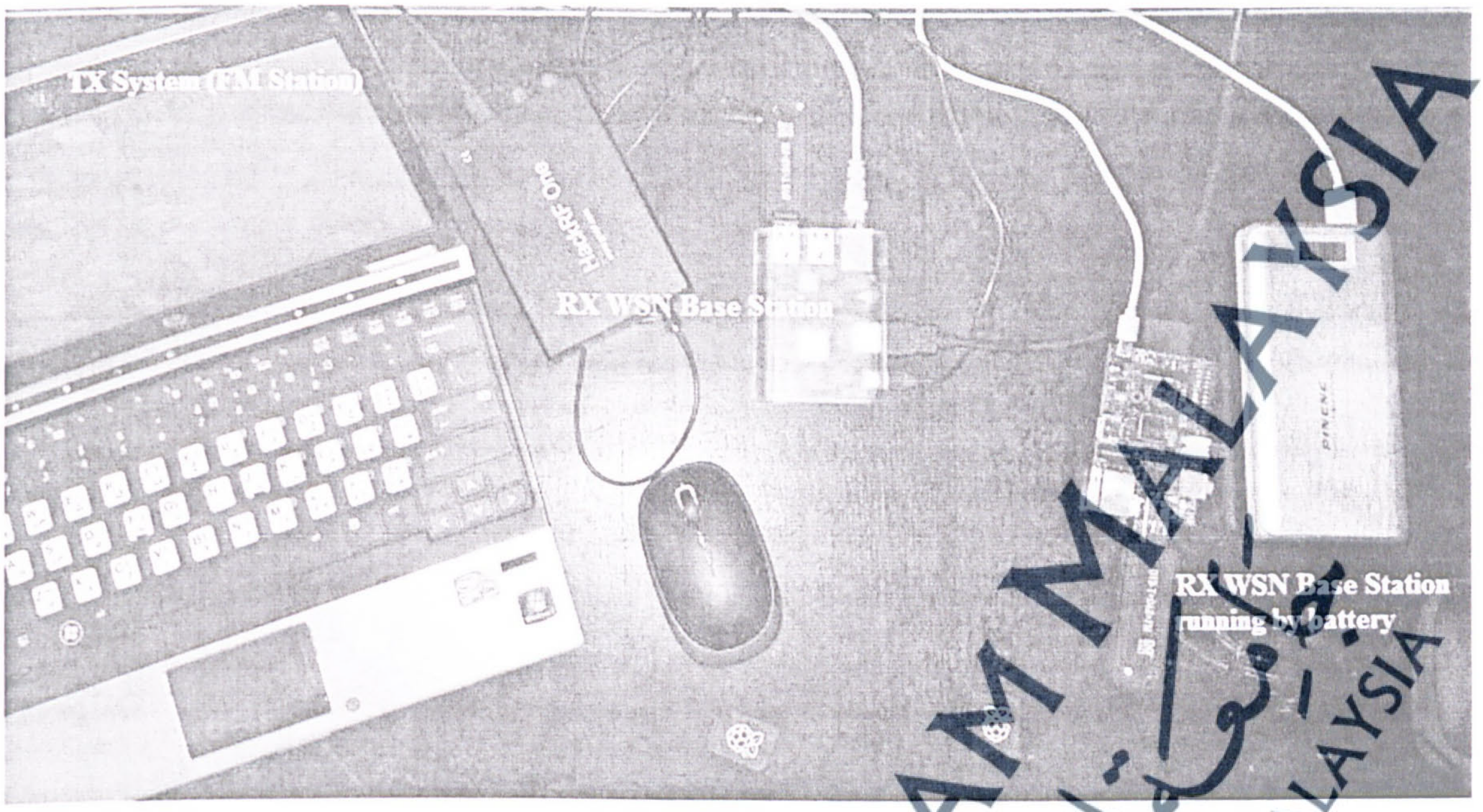

Figure 5.1: TX and RX full systems implementation.

5.3 WSN TX SYSTEM

Starting with the TX system, the system is divided into nine phases, each phase will be described in detail to give a better understanding to use.

5.3.1 INITIAL ECC PRIVATE KEY PHASE

The first phase is to create an initial ECC private key that will be used to encrypt the symmetric WSN key as shown in Figure 5.2, the initial key will be a combination of getting the current Linux user name using "whoami" Linux command (in our system username = 3140094) and the current date (Day, Year, Month), Figure 5.3 shows the output of the initial private key.

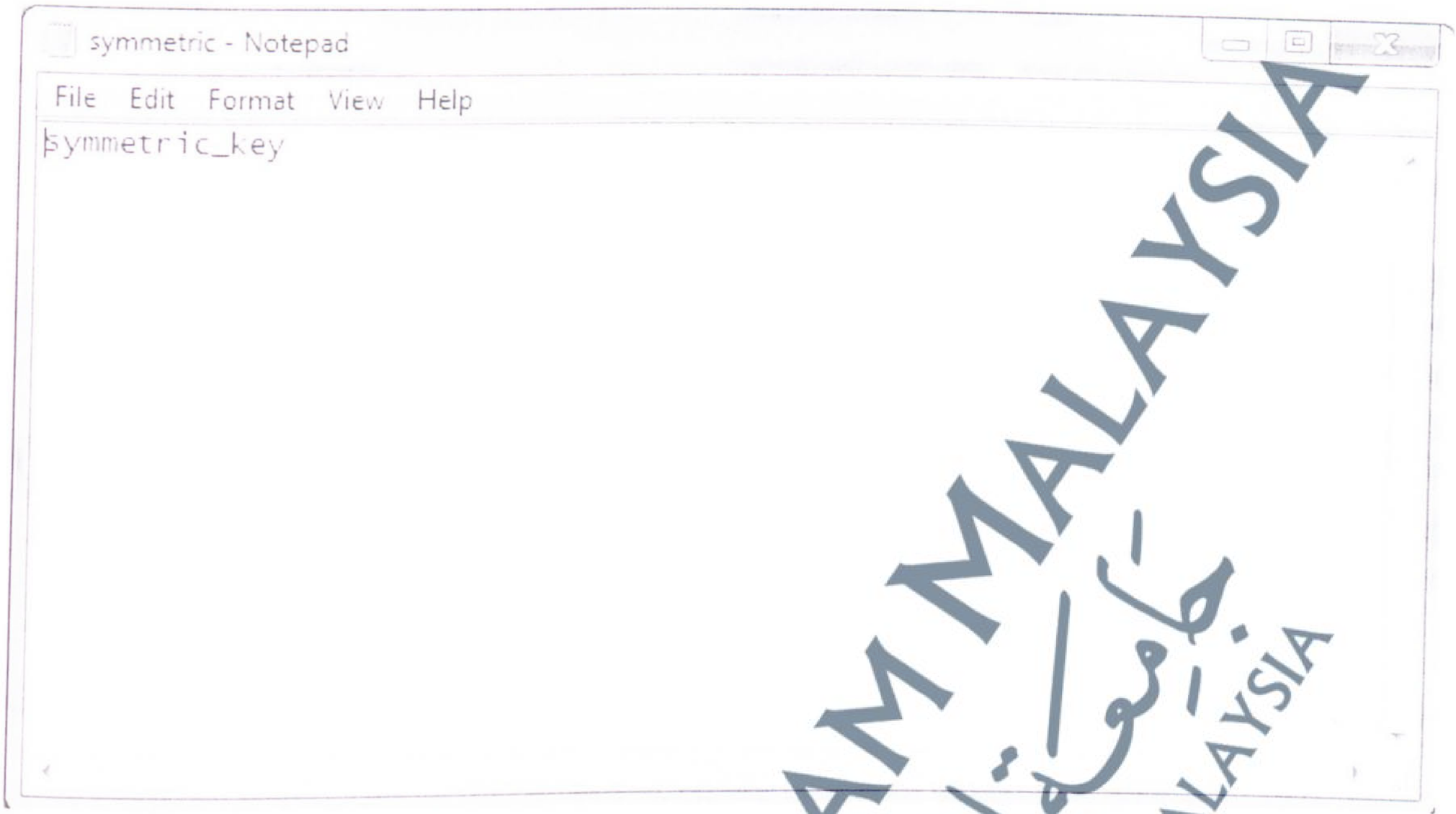

Figure 5.2: Symmetric Key

Figure 5.3: Initial ECC key creation.

5.3.2 CREATE PUBLIC KEY FROM PRIVATE KEY PHASE

Using SECCURE function, ECC public key will be derived from the ECC initial key, Figure 5.4 shows the result of deriving the public key from the private key.

