Issues & Operation Modes for Block Ciphers & Femtocells

C. Gobinath[1] K. Sandhiya[2]
[1,2]Student
[1,2]Department of Computer Engineering
[1]Sri Krishna Adithya College of Arts & Science, Coimbatore – 42 [2]United Institute of Technology, Coimbatore -20

Abstract— Cryptography is the process of writing using various methods ("ciphers") to keep messages secret. In modern times cryptography is considered to be a branch of both mathematical and computer science. At one time the subject was mainly a linguistic one, the key concern being the ability to recognize words and make words unrecognizable with a simpler cipher. Public key cryptography is a modern technique. Encryption key is called the public key. Decryption key is called the private key. To attack a cipher is to attempt unauthorized reading of plaintext, or to attempt unauthorized transmission of cipher text. The Data Encryption Standard (DES) defines an indexed set of permutations acting on the message space. It is widely used in Banking. There are basically two ways to make a stronger cipher: the stream cipher and a block cipher. A stream ciphers are commonly used nowadays in hardware applications. One of the best known early block ciphers is the Play fair system.
Key words: Public, Private, Encoder, Decoder, Data Encryption Standard, Cipher Keys, XOR, Femtocells

I. INTRODUCTION

Cryptography and Cryptanalysis is collectively known as Cryptology. The branch of mathematics encompasses both Cryptography and Cryptanalysis is called Cryptology and its practitioners are called Cryptologists. The art and science of breaking cipher text is called Cryptanalysis. Cryptography is the study of mathematical techniques related to information security aspects such as confidentiality, data integrity, entity authentication, and data authentication. Cipher is the way to encrypt data. Plaintext is the original data before encrypted and the data of the encryption output is called cipher text or cryptogram. Encryption is a process of encoding a message so that its meaning is not obvious. The reverse process is called Decryption.

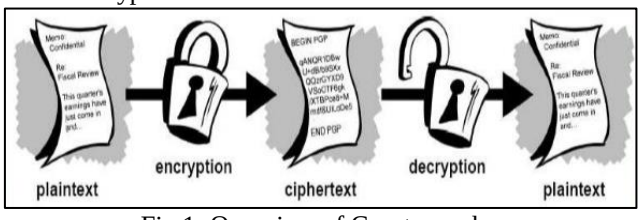

Fig 1: Overview of Cryptography

A. *Basic Terminologies*

The methods which used to encrypt plain text is called Ciphers. The difference between two Cipher ways that are symmetric cipher (secret key) and the asymmetric cipher (public key). In the secret key system, we use only one key to encrypt and decrypt. The transmitters and the receivers have to own the secret key. The concept of secret key is simple and fast. But it is hard to keep the key safety because as the involved parties number increase, the security of the secret key becomes unsafe. In order to solve this problem, someone invented the public key system or so called asymmetric cipher. There are two keys used in the cipher algorithm. The man owning the public key can encrypt the data, and only the man owning the secret key can decrypt the encrypted data. Asymmetric cipher is easy for key management, but the drawback is the computing speed is rather slow and complicated.

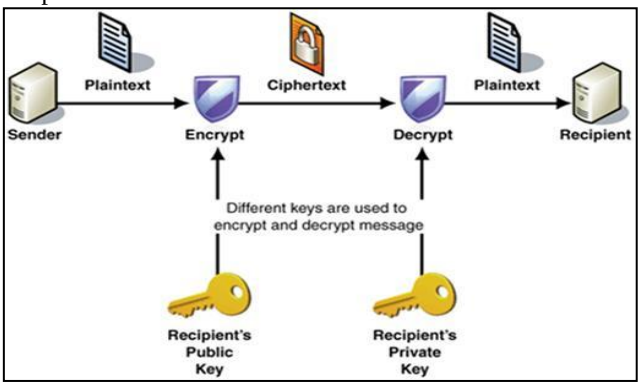

Fig. 2: Block Diagram of Encrypt & Decrypt

II. FAMILY OF ALICE & BOB

When cryptologists talk about encryptions, there are some rules involved inside such as message sender, receiver or attackers. There is a simply way to distinct these roles by naming the roles. Starting with the alphabet are Alice and Bob, two parties wanting to communicate in a secure manner. When more people are in the communication group, Carol and Dave will be used. Eve is a passive attacker who can get the information from Alice and Bob. Trent is a person who is trusted by all involved parties. Walter is a man who would protect Alice and Bob with some aspect. This is the basic sense about the communication family.

