International Journal of Applied Engineering Research ISSN 0973-4562 Volume 10, Number 16 (2015) pp 37255-37260

Porting presentation layer to ensure network security in mobile devices

Dayanand Lal.N[1]
[1]*Ph.D Scholar, Dept. of ECE, Dr. M.G.R Educational and Research Institute, Chennai, India,*
E-mail id: dayanandlal@gmail.com

Dr.G.Saravana Kumar[2]
[2]*Dean & professor, Dept. of ECE, Vel Tech high Tech Dr. Rangarajan Dr. Sakunthala Engineering College, Avadi, Chennai, India*
E-mail id: shawn_pooja2003@yahoo.co.in

Dr. S.Ravi[3]
[3]*Professor & Head, Dept. of ECE, Dr. M.G.R Educational and Research Institute, Chennai, India.*
E-mail id: ravi_mls@yahoo.com

Dr.Anand[4]
[4]*Professor, Dept. of ECE, Dr. M.G.R Educational and Research Institute, Chennai, India.*
E-mail id: harshini.anand@gmail.com

Abstract
Cryptographic algorithms are used in the presentation layer to protect the users in a network, the shared resources, global memory usage, kernels etc. This paper gives an overview on cryptographic schemes using parity concepts, digitadition based generator sequences and block ciphers. Specifically, block cipher is ported with short length key and the data is shared among authenticated users in both synchronous (TCP/IP) and asynchronous (UDP) connectivity between individual LPC1788 target hardware.

Keywords— CFB: Cipher Text feedback, CBC: Cipher Block Chaining

I. INTRODUCTION

A symmetric block cipher (Ex: DES (the Data Encryption Standard)) uses shared secret encryption, and offers the advantage that the key length can be short. This makes the algorithm best suited to implementation in hardware, and is faster compared to the software implementation. The key length argument can be explained as follows: Assuming that the only feasible attack on standard symmetric block cipher (ex: like DES) is to try each key in turn until a match is found, then 1,000,000 machines each capable of testing 1,000,000 keys per second would find (on average) one key every 12 hours. Most reasonable applications find this rather comforting and a good measure of the strength of the algorithm.

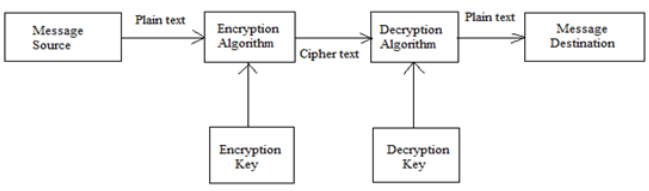

Fig 1: Encryption Method

Symmetric block cipher encryption algorithm is shown in the block diagram in figure 1, and has the desirable features that are considered for the development of metrics:

1. **Type**: Symmetric type of key (secret key or one-key) or asymmetric type of key (public key or two-key).
2. **Functions:** Message integrity, validation, digital signatures, Message privacy same type of algorithm, wouldn't be metric per se but may also be of the same interest to end users.
3. **Key size**: The size of Key is envisioned to deliver Relative value.
4. **Rounds**: Rounds are considered as imperative because rounds are almost similar word and block size, are worldwide appearances.
5. **Complexity of cryptographic mapping**: Attributes of encryption, decryption and key setup probably would specify number of operations kind of bit operations, modular multiplications and modular exponentiations.
6. **Data expansion**: Normally desirable, besides often mandatory, where encryption does not surge the size of plaintext data. Homophonic substitution and randomized encryption techniques that results in data expansion.
7. **Error propagation**: Decrypting ciphertext contains bit errors which may result in different effects on recovered plaintext, which includes the propagation of errors to subsequent plaintext blocks. Various error characteristics are suitable in various applications. Block size which naturally affects error propagation.

a. Symmetric Cryptography

Symmetric Cryptography is most customary form of cryptography. In symmetric cryptography, the tangled parties share a common secret (password, pass phrase, or key). The Data is encoded and decrypted using the same key. The

algorithm tend to be comparatively fast, but is dependent on the prior swapping of keys between the authenticated users. Any user owning a specific key can create coded messages using that key and use the same for decoding with the key. A secret key, which can be a number, a word, or just a string of random letters, is applied to the text of a message to change the content in a particular way. This may be as simple as shifting each letter by a number of places in the alphabet. As long as both originator and recipient know the secret key, then they can encrypt and decrypt all messages that use this key as shown in figure 2.

