Development of Advanced Encryption Standard (AES) Cryptography Algorithm for Wi-Fi Security Protocol

Research · April 2014

DOI: 10.13140/RG.2.2.20993.97124

2 authors:

Maghrib Alrammahi
University Of Kufa
7 PUBLICATIONS **4** CITATIONS
SEE PROFILE

Harleen Kaur
Jamia Hamdard University
142 PUBLICATIONS **2,281** CITATIONS
SEE PROFILE

ISSN No. 0976-5697

Volume 5, No. 3, March-April 2014

International Journal of Advanced Research in Computer Science

RESEARCH PAPER

Available Online at www.ijarcs.info

Development of Advanced Encryption Standard (AES) Cryptography Algorithm for Wi-Fi Security Protocol

Maghrib Abidalreda Maky Alrammahi[1,2]
[1]Department of Computer Science, Jamia Hamdard,
New Delhi, India
[2]University of Kufa, Najaf, Iraq

Harleen Kaur
Department of Computer Science, Jamia Hamdard,
New Delhi, India

Abstract:Today all organizations generally rely on wireless networks for ease of movement and less expensive than wired networks but also wireless networks suffer from some of the disadvantages is the presence of some of the threats to the security of networks penetrate through passwords for Wi-Fi networks by hacker and this is a big problem and resolve this issue and during the development and improvement of some of the algorithms used encryption in wireless networks and increase protection and help to the difficulty of penetrating passwords, at the present time there are different types of encryption algorithms to provide protection for wireless networks as well as the help of these algorithms to provide information security and the health of the user, and operate these algorithms to achieve three priorities encryption such as integrity, confidentiality and authentication. This can be achieved with these three priorities, and promote the development of the encryption algorithm AES.

Keywords: Wi-Fi Wireless Fidelity; Advanced Encryption Standard; Cryptography; Encryption; Decryption

I. INTRODUCTION

Wireless networks suffer dangerous than wired networks because of the signal sent into the air in the form of frequencies and this helps to break the message sent during the hackers if the message is not good in encryption or encrypted and use an algorithm weak Although wireless networking alters the risks associated with various threats to security, the overall security objectives remain the same as with wired networks preserving confidentiality, integrity and availability of information systems and the basic problem in wireless networks is a hacker for the purpose of damage or theft and the attack on the external data and information and we are have many types of hacker attacks on the networks of all kinds, but with regard to thesis only one type of hacker uses to penetrate the passwords in wireless networks (Wi-Fi) and his name password attack and Password attack the attacker tries to break the passwords stored in a database or network account password-protected file or passwords for wireless networks.

There are three main types of password attacks: dictionary attack, brute-force attack and Hybrid attack. First type it uses a dictionary attack on a list of a Word file, which is a list of possible passwords and brute-force attack is when the attacker tries every possible combination of characters and both types first and second are used for hacker passwords in wireless networks Cryptography is the process of encryption and decryption of data and information to protect and isolate it from hacker so encryption consists mainly of the rush of a message so that its contents cannot be accessed easily for the message, while decryption is the reverse process and these processes rely on special algorithms and certain when you send a text message from one side to the other side and the probability of this may be a plain-text message to penetrate and that is meant the encryption process is very weak and so very important used special algorithm if the message was sent in process of plain text to encrypted using algorithms to protect the message so you must design and develop an algorithm for lightening the message and through the use special of certain encryption keys and in the process of transmission and receipt or in the process of transmission of the message in the air.

