Impact Factor Value: 4.029 ISSN: 2349-7084
International Journal of Computer Engineering In Research Trends
Volume 4, Issue 12, December - 2017, pp. 547-551 www.ijcert.org

NHSKCA: A NEW HEURISTIC FOR SYMMETRIC KEY CRYPTOGRAPHIC ALGORITHM

Ira Nath*[1], Deepashree Bhattacharyya[2], Agnisuddha Mandal[3], Nandini Kundu[4], Oindrila De[5]
JIS College of Engineering, Kalyani, Nadia, West Bengal, 741235[1,2,3,4]

Ira.nath@gmail.com[1], alisharia.17@gmail.com[2], mandalagnisuddha@gmail.com[3], nandinikundu24@gmail.com[4], oindrilade26@gmail.com[5]

Abstract: - A plain text or clear text is basically any communicating language that human being speaks. A message or plain text can be understood by anybody who knows the language and as long as the message is not codified in any manner. So now we have to use coding scheme to ensure the information is hidden from anyone for whom it is not intended even those who can see the coded data. Cryptography is a method of storing and transmitting data in a particular form so that only those for whom it is intended can read and process it. Cryptography is the practice and study of hiding information. In modern times cryptography is considered as a branch of both mathematics and computer science and is affiliated closely with information theory, computer science and engineering. There are two basic types of cryptography-Symmetric key and asymmetric key cryptography. There are few well known symmetric key algorithms i.e, DES, RSA, MD5, etc. This paper describes cryptography, various symmetric key algorithms in detail and then proposes a new symmetric key algorithm. Algorithms for both encryption and decryption are also provided here. The advantages of this new algorithm are also explained properly.

Keyword: Cryptography, Symmetric Key, Plain Text, Security, Asymmetric Key.

---

1. Introduction

21st century can be promptly marked as the era of information. A lot of data are stored in the form of electronic messages. The transmission of this information or the data which can be in any form, be it, text, audio, video etc., is often through electronic medium such as mobile phone communication, electronic commerce, the on-line chat service etc. Now, as the saying goes 'there are two sides of the same coin'[1], similarly advanced technology calls upon a number of disadvantages along with its advantages. The information or the data that we want to deliver may possibly be stolen or monitored. If we have no appropriate protection measure against it, the important messages can leak out leading to inconceivable results.

To the rescue among many measures, comes up one of the remarkable, significant and vital measure which is cryptography that involves encryption and decryption. Ever since the earliest days of writing, people have had reasons to limit their information to a restricted group of people. Because of this, these people have had to develop ideas of making their information unable to be read by unwanted people. The general techniques used to hide the meaning of messages constitute the study known as cryptography. The word *cryptography* comes from the Greek words *kryptos* meaning hidden and *graphein* meaning writing. Cryptography is the study of hidden writing, or the science of encrypting and decrypting text [2].

Advances in cryptography appeared with unprecedented frequency in the 1970's as strong encryption-based protocols and hence new cryptographic applications emerged. On January 15th, 1977, the National Bureau of Standards adopted an encryption algorithm as a federal standard, the Data Encryption Standard (DES), marking a milestone in cryptographic research and development. In December 1980, the American National Standards institute adopted the same algorithm for commercial use in the United States [3].

Cryptography has not been used solely for diplomacy and warfare. It has also played a major role in the economy. The banking and finance industry has

been the leader in promoting the use of cryptography for protecting assets transferred via messages sent through large networks of computers and terminals. The major processes which constitute the cryptography are The Encryption, The Decryption, and the key generation. There are two types of encryption system-(1) Symmetrical Encryption System and (2) Asymmetrical Encryption System.

Today the cryptology is not just limited to data encryption and decryption as mentioned above, it has a wide range of usages. The field of cryptology is an emerging field in which continuous expansions and modifications are taking place. Cryptography is the study of mathematical techniques, algorithms and protocols that can provide four basic services for information security, namely privacy, authentication, data integrity and non-repudiation.

In this paper, in section 2 previous works are depicted. The proposed algorithm has been illustrated in section 3. The illustrative example has been depicted in section 4. In conclusion is shown in section 5.

