http://ejournal.seaninstitute.or.id/index.php/InfoSains
Jurnal Info Sains : Informatikan dan Sains, Volume 11, No 01 Maret 2021
E-ISSN.2797-7889, P-ISSN.2089-3329

Analysis And Implementation of Noekeon Algorithms For Encryption and Description of Text Data

[1]Noverta Efendi, [2]Fauzan Azim
[1,2]Electronic Engineering Vocational Education, Faculty of Teacher Training and Education, Universitas Muhammadiyah Riau, Jalan Tuanku Tambusai, Kota Pekanbaru, Provinsi Riau.
Email : noverta04@gmail.com[1], fauzanazim@gmail.com[2]

Keywords

Application Design
Encryption-decryption
text file encryption
Noekeon algorithm.

Abstract. As the times evolve, human needs increase. Including information needs. Therefore, sending and storing files through electronic media requires a process that can ensure the security and integrity of the file. To ensure the safety and integrity of a file, an encoding process is required. Encryption is performed when the file is sent. This process will convert the original file into a confidential unreadable file. Meanwhile, the decryption process is done by the recipient of the sent file. The personal file received will be converted back to the original file. By encoding, the original file will not be read by unauthorized parties but only by recipients who have a decryption key.

1. INTRODUCTION

Currently, one of the ways used for file security is to use a cryptographic system that is to encode the contents of the information (plaintext) into content that is not understood through the encryption process (chipper) and to regain the original data, the decryption process (decipher)—accompanied by using the correct key[1]. But with the development of the science of encoding or cryptography, efforts to obtain the key can be made by anyone, including those who are not authorized to have such information. Therefore, researchers on cryptography will constantly evolve to get increasingly powerful cryptographic algorithms, making efforts to break down cryptographic codes unlawfully become more complex[2].

Information communication today has expanded widely. Information communication in exchanging messages and transactions until the exchange of confidential information has used computer technology and a vast and complex global network. The breadth of information communication utilizing computer technology and global networks today led to the emergence of parties who want to steal such information[3]. The vast and complex global network makes it almost impossible to protect messages right to their destination. The threat of information theft has led many researchers to develop techniques or methods to provide security to the content of information in notes, one of which is data encoding techniques or cryptography[4].

Cryptography is the science and art of maintaining the confidentiality of messages by encoding them into a form that is no longer understood. The purpose of cryptography is to provide security in the form of / privacy, data integrity, authentication, non-repudiation[5]. In the field of cryptography, there are two main processes, encryption, and decryption[6]. Encryption is the process of encoding plaintext or messages into ciphertext. Decryption is the process of returning the ciphertext to its original plaintext[7].

2. METHOD

The early stage is the determination of the use of materials related to the research conducted. At this stage will be done identifying the problem and selecting algorithms and methods to solve it. Issues are found by following current technology issues and developments and studying research that has been done and published through scientific journals. The problem to be researched is how to secure data. To avoid theft or leakage of data on cloud storage, the encryption system is implemented with noekeonalgorithm. Stages with the following flow:

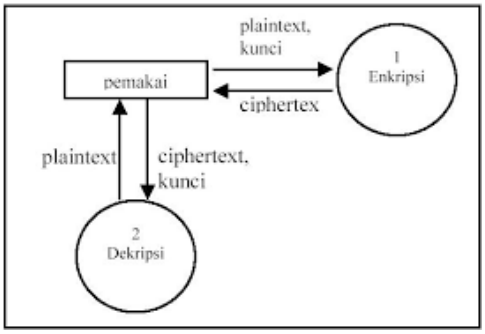

Figure 1. Noekeon Algorithm Work Process

2.1. Noekeon

Noekeon is a repeating code block with a block length and a key length of 128 bits each, consisting of a simple repeating spin transformation application, followed by an output transformation. Noekeon has 16 rounds (Nr) of iterations[8]. Each game is carried out three modifications, namely theta, offset shift consisting of two changes Pil1 and Pil2, and gamma[9].

Critical scheduling is done by converting a 128-bit primary key (code-key) into a working key. In Noekeon, there is a mode in which key scheduling is not performed, called direct-key mode, which serves the key scheduling process to eliminate related-key attack patterns[10].