II. LITERATURE REVIEW

There are several ways of classifying cryptographic algorithms and they will be categorized based on the number of keys that are employed for encryption and decryption, and further defined by their application and use and the three types of algorithms that will be discussed the first type is symmetric encryption and also known as Secret Key Cryptography and With a single key is used for both encryption and decryption, the sender uses the key to encrypt the plain and sends the encrypted text to the recipient, Receiver applies the same key to decrypt the message and recover normal and because it is used as a single key in the process of transmission and receiving, also called secret key encryption to encrypt the secret key and with this type of encryption it is clear that the key must be known on both sides of both the sender and the receiver and generally classified secret key encryption schemes as either stream ciphers or block ciphers, the second type is Asymmetric encryption and also known as Public Key Cryptography and describe the system encryption key two in the two parties can communicate securely safely through a communication channel is secure without having to exchange the secret key , and address the problem of the distribution of the secret key using two keys instead of one key and public key which can be known by everyone and sometimes equips from the server, and the private key, which must be kept confidential, and only known by the owner or recipient shall not be shared with any person, only one person , last type is hash functions and that uses a mathematical transformation to irreversibly "encrypt" information and as shown in Figure 1.

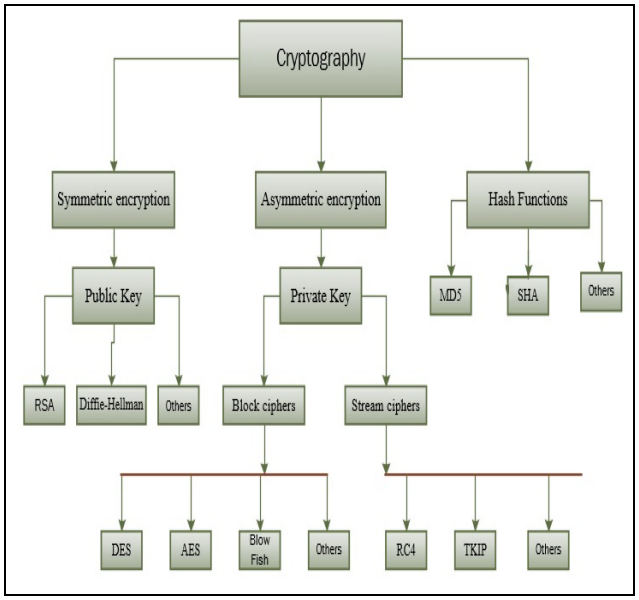

Figure 1 Types of Cryptography

Various Cryptographic Algorithms

a. ***Data Encryption Standard (DES)-*** It was designed in 1970's by IBM and was ratified in 1977 by the National Bureau of Standards (NBS) for commercial use. It is a block cipher that operates on 64-bit blocks employing a 56-bit key and 8 rounds [13].

b. ***Advanced Encryption Standard (AES)-*** It was designed by Vincent Rijmen and Joan Daemen and was introduced in 1998. The key length and block length are can include 128, 192, or 256 bits and 10, 12 and 14 rounds and data block of 128-bits and AES is a highly efficient and secure algorithm[14].

c. ***Rivest Cipher (RC)-*** Ronald Rivest developed this algorithm and thus, the name of the algorithm was put after Ronald's Rivest name. It provides a series of RC algorithms including RC1, RC2, RC3, RC4, RC5 and RC6 [15].RC1 was never published,RC2 was a 64-bit block cipher developed in 1987.RC3 was broken before ever being used,RC4 is the world's most widely used stream cipher,RC5 is a 32/64/128-bit block cipher developed in 1994,RC6, a 128-bit block cipher based heavily on RC5, was an AES finalist developed in 1997[24].

d. ***Blowfish-*** It was developed by Bruce Schneie and was first published in the year 1993. This block cipher has 8 rounds, having the block size about of 64 bits and the key length can vary from 32 to 448 bits[16].

e. ***TKIP-*** It was designed by Wi-Fi Alliance in 2002 and the suite of algorithms that works as a "wrapper" to WEP [23]. TKIP is a "wrapper" that goes around the existing WEP encryption. TKIP comprises the same encryption engine and RC4 algorithm defined for WEP. However, the key used for encryption in TKIP is 128 bits long. This solves the first problem of WEP: a too-short key length [25].

f. ***RSA-*** RSA stands for Ron Rivest, Adi Shamir and Leonard Adleman. RSA was named after the mathematician who invented it. RSA was first published in 1997 [17]. Variable size key and encryption block is used in RSA. The main advantage of the RSA algorithm is enhanced security and convenience. Using Public Key Encryption is also an advantage of this algorithm. RSA lacks in encryption speed [18].