2. Previous Works

2.1 MD5 Algorithm

The MD5 was designed by well-known cryptographer Ronald Rivest in 1991 [5]. The MD5 function is a cryptographic algorithm that takes an input of arbitrary length and produces a message digest that is 128 bits long. The digest is sometimes also called the "hash" or "fingerprint" of the input. The MD5 is used in many situations where a potentially long message needs to be processed and compared quickly. The most common application is the creation and verification of digital signatures.

2.2 RSA Algorithm

RSA algorithm is asymmetric cryptography algorithm. Asymmetric actually means that it works on two different keys i.e. Public Key and Private Key. As the name describes that the Public Key is given to everyone and Private Key is kept private.
An example of asymmetric cryptography:

1. A client (for example browser) sends its public key to the server and requests for some data.
2. The server encrypts the data using client's public key and sends the encrypted data.
3. Client receives this data and decrypts it.

Since this is asymmetric, nobody else except browser can decrypt the data even if a third party has public key of browser.

The idea of RSA is based on the fact that it is difficult to factorize a large integer. The public key consists of two numbers where one number is multiplication of two large prime numbers. And private key is also derived from the same two prime numbers. So, if somebody can factorize the large number, the private key is compromised. Therefore, encryption strength totally lies on the key size and if we double or triple the key size, the strength of encryption increases exponentially. RSA keys can be typically 1024 or 2048 bits long, but experts believe that 1024-bit keys could be broken in the near future. But till now it seems to be an infeasible task [6].

2.3 DES Algorithm

The Data Encryption Standard is a block cipher, meaning a cryptographic key and algorithm are applied to a block of data simultaneously rather than one bit at a time. To encrypt a plaintext message, DES groups it into 64-bit.

DES is the archetypal block cipher—an algorithm that takes a fixed-length string of plaintext bits and transforms it through a series of complicated operations into another cipher text bit string of the same length. In the case of DES, the block size is 64 bits. DES also uses a key to customize the transformation, so that decryption can supposedly only be performed by those who know the particular key used to encrypt. The key ostensibly consists of 64 bits; however, only 56 of these are actually used by the algorithm. Eight bits are used solely for checking parity, and are thereafter discarded. Hence the effective key length is 56 bits.

The key is nominally stored or transmitted as 8 bytes, each with odd parity.

One bit in each 8-bit byte of the *KEY* may be utilized for error detection in key generation, distribution, and storage. Bits 8, 16..., 64 are for use in ensuring that each byte is of odd parity.

Like other block ciphers, DES by itself is not a secure means of encryption but must instead be used in a mode of operation.

Decryption uses the same structure as encryption but with the keys used in reverse order. (This has the advantage that the same hardware or software can be used in both directions) [7].

3. Proposed Algorithm

3.1 AIDON Algorithm

The proposed algorithm named AIDON is a symmetric key cryptographic algorithm. It incorporates all the advantages of the DES, RSA and MD5 algorithms. It is primarily developed for privacy and confidentiality. It employs a single key for both encryption and decryption.

3.1.1 Key Generation Algorithm for AIDON

STEP 1: We take four prime numbers as input for key generation: 3, 7, 11 and 19.

STEP 2: We pair the four numbers this way: 3, 7 and 11, 19.

STEP 3: We multiply both 3*7 and 11*19 and obtain the products 21 and 209 respectively.

STEP 4: We perform addition of the two products and obtain the result: 230.

STEP 5: We convert this output (230) into its equivalent 8-bit binary number and we get 11100110.

STEP 6: We divide this binary number into two equal halves (4-bits each). Now we have 1110 and 0110.

STEP 7: 1110 is taken to the left and marked L and 0110 is taken to the right and marked R.

STEP 8: R is XORed with 1111 and we get 1001 as the output.

STEP 9: This output is taken to the left and again XORed with L. We get 0111 as the output.

STEP 10: Next, we swap the positions of the above outputs. To the left, we take 1001 and mark it as L' and to the right, we take 0111 and mark it as R'.

STEP 11: We concatenate both L' (1001) and R' (0111) and get a binary number 10010111 as the result.

STEP 12: Lastly, the above output (10010111) undergoes NOT operation and the desired result is referred as the KEY. The generated key is 01101000.