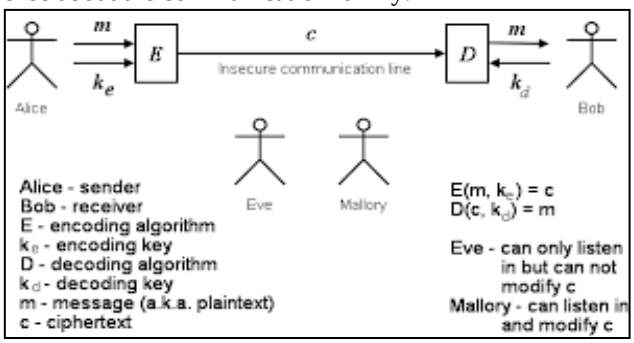

Fig 3: Communication Family of Alice and Bob

A. *Operation Modes for Block Ciphers*

Here we introduce some modes to implement block ciphers. These different modes are called as "Operation modes". We choose one of them to implement the block cipher by considering the different kind of outstanding threatens.

1) ECB (Electric Codebook Mode)

The simplest sense of block cipher is ECB mode. Each encryption and decryption of the data blocks are independent from one another. It means that the speed of ECB mode is very fast because the parallel inputs and outputs could be used. And the transmission errors will be confined inside the single block, and will not influence on the other blocks. The drawback of ECB mode is that the same plaintext input will have the same cipher text output. It would be an advantage that the attackers could take on.

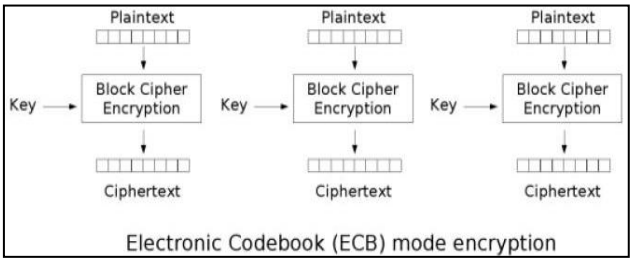

Fig. 4: ECB Mode for Encryption

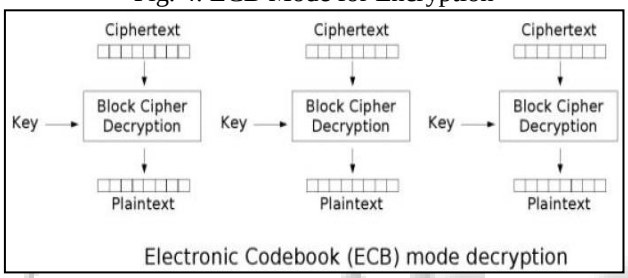

Fig. 5: ECB Mode for Decryption

2) CBC (Cipher Block Chaining Mode)

CBC mode efficiently solves the security problem of ECB. The encryption of CBC is to do XOR between the current plaintext and the former plaintext, then deal the result from the above with the key. And the output is the current cipher. Decryption is quite simple that we could the specification of the XOR. We could realize the detail by checking out the given below figure. (Notice that there is a IV, initialization vector in the first step where there is no former cipher text). The disadvantage of CBE is that the processing speed in CBC is slower than ECB because the parallel inputs cannot be used here.

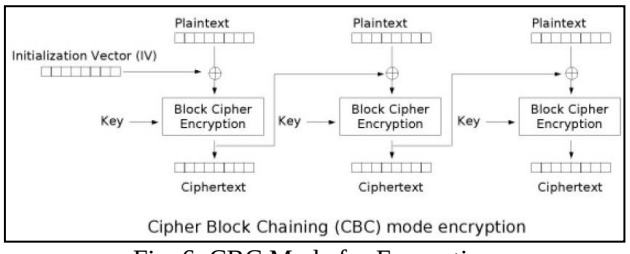

Fig. 6: CBC Mode for Encryption

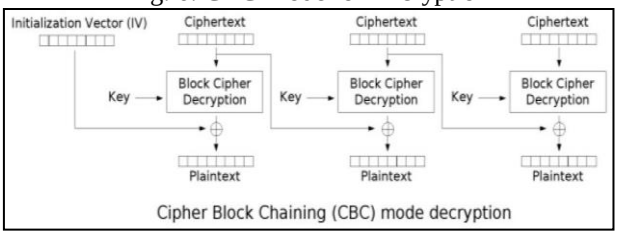

Fig 7: CBC Mode for Decryption

3) CFD (Cipher Feedback Mode)