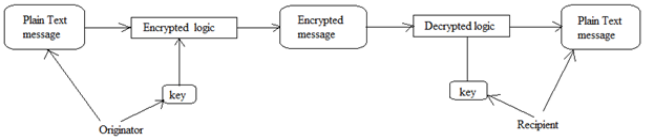

Fig 2: Symmetric cryptography

b. Asymmetric Cryptography

The secret keys is exchanging them over the Internet or a large network while preventing them from falling into the unidentified hands. The person who knows the secret key can easily decrypt the message. Any message (text, binary files, or documents) that are encrypted by using the public key can only be decrypted by applying the same algorithm, but by using the identical private key. Any message that is encrypted by using the private key can only be decrypted by using the identical public key. This means that you do not have to worry about passing public keys over the Internet. It needs for more processing power to both encrypt and decrypt the contented of the message as shown in figure 3. A problem with asymmetric encryption, however, is that it is slower than symmetric encryption.

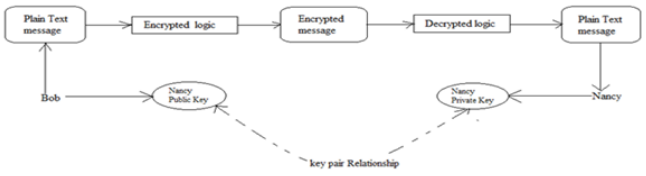

Fig 3: Asymmetric Cryptography

DES properties and strength

The necessary characteristics for block ciphers, which includes: each bit of ciphertext would almost depends on every bit of key and also on every bit of plaintext; existing shouldn't be a statistical relationship evident between plaintext and the ciphertext; altering any single plaintext or key bit should alter each ciphertext bit by probability $_{1/2}$ and altering a ciphertext bit would result in an impulsive alteration in the recovered plaintext block. Empirically, DES satisfies the basic objectives. Some known properties and anomalies of DES are given below.

(i) Complementation property
(ii) Fixed points

II. LITERATURE SURVEY

Gerhard A schloss et al projected paper [1] on the Layered Multimedia Data Model (LMDM) which adds structure to problematic statement for specifying hypermedia arrangements by dividing job somewhat, other manageable wreckages. The strength of DPL comprise: salvaging presentation patterns, universal model of the broadcasting management, admitting then preventing scheme dependence, besides generalization of outmoded simulation model. This article reviews theories of third layer LMDM and the Data Presentation Layers. Hence leases the requisites of the software preparations, labeled audio and pictorial expressions of the temporally linked data items specified happening inferior layers.

Sergei Semenov et al shapes that the paper [2] recommend some nontraditional approach to coding in a network. We elucidate that it's possible to apply coding not only in the direction of increasing the reliability of the transmitted information, but besides to improve such important characteristic of network, as mean message delay. Also we may consider the encryption of messages just as a coding process at presentation layer happening network. We discriminate diverse coding procedures at different network layers. In this case the concern on impact of coding at one layer to another layer. Thus, the problem of understanding the coding at neighbor network layers ascends.

Chaung Ming et al expresses [3], Instruction to devise computers have successfully become consumer electronics, and groundwork of the multicast multimedia networking presentation architecture that allows low-end computers, Example: Set-Top-Box or diskless networking Personal Computer, partaking plane multimedia presentation urgently obligatory. To encounter requirement, we counsel multicast multimedia networking presentation architecture, and corresponding presentation control mechanisms in the paper.