3.1.2 Encryption Algorithm for Heuristic AIDON

STEP 1: Take a number as input.

STEP 2: Generate the corresponding binary value of it.

[Binary value should be 8 digits e.g. for decimal 32 binary number should be 00100000]

STEP 3: Divide it into 4 bits each and consider one part as left and another part as right.

STEP 4: From key generation algorithmwe have got thekey.

STEP 5: XOR the right part with key.

STEP 6: XOR this output with the left part.

STEP 7: Take 1's complement of this output.

STEP 8: Swap it to the right and main right to the left.

STEP 9: XOR the right part with the key.

STEP 10: Take 1's complement.

STEP 11: Take 1's complement of left.

STEP 12: XOR the right part with left.

STEP 13: Swap it to the right and main right to the left.

STEP 14: Take reverse of left and right.

STEP 15: Take XOR of both and this would be the cipher text i.e. encrypted text.

3.1.3 Decryption algorithm for Heuristic AIDON

STEP 1: We have got the cipher text.

STEP 2: We find out every possibility of XOR and take two possibilities that return the cipher-text when XORed.

STEP 3: Let us consider the first number (n1) as left part and the second number (n2) as the right.

STEP 4: We take the reverse of both these numbers n1 and n2 and mark them as n1' and n2' respectively.

STEP 5: We take n1' and perform XOR operation with the key.

STEP 6: Then we perform 1's complement on this output and the final result is marked as n1''.

STEP 7: n1'' is then swapped to the left and XORed with n2' and the output is marked as n3.

STEP 8: Then we perform 1'a complement on n3 and the number we get is marked as ny (the second half of the plaintext) (we get it as 8 bits and consider the last 4 bit).

STEP 9: ny is XORed with the key and the output is taken to the left and the output is marked as ny'.

STEP 10: N1' undergoes 1's complement and is XORed with ny'.

STEP 11: This output is marked as nx (the first half of the plaintext) (we take the last 4 bits of the 8 bits no).

STEP 12: These two outputs obtained are then concatenated and we get the final output i.e. plain text.

4. Illustrative Example

4.1 Encryption Algorithm for Heuristic AIDON

Let the input is 200. Now according to the steps, we will get the following:

STEP 1: Corresponding binary value of 200 is 11001000.

STEP 2: On dividing it becomes 1100(left) and 1000 (right).

STEP 3: Make them 8 bits by adding 0 in front of them.

STEP 4: XOR the right part with key (01101000) = 01100000.

STEP 5: XOR this output with the left part (00001100) = 01101100.

STEP 6: Take 1's complement = 10010011.

STEP 7: After swapping at the left output is 00001000 and at right output is 10010011.

STEP 8: XOR the right (10010011) with key (01101000) = 11111011.

STEP 9: Take 1's complement of 11111011 = 00000100.

STEP 10: Take 1's complement of left (00001000) = 11110111.

STEP 11: XOR right (00000100) with left (11110111) = 11110011.

STEP 12: After swapping output at left is 10010011 and right become 11110011.

STEP 13: Reverse of left becomes 11001001 and right becomes 11001111.

STEP 14: Take XOR of both = 00000110.

4.2. Decryption Algorithm for Heuristic AIDON

STEP 1: we have got the cipher text 00000110.

STEP 2: we have every possibility of XOR and we take two numbers- 11001001 and11001111.

STEP 3: let the first number be 11001001 and second number be 11001111.

STEP 4: LET the (11001001) move to left and 11001111 moves to right.

STEP 5: reverse of left (11001001) =10010011 and of right (11001111) = 11110011.

STEP 6: XOR left (11001001) with key (01101000) =11111011.

STEP 7: 1's complement of 11111011= 00000100.

STEP 8: it is swapped to right and XORed with 11110011 = 11110111.

STEP 9: 1's complement of (11110111) = 00001000.

STEP 10: this is the second half of the plain text, and we consider last 4 bits =1000.

STEP 11: (00001000) is XORed with the key = 01100000.

STEP 12: 01100000 is swapped to the left.

STEP 13: (01100000) is XORed with 1's complement of (10010011) = 00001100.

STEP 14: this output is marked as first half of the plain text and we consider last 4 bits=1100

STEP 15: now we concatenate 1100 and 1000 = (11001000) is the required plain text.