The most serious problem or drawback is that it can destroy the data fitting the data size. CFB could solve this problem. CFB can deal with any data that even smaller than the block size. On the other hand, we can image this is a way transferring block cipher to stream cipher. Figure 8 is an example for 8-bit CFB. At the beginning, the former cipher text (or IV) is put into a shift registers. We assume that register shifts from right to left and the stuff inside the register would be encrypted with key. In general, the encryption output of the n bits is exactly the cipher text. And the decryption is as the former modes that using the XOR.

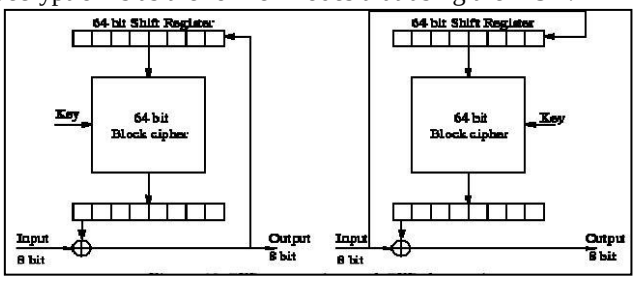

Fig. 8: CFD Encryption & Decryption

4) OFB (Output Feedback Mode)

OFB is similar to CFB that both the two modes could transfer block cipher into stream cipher. The most difference between them is that is that OFB put the output of the encryption into a register directly. So OFB is a little simpler than CFB. It is shown in the figure.

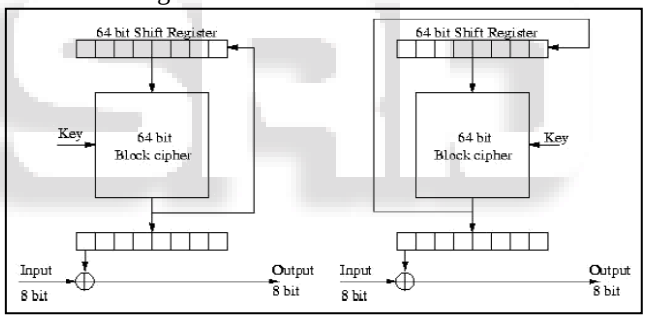

Fig. 9: OFB Encryption & Decryption

5) CTR (Counter Mode Or Sic, Segment Integer Counter)

The concept of CTR mode is also familiar to OFB. The difference between them is there is no register inside the CTR system. Instead of the register, the CTR mode uses the counter to do encryption. The counter would be added by 1 every time after encryption. The biggest advantage of CTR is that the parallel inputs can be used which means the processing time of CTR mode is rather fast. And the same time there is no such security problem happened in ECB mode in CTR mode.

CTR is a popular mode that used very often nowadays. There is so many different type of such mode just like CTR. CTR is also suitable the Multi- Processor machine. We just simply described the basic sense of CTR mode and put the simplest algorithm figure beyond. (The nonce here is the meaning as the IV above)