Subhat S.Ahmeda et al speaks [4], practically about Ad hoc networking which permits portable devices to launch communication self-directing an essential infrastructure. The fact that there remains no vital infrastructure and the devices be able to move randomly which gives rise to a various kind of difficulties, such as routing plus security. Attacks on routing etiquettes create various unwanted effects that can defeat the aims of ad-hoc routing, Ad hoc networks is plentiful vulnerable to malicious activities compared to wired network. Secure communication is important feature of network milieu. Consequently to afford secured ad hoc network: Substantiation, privacy, uprightness, non-repudiation and access control would be delivered. Authentication arises in first place to safeguard secure network operation, since some other amenities depend on verification of communication individuals.

A. Block cipher definitions

The concept of block cipher represents a function which maps n-bit plaintext blocks to n-bit ciphertext blocks; n is called the *block length*. It might be viewed as modest substitution cipher with a very great size character. The parameterized function is a k-bit key K,1 taking values from subset K (the *key space*) of set of all k-bit vectors Vk. It is assumed generally that key is always chosen randomly. The use of plaintext and ciphertext

blocks of equal size which avoids data expansion. Nearly which allows the unique decryption, an encryption function need to be one-to-one. For n-bit plaintext and cipher blocks text and fixed key, the encryption function remains bijection, outlining permutation on n-bit vectors. Each key hypothetically states different bijection.

B. Block Cipher Modes

It is desirable to make identical plaintext blocks encrypt to unalike cipher text blocks. Two methods are commonly used for this: CFB mode: a cipher text block is obtained by encrypting the previous ciphertext block, and xoring the resulting value with the plaintext. CBC mode: a cipher text block is obtained by first xoring the plaintext block with the previous cipher text block, and encrypting the resulting value. Necessary functions of cryptography for DES algorithm is shown in Table 1.

TABLE 1: NECESSARY FUNCTIONS OF CRYPTOGRAPHY FOR DES ALGORITHM

Types	Types of Algorithm	Functions	Other factors
Privacy	DES	Encrypt, Decrypt	Primary Use of keys
Authentication	DES	Compute and verify DES, Sign and Verify	NIL

III. REPORTED APPROACHES TO BLOCK BASED ENCRYPTION OF DATA

The Masonic cipher is one of the earliest reported works of partitioning data into blocks and using corresponding blocks to form the encrypted data. It consists of open ended matrix of three rows and three columns and can be strengthened with (i) a key (ii) magic square mapping for the cell numbers and so on. A simple block cipher following the masonic approach is shown in figure 4:

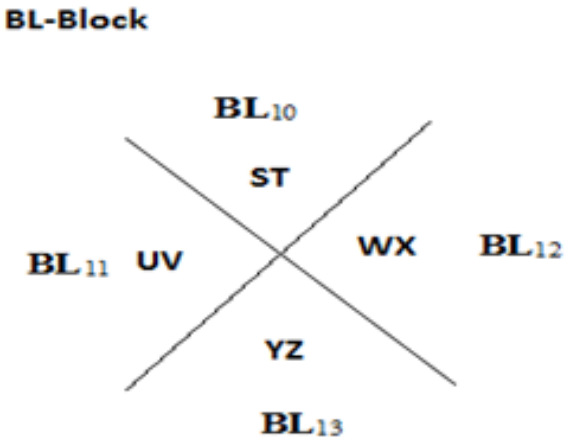

Fig 4: Simple Block Cipher

Thus for example: if key is QREFWX then the blocks selected are BL_9, BL_3 and BL_{12}.Individual letters inside a block can be indexed using frame markers like #.For example if key is AOYEKN then the encrypted data is BL_1 BL_8 BL_{13} BL_3 BL_6 BL_7#. Where # denotes that 'N' is the second element in the chosen block BL_7.

IV. IMPLEMENTATION OF BLOCK CIPHER

The implementation of the different blocks were done in Linux kernel in python language [implementation results are given in the results section]. The details are given in this section.

Step 1: Enter the key

Step 2: Map the key into the first N rows of the block matrix, where 'N' is the size of the key

Step 3: Form the blocks by filling the remaining cells with the remaining letters in the proper sequence.