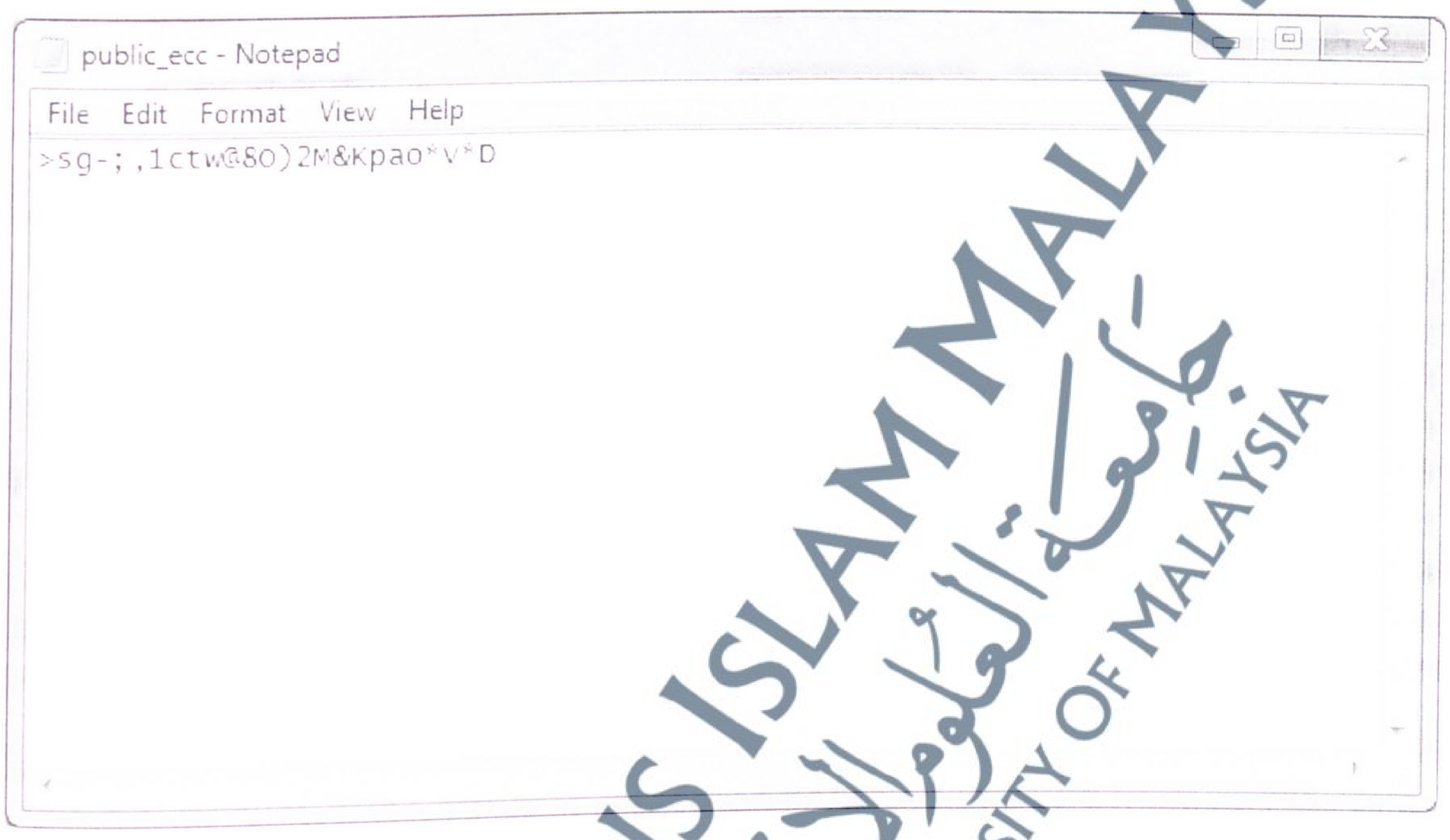

Figure 5.4: Output of Public ECC key derived from initial key using SECCURE function.

5.3.3 ENCRYPT SYMMETRIC KEY WITH ECC PUBLIC KEY PHASE

The WSN symmetric key will be encrypted with the ECC public key from previous step.

Figure 5.5 shows the output of the WSN symmetric key encryption.

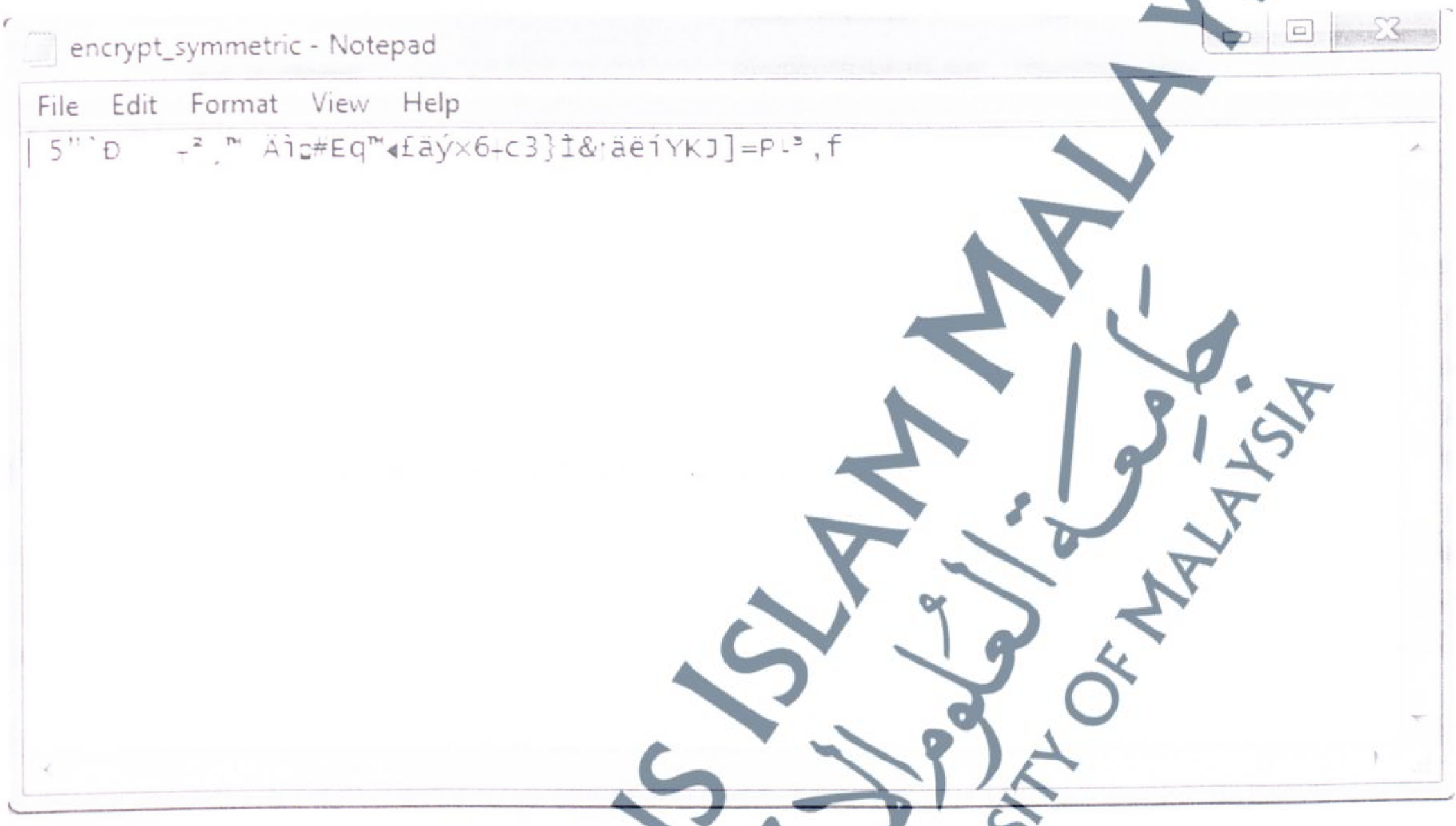

Figure 5.5: WSN Symmetric key encryption output.

5.3.4 CONVERT THE ENCRYPTED KEY TO BINARY PHASE

In this phase the encrypted key will be converted from ASCII to Binary, Figure 5.6 shows the output for converting the last phase result from ASCII to Binary.

