A Review on Ron's Cryptographic Algorithms

Dr. K. Thangadurai[1], V. Poongodi[2]

[1]*Assistant Professor, P.G. & Research Dept.of Computer Science, Government Arts College (Autonomous), Karur*
[2]*Assistant Professor, Department of Computer Application, Thanthai Hans Roever College, Perambalur*

Abstract

Nowadays due the technological development computer play a vital role in all fields to store and transfer the information. Security is required to transmit confidential information over the network. This is achieved by applying the cryptographic technique. Cryptography is a tool which is used to keep information confidential and to ensure its integrity and authenticity. The cryptography technique is divided into Symmetric Key Algorithm, Asymmetric Key Algorithm and Hybrid Algorithm. Symmetric Key Algorithm is classified into two ciphers namely stream cipher and block cipher. This paper describes three symmetric algorithm RC4, RC5, RC6 proposed by Ronald Rivest to achieve fast accessibility, Confidentiality and Security.

Keywords: *Cryptography, Encryption, Decryption RC4, RC5, RC6*

1. Introduction

Cryptography is the art or science encompassing the principles and methods of transforming an intelligible message into one that is unintelligible and then retransforming that message back to its original form [1]. The security in computer systems can be increased by is encrypting and decrypting the data. In this technique original message is called plain text. Encryption is the process of converting the plain text (original message) into cipher text (encrypted text). Decryption is the process of transferring the cipher text (encrypted text) into Plain Text (original message) which is shown in figure 1. Encryption and decryption are controlled by cryptographic keys.

2. Goals of Cryptography

2.1. Confidentiality

It is a service used to keep the content in a secret manner and when the Information is transmitted it has to be accessed only by the authorized party and not by anyone else [2].

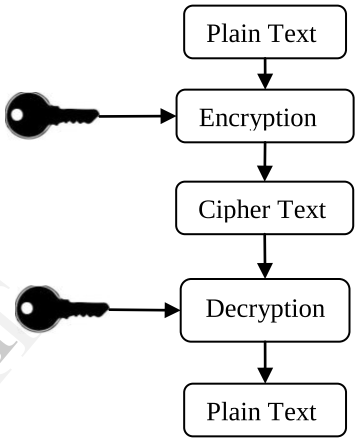


Figure 1. Encryption and Decryption Block Diagram

2.2. Authentication

The Authentication service is related to identification. Two parties entering into communication should identify each other. Information received by any system has to check the identity of the sender that whether the information is arriving from a authorized person or a false identity [2].

2.3. Data Integrity

This service addresses the unauthorized alteration of data. The information has not been altered by unauthorized or unknown that means no one in between the sender and receiver are allowed to alter the given message [2].

2.4. Non Repudiation

It prevents either sender or receiver from denying the message. Thus when a message is sent, the receiver can prove that the message was in fact send by the alleged sender. Similarly, when a message is received, the sender can prove the alleged receiver in fact received the message [2].

2.5. Access Control

This Access Control service is used to provide the access of information only to the authorized parties.

3. Cryptographic Techniques

The cryptographic techniques are broadly classified into different categories namely,

1. Symmetric Key Algorithm (Secret Key)
2. Asymmetric Key Algorithm (Public Key)
3. Hybrid Key Algorithm

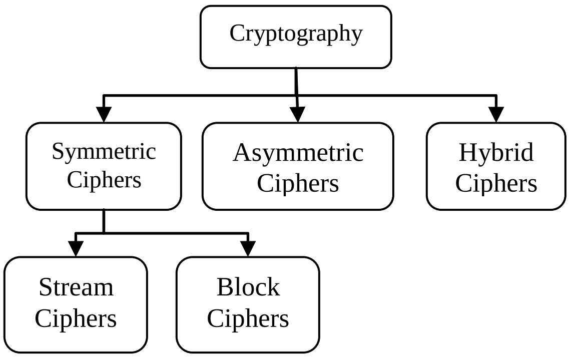


Figure 2. Main Areas within Cryptography

3.1. Symmetric Key Algorithm

Symmetric Key Algorithm is referred to as shared key encryption algorithm or secret key algorithm [3,4]. In this algorithm the sender and receiver (both the parties) uses the same key to encrypt or decrypt the data. The algorithm is further classified into Stream Cipher and Block Cipher. Symmetric Key Algorithm is extremely fast, and their relatively low complexity allows for easy implementation. Some Important symmetric key algorithms are DES, 3DES, AES, Blowfish, Twofish, Serpent, SEED, IDEA, RC2, RC4 and RC6.