Step 4: Once step 3 is formed the block elements are automatically assigned.

The Output obtained for the text '**HELLOWORLD**' is in figure 5:

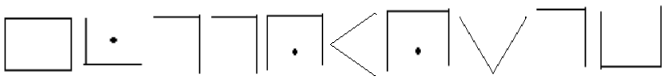

Fig 5: Block cipher output for the text 'HELLOWORLD'

Resultant blocks:

As we shown the output in the above line which explicates the word HELLOWORLD, thus the resultant blocks is being represented and drawn in figure 6.

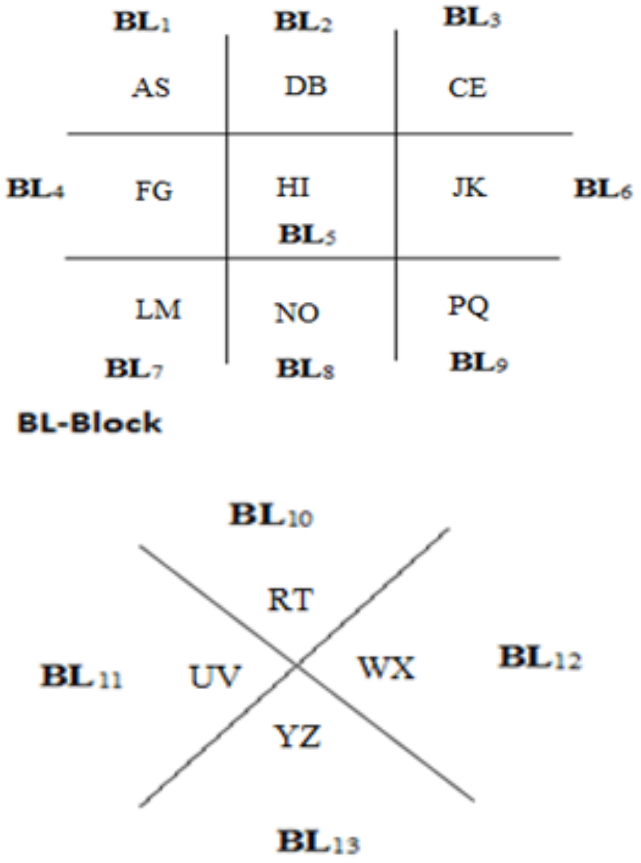

Fig 6: The blocks assigned in the cipher is shown

Table 2 represents symbolic output with block number.

TABLE 2: SYMBOLIC OUTPUT WITH BLOCK NUMBER

	B5		B12
	B3#		B8#
	B7		B10
	B7		B7
	B8#		B2

V. ENCRYPTION IN PRESENTATION LAYER USING SHORT LENGTH KEYS

The method of digitadition is used for generating keys of short length. Digitadition is the sum of the individual digits of a chosen number. This includes keys of self-code and generated code. A self-code is one which cannot be generated using digitadition of a given number (Ex:142857,10^6). In this work, self-numbers are avoided in the generator sequence. To identify a self-number, a check algorithm is used. A starting number (random choice) is initialized and using successive digitadition, a generator sequence of size 'p' is formed. A typical short length key has 'p'<=10. Using this 'p' length sequence a key with size four digits is generated.

A. Procedure for key generation

(i) The first two digits of the key is the initial number N_0

(ii) The final two digits is obtained using the relation

N_k-N_0+digitaddition (N_k) (1)

An example short length key for p=10 is illustrated below:
Initial number N_0=42

Generated Number $N_1 = N_0$+digitadition (N_0) = 42+6 =48
Digitadition $N_2 = N_1$+digitadition (N_1) = 48+12=60
$N_3 = N_2$+digitadition (N_2) = 60+6 =66
$N_4 = N_3$+digitadition (N_3) = 66+12=78

The generator sequence is 4248606678. Using this sequence, the generated key is 4251.