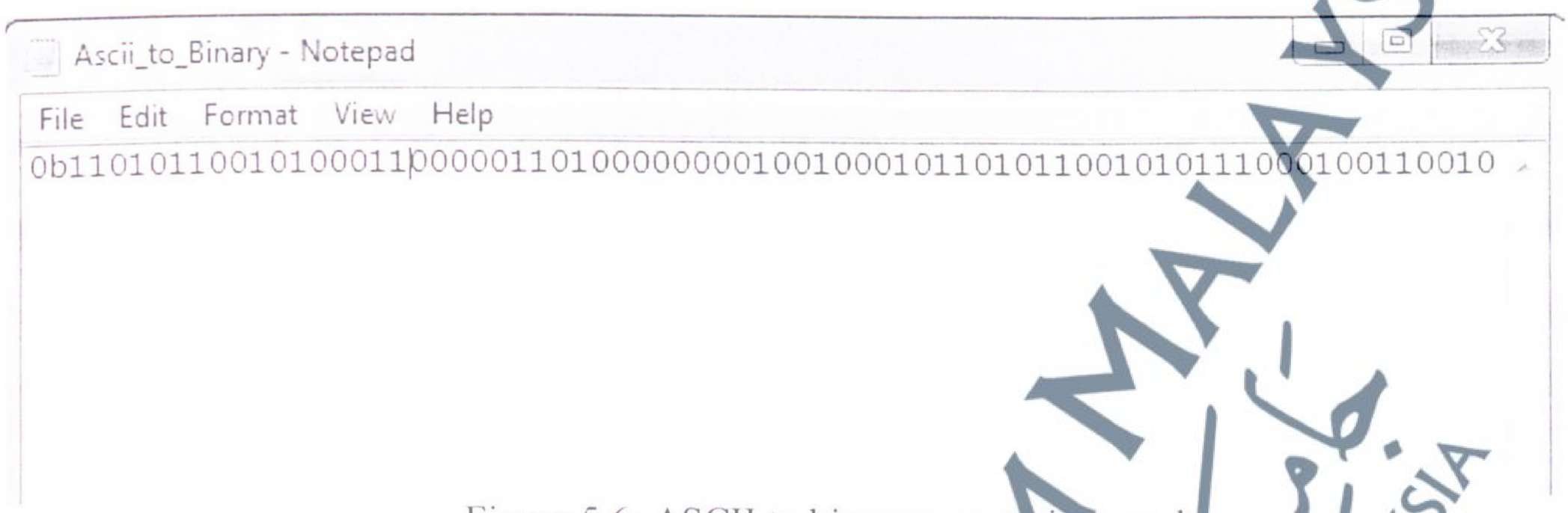

Figure 5.6: ASCII to binary conversion result.

5.3.5 FAKE CODE ENCAPSULATION PHASE

In this phase, fake code is added to the start and end of the last phase result, Figure 5.7 shows the result of adding the fake code.

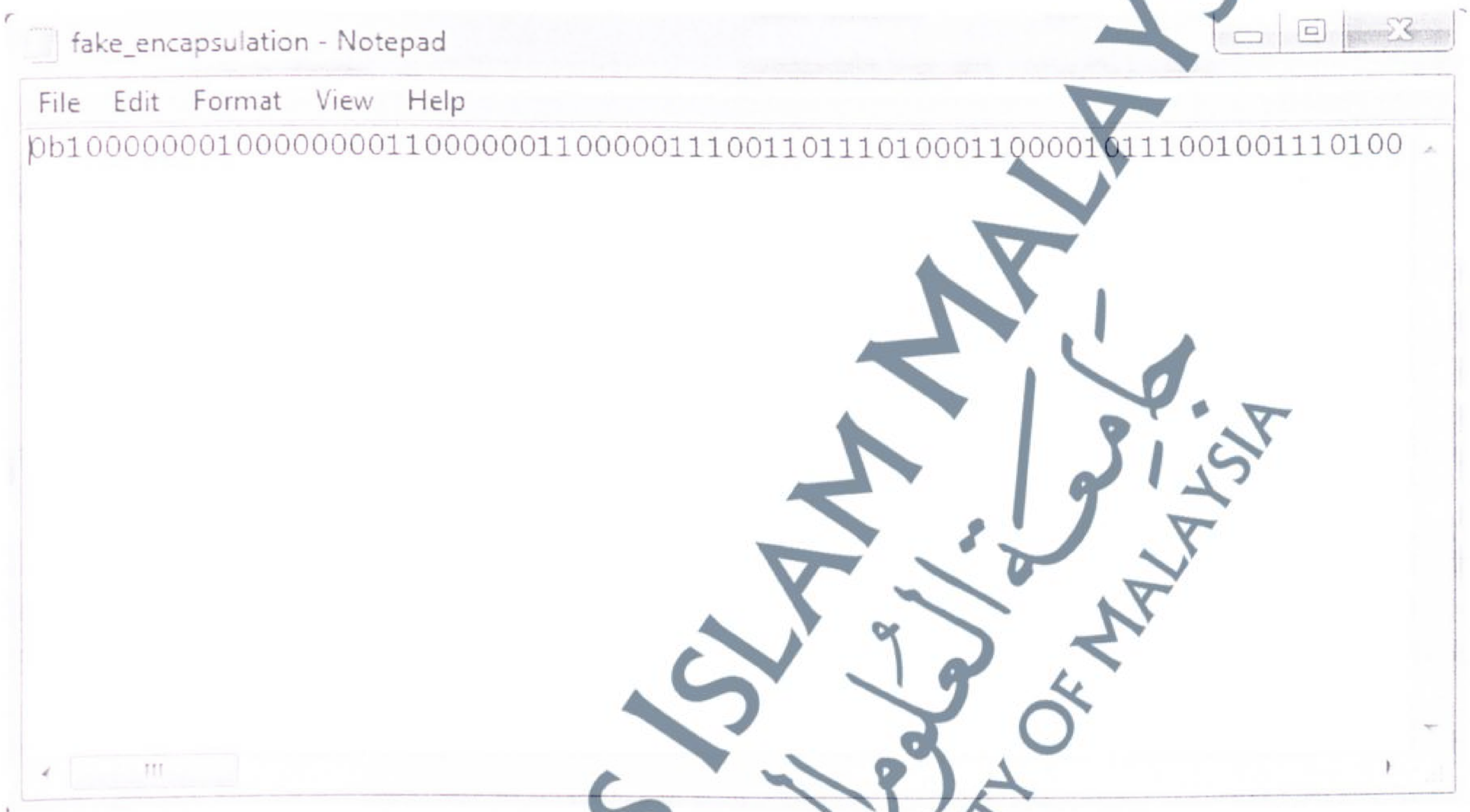

Figure 5.7: Fake code encapsulation phase.

5.3.6 SPREADING CODE PHASE

In this phase, a spreading code will be chosen depending on current time (minutes), the corresponding chosen spreading code will be XOR'd to spread with the output of the previous step. Figure 5.8 shows the spread output.

