A Dynamic Modular Cipher Cryptography Technique

Syed Haroon Hasan
PG Research Scholar Dept. of Computer Science
& Engineering, ASCT, Bhopal (M.P.)

Zuber Farooqui
Asst. Professor Dept. of Computer Science
& Engineering, ASCT,
Bhopal (M.P.)

ABSTRACT
Modern Internet protocols support several modes of operation in encryption tasks for data confidentiality to keep up with varied environments and provide the various choices, such as multi-mode IPSec support. To begin with we will provide a brief introduction on the modes of operation for symmetric-key Module ciphers. Different Module cipher modes of operation have distinct characteristics. For example, the cipher Module chaining (CBC) mode is suitable for operating environments that require self-synchronizing capabilities, and the output feedback (OFB) mode requires encryption modules only. When using symmetric-key Module cipher algorithms such as the Advanced Encryption Standard (AES), users performing information encryption often encounter difficulties selecting a suitable mode of operation. This paper describes a structure for analyzing the Module operation mode combination. This unified operation structure (UOS) combines existing common and popular Module modes of operation. UOS does multi-mode of operation with most existing popular symmetric-key Module ciphers and do not only consist of encryption mode such as electronic codebook (ECB) mode, cipher Module chaining (CBC) mode, cipher feedback (CFB) mode and output feedback (OFB) mode, that provides confidentiality but also message authentication mode such as the cipher Module chaining message authentication code (CBC-MAC) in cryptography. In Cloud Computing, information exchange frequently via the Internet and on-demand. This research provides an overview and information useful for approaching low-resource hardware implementation, which is proper to ubiquitous computing devices such as a sensor mote or an RFID tag. The use of the method is discussed and an example is given. This provides a common solution for multimode and this is very suitable for ubiquitous computing with several resources and environments. This study indicates a more effectively organized structure for symmetric-key Module ciphers to improve their application scenarios. We can get that it is flexible in modern communication applications.

Keywords
Symmetric key cryptography, Encryption, Decryption, Dynamic secret key, Cryptographic Pseudo-Random number generator, Hybrid technique, Transposition, Substitution.

1. INTRODUCTION
Data confidentiality is one of the security services in cryptography. The major concept in information security today is to continue to improve encryption algorithms.[2] There are two major types of encryption algorithms for cryptography, symmetric-key algorithms and public-key algorithms.[2] Symmetric-key algorithms also referred to as conventional encryption algorithms or single-key encryption algorithms are a class of algorithms that use the same cryptographic keys for both encryption of plaintext and decryption of ciphertext.[4] It remains by far the most widely used of the two types of encryption algorithms. Symmetric-key encryption algorithms can use either stream ciphers or Module ciphers. Module ciphers take a number of bits and encrypt them as a single unit, padding the plaintext so that it is a multiple of the Module size. Modules of 64 bits have been commonly used [3].

Module ciphers are designed to encrypt data in chunks of specific size [5]. A Module cipher specification will identify how much data should be encrypted each pass (called a Module) as well as what size should be applied to each Module. DES algorithm and Public key encryption are the famous examples of this type [1].

Despite its popularity, DES has been plagued with controversy. Some cryptographers objected to the closed-door design process of the algorithm. The debate about whether DES' key is too short for acceptable commercial security has raged for many years, but recent advances in distributed key search techniques have left no doubt in anyone's mind that its key is simply too short for today's security applications.[6] Triple-DES has emerged as an interim solution in many high-security applications, such as banking, but it is too slow for some uses. More fundamentally, the 64-bit block length encrypted by DES and most other well-known ciphers opens it up to attacks when large amounts of data are encrypted under the same key [2].

2. PHRASEOLOGY
A message is plaintext. The process of disguising a message in such a way as to hide its substance (as well as meaning) is encryption (also called enciphering) [3]. An encrypted message is ciphertext. The process of turning ciphertext back into plaintext is decryption (also termed as deciphering). A key is a piece of information (a parameter) that determines the functional output of a cryptographic algorithm or cipher. In encryption, a key specifies the particular transformation of plaintext into ciphertext, or vice versa during decryption.[4] The range of possible values of the key is called the key space. A cryptosystem is an algorithm, plus all possible plaintexts, ciphertexts, and keys.