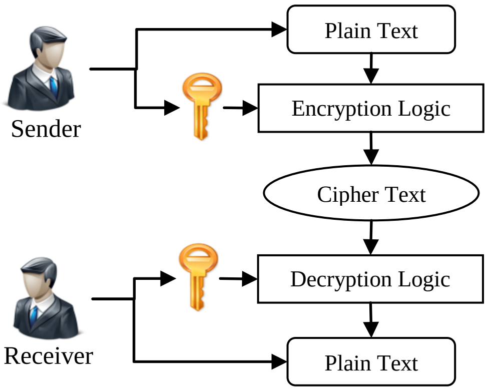


Figure 3. Symmetric Key Algorithm

3.1.1. Stream Cipher

A stream cipher is a method of encrypting plain text into cipher text. In this method, the cryptographic key and algorithm are applied to each binary digit in a data stream, one bit at a time.

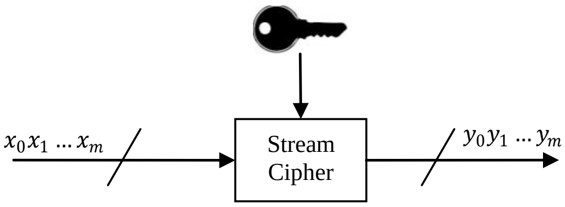


Figure 4.Principles of encrypting m bits with a stream

3.1.2. Block Cipher

A block cipher is one in which a block of plain text is treated as a whole and used to produce a cipher text block of equal length. A block size of 64 or 128 bit is used.

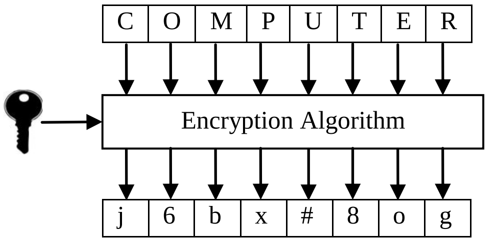


Figure 5. Block Cipher Encryption

3.2. Asymmetric Key Algorithm

Asymmetric Key Algorithm is also called Public Key Algorithm [3,4]. In this algorithm the sender and receiver uses two different keys namely Public Key and Private Key to encrypt and decrypt the data. The sender uses the receivers' public key for encrypting the plain text into cipher text. The receiver uses his private key for decrypting the cipher text into plain text. The Private Key used in this Algorithm is always kept confidential. Asymmetric Key Algorithm is slow and impose high computational burden compared to Symmetric Key Algorithm. The most familiar asymmetric key algorithm is RSA. Other asymmetric key algorithms are Diffe_Hellman, DSA, EIGamal, ECDSA and XTR

Table 1
Comparison of Symmetric Key Algorithms

S. No	Algorithm	Key Length (bits)	Rounds	Created By	Year
1.	Advanced Encryption Standards (AES)	128, 192, 256	9,11,13	Joan Daemen & Vincent Rijmen	1998
2.	Data Encryption Standards (DES)	56	16	IBM	1975
3.	Triple Data Encryption Standards (3DES)	168	48	IBM	1978
4.	Blowfish	32-448 (128 by default)	16	Bruce Schneier	1993

3.3. Hybrid Algorithm

In the modern cryptographic system the Symmetric Key Algorithm and Asymmetric Key Algorithm are used for the encryption and decryption process [3,4]. The Asymmetric Key Algorithms are used to distribute symmetric keys at the start session. Once a symmetric key is known to all parties of the session, faster symmetric key algorithms are used for the encryption and decryption process. This algorithm mainly simplifies the key distribution problem.