3. RESULT AND DISCUSSION

The encryption and decryption process of Noekeon's algorithm uses the key generation or scheduling process used in each round of encryption and decryption. The key stages of the neocon algorithm are as follows:

1. Input the user key.
2. They are padding the user key if the key length is less than 16 characters.
3. Form A0-A3 blocks of 32 bits or four characters each.
4. Performing a key scheduling round of 16 rounds (i), the operations on each game are as follows:
1. Perform xor A0 operations with RC(i).
2. Perform inverse theta operations against A0-A3.
3. Perform rotate_left operations A1 << 1
4. Perform operations rotate_left A2 << 5
5. Perform operations rotate_left A3 << 2
6. Perform gamma operations against A0-A3.
7. Perform rotate_right operation A1 >> 1
8. Perform rotate_right operation A2 >> 5
9. Perform operations rotate_right A3 >> 2
10. After the next round of operations, perform xor operations A0 and RC(16). 11. A0 – A3 will be the DK(0)-DK(3) decryption key.
12. Perform inverse theta operations against A0-A3.
13. A0-A3 will be the key to EK(0)-EK(3).

Table 1. RC Constants

i	Formula	RC(i)
0	-	0x80
1	RC[0] And 0x80 != 0 ? If True Rc[1] = Rc[0] << 1 Xor 0x1B If False RC[1]= Rc[0] << 1	0x1a
2	RC[1] And 0x80 != 0 ? If True Rc[2] = Rc[1] << 1 Xor 0x1B If False RC[2]= Rc[1] << 1	0x34
3	RC[2] And 0x80 != 0 ? If True Rc[3] = Rc[2] << 1 Xor 0x1B If False RC[3]= Rc[2] << 1	0x68

4	RC[3] And 0x80 != 0 ? If True Rc[4] = Rc[3] << 1 Xor 0x1B If False RC[4]= Rc[3] << 1	0xd0
5	RC[4] And 0x80 != 0 ? If True Rc[5] = Rc[4] << 1 Xor 0x1B If False RC[5]= Rc[4] << 1	0xba
6	RC[5] And 0x80 != 0 ? If True Rc[6] = Rc[5] << 1 Xor 0x1B If False RC[6]= Rc[5] << 1	0x6e
7	RC[6] And 0x80 != 0 ? If True Rc[7] = Rc[6] << 1 Xor 0x1B If False RC[7]= Rc[6] << 1	0xdc
8	RC[7] And 0x80 != 0 ? If True Rc[8] = Rc[7] << 1 Xor 0x1B If False RC[8]= Rc[7] << 1	0xa2
9	RC[8] And 0x80 != 0 ? If True Rc[9] = Rc[8] << 1 Xor 0x1B If False RC[9]= Rc[8] << 1	0x5e
10	RC[9] And 0x80 != 0 ? If True Rc[10] = Rc[9] << 1 Xor 0x1B If False RC[10]= Rc[9] <<1	0xbc
11	RC[10] And 0x80 != 0 ? If True Rc[11] = Rc[10] << 1 Xor 0x1B If False RC[11]= Rc[10] << 1	0x62
12	RC[11] And 0x80 != 0 ? If True Rc[12] = Rc[11] << 1 Xor 0x1B If False RC[12]= Rc[11] << 1	0xc4
13	RC[12] And 0x80 != 0 ? If True Rc[13] = Rc[12] << 1 Xor 0x1B If False RC[13]= Rc[12] << 1	0x92
14	RC[13] And 0x80 != 0 ? If True Rc[14] = Rc[13] << 1 Xor 0x1B If False RC[14]= Rc[13] << 1	0x3e
15	RC[14] And 0x80 != 0 ? If True Rc[15] = Rc[14] << 1 Xor 0x1B If False RC[15]= Rc[14] << 1	0x7c
16	RC[15] And 0x80 != 0 ? If True Rc[16] = Rc[15] << 1 Xor 0x1B If False RC[16]= Rc[15] << 1	0xf8