Encryption and decryption functions are represented as:

$$EK(M) = C$$

$$DK(C) = M$$

These functions have the property that:

$$DK(EK(M)) = M$$

Some algorithms use a different encryption key and decryption key .That is, the encryption key, K1, is different from the corresponding decryption key, K2. In this case:

$$EK1(M) = C$$

$$DK2(C) = M$$

$$DK2(EK1\ (M)) = M$$

The art and science of keeping messages secure is cryptography, and it is practiced by cryptographers. Cryptanalysis is the art and science of recovering the plaintext of a message (or breaking the cipher text) without access to the key.[1] Successful cryptanalysis may recover the plaintext or the key. Cryptanalysts are practitioners of cryptanalysis; that is, seeing through the disguise [5]. The branch of mathematics encompassing both cryptography and cryptanalysis is cryptology and its practitioners are cryptologists. In contrast, a code is a method used to transform a message into an obscured form, preventing those who do not possess special information, or key, required to apply the transform from understanding what is actually transmitted. The usual method is to use a list of common phrases or words matched with a codeword. Encoded messages are sometimes termed codetext, while the original message is referred to as plaintext [4].

3. FUNCTION OF CRYPTOGRAPHY

The main function of cryptography is to ensure information security which is protecting information and information systems from unauthorized access, use, disclosure, disruption, modification, perusal, inspection, recording or destruction. Cryptography includes techniques such as encryption/decryption, hashing, digital signatures, timestamps etc. to ensure information security [2]. Broadly speaking, cryptography performs following 4 key functions:

• **Confidentiality:** Protection against the disclosure of information to parties other than the intended recipient (for example: encryption and decryption) [14]

• **Authentication:** It should be possible for the receiver of a message to ascertain its origin; an intruder should not be able to masquerade as someone else (for e.g. public key cryptography and digital signatures) [13].

• **Integrity**: It should be possible for the receiver of a message to verify that it has not been modified in transit; an intruder should not be able to substitute a false message for a legitimate one (for e.g. hashing) [1].

• **Non-repudiation:** A sender should not be able to falsely deny later that he sent a message (for e.g. digital signatures with timestamps)[11]

4. TYPES OF KEY- BASED ALGORITHS

There are two general types of key-based algorithms:

• Symmetric Algorithms: These are also referred to as secret-key algorithms, single key algorithms, conventional algorithms, Symmetric algorithms, private-key algorithms or one-key algorithms [4]. These are the algorithms where the encryption key can be calculated from the decryption key and vice versa [3]. In most symmetric algorithms, the encryption key and the decryption key are trivially related, often identical. Encryption and decryption with a symmetric algorithm are denoted by:

$$EK(M) = C \quad DK(C) = M$$

- ***Cryptosystems*** The combination of algorithm, key , and key management functions used to perform cryptographic operations. Cryptosystem is represented by 5 tuples[1]:

  Quintuple (E, D, M, K, C)
  M set of plaintexts
  K set of keys
  C set of ciphertexts
  E set of encryption functions
  e: $M \times K \rightarrow C$
  D set of decryption functions
  d: $C \times K \rightarrow M$

- ***Plaintext–*** A message in its natural format readable by an attacker
- ***Ciphertext*** **–** Message altered to be unreadable by anyone except the intended recipients
- ***Key***– Sequence that controls the operation and behavior of the cryptographic algorithm**.** Key space– Total number of possible values of keys in a crypto algorithm. Keys are rules used in algorithms to convert a document into a secret document

  Symmetric algorithms can be represented diagrammatically as:

These algorithms require that the sender and receiver agree on a key before they can communicate securely. The security of a symmetric algorithm rests in the key; divulging the key means that anyone could encrypt and decrypt messages. As long as the communication needs to remain secret, the key must remain secret. Some examples of popular and well-respected symmetric algorithms include Twofish, Serpent, AES (Rijndael), Blowfish, CAST5, RC4, 3DES, and IDEA. Symmetric algorithms can be divided into two categories: stream ciphers and Module ciphers.