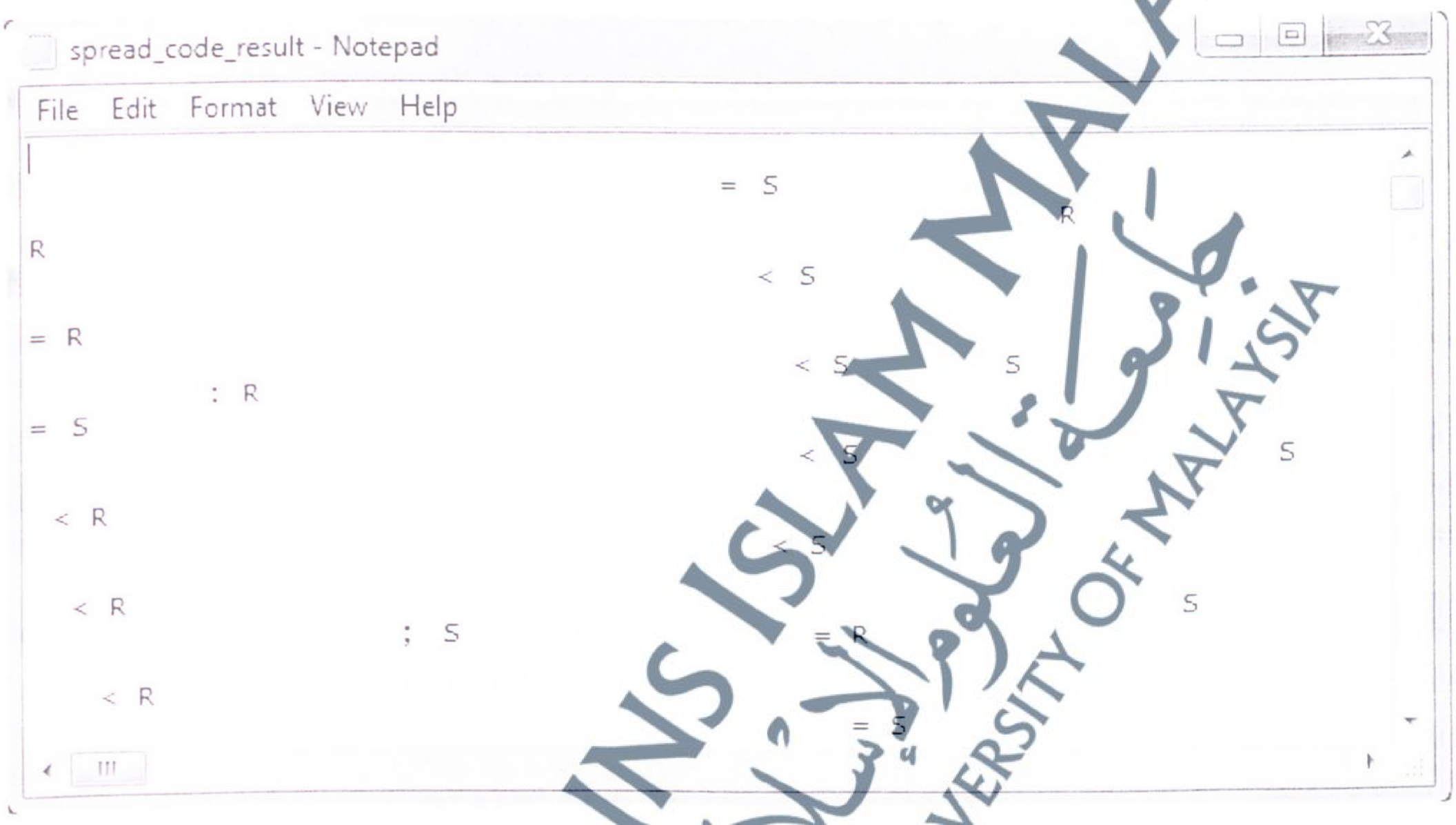

Figure 5.8: Spread Code phase result.

5.3.7 XOR ENCRYPTION PHASE

In this phase the spread code phase result will be XOR'd with binary code. Figure 5.9 shows the XOR encryption result.

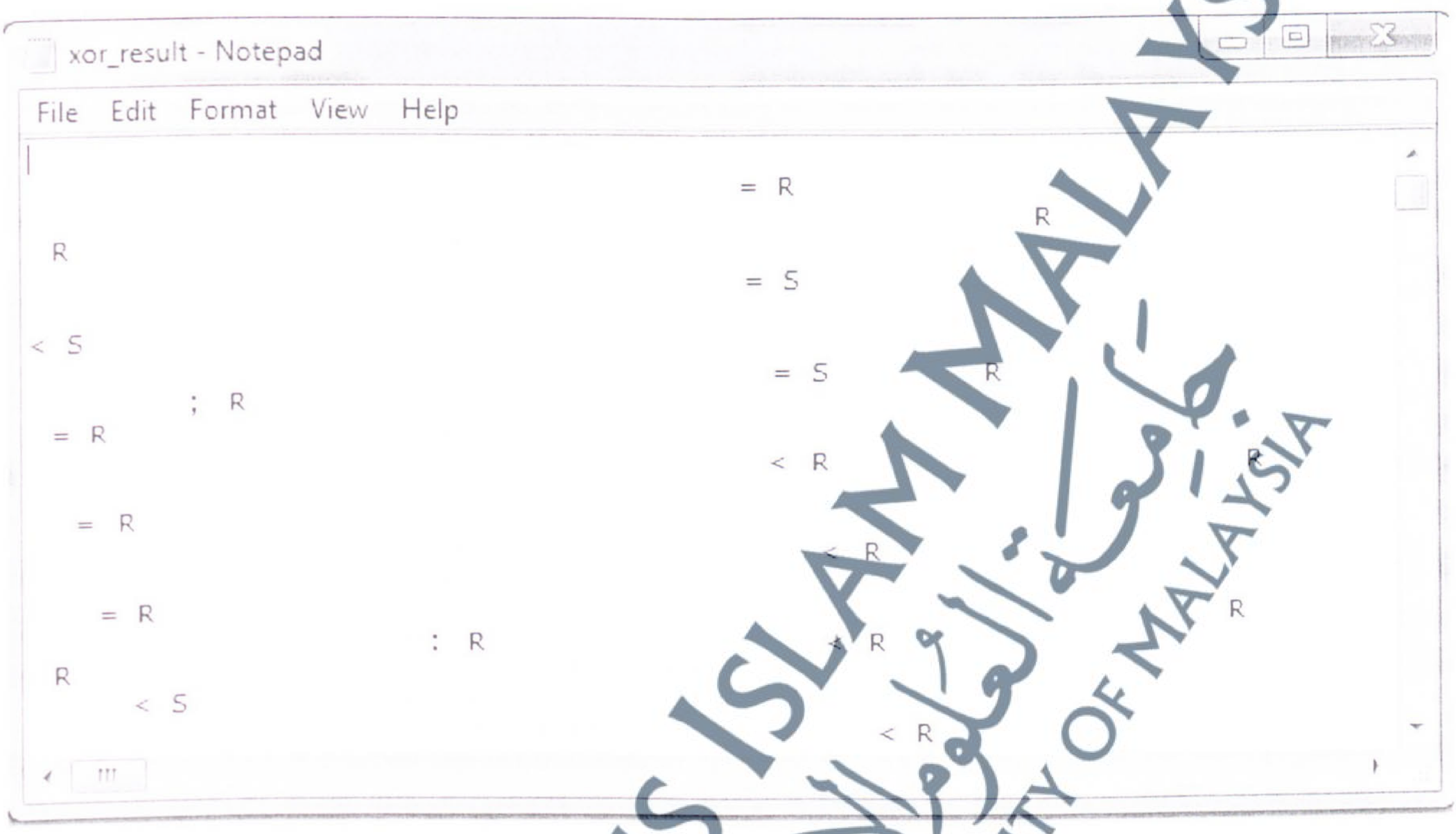

Figure 5.9: XOR encryption phase output.

5.3.8 PACKET ENCODER PHASE

In this phase packet GNURadio will encode the result of the last phase to prepare it for modulation phase.

Figure 5.10 shows the output of the encoder phase.

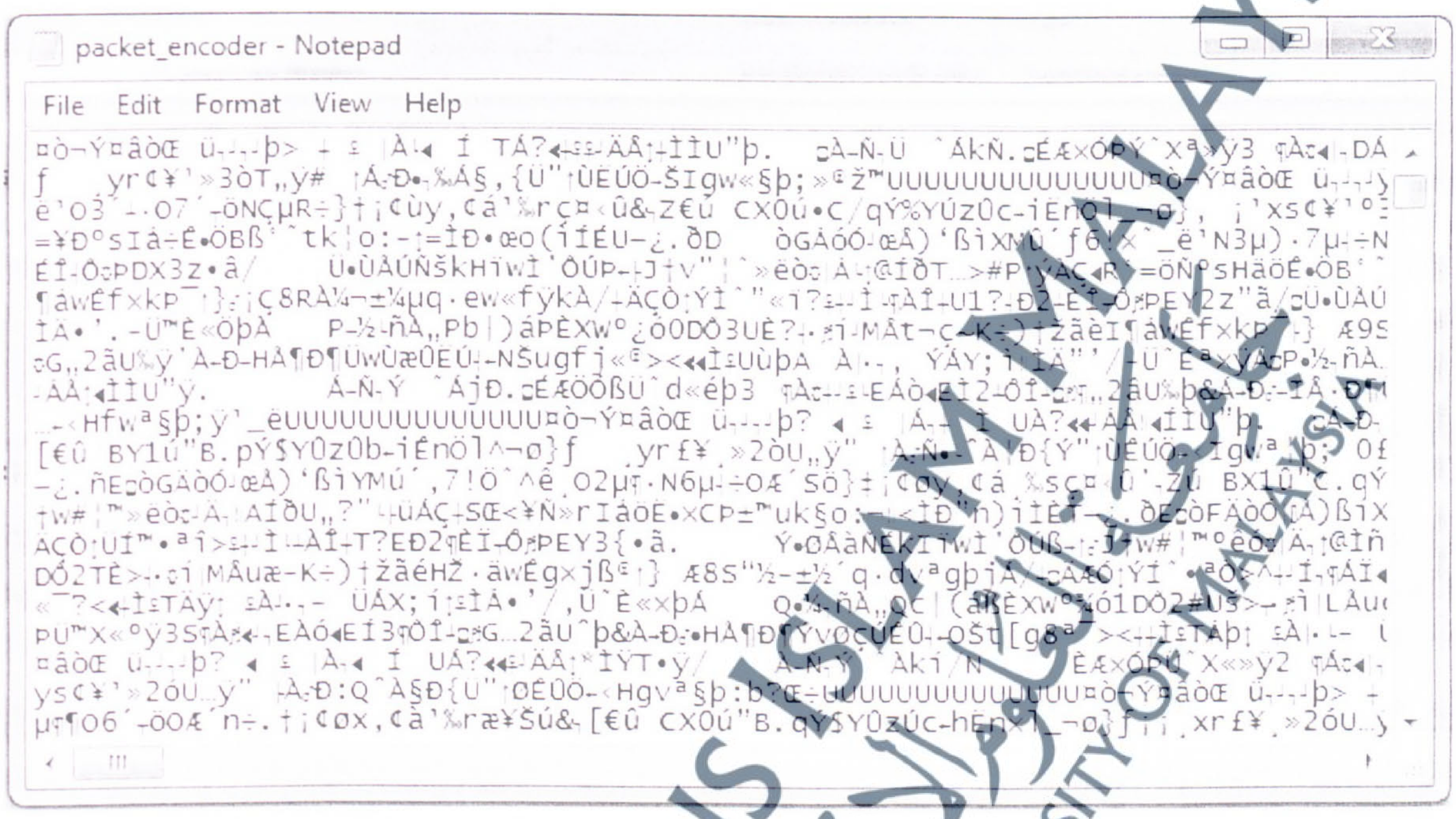

Figure 5.10 shows the output of the packet encoder phase.