Analysis of the key scheduling process in Noekeon's algorithm can be described as follows:
Key Scheduling :
Input Key : 12345000000000000
Key(Bit) :
00110001;00110010;00110011;00110100;
00110101;00110000;00110000;00110000;
00110000;00110000;00110000;00110000;
00110000;00110000;00110000;00110000;
A0 : 00110001;00110010;00110011;00110100
= 825373492
A1 : 00110101;00110000;00110000;00110000
= 892350512
A2 : 00110000;00110000;00110000;00110000
= 808464432
A3 : 00110000;00110000;00110000;00110000
= 808464432
Round (0)Scheduling Key :
A0 = A0 Xor RC(0) = 825373620
Theta Inv Process : A0 : 825373620
A1 : 892350512
A2 : 808464432
A3 : 808464432 T = A0 Xor A2
= 16909188

A0 = A0 Xor RC(16) = 2504158901 DK(0) = A0 = 2504158901
DK(1) = A1 = 334622109 DK(2) = A2 = 3718075253 DK(3) = A3 = 205715165
Theta Inv Process :
A0 : 2504158901
A1 : 334622109
A2 : 3718075253
A3 : 205715165 T = A0 Xor A2
= 1222589888
Temp = T<<8 Xor T>>8 = 527769461 A1 = T Xor Temp Xor A1 = 1146867496 A3 = T Xor Temp Xor A3 = 1541985384 T = A1 Xor A3 = 531831616
Temp = T<<8 Xor T>>8 = 4077187844 A0 = T Xor Temp Xor A0 = 2046134001 A2 = T Xor Temp Xor A2 = 824884017
Temp = T<<8 Xor T>>8 = 2248312322 A1 = T Xor Temp Xor A1 = 2989536694 A3 = T Xor Temp Xor A3 = 3073422774 T = A1 Xor A3 = 83886080
Temp = T<<8 Xor T>>8 = 327685
A0 = T Xor Temp Xor A0 = 876032945 A2 = T Xor Temp Xor A2 = 892678197 A1 = A1 << 1 = 1684106093
A2 = A2 << 5 = 2795898534 A3 = A3 << 2 = 3703756506
Gamma Process :
A0 : 876032945
A1 : 1684106093
A2 : 2795898534
A3 : 3703756506
A1 = A1 Xor ((Not A3) And (Not A2)) = 1702380140
A0 = A0 Xor (A2 And A1) = 269955477 A0 = A3 = 3703756506
A3 = A0 = 269955477
A2 = A2 Xor A3 Xor A1 Xor A0 = 252420997
A1 = A1 Xor (Not A3 And Not A2) = 2241334790
A0 = A0 Xor (A2 And A1) = 3653948638 A1 = A1 >> 1 = 1120667395
A2 = A2 >> 5 = 678976796 A3 = A3 >> 2 = 1141230693
I(0) = A0 = 2046134001 I(1) = A1 = 1146867496
I(2) = A2 = 824884017 I(3) = A3 = 1541985384
Based on the analysis of key scheduling that has been done, the key is obtained for the encryption and decryption process as follows:
Input key : 12345 Encryption key :
I(0) = A0 = 2046134001 I(1) = A1 = 1146867496
I(2) = A2 = 824884017 I(3) = A3 = 1541985384
Decryption key :
DK(0) = A0 = 2504158901 DK(1) = A1 = 334622109 DK(2) = A2 = 3718075253 DK(3) = A3 = 205715165

3.1 Encryption Process Analysis

Encryption analysis in Noekeon's algorithm uses input blocks of 32 bits in length. Here is the description of the operation of the encryption process in Noekeon's algorithm:

1. Input Plaintext from the user.
2. They are padding the plaintext if the mod length of 16 is not equal to 0.
3. Form A0-A3 input blocks that are 32 bits or four characters long, respectively.

4. Perform an encryption loop of 16 rounds(i) which can be described as follows.
1. Perform xor A0 operations with RC(i).
2. Perform theta operations against A0-A3 using K(0)-K(3).
3. Perform rotate_left operations A1 << 1
4. Perform operations rotate_left A2 << 5
5. Perform operations rotate_left A3 << 2
6. Perform gamma operations against A0-A3.
7. Perform rotate_right operation A1 >> 1
8. Perform rotate_right operation A2 >> 5
9. Perform operations rotate_right A3 >> 2
10. After the next round of operations, perform xor operations A0 and RC(16).
11. Perform theta operations against A0-A3 using K(0)-K(3).
12. Break down blocks A0-A3 into bytes of ciphertext characters.