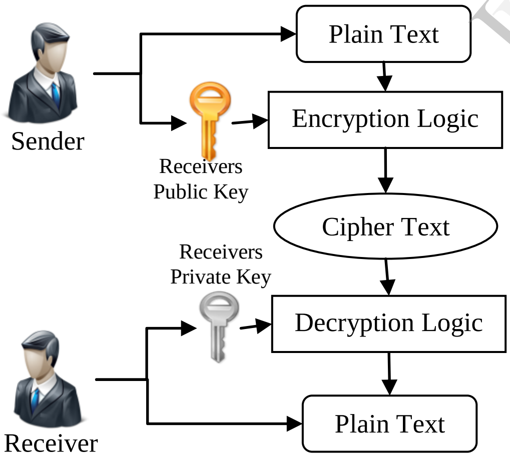


Figure 6. Asymmetric Key Algorithm

4. Overview of Ron's Cryptographic Algorithms

This section gives the detail explanation of cryptographic algorithms developed by Ronald Rivest, one of the inventors of the RSA public key cryptography algorithm and co-founders of RSA security. Ronald developed three Symmetric key algorithms namely Rivest Cipher4 (RC4), Rivest Cipher5 (RC5) and Rivest Cipher6 (RC6). Among them RC4 belong to the stream cipher category and the remaining two algorithms RC5 and RC6 are belong to the block cipher category which is shown in figure 7.

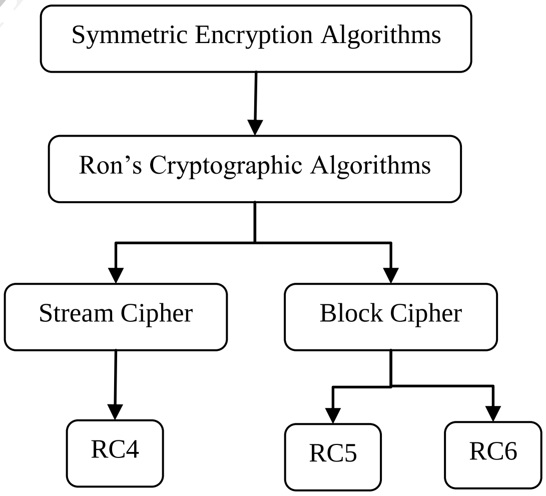

Symmetric Encryption Algorithms
Ron's Cryptographic Algorithms
Stream Cipher
Block Cipher
RC4
RC5
RC6

Figure 7. Ron's Cryptographic Algorithms

4.1. Rivest Cipher4 (RC4)

RC4 is a stream cipher from RSA Data Security. It was one of the popular and fastest symmetric key algorithms invented in the year 1987[5,6]. The algorithm uses a variable sized key from 1 to 256 bits is used to initialize a 256-byte state vector S. The same algorithm is used for both encryption and decryption. For encryption and decryption, a byte k is generated from S by selecting one of the 255 entries. As each value of k is generated, the entries in S are once again permuted.The principle of RC4 algorithm is divided into two stages.

1. Key-Scheduling algorithm (KSA)
2. Pseudo Random Generation Algorithm (PRGA).

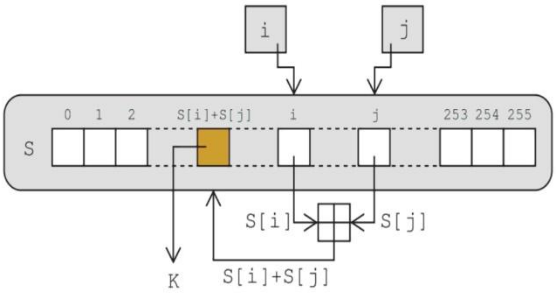


Figure 8. An overview of RC4 [5]

4.1.1. Key-Scheduling Algorithm (KSA)

The main function of the Key-Scheduling Algorithm is to complete initialization of RC4 Key. The algorithm first initializes the S table with the identity permutation. Once the S array is initialized, shuffling of the array is performed using the key to make it a permutation array. For this operation, S array is processed for 256 iterations [5,6]. The pseudo-code for the key scheduling algorithm is given below

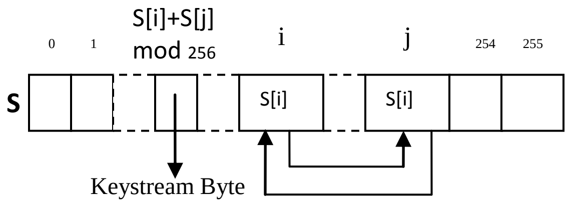
```
for  i from 0 to 255
        S [ i ] : = i
endfor
j : = 0
for i from  0 to 255
      j : = ( j +  S [ i ] + key [ i  mod  key length ] )
   mod 256
        swap  values of  S [ i ]  and  S [ j ]
endfor
```

Finally the S array is generated and it is used in the PGRA to generate the key stream.

