## 3 Security of Wireless Sensor Network

In this section, we tried to analyze the security in ZigBee specification released by ZigBee Alliance, including whole security architecture, security mechanisms of each layer and the cryptography in current ZigBee specification.

At last, we provide a method of improving the encryption method in ZigBee specification. As a comparison, we formulate the current cryptography and the providing one.

### 3.1 Security Mechanism in ZigBee Specification

We learned about the security mechanisms elaborated in the specification released by ZigBee Alliance.

#### 3.1.1 Security Service Provider

As Specified in ZigBee Specification [1], security service provider includes methods for key establishment, key transport, frame protection and device management. As Fig.1 shows, ZigBee standard construct mechanisms for the network layer and application support sub-layer. Application support sub-layer provides security management and mapping services. ZDO is responsible for device management, including security policies management and security configuration management. Application layer provides the application services to ZDO and ZigBee.

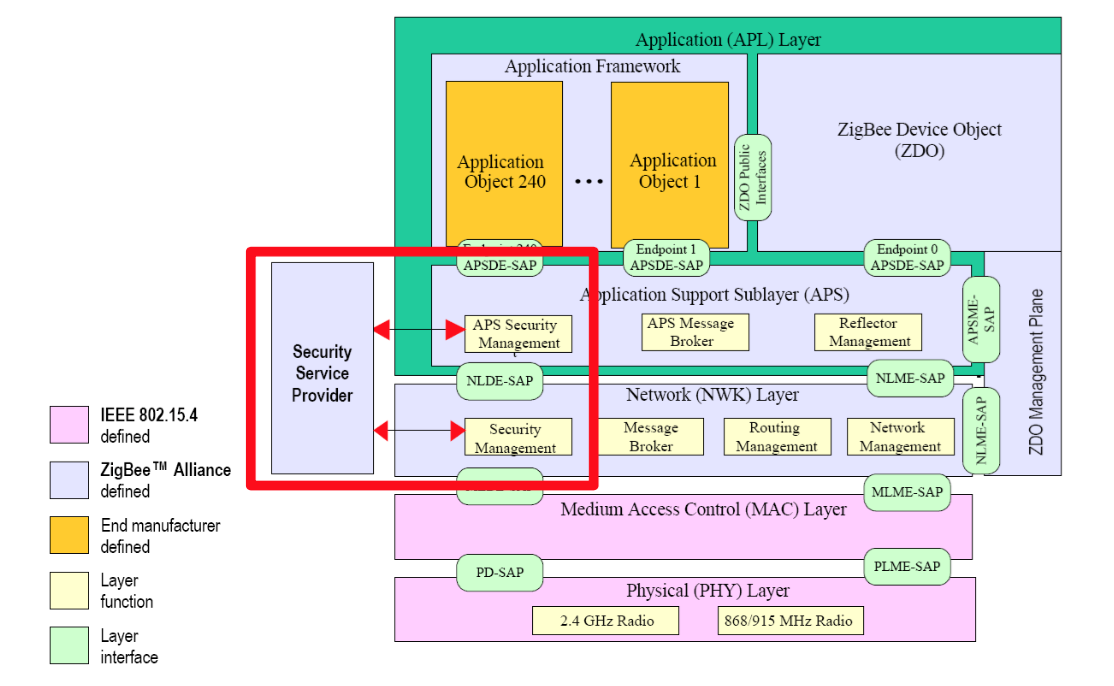


Fig.1 Security Service Provider in ZigBee stack [2]

#### 3.1.2 Security Design Choices

Based on the assumption of ZigBee security implementations, the ZigBee specification used the notion of Open Trust Model.

It allows re-use of the same keying material among different layers on the same device and it allows end-to-end security to be realized on a device-to-device basis rather than between pairs of particular layers (or even pairs of applications) on two communicating devices. [1]

#### 3.1.3 Security Keys

ZigBee devices use 128-bit symmetric encryption keys to provide security amongst a network. It is based on a link key and a network key.

Unicast communication between APL peer entities is secured by means of a 128-bit link key shared by two devices, while broadcast communications are secured by means of a 128-bit network key shared amongst all devices in the network. [1]

If using the security mode, the ZigBee stack will offer three types of keys used to secure communications:

(1) Master key:

used to derive the other key assisting symmetric key process. The network must first have the trust center to generate the master key to derive network key and link key to other devices.

(2) Network Key:

used to protect the confidentiality and integrity of broadcast and data. It also provide protection for network authentication. The network key is shared by multiple devices in the network, only in the broadcast message.

(3) Link key:

used to protect the confidentiality and integrity of the unicast data between two devices. The link key is only owned by two devices in communication, so that a single device requires multiple keys to protect each end to end session.

In ZigBee Pro, the administrator uses a symmetric key establishment method to derive network key and link key, but this requires the master key generated by the trust center.

#### 3.1.4 Trust Centre

As we mentioned above, Trust Center is a secure device for distributing keys and allowing devices to join the network. Trust Center has two modes, namely residential mode and business mode (known as the standard mode and high-safety mode in ZigBee Pro).

Residential mode consumes fewer resources, but does not create keys or expand with the growing of network size. Commercial mode establishes and maintains keys, therefore has good scalability, but it requires more memory. In order to reduce storage requirements, the commercial mode can also share security key for high security applications.

As known to all, there are three device types in a ZigBee network: coordinator, router, and end device. Trust center is an application among the network. In a wireless network, the coordinator usually configures the security level. In most applications, the coordinator is configured as trust center.

### 3.2 Security Risks

#### 3.2.1 Physical Attack

The most common way of attacking is physical attack. Most ZigBee devices record their keys in the hardware memory, attackers could get these keys by interfacing the devices. As known to all, the ZigBee devices use AES algorithm as the cryptography method. So that the key will be the same among the whole wireless sensor network. [3]

Obviously, it is a big risk of security.

#### 3.2.2 Eavesdropping Attack

When the ZigBee is working in non-secure mode, the transmission data will not be encrypted and therefore data may be eavesdropping from external.

As we did in the previous lab, Fig.2 shows the packet of communication among the wireless sensor network. With the Wireshark tool, we could get the data easily. As we see in this picture, the ‘AF Data’ in red square frame shows the ASCII of the data, it indicates the data is ‘2 blank 3’, ‘5’, ‘4 blank 5’ and ‘9’ respectively.

This undoubtedly left a security risk of wireless sensor network.