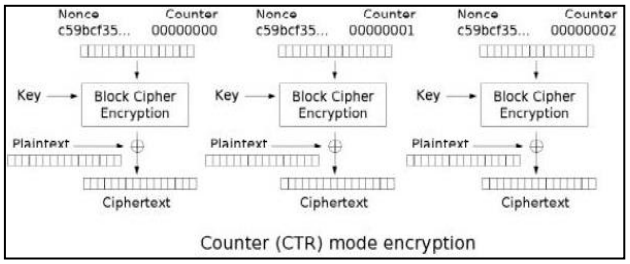

Fig. 10: CTR mode encryption

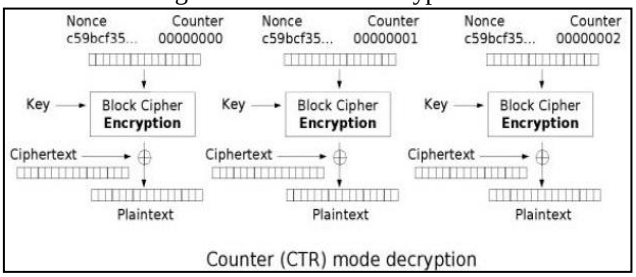

Fig. 11: CTR mode decryption

III. ADVANTAGES & DRAWBACKS FOR THE MODES ABOVE

	ADVANTAGE	DRAWBACK
ECB	Parallel en/decryption simple and fast.	Insecure, handling constant data size.
CBC	Secure	Serious en/decryption slow, handling constant data size.
CFD	Secure, handling data with any size.	Serious en/decryption, slow.
OFB	Secure, handling data with any size. Simpler and faster than CFD.	Serious en/decryption slow.
CTR	Parallel en/decryption handling data with any size, secure.	Insecure.

Table 1:

IV. IMPLEMENTING THE FEMTOCELL

To overcome the signal problems we are introducing femtocell with encryption and decryption security. Femtocells are recently developed and rapidly evolving field. Quite often, it is noticed that cell-phone signals are strongly attenuated, when indoors, leading to call dropping or poor call quality. Femtocells are mini based stations that are deployed in user homes so that the user can directly connect to the cellular network through the femtocell instead of the outdoor macro cell, thereby increasing call quality. Recently we have seen tremendous growth in the fields of wireless networks and telecommunications. There are four billion mobile phones users in the world today, and the numbers continue to rise. However, cellular phones continue to face issues such as poor signal strength and call quality when used indoors. At the same time, there has also been a huge development in Voice over IP(VoIP) applications. This technology allows users to make free calls through the internet, through the internet, thereby acting as a potential threat to mobile operators around the world.

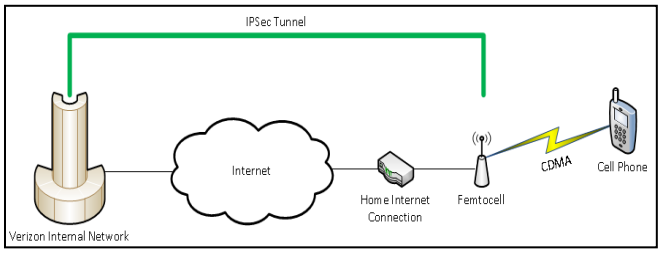

Fig. 12: Overview of Femtocell

A. *Operation on Femtocell*

It is adjustable to Environmental factors and can adjust signal strength. A broadband internet connection is a perquisite for connecting a femtocell. The femtocell enables encryption for all voice calls and data sent or received by the mobile phone. This makes it impossible for an external user to break into a users home network. To a standard 3G cellular phone, the femtocell appears as another cell site or macro cell, hence communicating with it as it would with a macrocell, when the mobile phone is used outdoors. Since femtocells operate at very low radio power levels, battery life is high. Also, as the distance between the femtocell and the mobile handset is short, call quality is excellent.

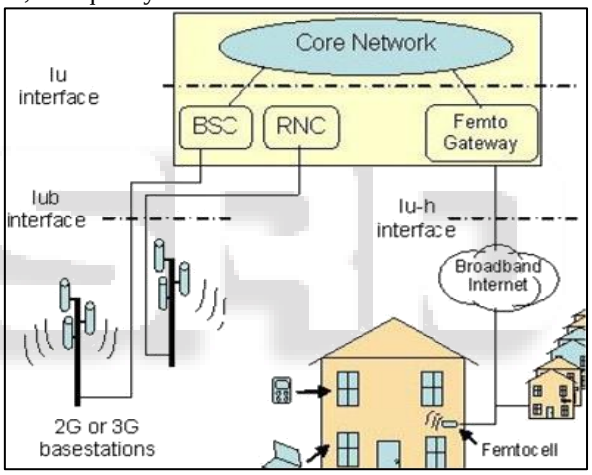

Fig 13: Femtocell Development

B. *Encryption/Decryption in Femtocells*

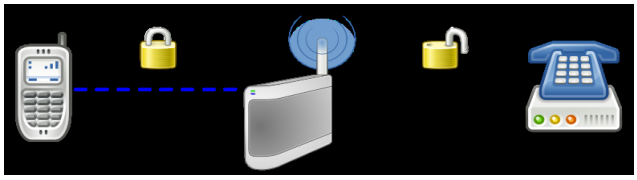

Fig. 14: Femtocells in Encryption /Decryption

Only the phone to femtocell OTA traffic is encryption / decryption happens on the box.