4.1.2. Pseudo-Random Generation Algorithm (PRGA)

The PGRA is used to generate the keystream of the size of the message to encrypt and it has the capacity to generate the keystream of any size [5,6]. To Perform the PRGA operation, firstly, assign (or initialize) any two index to 0 and then the generation of keystream starts one byte at a time until it reaches the size of the message. For computing the each new byte the following steps are used.

- Compute new value of i and j
  i : = (i + 1) mod 256
  j : = (j + S [i]) mod 256
- To have a dynamic state swapping process is performed between S [i] and S [j]
- Retrieve the next byte of the keystream from the S array at the index
  S [i] + S [j] mod 256



The pseudo-code for the pseudo-random generation algorithm is given below

```
i  : = 0
j  : = 0
while Generating Output :
    i : = (i + 1) mod 256
    j : = (j + S [ i ] ) mod 256
    swap values of  S [ i ] and S [ j ]
    K : = S [ (S [ i ] + S [ j ] )  mod 256 ]
    output K
endwhile
```

4.1.3. Steps for RC4 Algorithm

The steps for RC4 encryption algorithm is as follows [5,6]:

Step 1 : Get the data to be encrypted and the selected key.
Step 2 : Create two string arrays.
Step 3 : Initiate one array with numbers from 0 to 255.
Step 4 : Fill the other array with the selected key.
Step 5 : Randomize the first array depending on the array of the key.
Step 6 : Randomize the first array within itself to generate the final key stream.
Step 7 : XOR the final key stream with the data to be encrypted to give cipher text.

4.1.4. RC4's Success:

- Random nature of S-Box changes which makes it difficult to locate a value in its table. Through the use of a 256 byte internal key,an S-box RC4 can be in 256!*2562 possible states, which represents quite a large making an attack on its table structure very difficult.
- Speed: It uses a few simple loops and swapping of bytes making it extremely fast.
- Simplicity
- Efficient implementations in both software and hardware
- Very easy to develop.

4.1.5. RC4's Weakness:

- Short key length means that the pseudorandom generator will repeat, which permits passive monitoring to gather data that can be statistically analyzed.
- Weak keys
- The most important weakness of RC4 comes from the insufficient key schedule; the first bytes of output reveal information about the key. This can be corrected by simply discarding some initial portion of the output stream.
- This is known as RC4-dropN, where N is multiple of 256, such as 768 or 1024.

4.2. Rivest Cipher5 (RC5)

RC5 is a symmetric block cipher algorithm published in the year 1994 [7, 8]. This algorithm is designed to be suitable for both hardware and software. This algorithm provides block size of RC5 is variable and can be 32, 64, or 128 bits. The key size is also variable and can be between 0 and 2048 bits. Although 12 rounds is the standard number for 64 bit RC5, the number of rounds is also variable and can be between 1 and 255. It is a parameterised algorithm and particularly the RC5 algorithm is designated as RC5-w/r/b and the detail of the parameter are shown in the table 2.

Table 2
RC5 Parameters

Parameter	Definition	Allowable Values
w	Word Size in bit, RC5 encrypt 2-word blocks	16, 32, 64 , 128
r	Number of rounds	0,1,.....255
b	Number of bytes in the secret key K	0, ... 255

RC5 algorithm consists of three components, namely, (1) *Key Expansion*, (2) *Encryption Algorithm*, and (3) *Decryption Algorithm*. This algorithm uses the three primitive operations shown in table 3.

Table 3.
RC5 Primitive Operations

S. No	Primitive Operations	Details
1.	Addition	Two's complement addition of words, denoted by "+". This is modulo-2w addition. The inverse operation subtraction of words denoted by "-".
2.	Bit-wise exclusive-OR	Bit-wise exclusive-OR of words
3.	Left Circular Rotation	A left-rotation (or "left-spin") of words: the rotation of word x left by y bits is denoted x <<< y. The inverse is the right circular rotation of word x by y bits is denoted by x>>>y.

4.2.1. Key Expansion

The key expansion routine expands the user's secret key K to fill the expanded key array S. The key expansion algorithm uses two magic constants. The key expansion algorithm performs a complex set of operations on the secret key to produce the total subkeys represented as t. Each subkey is one word in length. Two subkeys are used in each round and two subkeys are used on an additional operation that is not part of any round, *so t=2r+2*.