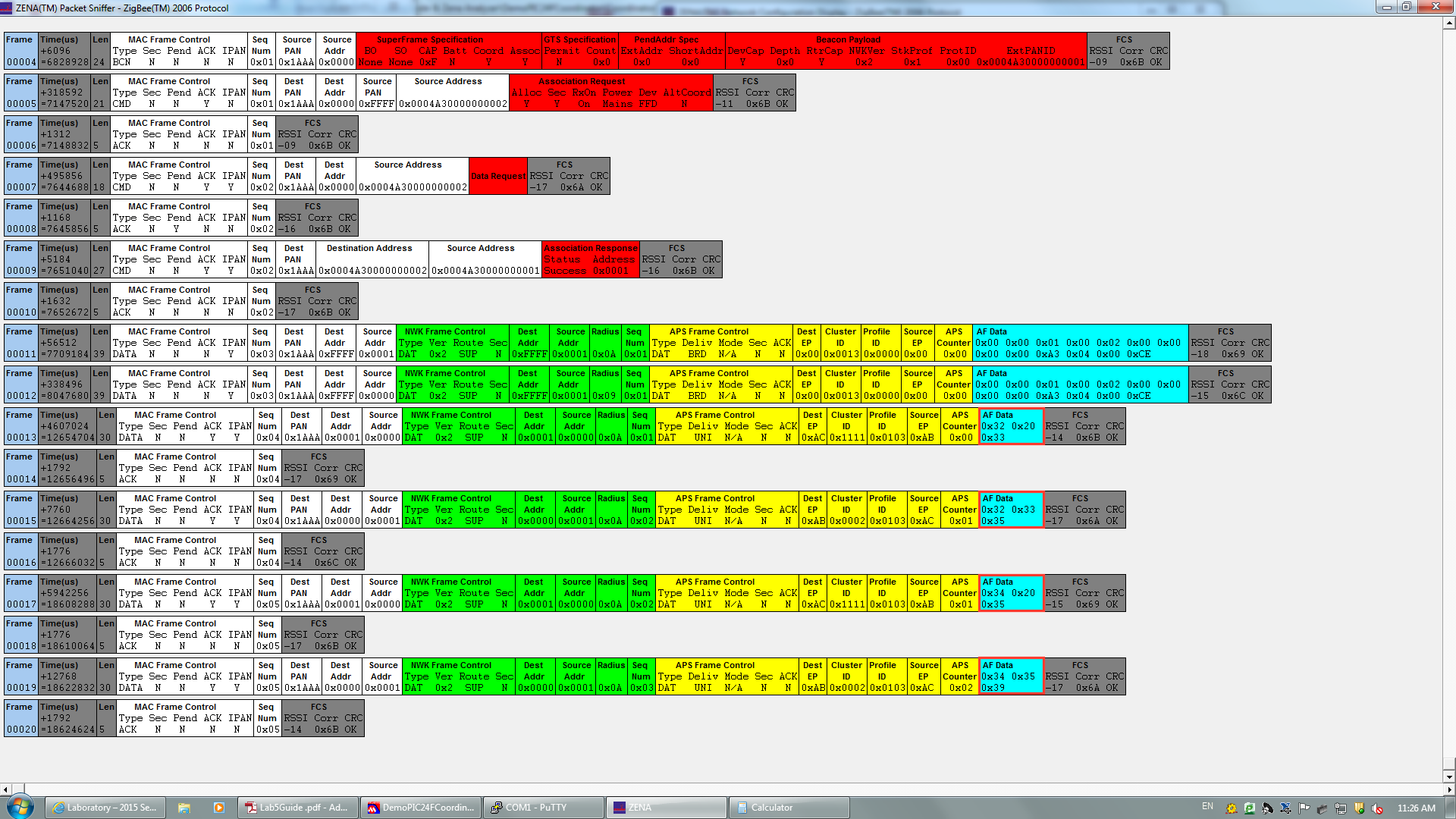


Fig.2 Packets of communication among WSN

#### 3.2.3 Security Key Attack

As the key may be transmitted in plain text during transmission process, therefore key is likely to be stolen and thus for decrypting the communication data.

In addition, attackers may use reverse engineering to analysis firmware of some of the smart devices, derive key to decrypt communications command, and then forged the trusted command to attack.

Researchers at Black Hat and Def Con warned about security flaws in Internet of Things devices. Li Jun and Yang Qing of Qihoo360's Unicorn team, presented their idea at Dec Con 23. [4] In their report, they focused on showing how to get the key by accessing to the devices and sniffering the network packets.

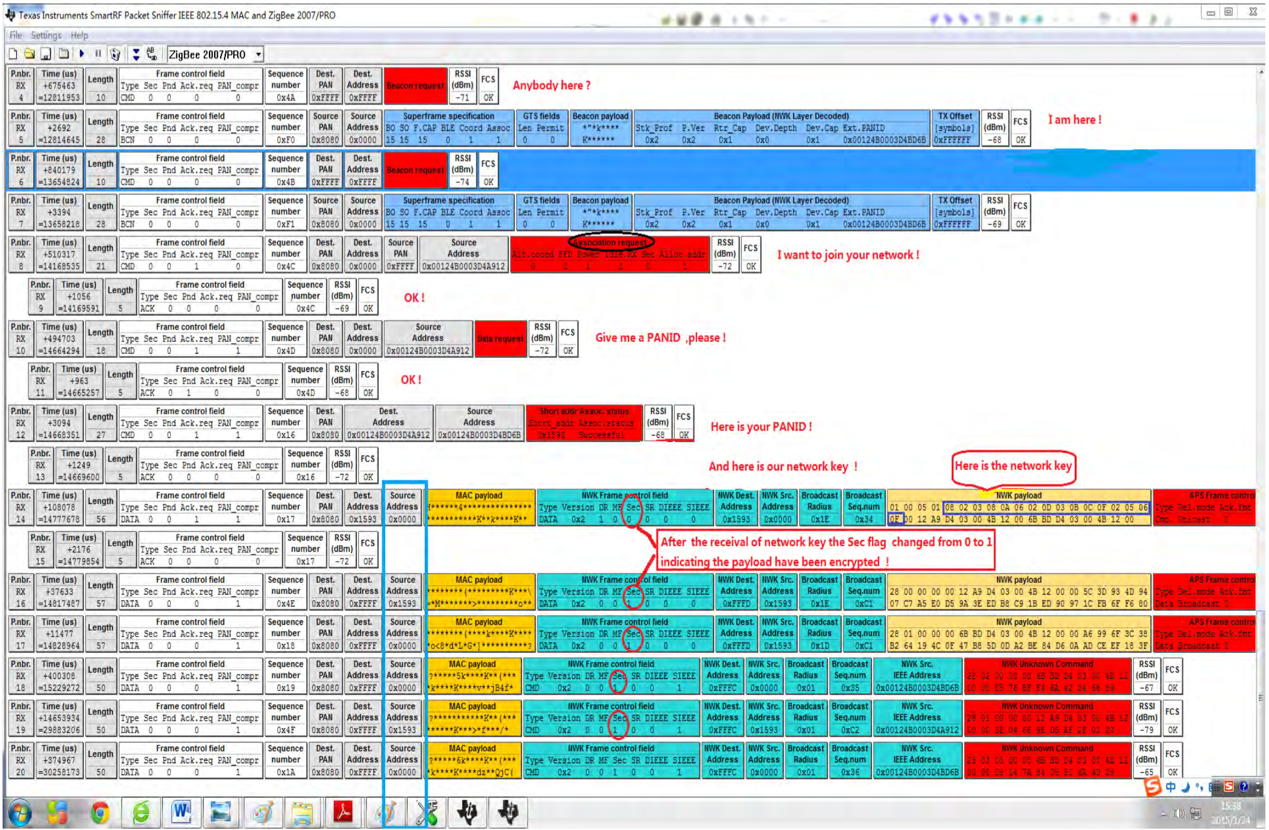


Fig.3 Find the encryption key by sniffing [4]

### 3.3 A Method of Improving ZigBee Security Performance

As we stated in 3.2.2, there is a security risk for the ZigBee network based on Microchip ZigBee Stack 2006. Attackers could easily get the data by sniffering the network. So that we implement the method of cryptography in order to improve the security of currently used Microchip hardware.

#### 3.3.1 Symmetric Key Cryptography

As we reviewed before, the ZigBee specification is using AES-128 method for cryptography. AES-128 is known as the symmetric key cryptography, which means both sides share the same private key for encrypting and decrypting.

The main reason for using symmetric key cryptography in embedded systems is that they are simple and fast. It has a very big security issue that both sides need to know the key in some way. In ZigBee networks, this private key is usually installed during the device production period.

AES is based on the Rijndael cipher developed by two Belgian cryptographers, Joan Daemen and Vincent Rijmen, who submitted a proposal to NIST during the AES selection process. [5]

We will elaborate our algorithm later in part 3.3.3.

#### 3.3.2 Cryptography based on Microchip ZigBee Stack

Our application is based on Microchip ZigBee Stack 2006, Microchip PIC24 MCU and MRF24J40 transceivers. As the security function in Microchip ZigBee Stack is only supplied in the Pro Stack version and is not free to use. So we choose to implement an AES-128 cryptography in the application layer.

We tested the method with a coordinator and router. When the coordinator sends a string, it will encrypt the string before sending. The router gets the encrypted string and decrypts it into the real message, then it will send it back with plain text to coordinator for verifying. Figures below shows the Serial command and the packets sniffered among transmission.

Case 1: Input Plain text is “helloworldabcdef”.