5.3.9 GMSK MODULATION PHASE

This is the last phase before sinking data into the HackRF One, the output of the last phase will be modulated using GMSK. Figure 5.11 shows the output of GMSK Modulation phase.

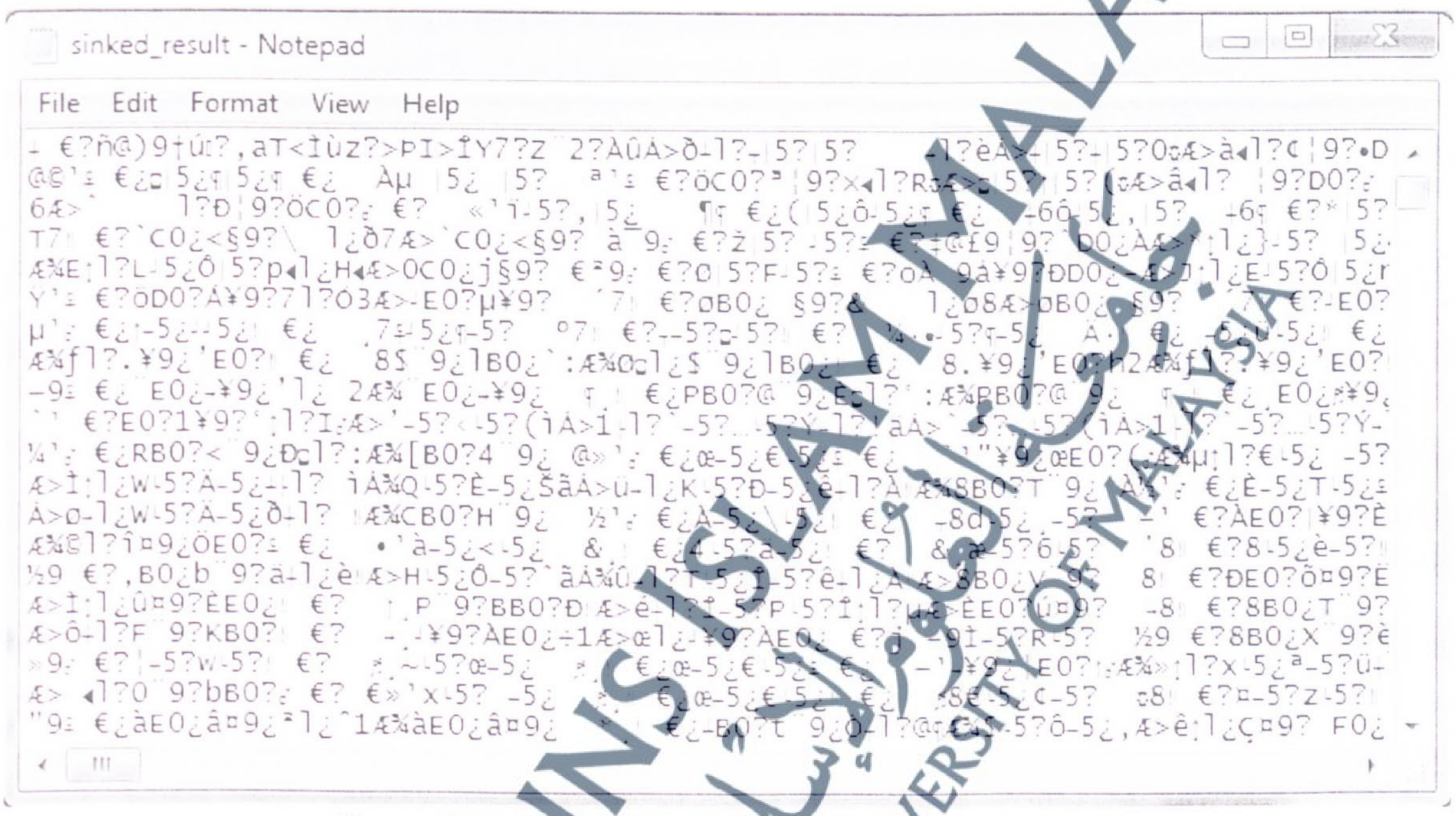

Figure 5.11 GMSK Modulation phase output.

5.4 WSN RX SYSTEM

The first phase in TX system is to create an initial ECC private key that will be used to encrypt the symmetric WSN key, the initial key will be a combination of getting the current Linux user name using "whoami" Linux command (in our system username = 3140094) and the current date (Day, Year, Month), Figure 5.12 shows the output of the initial private key.

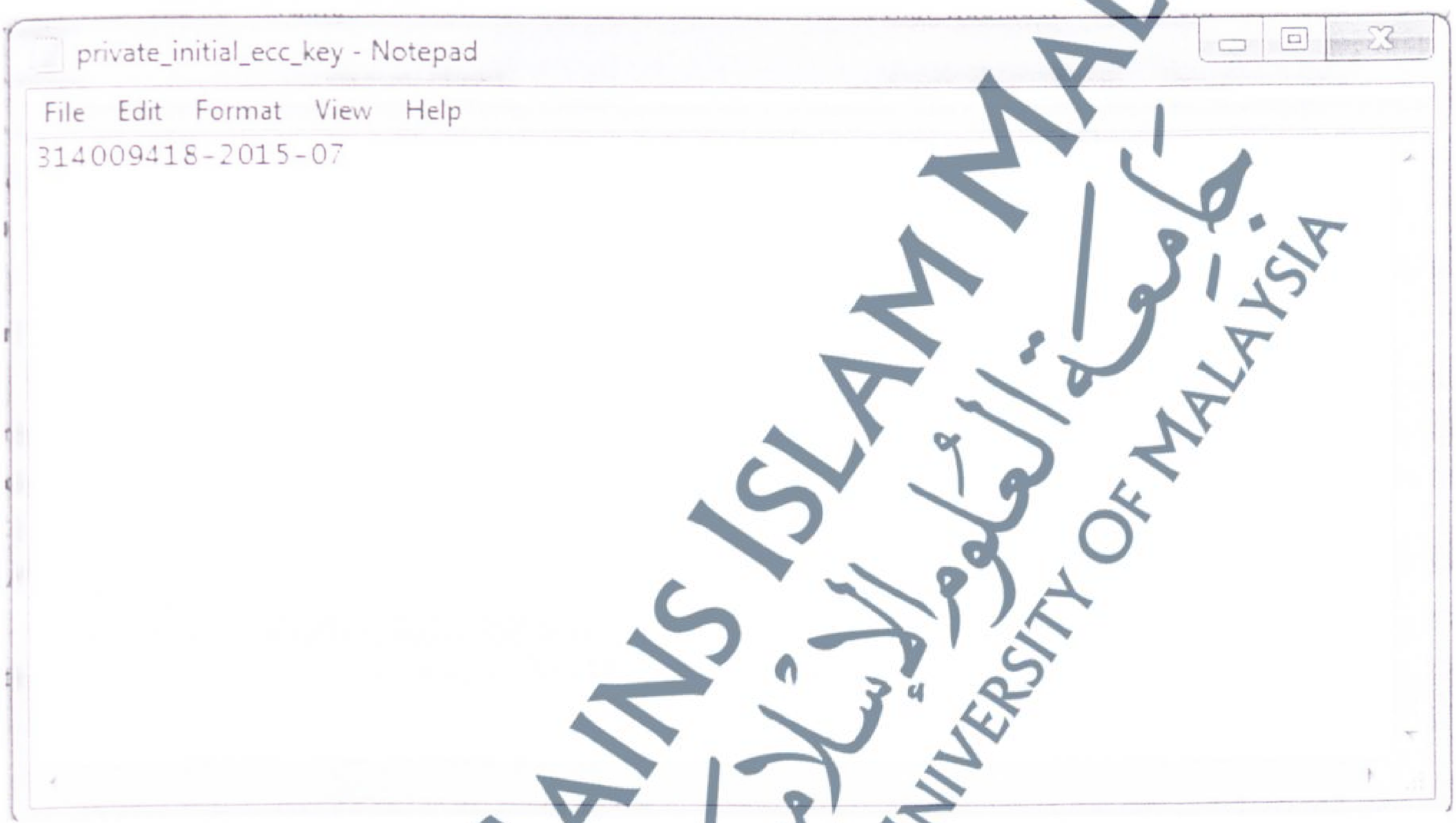

Figure 5.12: Symmetric Key.