Where 42 is the initial two digit number N_0 and
51 is N_4-N_0+digit addition (N_4) using equation (1)

B. Decryption of short keys

The properties of the key generated using the above procedure is used in the decryption. This includes:

1. There is no non-recursive formula for the partial sum of a digitadition series, given its first and last terms.
2. To get the sum of all the digits in a digitadition series, simply subtract the first number from the last and add the sum of the digits in the last number.
3. There is no non recursive formula that generates all self-numbers.
4. Multiple generators for a generated number can exist only if the number exceeds 100

[Ex: both 91 and 100 generate the 3 digit number 101]. However, for a given initial number No, the 'p' size generator sequence is unique.

From the received short key the generated series of size 'p' can be recovered. This sequence is the decrypted key. For the illustration shown, the received short length key is 4251 and the decrypted key is 4248606678. Thus, the short key is publicly distributed and authenticated users (knowing equation (1)) alone can generate the 'p' size medium key. The pseudo code for decryption is as follows:

Global information shared in common
Size of initial number N_0 =2
Step 1: Received key 4251
Step 2: Using the global information the initial two digits are separated. Thus N_0=42
Step 3: The number N_0 and the second two digit number 51 are related as **N_m-42+(7+8)=51 and also the sum of 4+2+4+8+6+0+6+6+7+8=51**
Step4: Using retrograde analysis, and using the information in

step 3, terms up to and including N_m is decrypted and the medium key is generated.

C. *Identifying a self-number:*

Step 1: Form S= (d[N] +c)/2, where c=9 if d[N] is odd and c=0 if d[N]=even; and d[N] is the digital root of the number N.
Step 2: Subtract *S* from N.
Step 3: Check the remainder to see if it generates *N*. If it does not, subtract 9 from the last result and repeat step 2.
Step 4: Continue subtracting 9's, each time checking the result to see if it generates N.
Step 5: If this fails to produce a generator of N in k steps, where k is the number of digits in N, then N is a self-number.

VI. IMPLEMENTATION

The hardware implementation is done using the key generation techniques explained in this paper on LPC1788 ARM Board. The data transfer between the users is demonstrated both in synchronous (TCP/IP) and the asynchronous (UDP).
The various tasks includes,

1. Block encryption
2. UDP Implementation
3. Adding Block encryption code
4. Target hardware initialization and boot up
5. LAN/ wireless connectivity between the target hardware

(i) *In what way does DES encryption Works in "Emac_EasyWeb" Code?* Through UDP (Communication will happen through Ethernet), we can send encrypted (DES) data to the Specific Destination. The Destination will receive the encrypted data and it will decrypt using the DES algorithm.

(ii) *UDP Implementation in "Emac_EasyWeb":* The Emac_EasyWeb is the example code that will provide along with this document. We have demonstrated the DES encryption algorithm using this Emac_EasyWeb Example. The Emac_EasyWeb is based on TCP/IP communication. In this experiment, we are only using UDP for transmission and reception. So that, we have to modify some changes in Emac_EasyWeb project.

VII. RESULTS

Case (i) Implementation of block cipher

An example is shown in the figure 7 with the key "ASD" and the data to be encrypted as "HELLOWORLD".

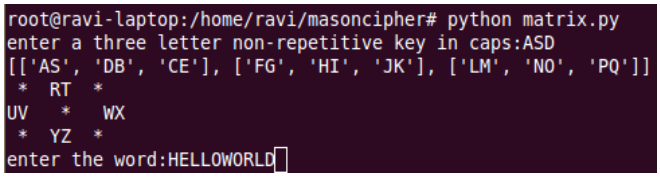

Fig 7: Sample key of 3 letters encrypted in HELLOWORLD

Case (ii) Implementation of short key and decryption

The decryption of the medium key using the short key is implemented in Linux kernel using python language. The short key '4783' is given as input and the decrypted key is obtained. The obtained generated sequence is as follows:
From the short key the information known to authenticated users are: (i) N_0=47;

(ii) N_m-N_0+sum of digits [N_0 to N_m] =83.