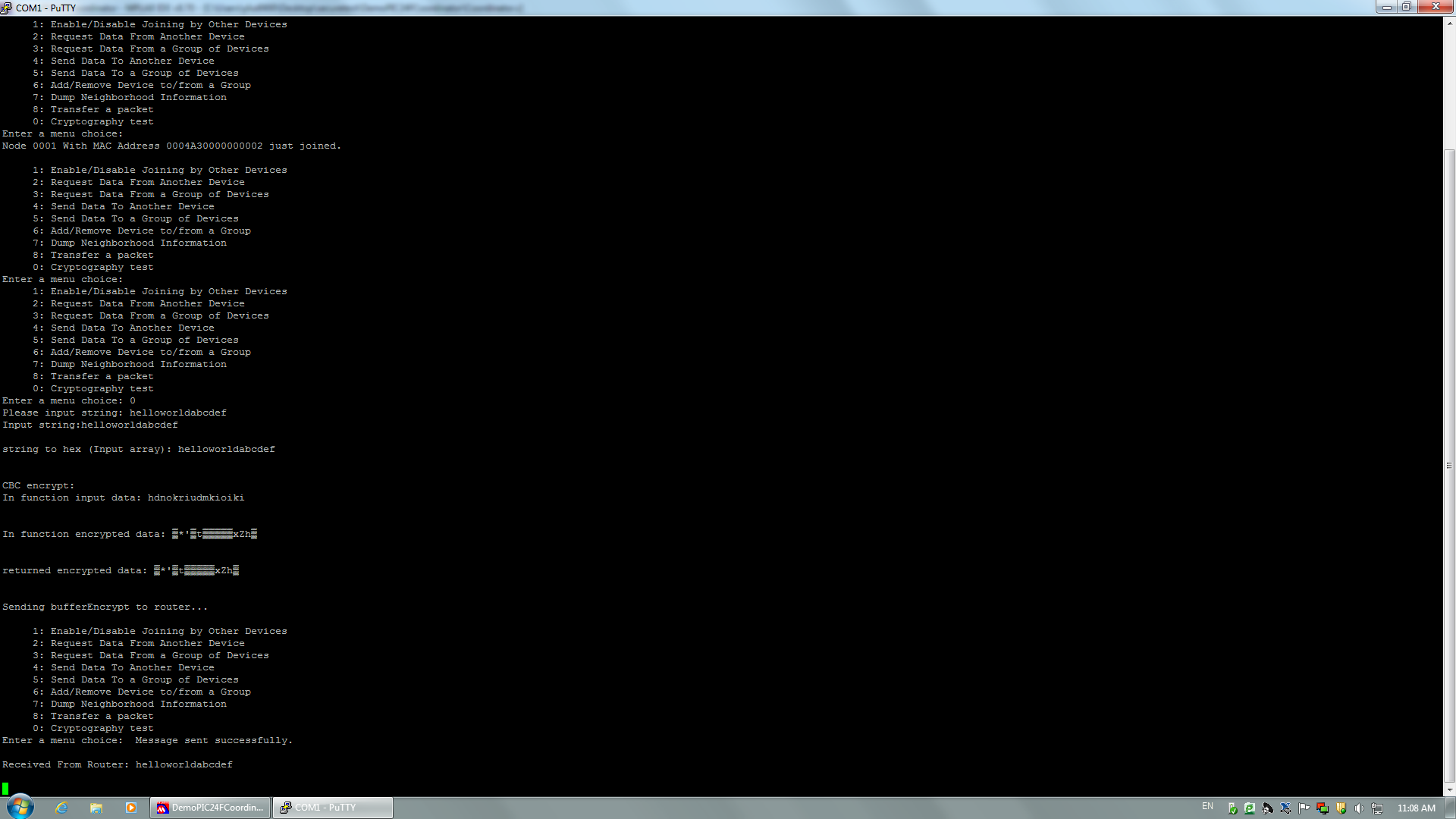


Fig.4 Serial command of Case 1

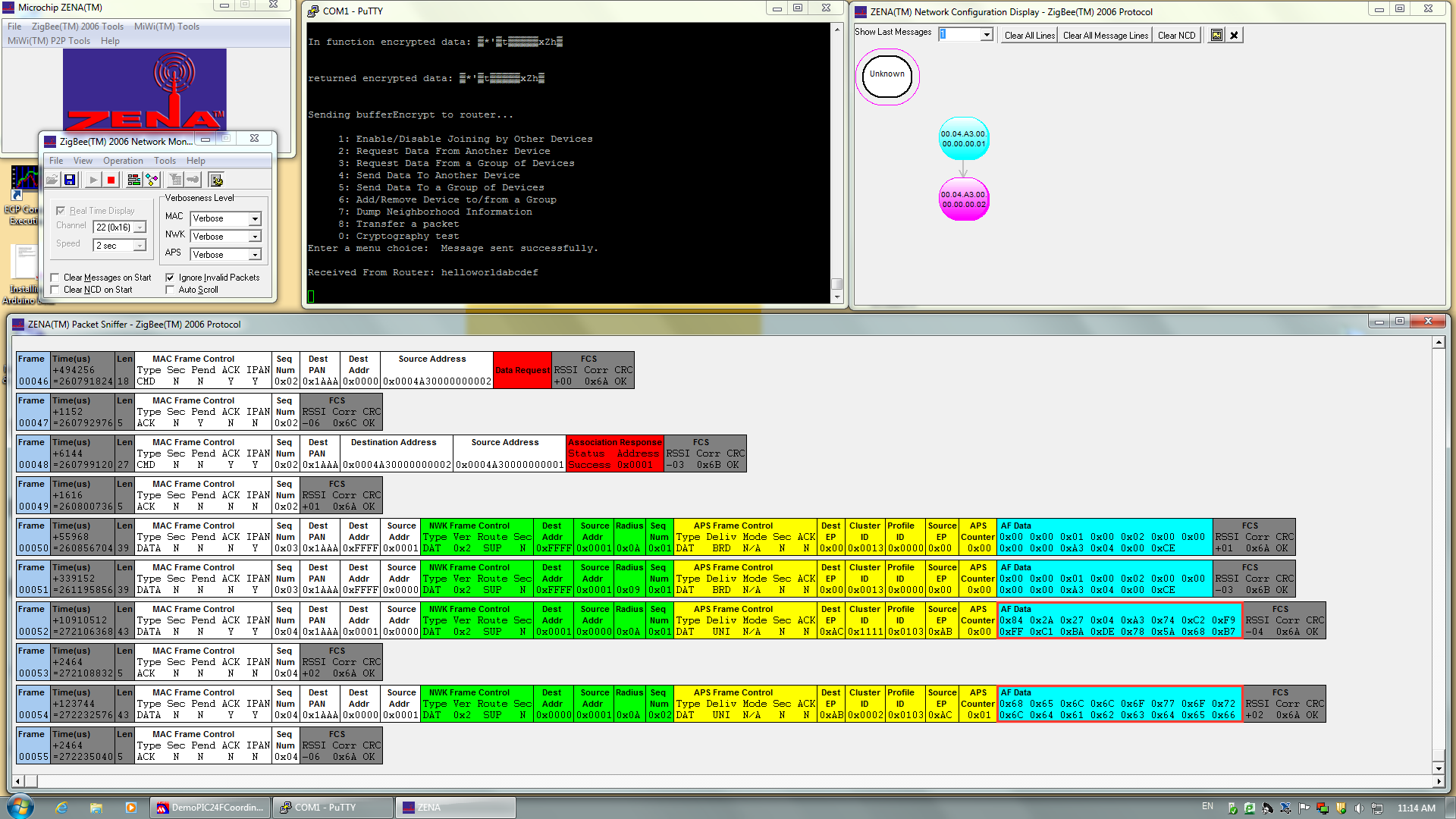


Fig.5 Transmission packets of Case 1

Case 2: Input Plain text is “abcdefghijklmnop”.