5.4.1 GMSK DE-MODULATION PHASE

In this phase a GMSK demodulation process will start to demodulate the incoming signal.

No printed out put came out from phase as shown in Figure 5.13.

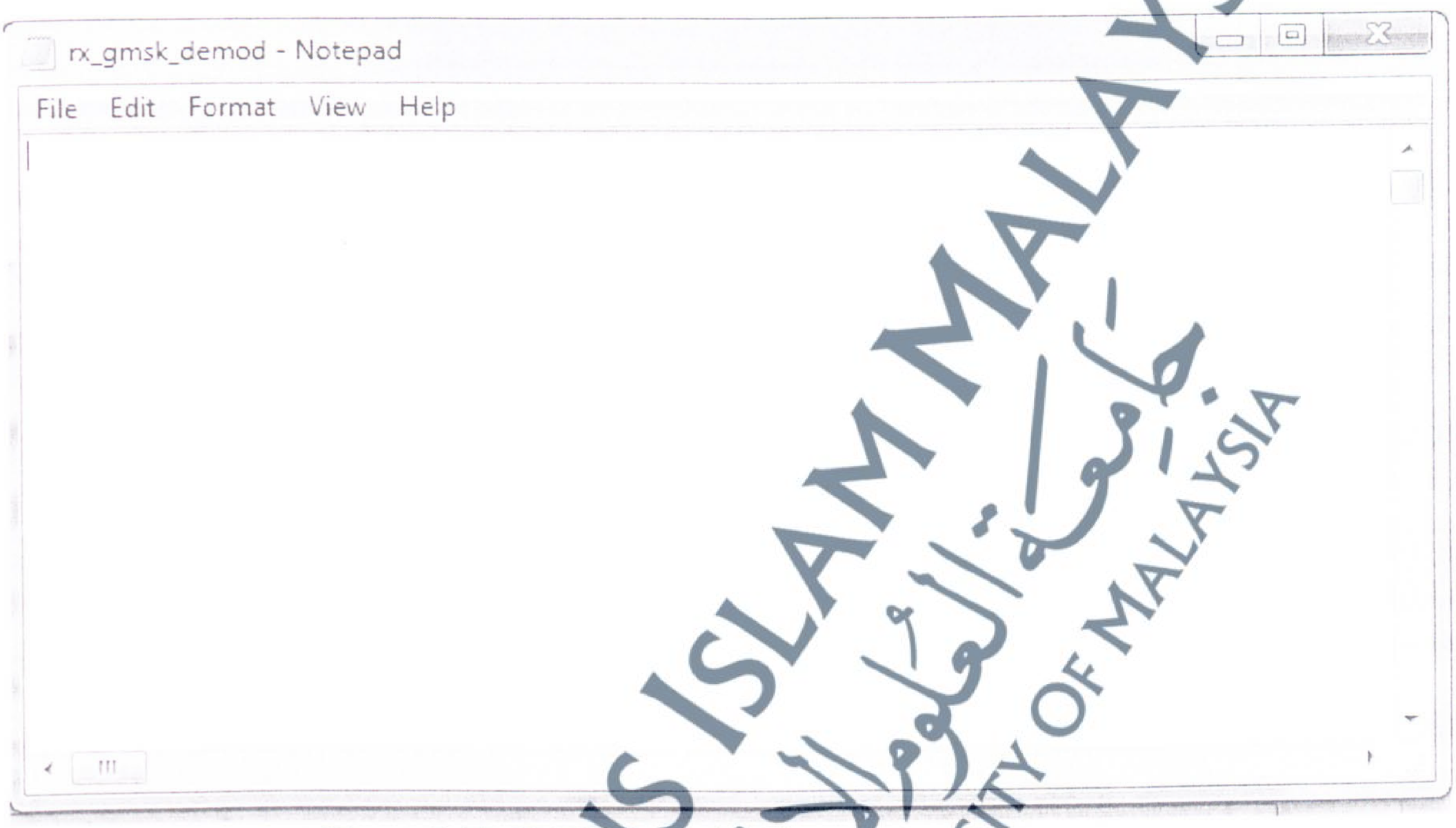

Figure 5.13 GMSK demodulation phase output.

5.4.2 PACKET DECODER PHASE

The output from the GMSK demodulation phase will be decoded. Figure 5.14 shows the packet decodes output.

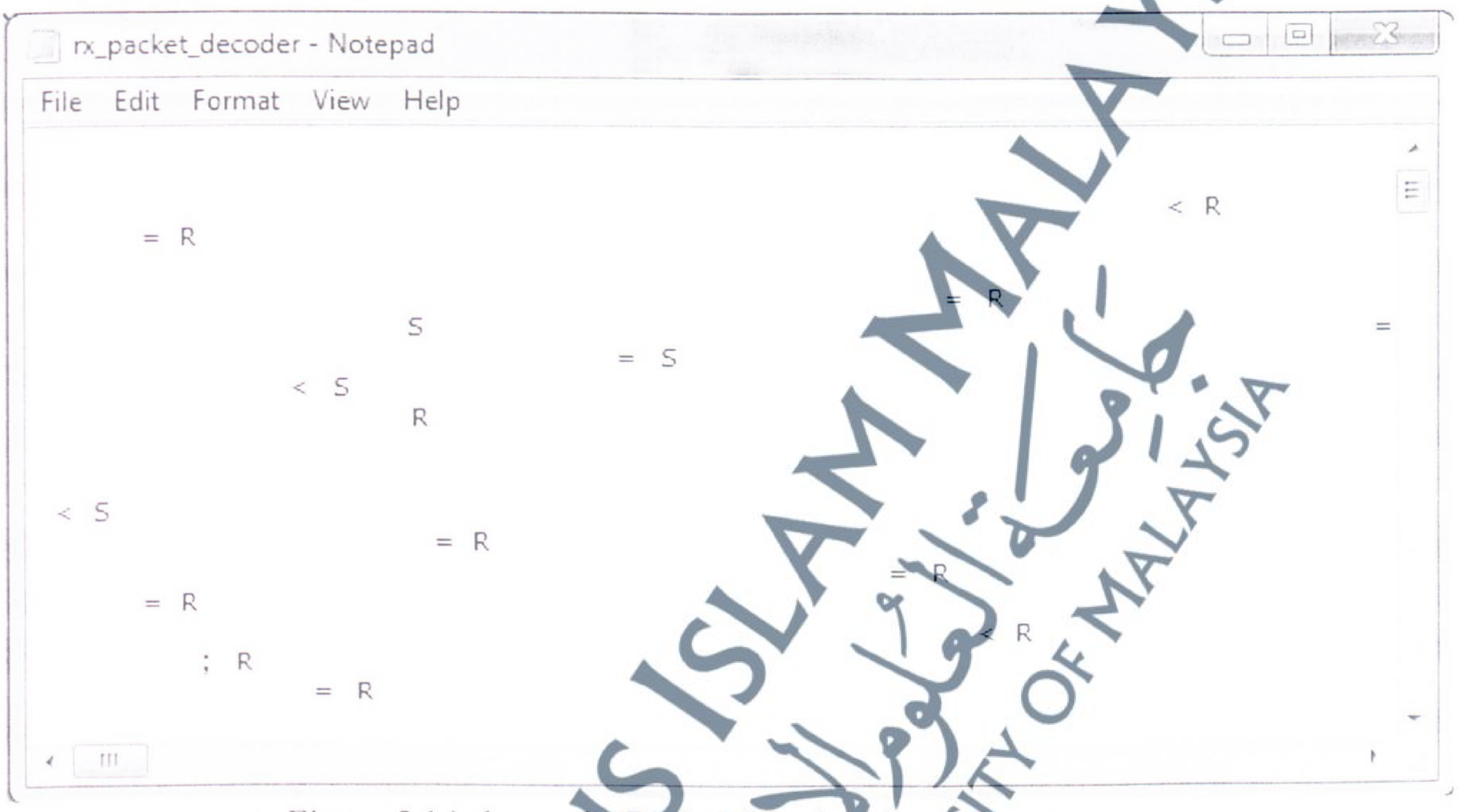

Figure 5.14 shows the Packet decoder phase output.