g. ***Diffie-Hellman-*** This algorithm was introduced in1976 by Diffie-Hellman. The Diffie-Hellman algorithm grants two users to establish a shared secret key and to communicate over an insecure a communication channel [19] One-way authentication is free with this type of algorithm. The biggest limitation of this kind of algorithm is communication made using this algorithm is itself vulnerable to man in the middle attack [20].

h. ***Massage Digest 5 (MD5)-*** The MD5 algorithm was developed by Rivest in 1991, is an extension of the MD4 message-digest algorithm and is a bit slower than MD4. This algorithm results in a 128-bit hash value. It is mostly used in security-based applications. MD5 is more secure than MD4 [21]. It is suitable to use for standard file verifications but it has some flaws and therefore, it is not useful for advanced encryption applications [22].

i. ***Secure Hash Algorithm (SHA)-*** Algorithm for NIST's Secure Hash Standard (SHS). SHA-1 produces a 160-bit hash value and describes five algorithms in the SHS: SHA-1 plus SHA-224, SHA-256, SHA-384, and SHA-512 that can produce hash values that are 224, 256, 384, or 512 bits in length [12].

After studying the types of encryption algorithms and watch and differences among them and each algorithm to the environment their own differences on the size and length of each algorithm and the number of rounds and this is very important in increasing protection because if increased tours helps to increase the protection and not only that, but also on the length of the data and some of the properties, In the paper when using wireless networks should use the encryption of the first type is to use a single key in the process of transmission and receipt, while the second type is the use of two keys different first sometimes be outfitted from the server and the public key and the second will be the recipient and the private key and third type of hash functions cryptography uses some calculations to send the output is only used in the encryption process on the one hand and the only one not used with the second party (decryption),

III. PROPOSED AES ALGORITHM

AES is the most famous and most used extensively block cipher. It has three versions (AES-128, AES-192, and AES-256) vary in sizes their keys (128-bit and 192 -bit and 256-bit) and the number of rounds (10.12, and 14, respectively), as in figure 2.

Algorithm	Key Length	Block Size	Number of Rounds
AES-128	4	4	10
AES-193	6	4	12
AES-256	8	4	14

Figure 2 Types of Algorithms

To encrypt and decrypt there are four different steps for AES algorithm:

a. ***Sub Byte-*** In this step, the Sub-bytes of data in plain text are replaced by some pre-defined values of the switch box are call substitution box. Replacements

box is a box is usually used replacement rijndael. Substitution box is reversible

b. Shift Rows- In the process of transformation rows in the matrix 4 × 4 is shifted to the left r bits and r varies with the rows of the matrix and the r depends on the key and the row number (r=0 for row1, r=1 for row2, r=2 for row3, r=3 for row 4).

c. Mix Columns- Mix columns or shift column combination is working on the column during the State of the column, and treat each column as a four-term polynomial. Considered columns as polynomials on GF (28) and hit the module X4 + 1 with polynomial fixed (Q) obtained from (Q) = {2} X3 + {3} X2 + {1} {x }+{1}.

d. Add Round Key- Add round key is a major step in the tour is xored data with 128-bit sub key of the current round using a major expansion, Add round key is used in two different places and through the beginning of this one is when r = 0 then tour through other tours, which is when 1≤ round≤ Nr, where Nr is the maximum number of rounds.

In each round, we use the four steps that have been mentioned previously with the exception of the first round, which is used as one step add a key round in the final round three steps we use except Mix column in both processes in encryption and decryption , as shown in the following steps:
Round 1:
A. Add Round key.
Following Rounds:
A. Sub Bytes.
B. Shift Rows.
C. Mix Column.
D. Add Round Key.
Final Round:
A. Sub Bytes.
B. Shift Row.
C. Add Round Key.

Through this section will explain the work flowchart of the algorithm and how it works initially get into writing and then turn it into a Matrix and the dimensions depend on the size of the data and the length of the data and then added the key and then start the encryption process depending on the rounds at each stage and contains the algorithm in general four steps in each round without the first round content to only one step and last of round content to three steps as in figure 3.