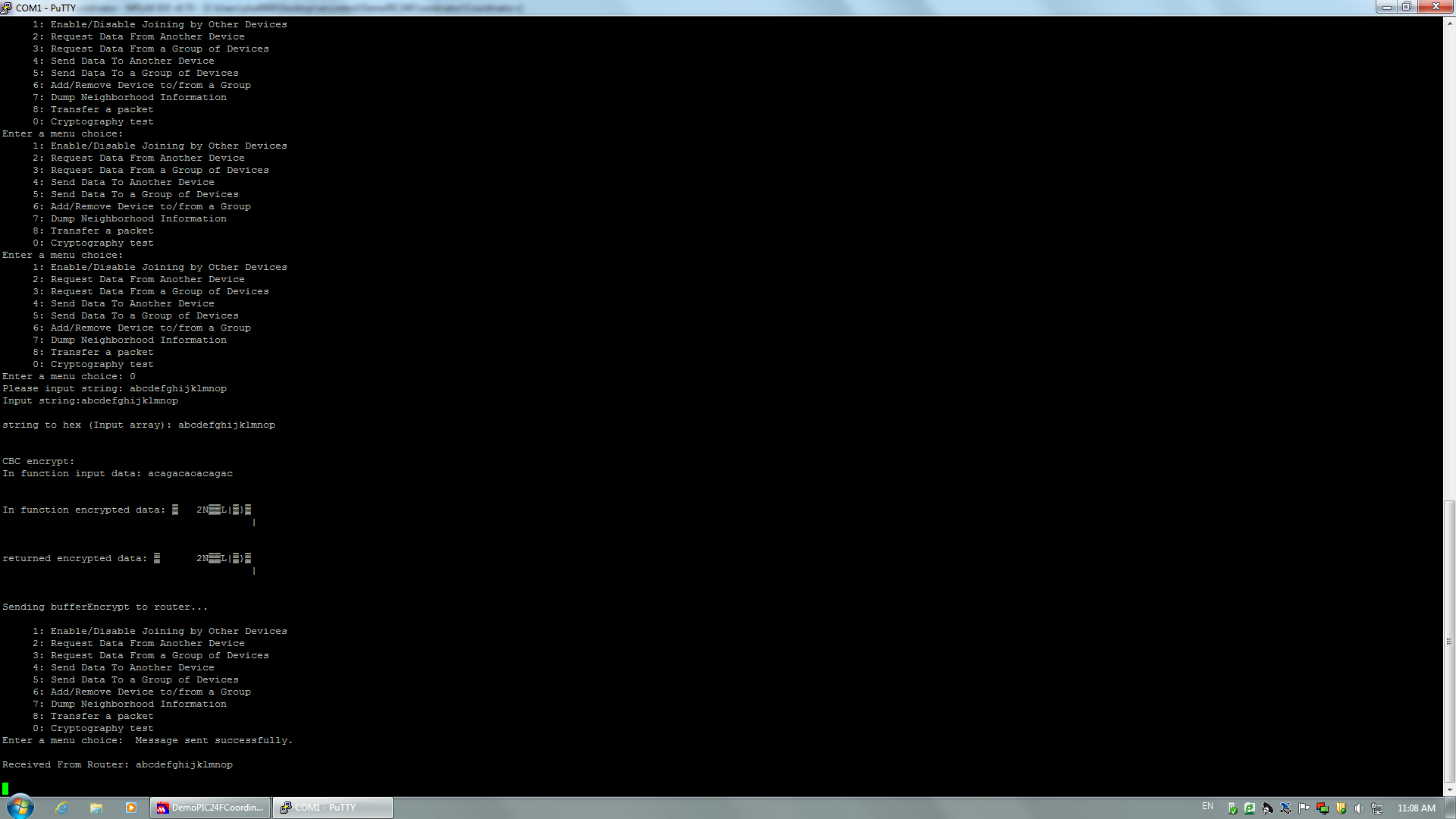


Fig.6 Serial command of Case 2

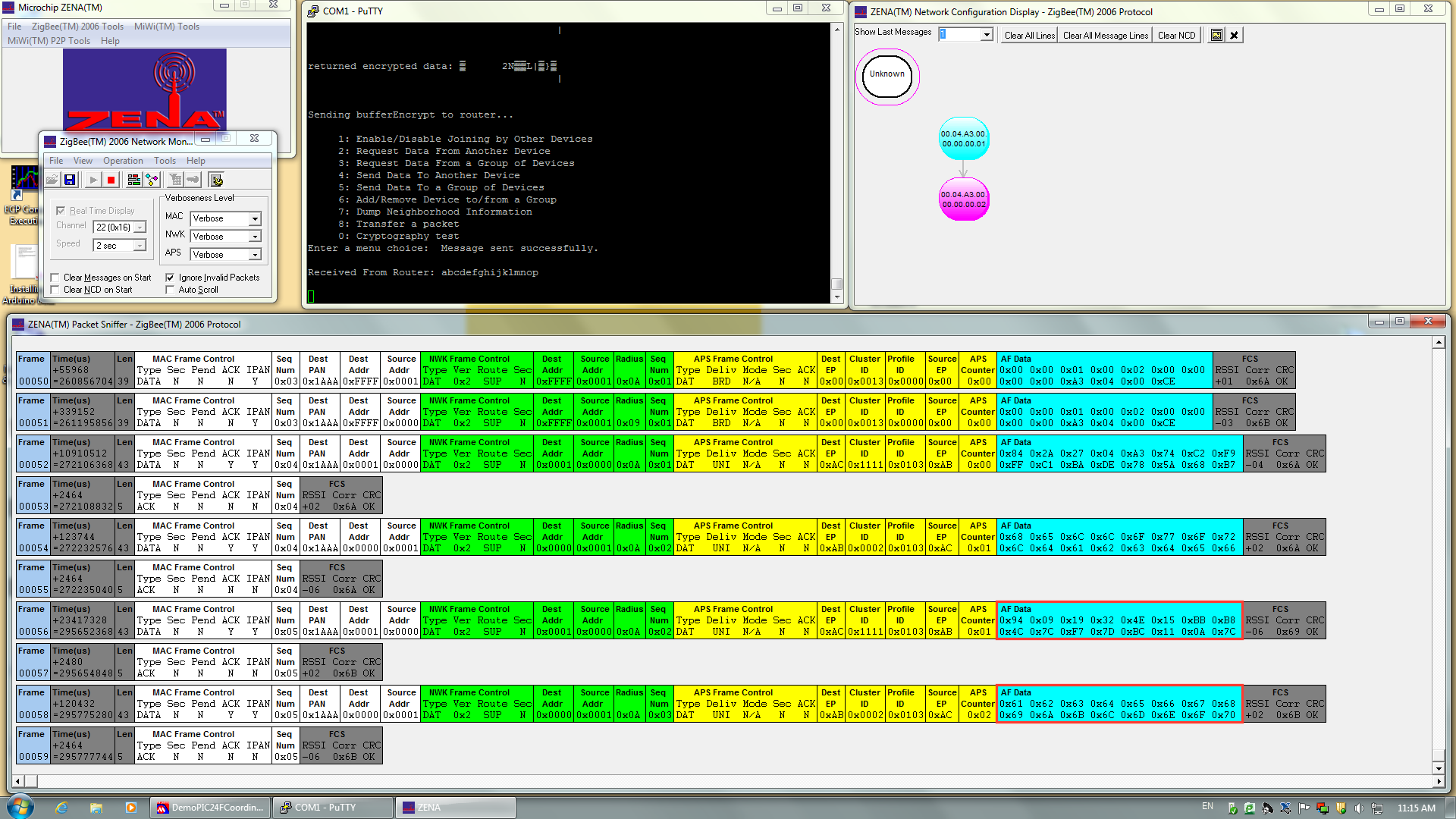


Fig.7 Transmission packets of Case 2

Case 1: Input Plain text is “1234567890123456”.