• A Module cipher is a symmetric key cipher operating on fixed-length groups of bits, called Modules, with an unvarying transformation [13]. A Module cipher encryption algorithm might take (for example) a 128-bit Module of plaintext as input, and output a corresponding 128-bit Module of ciphertext. The exact transformation is controlled using a second input — the secret key. Decryption is similar: the decryption algorithm takes, in this example, a 128-bit Module of ciphertext together with the secret key, and yields the original 128-bit Module of plaintext.

• A stream cipher is a symmetric key cipher where plaintext bits are combined with a pseudorandom cipher bit stream (keystream), typically by an exclusive-or (XOR) operation. In a stream cipher the plaintext digits are encrypted one at a time, and the transformation of successive digits varies during the encryption. An alternative name is a state cipher, as the encryption of each digit is dependent on the current state. In practice, the digits are typically single bits or bytes [13].

- **Public-key Algorithms:** This cryptographic approach involves the use of asymmetric key algorithms that is, the non-message information (the public key or the encryption key) needed to transform the message to a secure form is different from the information needed to reverse the process (the private key or the decryption key). The person who anticipates receiving messages first creates both a public key and an associated private key, and publishes the public key [2]. When someone wants to send a secure message to the creator of these keys, the sender encrypts it (transforms it to secure form) using the intended recipient's public key; to decrypt the message, the recipient uses the private key.

Encryption using public key K is denoted by:

$$EK(M) = C$$

Even though the public key and private key are different, decryption with the corresponding private key is denoted by:

$$DK(C) = M$$

Unlike symmetric key algorithms, a public key algorithm does not require a secure initial exchange of one or more secret keys between the sender and receiver.[3] The particular algorithm used for encrypting and decrypting was designed in such a way that, while it is easy for the intended recipient to generate the public and private keys and to decrypt the message using the private key, andwhile it is easy for the sender to encrypt the message using the public key, it is extremely difficult for anyone to figure out the private key based on their knowledge of the public key [13].

The use of these keys also allows protection of the authenticity of a message by creating a digital signature of a message using the private key, which can be verified using the public key [1].

One Time Pad

One-time pad (OTP), also called Vernam-cipher or the perfect cipher, is a crypto algorithm where plaintext is combined with a random key. It is the only existing mathematically unbreakable encryption [13][14].

We can only talk about one-time pad if some important rules are followed. If these rules are applied correctly, the one-time pad can be proven unbreakable (see Claude Shannon's "Communication Theory of Secrecy Systems"). Even infinite computational power and infinite time cannot break one-time pad encryption, simply because it is mathematically impossible. However, if only one of these rules is disregarded, the cipher is no longer unbreakable. Processing [13]14]. However, the security of these algorithms relies on long term symmetric keys that contradict the original idea of one time pad. However, increasing the cryptographic key size is not always the best solution, since no matter how large the key is, its cryptography is still ultimately breakable [5].

5. PROPOSED ALGORITHM

We propose a new consolidation algorithm that generates a dynamic key type of Secure Secret Key Process" called "A dynamic modular cipher cryptographic technique", a dynamic key of 164 bits. Mechanism has been formally analyzed for performance between safety and performance. Once the operation is run, the key has been abandoned. The concept of mobility is based on OTP

5.1 Modular Dynamic Key Generation

In the proposed work the dynamic key is generated using Cryptographic Pseudo-Random number generator (CPRNG). User input a text key 'IK' .Minimum size of IK is 9 bits and it can have maximum 18 bits. Depending upon text key size a base value (y_0) is determined from base table i.e table 1. A fragmentary generated key is concatenated with the key entered by user to produce a matrix of size 14X14.A randomize function (F_r) is used to generate the key. The function F_r involves various matrix operations such as multiplication, Shift Cipher operation, modulus etc .In which the random number y_0 is added to the final matrix to produce the dynamic key.

Detailed Algorithm:

A. Process to Generate Key:

1. User input a key (IK) of size between 9 to 18 char
2. Data is processed in the form of binary digits
3. Apply CPRNG to get fragmentary generated key
4. Perform matrix transpose to shuffle key matrix. It will generate a key of size 1568 bits.
5. Calculate Hash value of key to get final version of dynamic key. Hashing algorithm is applied to get 164 bit key.