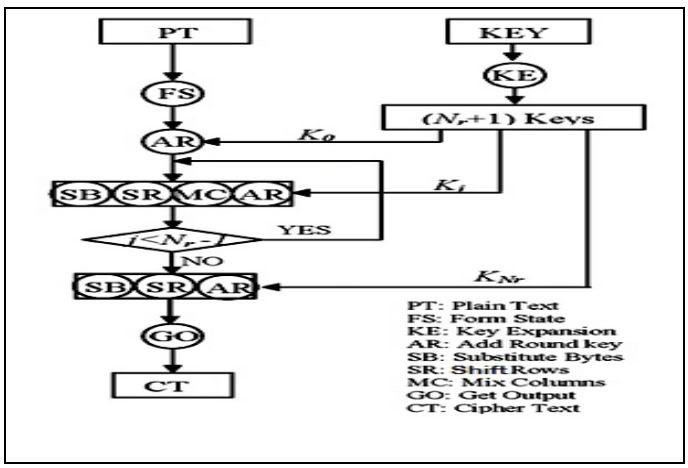

Figure 3 Flowchart of AES Algorithm

AES encryption and decryption algorithms use a key table generated from the major group of seed bytes. AES specifications indicate that this is the key expansion routine. Generating, in essence, multiple keys from the initial key instead of using a single key greatly increases the deployment of bits and although not overwhelmingly difficult, the key to understanding the expansion is one of the hardest parts of the algorithm AES. All codes of AES algorithm is written by Visual Studio project and the use of a programming language written in C #

```
private int Nr;
protected byte[] Encrypt128Bit (byte[] block)
    {
      AddRoundKey (block, 0);
      //Nr=10,12 or 14 depending on key size
      for (int i = 1; i < Nr; i++)
      {
        SubBytes(block);
        ShiftRows(block);
        MixColumns(block);
        AddRoundKey(block, i);
      }
      SubBytes(block);
      ShiftRows(block);
      AddRoundKey(block, Nr);
      return block;
    }
```

Figure 4 AES Algorithm for Encryption

```
Private int Nr
protected byte[] Decrypt128Bit(byte[] block)
    {
      AddRoundKey(block, Nr);
      //Nr=10,12 or 14 depending on key size
      for (int i = Nr - 1; i > 0; i--)
      {
        InvShiftRows(block);
        InvSubBytes(block);
        AddRoundKey(block, i);
        InvMixColumns(block);          }
      InvShiftRows(block);
      InvSubBytes(block);
      AddRoundKey(block, 0);
      return block;
    }
```

Figure 5 AES Algorithm for Decryption

First, confirm that you have the correct template for your paper size. This template has been tailored for output on the US-letter paper size. If you are using A4-sized paper, please close this template and download the file for A4 paper format called "CPS_A4_format".

IV. EXPERIMENTAL RESULTS

After written the all codes of AES algorithm by use language c# .Net and design of program and apply all codes inside him and the program his name AES CRYPTOGRAPHY ALGORITHM | VER 1.0 gradually and we will explain all the steps in the next test. We will test the program in terms of the choice of the type of algorithm depending on the length of the data and then insert the key before the transmitter and receiving and is considered the key is to check between the two parties and then enter the information , for example, which will be sent between the sender and the recipient (between computer and access point) and then We are begin testing the algorithm in terms of the work of protection of information through the testing process in the transmitter encryption and decryption in the

process of receiving and what will be achieved by the algorithm after testing this algorithm .