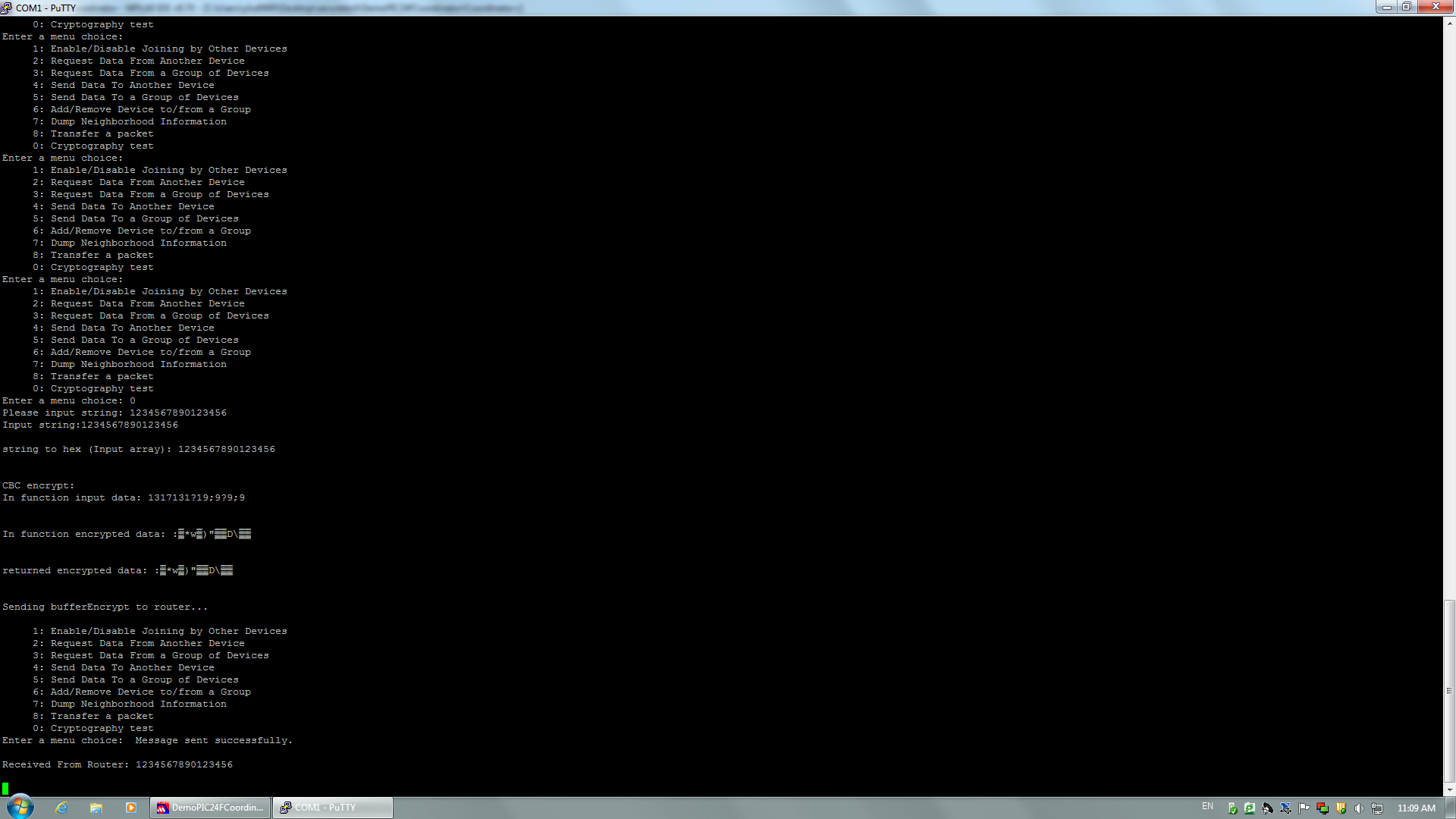


Fig.8 Serial command of Case 3

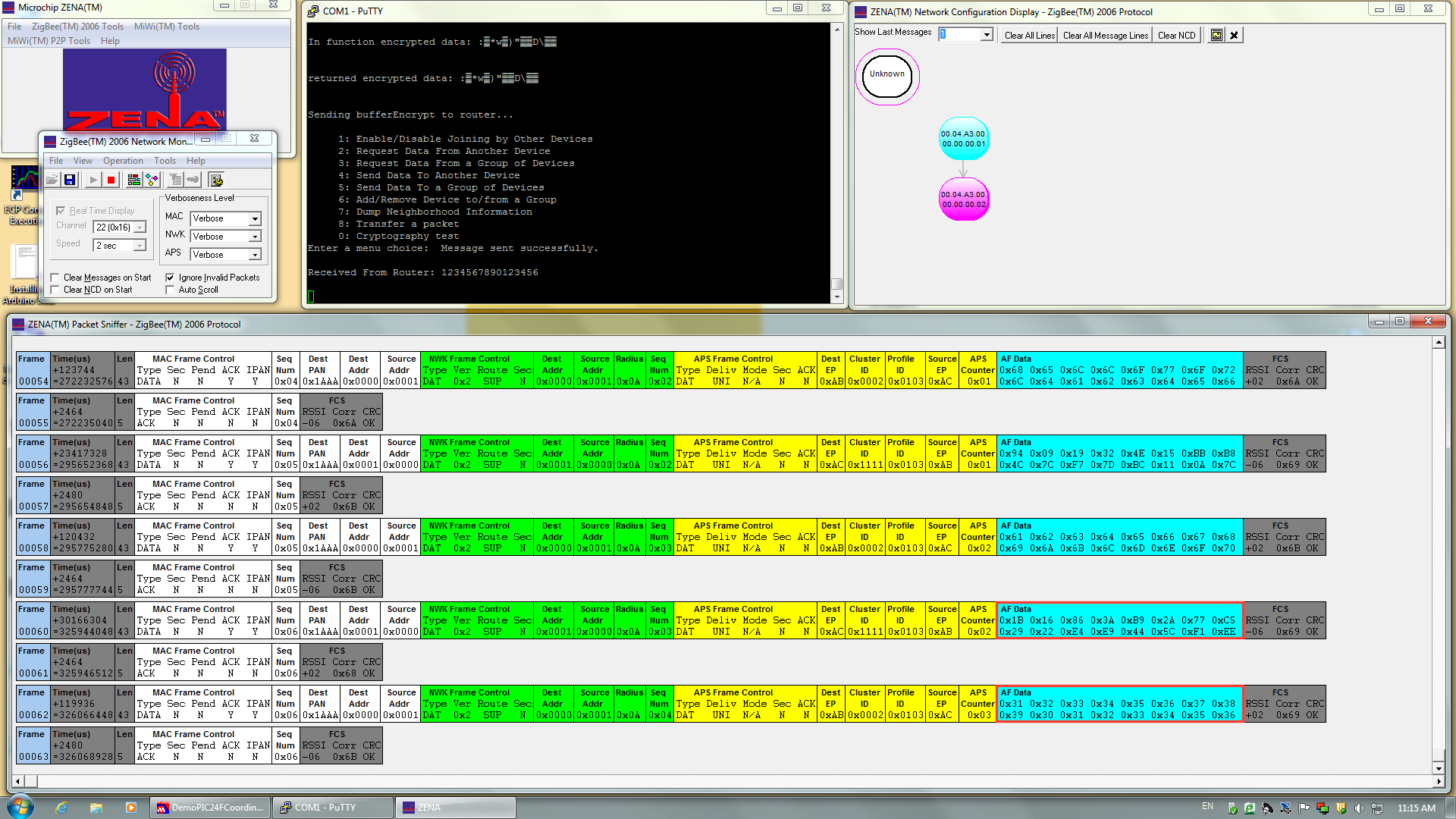


Fig.9 Transmission packets of Case 3

#### 3.3.3 Elaboration of Cryptography Algorithm

We choose AES-CBC (Cipher Block Chaining) mode as our algorithm, which is also part of the implementation in the ZigBee specification. Referring to the documents released by National Institute of Standards and Technology (NIST), we used the recommended vectors and keys for CBC mode. [6]

##### 3.3.3.1 AES Algorithm

We used AES-128 which means the length of key is 128 bits. All the encryption is operating in a 4 × 4 byte matrix called "cipher". The initial value is the first block of plain text. The encryption actually consists of many rounds of operation. Each round of operation contains four functions: AddRoundKey, SubBytes, ShiftRows and MixColumns. These functions are the main operation of AES algorithm and as elaborated below.

(1) AddRoundKey: Each byte will XOR (exclusive or) with the round key (produced by the function KeyExpansion).

(2) SubBytes: Then each byte will be replaced according to a nonlinear method.

(3) ShiftRows: After that, each row of the matrix will be cyclic shifted to left.

(4) MixColumns: At the end, mix each column according to linear conversion.

Obviously, the decryption is the inverse operation of encryption.

##### 3.3.3.2 CBC mode

The CBC (Cipher Block Chaining) mode is a confidentiality mode whose encryption process features the combining (Chaining) of the plaintext blocks with the previous cipher text blocks. [6]

Similar to other modes in AES, it also requires the initialization vector (IV) to do the operations. The IV vector could be public but it has to be unpredictable. The CBC mode and the process is shown as follows:

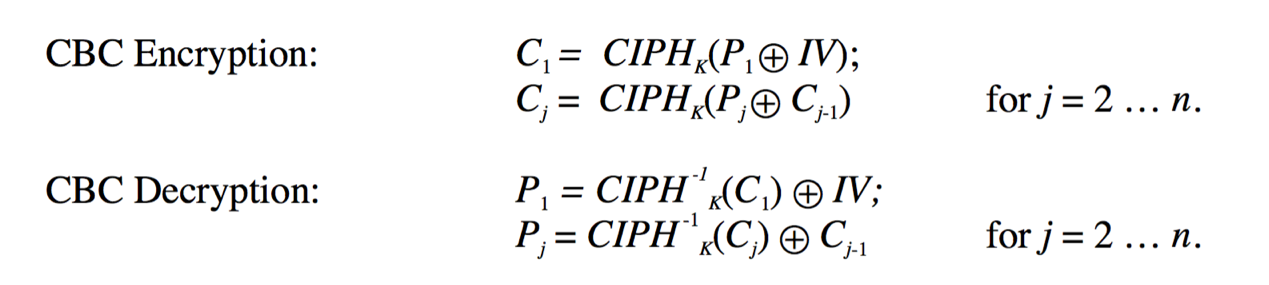


Fig.10 AES CBC mode definition [6]