B. Process to perform Encryption:

1. Determine total number of Modules. Apply padding bits to have 54 bit Modules.
2. Divide the dynamic key into 4 parts.
3. Encryption of every Module involve below steps:

a. Iteration 1

- Transposition is performed on matrix.
- Perform XOR on transposed matrix and dynamic key first part.
- Add matrix to dynamic key second part.
- Iteration one cipher will be known as fragmentary cipher1

b. Iteration 2

- XOR fragmentary cipher1and dynamic key part 1
- Perform Transposition of step 1 output and inbuilt key (IK)
- Perform Substitution operation on step 3 output.
- Iteration one cipher will be known as fragmentary cipher11

C. Decryption:

a. **Iteration 1**

Decryption of Module 1:

- Perform Substitution on fragmentary cipher11 & Dynamic key part 4
- Perform XOR on first step output and dynamic key part 1
- Perform Inverse Transpose on matrix
- Perform Transposition of Input Key (IK) with step 3 output.
- Iteration 1 plaintext is generated

Decryption of Module 2 to Module n:

- Perform Shift Cipher operation on fragmentary cipher11
- Perform XOR of Step 1 output and Dynamic key Part 2
- Apply Substitution operation on Step 1 and Step 2 output
- Plaintext of further Modules is generated

b. **Iteration 2**

Decryption of Module 1

- Perform Substitution of Iteration 2 Fragmentary Cipher Module 1
- Perform Inverse Transposition on Step 1 output and IK
- Perform XOR on step 2 output and dynamic key part 2

Module 2 to n

- Perform XOR of Dynamic key part 2 &Iteration 1 Cipher Module 2
- Perform XOR on fragmentary cipher2 & IK

- Perform Substitution on Step 3 output
- Iteration 2 Fragmentary Cipher Module2 is generated

5.2 Function used in Encryption

SHIFT CIPHER FUNCTION:

The Shift Cipher function used in encryption algorithm.

Following is the process to perform Shift Cipher operation:

- Convert the letter into the number that matches its order in the alphabet starting from 0, and call this number **X**.
  (A=0, B=1, C=2, ...,Y=24, Z=25)
- Calculate: **Y** = **(X + K)** mod **26**
- Convert the number **Y** into a letter that matches its order in the alphabet starting from 0. (A=0, B=1, C=2, ...,Y=24, Z=25)

$$C_t=DK(M_t) = (M_t + DK_t) \bmod 26$$

Where $1 \leq t \leq 164$

At the receiver end operation is as follows:

$$M_t=DK_t(C_t)=(C_t-DK_t) \bmod 26$$

6. PERFORMANCE ANALYSIS

The striking feature of this algorithm is that the key is dynamic and the encryption and decryption process constitutes of two Iterations. Multiple Iterations make cryptanalysis even harder. Furthermore the time taken to process an average size plaintext is comparatively very little. However the main merit of the algorithm is little amounting of computational time that one has to spend to encrypt a message.

Table I: Comparison of dynamic key and session key:

Issues	Dynamic Key	Session Key
Key Exchange	Once	Every Session
Lifetime	Within a message	Within Session
Key Reusable	No	Yes
Vulnerable under man in middle Attack	No	Yes
From a compromised cryptographic key , adversary can	Decrypt a message	Decrypt all messages in the session
From a compromised key exchange protocol	Cryptographic system is still safe	Cryptographic system and session are vulnerable

Table II: Analysis of Proposed algorithm

Module Size	Plaintext size	No. of Modules	Complexity of Aritho-Logic Operations
54 bits	108 bits	2	7+8=15
	216 bits	4	7+8*3=31
	324 bits	6	7+8*5=47
	540 bits	10	7+8*9=79
	580 bits	12	7+8*11=95
	840 bits	18	7+8*17=143
	1240 bits	26	7+8*25=207
	1600 bit	33	7+8*32=263

Table III: Comparative Analysis of key size and Module size

Algorithm	Key Size (Bits)	Module Size(Bits)
DES	64	64
3DES	192	64
Rijndael	256	128
Blowfish	448	64
A Dynamic Modular Cipher Cryptographic Technique	164 hashed from 1568 bit long key	54