The results are shown by various screen shots from the figure 6-13.And finally the result in this section. Initially increase protection in wireless networks and as we have seen previously after the test program found that the encryption process conducted properly and highly protected through encryption and decryption of information in the transmitter and receiving. As well as ease of use and the program tested in a simple and not complicated and so that many people and this can use the program is an important factor for the program and algorithm. Another factor that can we conclude from the previous test is through coverage and high efficiency in the encrypted information through the results that we've seen in the test so that we can apply this algorithm in many applications, including the protection of information and the protection of passwords in wireless networks are used in a wide coverage. As well as other factors which productivity and efficiency and elegance program, especially the development of the algorithm to suit the work and show the highest rate of protection expected by the final design of the program and the algorithm

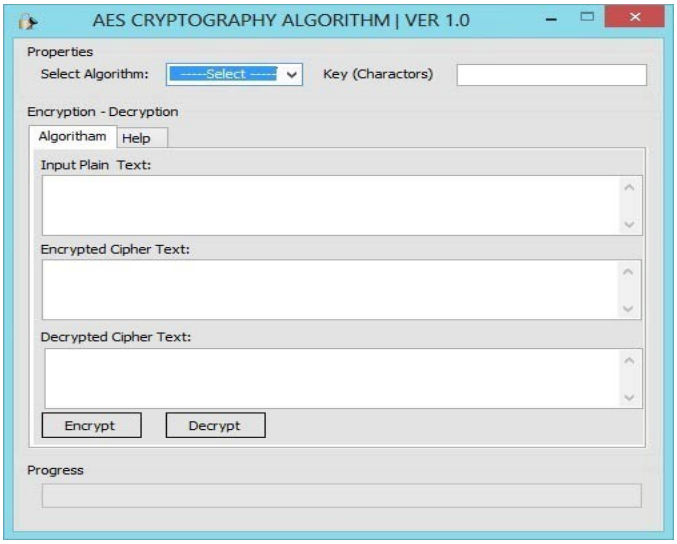

Figure 6: Screen shot- AES Cryptography for Selecting Algorithm

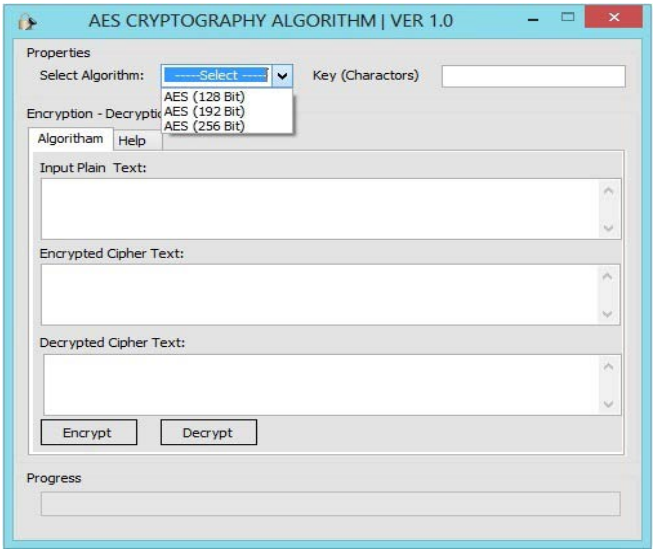

Figure 7: Screen shot- AES Cryptography for Selecting Algorithm 2

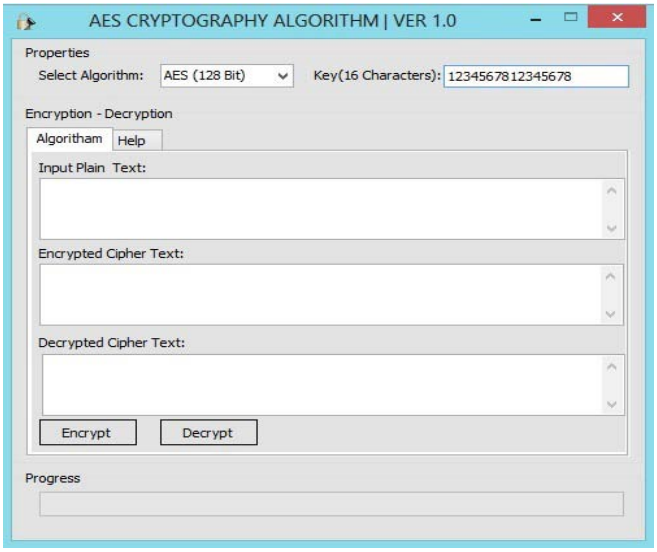

Figure 8: Screen shot- AES Cryptography for Selecting Algorithm and Key (16-bits)