5.4.3 XOR DECRYPTION PHASE

The output of the packet decoder phase will be decoded by XOR with simple binary code.

Figure 5.15 shows the output of the XOR decryption phase.

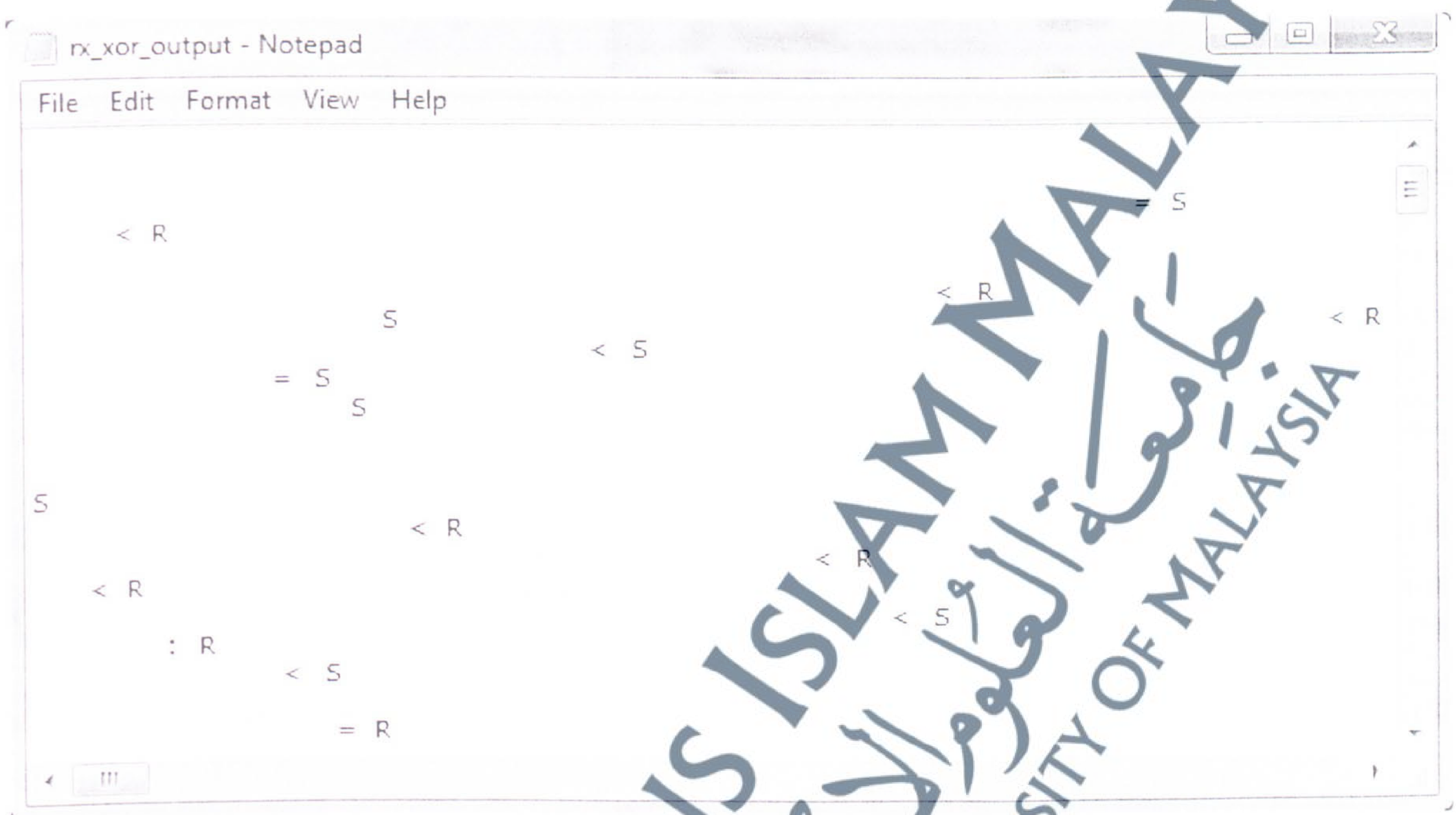

Figure 5.15: XOR decryption phase.

5.4.4 CODE DE-SPREAD PHASE

The output of the XOR decryption phase will be de-spread, same as RX system, the chosen spreading code depends on time. Figure 5.16 shows the output of the de-spread phase.

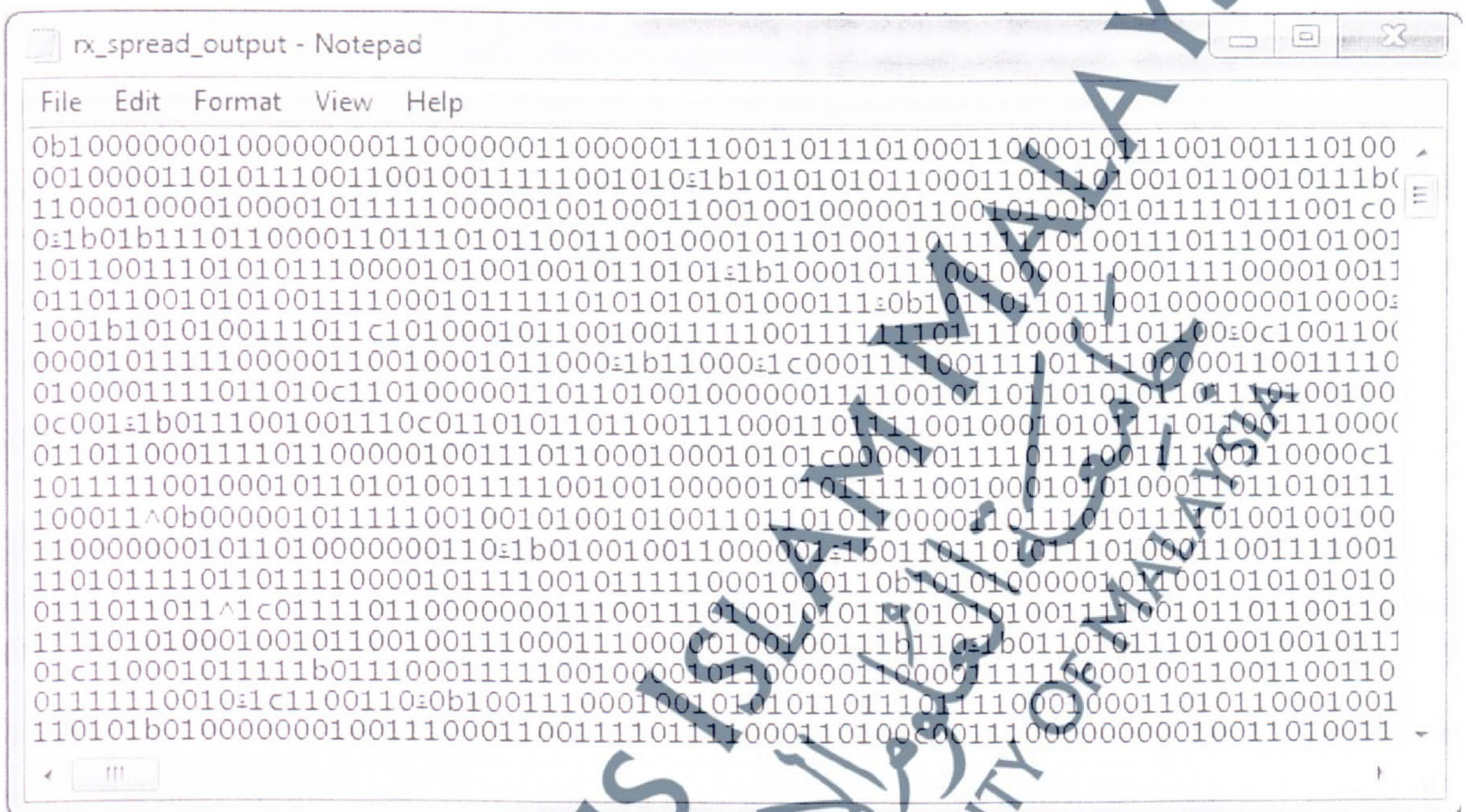

Figure 5.16: De-spread phase output.

5.4.5 FAKE CODE DE-CAPSULATION PHASE

In this phase, the output of the last phase will search for the prefix and suffix codes and save what's in between in a new file. Figure 5.16 shows the output of the de-capsulation phase.