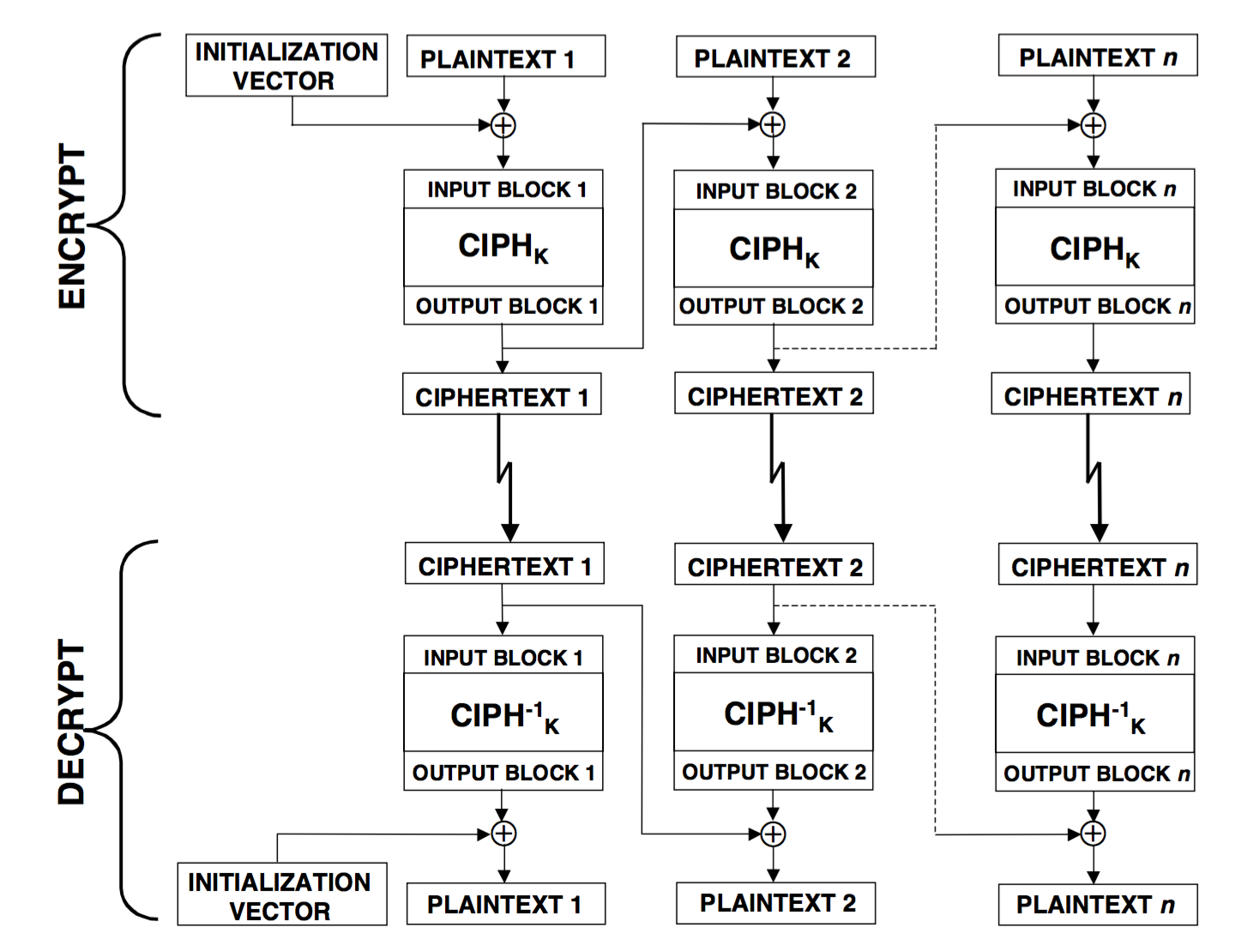


Fig.11 AES CBC mode process [6]

CBC mode is actually a cyclic pattern. In the very beginning, the first block plain text do the XOR operation with the initialization vector (IV) to get the first block of cipher text. Then this first block of cipher text will XOR with the second block of plain text to get second cipher text. Each block of plain text will XOR with the previous output block of cipher text to get the output cipher text of this round. The purpose of using CBC mode is to enhance the difficulty of cracking.

The complete codes for cryptography implementation in Coordinator and Router are attached in appendix.

## References

[1] ZigBee Specification - Document 053474r17. Retrieved from:

http://www.zigbee.org/

[2] Robert Cragie. "ZigBee Security." 2009. ZigBee Alliance. Retrieved from:

https://docs.zigbee.org/

[3] [Brad Bowers](http://www.ciscopress.com/authors/bio/652844d8-8afc-4ef4-9761-7242c5774609). "ZigBee Wireless Security: A New Age Penetration Tester's Toolkit." 2012. CISCO Press.

[4] LI Jun, YANG Qing. "I’M A NEWBIE YET I CAN HACK ZIGBEE: Take Unauthorized Control Over ZigBee Devices." 2015. DEF CON 23 Hacking Conference.

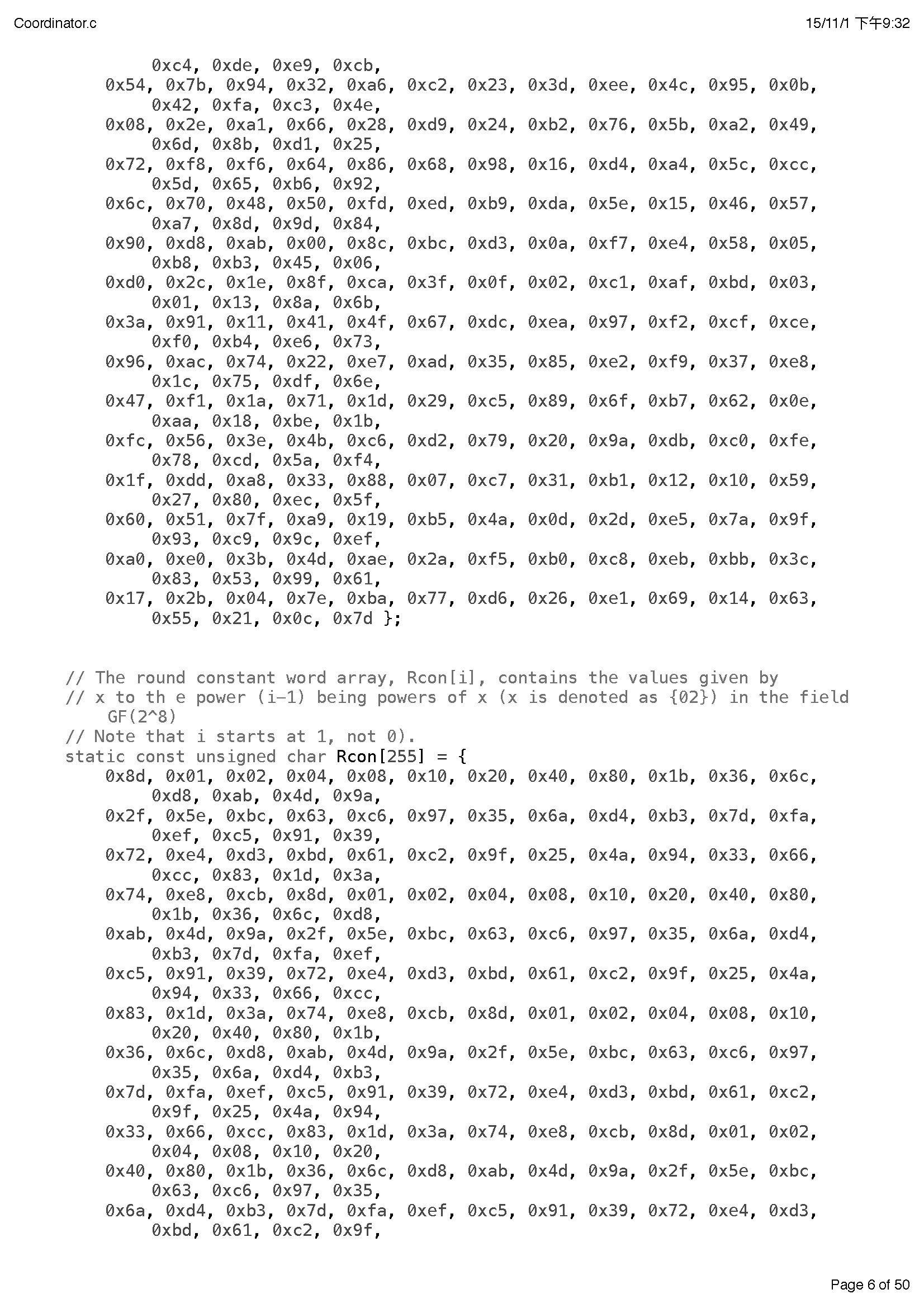
[5] Daemen, Joan, and Vincent Rijmen. "AES proposal: Rijndael." 1999.

[6] Dworkin, Morris. "Recommendation for block cipher modes of operation. methods and techniques." No. NIST-SP-800-38A. NATIONAL INST OF STANDARDS AND TECHNOLOGY GAITHERSBURG MD COMPUTER SECURITY DIV, 2001.