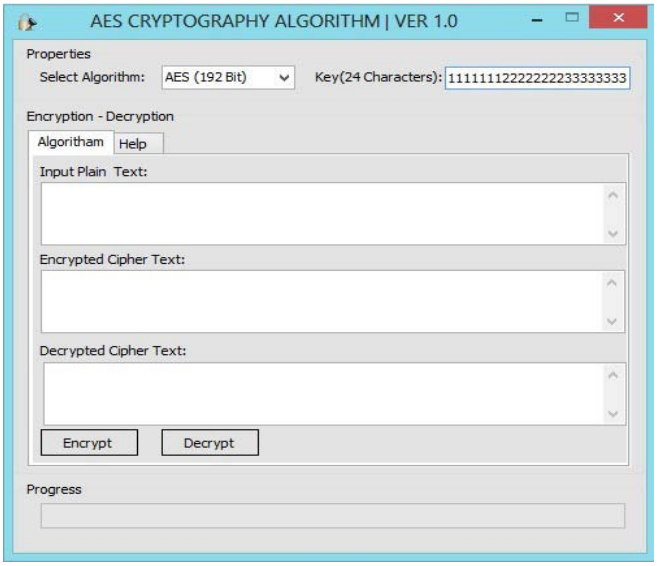

Figure 9: Screen shot- AES Cryptography for Selecting Algorithm and Key (24-bits)

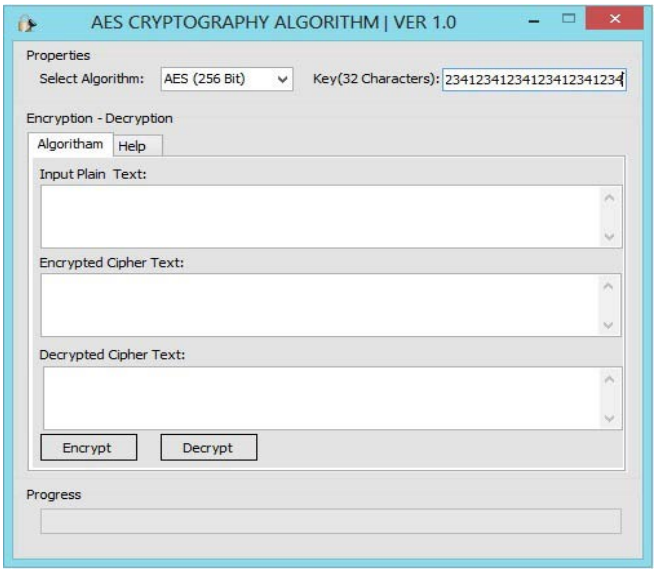

Figure 10: Screen shot- AES Cryptography for Selecting Algorithm and Key (32-bits)