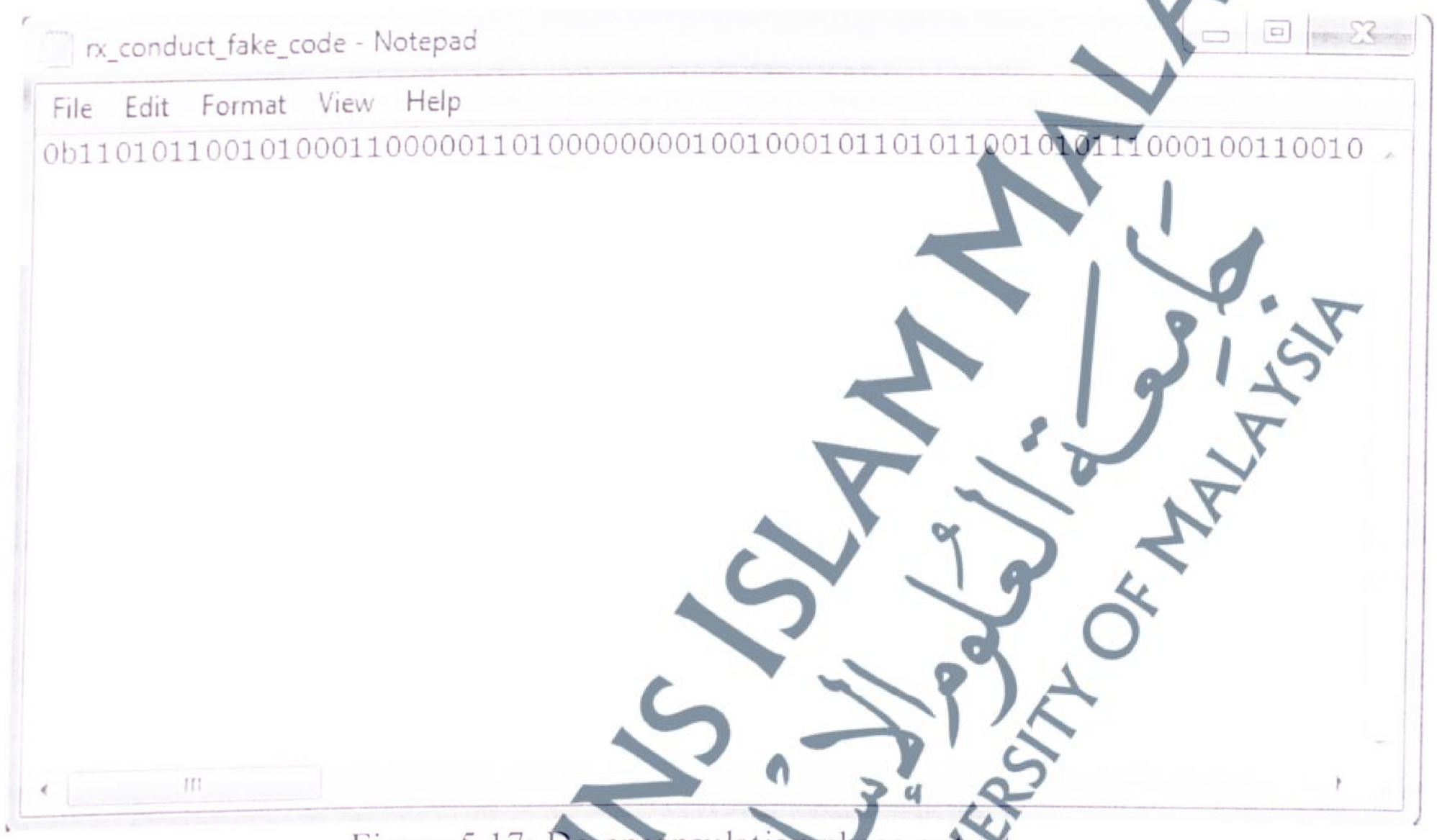

Figure 5.17: De-encapsulation phase output.

5.4.6 BINARY TO ASCII PHASE

The output of the last phase will be converted from binary to ASCII to gain the symmetric encrypted key. Figure 5.18 shows the output of the conversion phase.

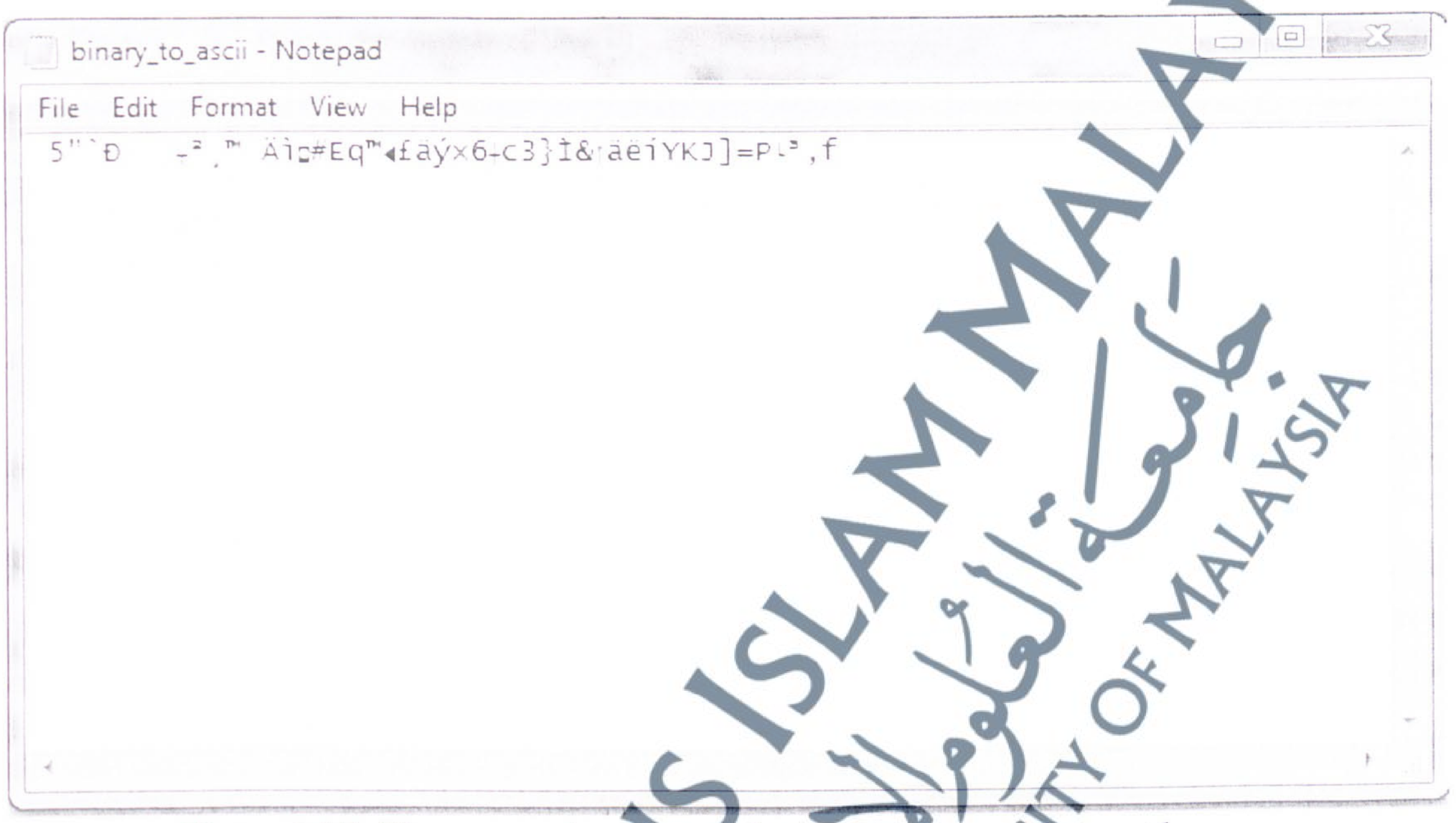

Figure 5.18: The conversion output shows the encrypted secret key.

5.4.7 SYMMETRIC KEY DECRYPTION PHASE

The output of last phase will be decrypted using the initial key to gain the symmetric key.

Figure 5.19 shows the decrypted secret key.

Figure 5.19: The final phase for gaining the secret key.

5.4.8 SEND THE SYMMETRIC KEY TO SENSOR NODES

The next phase is to send the symmetric key to WSN sensor nodes using ZigBee, but this is not within the research limit. The research limit is to send the key securely from FM station to the WSN base station.

5.5 CONCLUSION

This chapter described step by step evaluation for the TX and RX systems by showing the output of every phase; beginning with encrypting the secret key in the TX system and up to de-crypting the key in the RX system. ECC was used to encrypt the secret key and embed it in FM band, and send the key securely within few seconds as: first, it's hard to sniff because of the transmission's short time (to any listener, it is just an FM distortion), and the secure ECC encryption layer keeps the secret key safe.