Using this information and retrograde analysis the successive digits of the key is obtained as:
(i) N_1=47+digitadition(47)=58;
(ii) N_2=58+digitadition(58)=71;

And so on to decrypt the medium key '4758717995109119'.
An encrypted key and a decrypted medium key is as shown in figure 8.

Fig 8: Shows the result of decrypted medium key

The metrics measured under cryptographic schemes is shown in table 3.

TABLE: 3 METRICS USED

Metrics	Area of research	Methodology	Hardware	Type	Metrics
Cryptography	Network Security				
Block concept		Block cipher		✓	
Short key		✓		Public	
Kernel			Linux		
Language			Python		
Time Complexity					✓
Memory Usage					Less
1788 ARM			✓		

Conclusion

Computational complexity in decrypting the medium key is reduced to finite number of clock cycles. The size of the short key is always fixed i.e. four. The number of blocks was thirteen and the advantage is that the key can be placed anywhere among the 13 blocks, though for convenience, it is started from top left. The resultant obtained in form of symbolic output and also represented it block numbers. As the short key is publicly distributed and authenticated users alone can generate the medium key. Therefore the data transfer can be done safely between users both in synchronous and asynchronous. The inference here result in less memory usage compared to others and the frequency of short key generation is faster.

References

[1] Gerhard A Schloss, Micheal J Wynblatt," Presentation layer primitives for the layered multimedia Data Model", Computer science department, state university of new York at stony Brook.

[2] Evgenii Krouk, Sergei Semeniv "A joint coding at neighbor network layers", St-Peter state university of aerospace Instrumentation, Bolshia Morskaia Str., 67,St-petersberg,19000,Russia, Nokia Technology Platforms, PO Box 86,FIN-24101 Salo, Finland.

[3] Chung-ming huang and hsu-yang Kung, "A Synchronization Infrastructure for Multicast Multimedia at the Presentation Layer", laboratory of multimedia networking, Institute of information engineering, National cheng Kung university, Tainan, Taiwan 70101.

[4] Shubat S.Ahmeda, "ID-Based and Threshold Security Scheme for ad hoc Network", Department of computer Engineering, Elfath University, Tripoli, Libya.

[5] Sombir Singh, Sunil K Maakar, Dr. Suresh kumar," Enhancing the security of DES algorithm using Transportation cryptography techniques", BRCM CET, Bahal, India.

[6] Pallavi H.Dixit, Dr.Uttam L. Bombale, Vinayak B.Patil "Comparitive implementation of Cryptographic algorithms on ARM Platform", Shivaji University, Kolhapur, Maharashtra, India.

[7] Ajay Bhushan, Ajeet K. Bhartee, Pawitar Dulari," A Study of TORDES with other Symmetric Key Algorithms", G.C.E.T. Greater Noida (U. P.), Volume 2, Issue 12, December 2012.

[8] Soheila Omer AL Faroog Mohammed Koko, Dr.Amin Babiker A/Nabi Mustafa, " Comparison of Various Encryption Algorithms and Techniques for improving secured data Communication **",** AL Neelain University, Faculty of Engineering. Khartoum,Sudan, Dean of Faculty of Engineerning, AL Neelain University, Khartoum, Sudan, Volume 17, Issue 1, Ver. III (Jan – Feb. 2015), PP 62-69.

[9] http://media.johnwiley.com.au/product_data /excerpt/28/07803535/0780353528.pdf

[10] Chetan kumar k v,S Sujatha," VLSI Implementation of DES & TDES Algorithm with Cipher Block Concept", ISSN: 2319–6378, Volume-2, Issue-7, May 2014.

[11] A.Menezes, P.van Oorschot, S.Vanstone,"Handbook of Applied cryptography", CRC Press

[12] Mansoor Ebrahim, shujaat khan, umer Bin Khlid,"Symmetric algorithm Survey: A Compartive Analysis", IQRA University main campus, Defense view Karachi, International Journal of Computer Applications (0975 – 8887) Volume 61– No.20, January 2013.