## Appendix I Variables and functions definitions in both Coordinator and Router



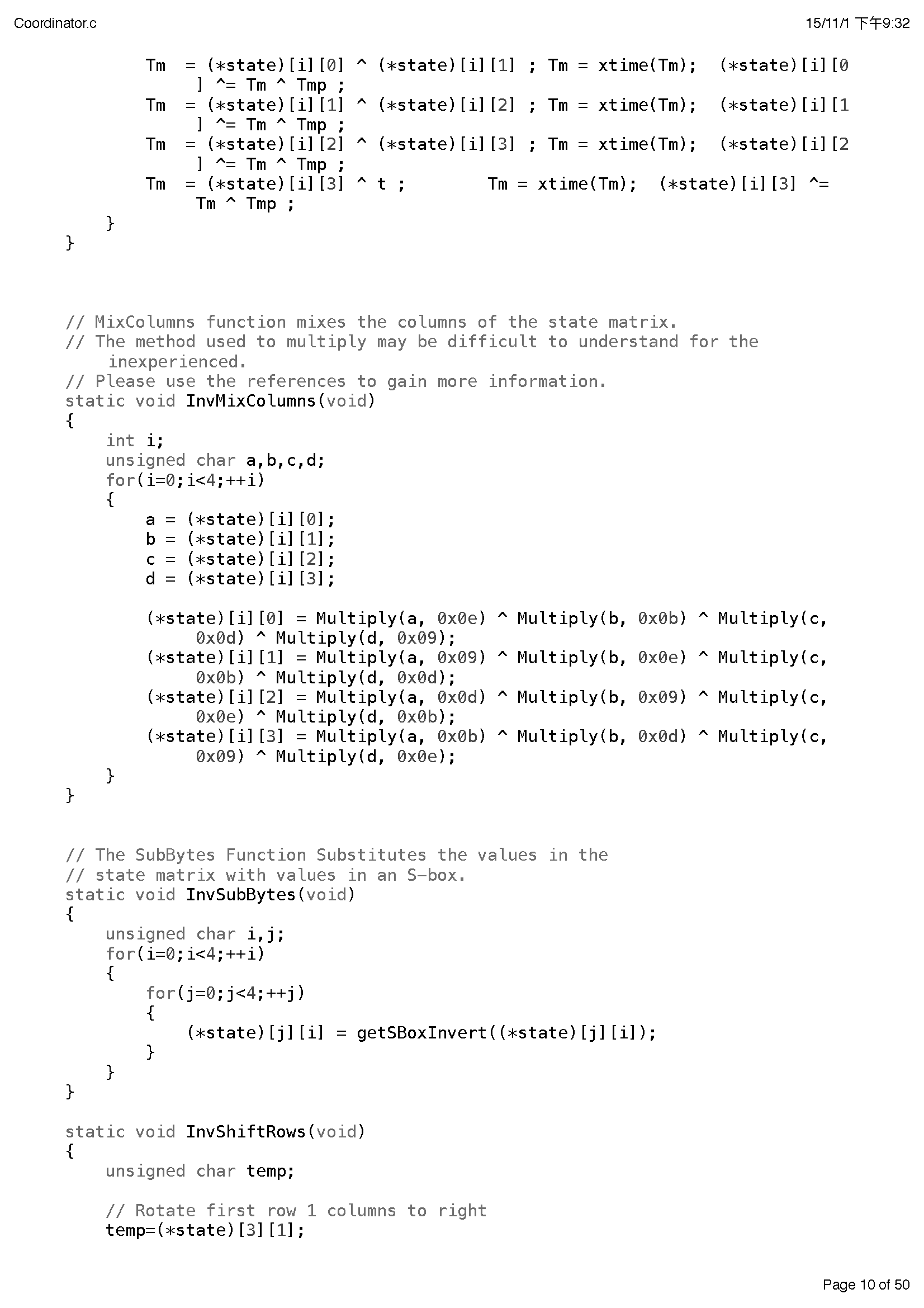


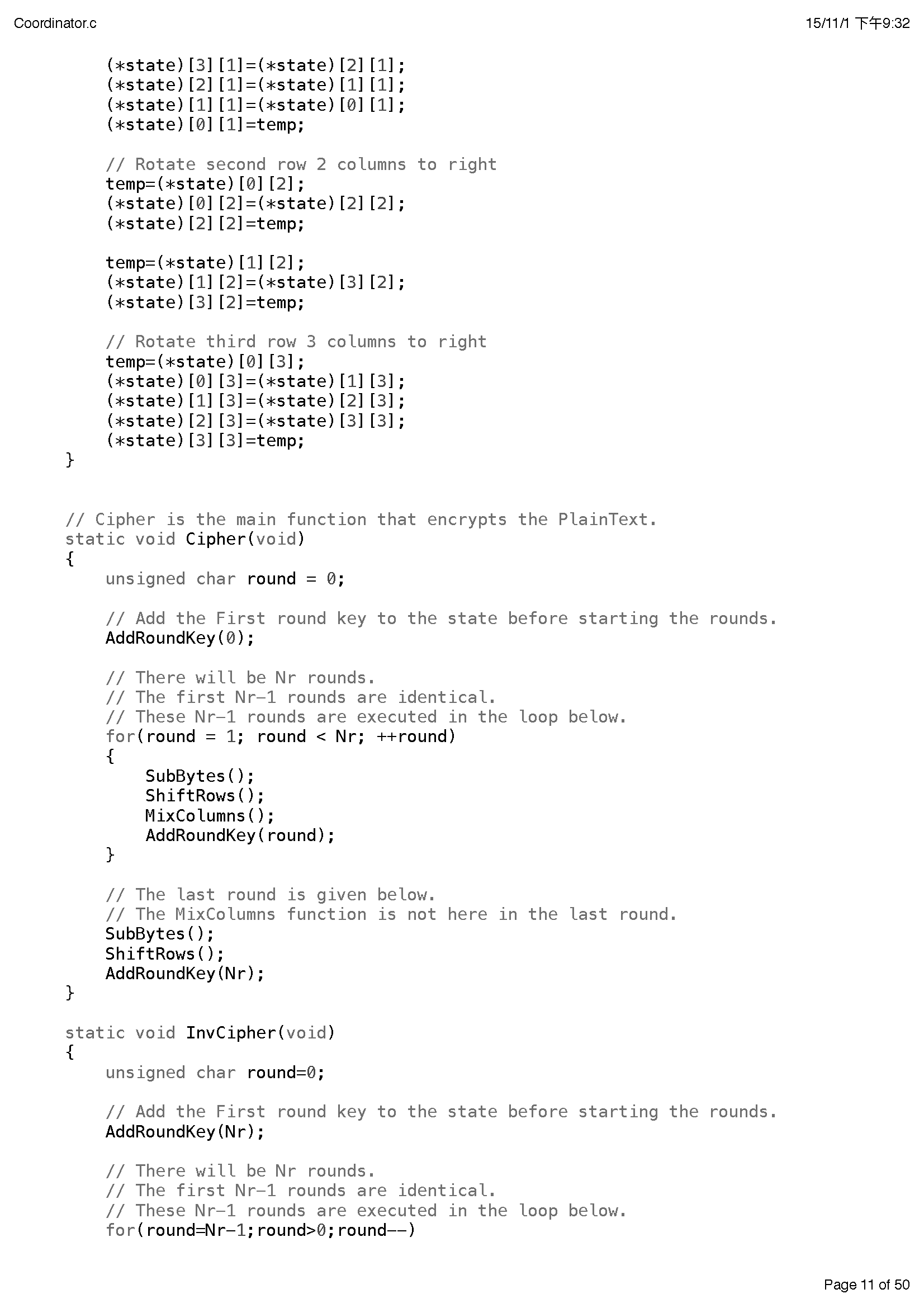




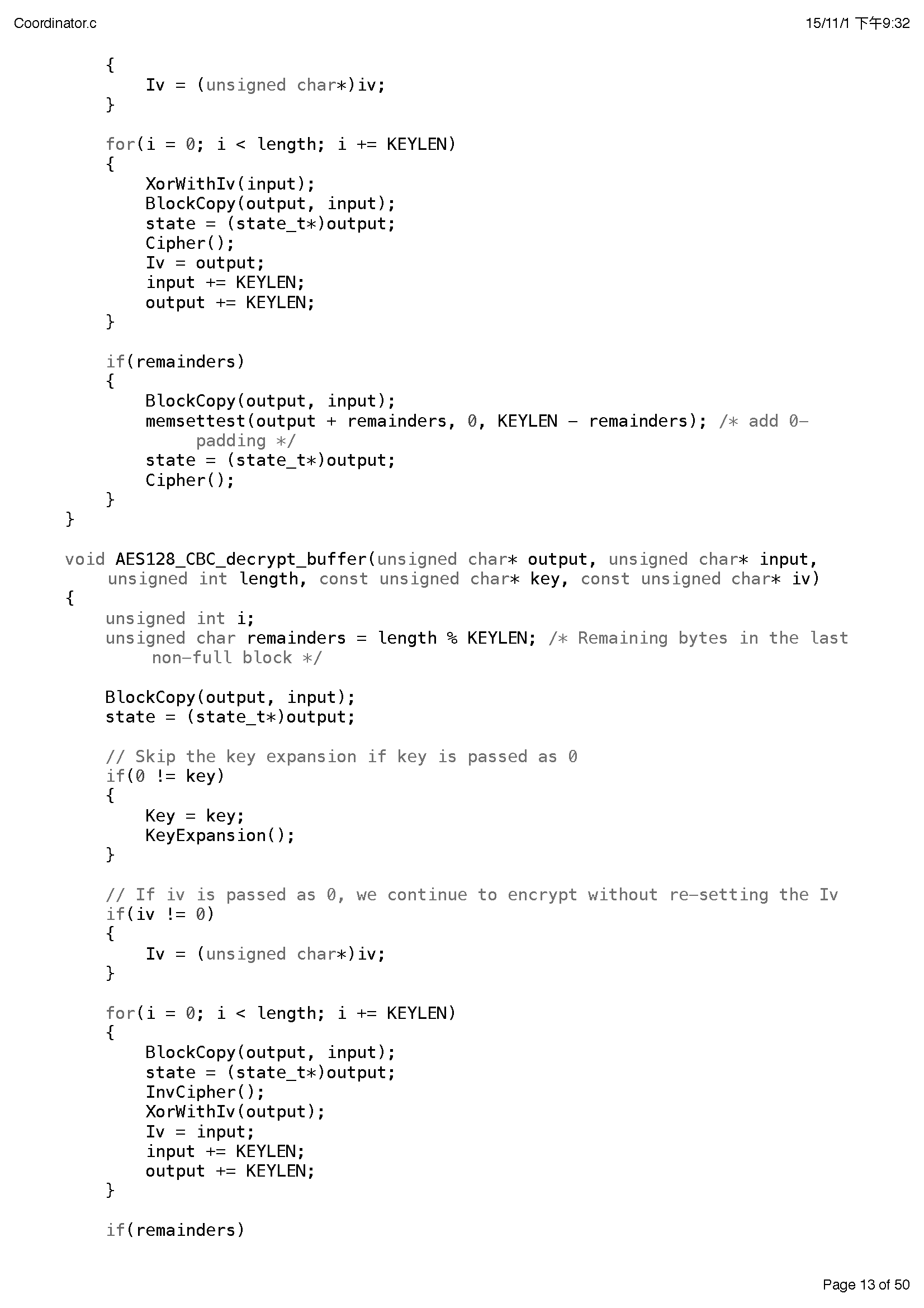




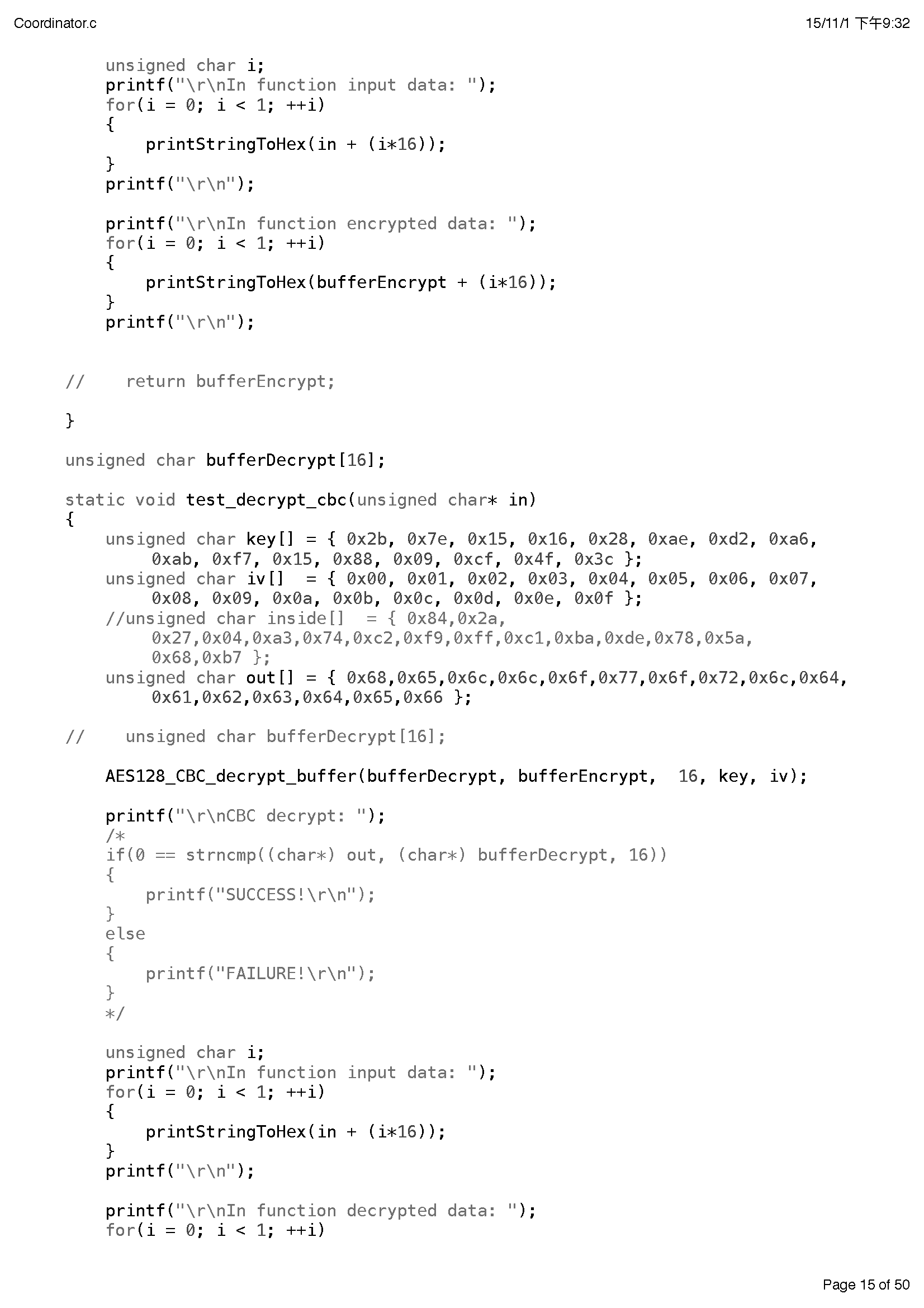