5. Conclusion

This paper has briefly described how cryptography works and devised a new approach for symmetric key cryptography. The reader must beware, however, that there are a number of ways to attack every one of these systems; cryptanalysis and attacks on cryptosystems, however, are well beyond the scope of this paper. In the words of Sherlock Holmes (ok, Arthur Conan Doyle, really), "What one man can invent, another can discover" ("The Adventure of the Dancing Men"). There are a lot of topics that have been discussed above that will be big issues going forward in cryptography. As compute power increases, attackers can go after bigger keys and local devices can process more complex algorithms. Some of these issues include the size of public keys, the ability to forge public key certificates, which hash function(s) to use, and the trust that we will have in random number generators. Cryptography is a particularly interesting field because of the amount of work that is, by necessity, done in secret. The irony is that secrecy is *not* the key to the goodness of a cryptographic algorithm. Regardless of the mathematical theory behind an algorithm, the best algorithms are those that are well-known and well-documented because they are also well-tested and well-studied! In fact, time is the only true test of good cryptography; any cryptographic scheme that stays in use year after year is most likely a good one [8].

References

1. Debasis Das, U.A. Lanjewar and S.J. Sharma,"The Art of Cryptology: From Ancient Number System to Strange Number System", IJAIEM, Volume 2, Issue 4, April 2013, ISSN 2319-4847.

2. David Naccache, "Cryptography and Security: From Theory to Applications", Springer, 2012.
3. H.B. Pethe, Dr. S. R. Pande, "An overview of Cryptographic Hash Function M-5 and SHA", IOSR-JCE, 2016.
4. Ius Mentis: Law and technology explained, "The MD5 cryptographic hash function", Oct 1, 2005.
5. Alok Kumar Kasgar, Mukesh Kumar Dhariwal, NeerajnTantubay, Hina Malviya, "A Review Paper of Message Digest 5 (MD5)", IJMEMR, Volume1, Issue 4, December 2013, ISSN: 2320-9984 (Online).
6. Evgeny Milanov, "The RSA Algorithm", June, 2009.
7. Avi Kak, "Public-Key Cryptography and the RSA Algorithm", Lecture Notes on "Computer and Network Security", February 16, 2017.
8. William Stallings, "Cryptography and Network Security: Principles and Practices", Publisher: Prentice Hall, November 16, 2005, Pages-592.

Authors

Ira Nath is presently working as an Assistant Professor in the Department of Computer Science and Engineering of JIS College of Engineering, India. She received the Master of Technology (M.Tech.) degree in Software Engineering from the Maulana Abul Kalam Azad University of Technology, India formerly West Bengal University of Technology, India in 2008. She also received the degree of Bachelor of Technology (B.Tech.) in Computer Science and Engineering from the same university in 2005. She is presently pursuing her Ph.D in Computer Science & Technology at Indian Institute of Engineering Science and Technology (IIEST), Shibpur, India. Her research interests include Network Security regenerator placement, survivability and routing and wavelength assignment in translucent WDM optical Networks.

Deepashree Bhattacharyya is a student of JIS college of Engineering pursuing Computer Science & Engineering. She was trained as an efficient computer science engineer; she is an elegant leader, a great speaker and an expert in technicalities. Cryptography has always caught her interest and eventually she came out with bright colors with her new cryptographic algorithm.

Agnisuddha Mandal completed her schooling from North Point Senior Secondary Boarding School, Kolkata and is presently pursuing her B. Tech in Computer Science & Engineering at JIS College of Engineering, Kalyani. She is keen for research; her areas of interests include cryptography, network security, algorithm design and software engineering.

Nandini Kundu. completed her secondary and higher secondary education from Nava Nalanda High School. Now she is pursuing B.Tech from JIS College of Engineering in computer science and engineering. Her aim is to become a software engineer. Her areas of interest are network security, programming languages.

Oindrila De has completed schooling from DAV School, Dhanbad, Jharkhand. She is currently pursuing B.Tech in Computer Science and Engineering from JIS College of Engineering, Kalyani, West Bengal. She is keenly interested in research work related to cryptographic algorithms. Her others areas of interest are web development and machine learning.