Table IV: Comparison of Time complexities

Algorithm	Megabytes processed	Time Taken	MB/Second
DES	256	5.998	21.340
3DES	256	6.159	20.783
Rijndael	256	4.164	61.010
Blowfish	256	3.976	64.386
Proposed Algo	256	3.883	64.06

7. CONCLUSION & FUTURE WORK

This is a symmetric key cryptography algorithm which uses the concept of dynamic key & Module Cipher. Dynamic key is generated by using CPRNG (Cryptographic Pseudo-Random number generator).Variable length plaintext is encrypted by using dynamic key of size 164. This is a Module cipher technique. Furthermore the major merit of the proposed algorithm is that it is hard to break and the time taken to execute the algorithm is comparatively very little.In the future work the algorithm will be tested in front security level are

verified in this paper with other well known algorithms. More work on the key size and key sharing technique may be optimized in future.

8. REFERENCES

[1] Zeenat Mahmood," Hybridize Dynamic Symmetric Key Cryptography using LCG", International Journal of Computer Applications (0975 – 8887) Volume 60– No.17.

[2] Behrouz A. Forouzan,"Cryptography & Network Security" Tata McGraw Hill, ISBN 13-978-0-07-066046-5.

[3] M. Blaze, W. Diffie, R. L. Rivest, B. Schneier, T. Shimomura, E. Thompson, and M. Wiener," Minimal Key Lengths for Symmetric Ciphers to Provide Adequate Commercial Security",Report of Ad Hoc Panel of Cryptographers and Computer Scientists, Jan. 1996.

[4] Ayushi, " A Symmetric Key Cryptographic [Algorithm "International Journal of Computer Applications (0975 8887) Volume 1 – No. 15

[5] W. Diffie and M. E. Hellman, "New directions in cryptography, " IEEE Transactions on Information Theory, vol. 22, no. 6, pp. 644-654, 1976

[6] Huy Hoang Ngo, Xianping Wu, Phu Dung Le, Campbell Wilson, and Balasubramaniam Srinivasan "Dynamic Key Cryptography and Applications " International Journal of Network Security, Vol.10, No.3, PP.161{174, May 2010

[7] R. Divya & T. Thirumurugan, "A Novel Dynamic Key Management Scheme Based On Hamming Distance for Wireless Sensor Networks", International Journal of Scientific & Engineering Research Volume 2, Issue 5, May- 2011,ISSN 2229-5518

[8] Yunpeng Zhang, Fei Zuo, Zhengjun Zhai and Cai Xiaobin. 2008. A New Image Encryption Algorithm Based on Multiple Chaos System. International Symposium on Electronic Commerce and Security. 347-350.

[9] Xukai Zou, Yogesh Karandikar and Elisa Bertino, "A Dynamic key management solution to access hierarchy", International Journal of Network Management 2007; 17: 437- 450

[10] P. Hellekalek "Good random number generators are (not so) easy to find Mathematics and Computers in Simulation "46 (1998) 485±505

[11] Dr. Ranjan Bose and Amitabha Banerjee "IMPLEMENTING SYMMETRIC CRYPTOGRAPHY USING CHAOS FUNCTIONS"

[12] L. Law, A. Menezes, M. Qu, J. Solinas, S. Vanstone, "An effcient protocol for authenticated key agreement," Designs, Codes and Cryptography, vol. 28, no. 2, pp. 119-134, 2003

[13] http://www.pro-technix.com/information/crypto/pages/vernam_base.html

[14] http://www.cryptomuseum.com/crypto/otp.htm

[15] F. Sun, S. Liu, Z. Li and Z. Lü., 2008. A novel image encryption scheme based on spatial chaos map. Chaos, Solitons and Fractals, 38 (3), 631 – 640.

9. AUTHOR'S PROFILE

Syed Haroon Hasan has completed BE from SCET Bhopal and Pursuing M.Tech from All Saints' College of Technology, Bhopal

Zuber Farooqui is Asst. Professor in CSE/IT Dept. ASCT, Bhopal. He has completed B.Tech & M.Tech from Bhopal.