Analysis of the encryption process in Noekeon's algorithm can be described as follows.

Plaintext : "zizi encryption 12" Input Block Formation :
Input Block (0) : 01100101;01101110;01101011;01110010
Input Block (1) : 01101001;01110000;01110011;01101001
Input Block (2) : 00100000;01111010;01101001;01111010
Input Block (3) : 01101001;00100000;00110001;00110010
End (4) BLok encryption:

A0 : 1701735282
A1 : 1768977257
A2 : 544893306
A3 : 1763717426
Round (0) Encryption :
A0 = A0 Xor RC(0) = 1701735410
Theta Process : A0 : 1701735410
A1 : 1768977257
A2 : 544893306
A3 : 1763717426

K(0) : 2046134001
K(1) : 1146867496
K(2) : 824884017
K(3) : 1541985384
T = A0 Xor A2
= 1158939272
Temp = T<<8 Xor T>>8 = 2621938759
A1 = T Xor Temp Xor A1 = 2955144614
A3 = T Xor Temp Xor A3 = 2960371709
A0 = A0 Key Xor(0) = 479980803
A1 = A1 Key Xor(1) = 4101513870
A2 = A2 Key Xor(2) = 290509387
A3 : 2926440023
A1 = A1 Xor ((Not A3) And (Not A2)) = 3923792957
A0 = A0 Xor (A2 And A1) = 865995842
A0 = A3 = 2926440023
A3 = A0 = 865995842
A2 = A2 Xor A3 Xor A1 Xor A0 = 2864567542

Round operations are performed in 16 rounds. After the round is complete then the operation is continued as follows.

A0 = A0 Xor RC(16) = 2594189566
Theta Process :
A0 : 2594189566
A1 : 347116736
A2 : 563119268
A3 : 4101676072
K(0) : 2046134001
K(1) : 1146867496
A2 Xor Key(2) = 280641429
A3 = A3 Xor Key(3) = 2125305365 T = A1 Xor A3 = 4286124968
Temp = T<<8 Xor T>>8 = 3521958380 A0 = T Xor Temp Xor A0 = 3451941963 A2 = T Xor Temp Xor A2 = 1043332561

After the process is complete, the ciphertext can be obtained by breaking block A0-A3 into bytes of characters that can be seen as follows:

Output(0) : 205
Output(1) : 192
Output(2) : 116
Output(3) : 75
Output(4) : 129
Output(5) : 212
Output(6) : 133
Output(7) : 189
Output(8) : 62
Output(9) : 47
Output(10) : 253
Output(11) : 209
Output(12) : 126
Output(13) : 173
Output(14) : 150
Output(15) : 21

Then obtained the results of encryption as follows:

Plaintext : "Zizi encryption 12" Chiperteks : ²OsY¶a_áý_êÛ□1Š_(_[X_ä¹sr&v´'½{

3.2 Decryption Process Analysis

The decryption process in Noekeon's algorithm uses input blocks of 32 bits in length. Here is the description of the operation of the

A3 = A3 Xor Key(3) = 3952835477
T = A1 Xor A3 = 534993179
Temp = T<<8 Xor T>>8 = 4165400646
A0 = T Xor Temp Xor A0 = 4215163998
A2 = T Xor Temp Xor A2 = 4143280918
A1 = A1 << 1 = 3908060445
A2 = A2 << 5 = 3735970526
A3 = A3 << 2 = 2926440023
Gamma Process :
A0 : 4215163998
A1 : 3908060445
A2 : 3735970526
A1 = A1 Xor (Not A3 And Not A2) = 2912974644
A0 = A0 Xor (A2 And A1) = 114145891
A1 = A1 >> 1 = 1456487322
A2 = A2 >> 5 = 3042307751
A3 = A3 >> 2 = 2363982608

encryption process in Noekeon's algorithm:

1. Input ciphertext from the user.
   K(2) : 824884017
   K(3) : 1541985384 T = A0 Xor A2
   = 3140531290
   Temp = T<<8 Xor T>>8 = 1779395087 A1 = T Xor Temp Xor A1 = 3314502293 A3 = T Xor Temp Xor A3 = 625295997 A0 = A0 Key Xor(0) = 3814045199
   A1 = A1 Xor Key(1) = 2178188733
   A2 =
2. Form A0-A3 input blocks that are 32 bits or 4 characters long, respectively.
3. Decryption rounds of 16 rounds(i) are performed from rounds 16 – 1 (inverted) which can be described below.
4. Perform theta operations against A0-A3 using K(0)-K(3).