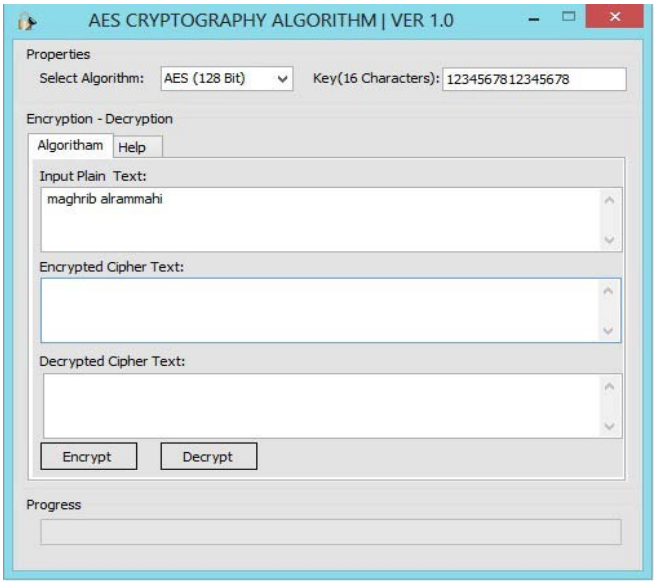

Figure 11: Screen shot- AES Cryptography for Input Plain Text

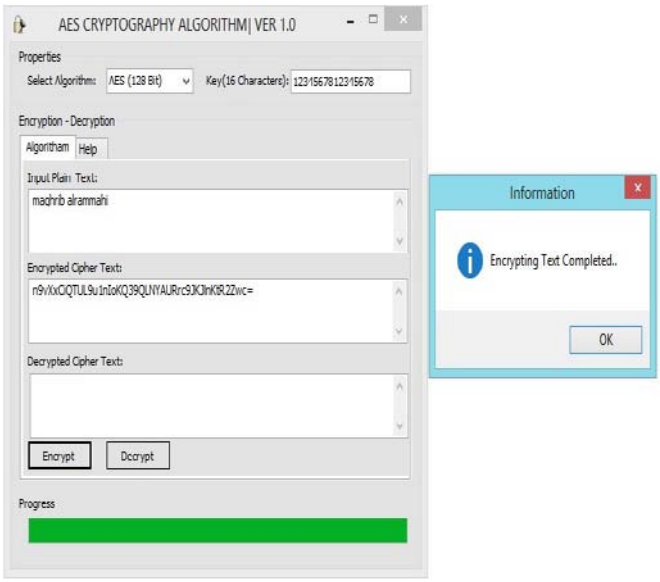

Figure 12: Screen shot- AES Cryptography for Encryption

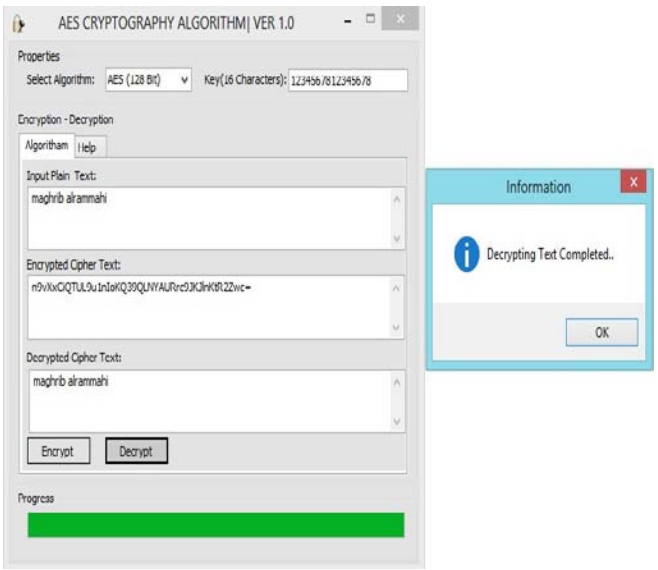

Figure 13: Screen shot- AES Cryptography for Decryption

V. CONCLUSION

Although it is impossible to complete elimination of all risks by the hacker linked to wireless networks, but it is possible to achieve a reasonable level of protection of public security, especially passwords in wireless networks and through the adoption of the assessment and management of risk. Through different types of encryption and every type used in a particular case depending on the type of network and through the importance of protecting the information and passwords from hackers must configure and develop algorithms to increase protection and prevent hackers from penetration and direct access to the data and passwords. So will be configured a certain algorithm called AES algorithm purpose of increasing the protection of hackers in wireless networks. In this paper and identified basic problems and weaknesses and gaps in wireless networks and through the completion of the final analysis and design of the program noted that the strength of protection depends on the type of algorithm used, the length of the number of bits of the algorithm, as well as the length of the key. It is not good to use data -length and short lengths short keys, because by using the powerful software one can breach the network, as well as short keys very easily and is able to break passwords and this, as we saw earlier in the seasons and with the images how they were breaking passwords, and therefore we see in the algorithm it contains three types of height in the data and the keys and this helps in the more difficult and hacker break passwords. The AES algorithm was developed and the use of encryption to prevent or reduce the hacker and security information and passwords.