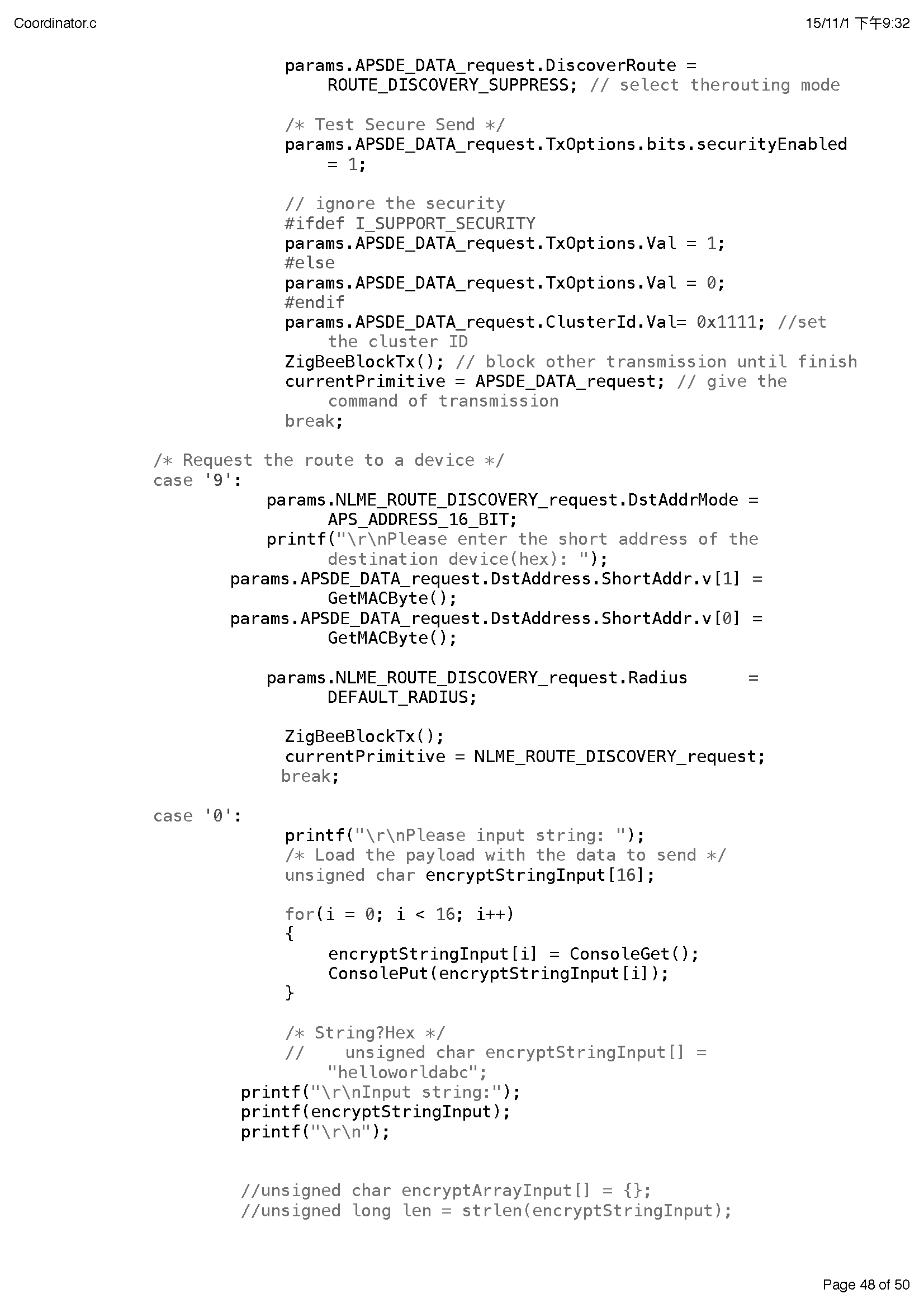








## Appendix II Process menu definition in Coordinator (Encryption)







## Appendix III Message receiving and handling in Router (Decryption)







## Appendix IV Displaying of plain text in Coordinator