5. Perform xor A0 operations with RC(i).
6. Perform rotate_left operations A1 << 1
7. Perform operations rotate_left A2 << 5
8. Perform operations rotate_left A3 << 2
9. Perform gamma operations against A0- A3.
10. Perform rotate_right operation A1 >>
11. Perform rotate_right operation A2 >>
12. Perform operations rotate_right A3 >>
13. Perform theta operations against A0-A3 using K(0)-K(3).
14. Breaks block A0-A3 into bytes of ciphertext characters.

Analysis of the decryption process in Noekeon's algorithm can be described as follows:chipertext: ²OsY¶a_áý_êÛ1Š_(_[X_ä¹sr&v´'1/2{ Input
Block Formation :
Input Block (0) : 11001101;11000000;01110100;01001011
Input Block (1) : 10000001;11010100;10000101;10111101
Input Block (2) : 00111110;00101111;11111101;11010001
Input Block (3) : 01111110;10101101;10010110;00010101
End (4) BLok
A0 : 3451941963
A1 : 2178188733
A2 : 1043332561
A3 : 2125305365
Round (0) Decryption :
Theta Process :
A0 : 3451941963
A1 : 2178188733
A2 : 1043332561
A3 : 2125305365
K(0) : 2504158901
K(1) : 334622109
K(2) : 3718075253
K(3) : 205715165 T = A0 Xor A2 = 4092561818
Temp = T<<8 Xor T>>8 = 1970959738 A1 = T Xor Temp Xor A1 = 121731421 A3 = T Xor Temp Xor A3 = 4164446965 A0 = A0 Key Xor(0) = 1484921598
A1 = A1 Xor Key(1) = 347116736 A2 = A2 Key Xor(2) = 3820138148 A3 = A3 Xor Key(3) = 4101676072 T = A1 Xor A3 = 3771336936
Temp = T<<8 Xor T>>8 = 585638632
A0 = T Xor Temp Xor A0 = 2594189566 A2 = T Xor Temp Xor A2 = 563119268 A0 = A0 Xor RC(0) = 2594189318

A1 = A1 << 1 = 694233472 A2 = A2 << 5 = 839947396 A3 = A3 << 2 = 3521802403
Gamma Process :
A0 : 2594189318
A1 : 694233472
A2 : 839947396
A3 : 3521802403
A1 = A1 Xor ((Not A3) And (Not A2)) = 627319512
A0 = A0 Xor (A2 And A1) = 3131060358 A0 = A3 = 3521802403
A3 = A0 = 3131060358
A2 = A2 Xor A3 Xor A1 Xor A0 = 2084501113
A1 = A1 Xor (Not A3 And Not A2) = 606415832

A0 = A0 Xor (A2 And A1) = 4123939579
A1 = A1 >> 1 = 303207916 A2 = A2 >> 5 = 3420583859 A3 = A3 >> 2 = 2930248737

Round operations are performed in 16 rounds. After the round is complete then the operation is continued as follows.
Theta Process :
A0 : 4215163998
A1 : 4101513870
A2 : 4143280918
A3 : 3952835477
K(0) : 2504158901
K(1) : 334622109
K(2) : 3718075253
K(3) : 205715165 T = A0 Xor A2 = 231423816
Temp = T<<8 Xor T>>8 = 2201125682 A1 = T Xor Temp Xor A1 = 2055315188 A3 = T Xor Temp Xor A3 = 1700972527 A0 = A0 Xor Kunci(0) = 1853629163 A1 = A1 Xor Kunci(1) = 1768977257 A2 = A2 Xor Kunci(2) = 728244323 A3 = A3 Xor Kunci(3) = 1763717426 T = A1 Xor A3 = 5259867
Temp = T<<8 Xor T>>8 = 188877634 A0 = T Xor Temp Xor A0 = 1701735410 A2 = T Xor Temp Xor A2 = 544893306 A0 = A0 Xor RC(0) = 1701735282