VI. REFRENCES

[1]. Dhall, S., Pal, S.K., “Design of a New Block Cipher Based on Conditional Encryption”, Information Technology: New Generations (ITNG), pp. 714 –718, 2010.

[2]. Hui Shi , Yuanqing Deng , Yu Guan, “Analysis of the avalanche effect of the AES S box”,Artificial Intelligence, Management Science and Electronic Commerce (AIMSEC) , pp. 5425 – 5428, , 2011.

[3]. Mandal, A.K., Parakash, C., Tiwari, A., “Performance Evaluation of Cryptographic Algorithms: DES and AES”, Electrical, Electronics and Computer Science (SCEECS), pp. 1 – 5, 2012.

[4]. Dewangan, C.P., Agrawal, S., Mandal, A.K., Tiwari, A. , “Study of avalanche effect in AES using binary Codes”, Advanced Communication Control and Computing Technologies (ICACCCT), 2012 IEEE International Conference, pp. 183 – 187, 2012.

[5]. Moh'd, A., Jararweh, Y., Tawalbeh, L., “AES-512: 512-Bit Advanced Encryption Standard Algorithm Design and Evaluation”, Information Assurance and Security (IAS), Page(s): 292 – 297, 2011.

[6]. ChiaLongWu, ChenHaoHu ,“Computational Complexity Theoretical Analyses onCryptographic Algorithms for Computer SecurityApplication”, Innovations in Bio-Inspired Computing and Applications(IBICA), pp. 307 - 311, ,2012.

[7]. Dubai, M.J., Mahesh, T.R., Ghosh, P.A., “Design of new security algorithm: Using hybrid Cryptography architecture”,

Electronics Computer Technology (ICECT), pp. 99 – 101, 2011.

[8]. Mandal, B.K., Bhattacharyya, D., Bandyopadhyay, S.K., "Designing and Performance Analysis of a Proposed Symmetric Cryptography Algorithm", Communication Systems and Network Technologies (CSNT), pp. 453 – 461, 2013.

[9]. Isaac, E.R.H.P., Isaac, J.H.R., Visumathi, J., "Reverse Circle Cipher for Personal and Network Security", Information Communication and Embedded Systems (ICICES), Page(s): 346 – 351,2013 .

[10]. Fei Shao, Zinan Chang, Yi Zhang, "AES Encryption Algorithm Based on the High Performance Computing of GPU", Communication Software and Networks, pp. 588 – 590, 2010.

[11]. Datta, K., Shrivastav, V., Sengupta, I., Rahaman, H., "Reversible Logic Implementation of AES Algorithm", Design & Technology of Integrated Systems in Nanoscale Era (DTIS), pp. 140 – 144, 2013.

[12]. Aaron E. Earle, "Wireless Security Handbook", Published by Auerbach Publications Taylor & Francis Group, 2006.

[13]. http://searchsecurity.techtarget.com/definition/Data-Encryption-Standard

[14]. http://www.truecrypt.org/docs/aes

[15]. http://en.citizendium.org/wiki/Rivest_ciphers

[16]. https://www.schneier.com/blowfish.html.

[17]. http://searchsecurity.techtarget.com/definition/RSA.

[18]. http://www.emc.com/emc-plus/rsa-labs/standardsinitiatives/Advantages-and-disadvantages.htm

[19]. http://searchsecurity.techtarget.com/definition/Diffie-Hellman-key-exchange.

[20]. http://technet.microsoft.com/enus/Library/cc962033.aspx.

[21]. http://www.accuhash.com/what-is-md5.html.

[22]. http://pcsupport.about.com/od/termsm/g/md5.htm.

[23]. http://en.wikipedia.org/wiki/Temporal_Key_Integrity_Protocol.

[24]. http://en.wikipedia.org/wiki/RC_algorithm.

[25]. http://www.networkworld.com/reviews/2004/1004wirelesstkip.html.