Techniques used to generate Subkeys

- The subkeys are stored in a t word array labelled S[0],S[1],…,S[t+1].
- The parameters r and w as inputs.
- Then the b byte key, K[0,…,b-1] is converted into a c-word array L[0,…,c-1].
- On a little-endian machine , this is accomplished by zeroing out the array L and copying the string K directly into the memory positions represented by L.
- If b is not an integer multiple of w, then a portion of L at the right end remains zero.
- Finally a mixing operation is performed that applies the contents of L to the initialized value of S to produce a final value fro the array S.

4.2.2. Encryption Algorithm

In the encryption algorithm, RC5 input block consist of two w-bit registers A and B and the output is also placed in the same register. The variables LE_i and RE_i refer the left and right half of the data after round i has completed. The algorithm is follows:

```
$LE_0$ = A+S[0];
$RE_0$ = B+S[1];
for i= 1 to r do
        $LE_i$=(($LE_{i-1}$ XOR $RE_{i-1}$)<<<$RE_{i-1}$)+S[2*i];
        $RE_i$=(($RE_{i-1}$ XOR $LE_i$)<<<$LE_i$)+S[2*i+1];
```

The cipher text result contains the two variables LEr and REr each of the r rounds consists of a substitution using both words of data. A permutation is computed using both words of data and a substitution that depends on the key. One round of RC5 is equivalent to two rounds of DES.

4.2.3. Decryption Algorithm

The decryption routine can easily derive from the encryption routine of RC5.The encryption algorithm a 2w bits of cipher text as output. Those bits are initially assigned to the two one-word variables LD_r and RD_r. The variables LD_i and RD_i refer to the left and right half of the data before round i has begun, where the rounds are numbered from r down to 1.

```
for  i = r down to 1 do
    RDi-1=((RDi-S[2*i+1]>>>LDi)XORLDi);
    LDi-1=((LDi-S[2*i]>>>RDi) XOR RDi-);
                B = RD0-S[1];
                A = LD0-S[0];
```

4.3. Rivest Cipher6 (RC6)

RC6 is a symmetric key block cipher derived from RC5. It was designed in the year 1998 by Ron Rivest in collaboration with his associates from RSA Laboratories [9,10]. RC6 includes many new features, which are not available in RC5. RC6 algorithm has a modified Feistel structure and presented symbolically as RC6-w/r/b and the derails of w/r/b are given in table4.

Table 4
RC6 Parameters

Parameter	Definition
w	represent 32 bits as the size of word
r	It denotes number of round for encryption. If the size of block is 128 bits, then r, the number, is 20
b	16, 24 and 32 byte key

4.3.1 Structure of the RC6 Algorithm

RC6 algorithm contains four components they are (1) Basic Operation, (2) Key Schedule, (3) Encryption and (4) Decryption

Basic Operation

For all variants, RC6- w/r/b operates on units of four w-bit words using the following six basic operations. The base-two logarithm of *w* will be denoted by *lg w.*

- a + b integer addition modulo 2w
- a - b integer subtraction modulo 2w
- a Åb bitwise exclusive-or of w-bit words
- a X b integer multiplication modulo 2w
- a<<<b rotate the w-bit word a to the left by the amount given by the least significant *lg w* bits of *b*
- a>>>b rotate the w-bit word a to the right by the amount given by the least significant *lg w* bits of *b*

Key Schedule

The key schedule of RC6-w/r/b is similar to the key schedule of RC5-w/r/b. The user supplies a key of b bytes. From this key, 2r + 4 words (w bits each) are derived and stored in the array S [0, 2r + 3]. This array is used in both encryption and decryption

Encryption

The encryption process in RC6 is relatively simple. RC6 consist of four w-bit registers (A, B, C, D) which is used to store the initial input plain text and the final output cipher text is also stored in the same register. The first byte of plaintext or cipher text is placed in the least significant byte of A; the last byte of plaintext or cipher text is placed into the most significant byte of D. The pseudo-code for the encryption is given below.

```
Input       :   Plain text stored in four w-bit input
                 registers A, B, C, D
                Number of r rounds
                w-bit round keys S[0,…,2r + 3]
Output      :   Cipher Text stored in A, B, C, D
Procedure   :   B = B + S[0];
                D = D + S[1];
                for i = 1 to r do
                 {
                     t = (B (2B + 1)) ⋘ log w;
                     u = (D (2D + 1)) ⋘ log w;
                     A = ((A ⊕ t) ⋘ u) + S[2i];
                     C = ((C ⊕ u) ⋘ t) + S[2i+1];
                     (A, B, C, D) = (B, C, D, A);
                A = A + S[2r+2];
                C = C + S[2r+3];
```