After the process is complete, the plaintext can be obtained by splitting block A0-A3 into byte characters that can be seen as follows:

Output(0) : 101
Output(1) : 110
Output(2) : 107
Output(3) : 114
Output(4) : 105
Output(5) : 112
Output(6) : 115
Output(7) : 105
Output(8) : 32
Output(9) : 122
Output(10) : 105
Output(11) : 122
Output(12) : 105
Output(13) : 32
Output(14) : 49
Output(15) : 50

Then obtained the results of decryption as follows:

Plaintext : "zizi encryption 12"

4. CONCLUSION

With the completion of this research which includes the process of encryption and decryption of messages using the Noekeon algorithm, it can be concluded that Noekeon's algorithm can be applied in encryption and decryption of text messages by dividing the characters contained in the text into blocks - Noekeon blocks so that it can be processed into noekeon rotation operations into ciphertext or plaintext. The process of designing and developing a text message encoding application using Noekeon's algorithm begins with analyzing Noekeon's algorithm both in the process and its provisions. The Next Stage is to create a neocon interface and process modules consisting of key initialization, key generation, encryption, and decryption.

REFERENCES

[1] N. M. D. Oktafiansyah, F. Agus, and S. Maharani, "Penerapan Kriptografi Dengan Algoritma Data Encryption Standart Pada Text Hasil Konversi Dari Citra," *Semin. Nas. Ilmu Komput. dan Teknol. Inf.*, vol. 1, no. 1, pp. 85–89, 2016.

[2] Y. Wiharto and A. Irawan, "Enkripsi Data Menggunakan Advanced Encryption Standart 256," *Kilat*, vol. 7, no. 2, pp. 91–99, 2018, doi: 10.33322/kilat.v7i2.352.

[3] S. Wardoyo and R. Fahrizal, "Aplikasi Teknik Enkripsi Dan Dekripsi File Dengan Algoritma Blowfish Pada Perangkat Mobile Berbasis Android," *Setrum Sist. Kendali-Tenaga-elektronika-telekomunikasi-komputer*, vol. 3, no. 1, p. 43, 2016, doi: 10.36055/setrum.v3i1.497.

[4] A. Saputra and A. Widyanto, "Enkripsi Dan Dekripsi File Dengan Algoritma Blowfish," *J. Sist. Inf. Dan Teknol. Inf.*, vol. 4, no. 1, pp. 22–30, 2015.

[5] M. I. Assegaf, R. Destias, N. Sitaresmi, and Y. Wiharto, "Implementasi Enkripsi-Dekripsi dengan Algoritma RC2 Menggunakan Java," *J. Media Inform. Budidarma*, vol. 4, pp. 898–903, 2020, doi: 10.30865/mib.v4i4.2256.

[6] E. L. Hakim, Khairil, and F. H. Utami, "Aplikasi Enkripsi Dan Deskripsi Data Menggunakan Algoritma Rc4 Dengan Menggunakan Bahasa Pemrograman Php," *J. Media Infotama*, vol. 10, no. 1, pp. 1–7, 2014.

[7] D. Adhar, "Implementasi Algoritma Des (Data Encryption Standard) Pada Enkripsi Dan Deskripsi Sms Berbasis Android," *J. Tek. Inform. Kaputama*, vol. 3, no. 2, pp. 53–60, 2019, [Online]. Available: https://jurnal.kaputama.ac.id/index.php/JTIK/article/view/185.

[8] A. H. Lubis, "ENKRIPSI DATA DENGAN ALGORITMA KRIPTROGRAFI NOEKEON," *CESS(JournalOfComputerEngineering,System AndScience)*, vol. 2, no. 1, pp. 97–101, 2017.

[9] C. Kurniawan, "Algoritma Kriptografi Noekon," [Online]. Available: http://ilmusisteminfo.com/upload/file_pdf/Kriptografi dan Algoritma 1567687693.pdf.

[10] I. Utomo, W. Mulyono, W. S. Sari, D. R. Ignatius, M. Setiadi, and C. A. Sari, "M ODIFIKASI E NKRIPSI G AMBAR M ENGGUNAKAN 64- BIT K UNCI P ADA A LGORITMA D ATA E NCRYPTION S TANDARD (DES)," *Din. Rekayasa*, vol. 12, no. 2, 2018.