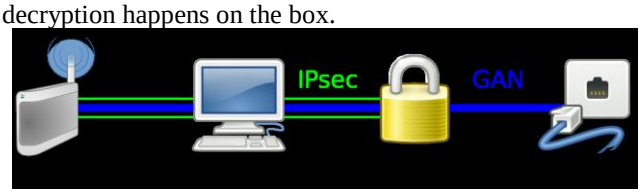

Fig 15: HNB mode with PC

In the above diagram we understand that OTA encryption optional and traffic decoded in the HNB (Home Node B).The only the SeGW (Security Gate Way) access it used for authentication/ encryption when connection and all traffic in plain text.

C. Interference Issues in Femtocells

Although the growth of the femtocell could see a sharp rise in the popularity of cellular phones, there are still concers regarding interference between femtocells and the external macrocell as well as similar such devices. Since the femtocell and macrocell operate in the same range of frequencies, there is bound to be interference. The main problem of interference arises from the fact that femtocells are installed in an ad-hoc manner, or independent of the structure of the carrier frequency with respect to macrocell. To find an effective and logical solution to this drawback, the Femto-forum has been involved in conducting research into mitigating the problem of interference in femtocells.

The promising femtocell is being tested extensively by mobile operators around the world. However, there are still some issues that need to be worked on for femtocells to be implemented as fault-free devices. In the years to come, femtocells may also be able to operate efficiently using EDGE Standars. A number of hardware evolutions are required before high usability and quality of service are achieved. This may take a few years to achieve. Mobile operators must continue partnering with internet service providers, so as to make the femtocell a reasonable means of improving cellular communication indoors. There is still sufficient capacity available in the macro network, so there is still no immediate need of femtocells to help alleviate the pressure on macrocells. However, femtocells can be immense help in rural areas where the distances between homes and the nearest macrocell, could be many miles. The development of femtocells can also help speed up the evolution of Universal Mobile Access.

REFERENCES

[1] 3GPP .Security of H(e)NB. Technical Report TR 33.820,3G Partnership Project, Dec 2009.
[2] Chandrasekhar V, Andrews J, Gather A; Femtocell networks: a survey; IEEE communications magazine.
[3] Femto Forum; Interference Management in UMTS Femtocells; 2008, available online at ww.femtoforum.org
[4] D.Hankerson , A.Menezes and S.Vanstone. Guide to Elliptic Curve Cryptography, Springer Verlag 2004.
[5] I.Blake, G.Seroussi and N.Smart. Advances in Elliptic Curve Cryptography, Cryptography, Cambridge University.
[6] Chodi D, Monajemi P, Kang S, Villasenor J; Dealing with Loud Neighbors: The benefits and Tradeffos of Adaptive Femtocell Access; IEEE Global TelecomCmuniations Conferene 20078.
[7] J D. Bonesh, A.Sahai and B.Waters. Fully Collusion Resistant Traitor Tracing with Short Ciphertexts and private Keys. In proceedings of Eurocrypt 2006, Lecture Notes in Computer Science.
[8] D. Boneh, R. Canetti, S. Halevi and J. Katz. Chosen-Ciphertext Security from Identity-Based Encryption. SIAM J. Compute. 36(5): 1301-1328, 2007.
[9] J. Coron. A Variant of Boneh-Franklin IBE with a Tight Reduction in the Random Oracle Model. Des. Codes Cryptography 50(1): 115-133, 2009.
[10] R. Balasubramanian and N. Koblitz. The Improbability that an Elliptic Curve has Subexponential Discrete Log Problem under the MenezesCOkamotoCVanstone Algorithm. J. Cryptology, 11, pp. 141C145, 1998.