Decryption

Decryption operation performs in a similar way as encryption. The main difference is that the *cipher text* is given as input and produce output as *plain text*. The pseudo-code for the decryption is shown below.

```
C = C + S[2r+3];
A = A + S[2r+2];
for i = r downto 1 do
 {
      (A, B, C, D) = (D, A, B, C);
       u = (D (2D + 1)) ⋘ log w;
       t = (B (2B + 1)) ⋘ log w;
       C = ((C - S[2i+1]) ⋙ t) ⊕ u;
       A = ((A - S[2i]) ⋙ u) ⊕ t;
 }
D = D - S[1];
B = B - S[0];
```

Table 5.
Comparisons of RC4, RC5 And RC6 Algorithm

Algorithm	RC4	RC5	RC6
Symmetric Cipher Type	Stream Cipher	Block Cipher	Block Cipher
Block Size	-------	32, 64 or 128 bits (64 suggested)	
Rounds	256	1-255 (12 suggested originally)	20
Key Size	40–2,048 bits	0 to 2040 bits (128 suggested)	128, 192, or 256 bits
Designer	Ron Rivest	Ron Rivest	Ron Rivest, Matt Robshaw, Ray Sidney, Yiqun Lisa
Published Year	1994	1994	1998

5. Conclusion

Cryptography is a science of secret writing. This technique is to achieve these various algorithms are developed by various people. This paper presents a detailed study of Symmetric Key Algorithms RC4, RC5 and RC6 developed by Ron's and other associates. In this study the three algorithms are analysed separately by the block size, key size, encryption and decryption process and the comparative analysis is also performed.

6. References

[1] William Stallings, "Cryptography and Network Security" 4th Ed, Prentice Hall, 2005, PP. 58-309.

[2] Surya, C.Diviya, "A Survey on Symmetric Key Encryption Algorithms", International Journal of Computer Science & Communication Networks, Volume 2, Number 4, 2012, pp. 475-477.

[3] Gurpreet Kaur, Manish Mahajan, "Evaluation and Comparison of Symmetric Key Algorithms", International Journal of Science, Engineering and Technology Research, 2013, pp.1960-1962.

[4] Kamini H. Solanki, Chandni R. Patel, "New Symmetric Key Cryptographic algorithm for Enhancing Security of Data", International Journal of Research in Computer Engineering and Electronics, Volume 1, Issue 3, 2012, pp. 1-5.

[5] Ed Dawson, Helen Gustafson, Matt Henricksen, Bill Millan, "Evaluation of RC4 Stream Cipher", Information Security Research Centre Queensland University of Technology, 2002

[6] Nidhi Singhal, J.P.S.Raina, Comparative Analysis of AES and RC4 Algorithms for Better Utilization, International Journal of Computer Trends and Technology, July to Aug Issue, 2011, pp. 177-181

[7] Harsh Kumar Verma, Ravindra Kumar Singh,Performance Analysis of RC5, Blowfish and DES Block Cipher Algorithms, International Journal of Computer Applications, Volume 42, Number 16, 2012, pp. 8-14.

[8] Jay Singh, Brajesh Kumar, Asha Khatri, Securing Storage Data in Cloud Using RC5 Algorithm, International Journal of Advanced Computer Research, Volume 2, Issue 6,2012, pp. 94-98.

[9] Ashwaq T. Hashim, Janan A. Mahdi and Salma H. Abdullah, "A Proposed 512 bits RC6 Encryption Algorithm", , Volume 10, Number.1, 2010, pp. 11-25.

[10] Kirti Aggarwal,Jaspal Kaur Saini, Harsh K. Verma, Performance Evaluation of RC6, Blowfish, DES, IDEA,CAST-128 Block Ciphers, International Journal of Computer Applications, Volume 68, Number 25, 2013, pp. 10-16.