ISSN: 0975-833X

Available online at http://www.journalcra.com

International Journal of Current Research
Vol. 3, Issue, 4, pp.241-244, April, 2011

INTERNATIONAL JOURNAL OF CURRENT RESEARCH

RESEARCH ARTICLE

HYBRID CRYPTOGRAPHY BY THE IMPLEMENTATION OF RSA AND AES

Palanisamy, V. and Jeneba Mary, A.

Department of Computer science and Engineering, Alagappa University, Karaikudi-630003

ARTICLE INFO

Article History:
Received 11th January, 2011
Received in revised form
24th February, 2011
Accepted 15th March, 2011
Published online 27th April 2011

Key words:
Advanced Encryption Standard (AES),
Symmetric key asymmetric key, RSA

ABSTRACT

The Rijndael algorithm mainly consists of a symmetric block cipher that can process data blocks of 128, 192 or 256 bits by using key lengths of 128, 196 and 256 bits. This work using Rijndael cryptography symmetric algorithm for data encryption/decryption and RSA cryptography asymmetric algorithm for Rijndael key's encryption/decryption. The encryption and decryption of any data has a secure key, which is used for data encryption. For this purpose asymmetric key is used. This work securing the data key using RSA algorithm. Here RSA key size is 128-bytes. This work also generating two pairs of keys; public and private key. Using Public key it encrypts the data key and other one is public and private key pair ,which will send to other person, so that opposite person can decrypt the encrypted key using his public and private key.

INTRODUCTION

The interpolation attack is a technique for attacking block ciphers built from simple algebraic functions. A block cipher algorithm may not include any algebraic property that can be efficiently distinguishable, since an interpolation attack can be applied to such a block cipher which leads to the leakage of information about the secret key. This mathematical property has effective implications using a block cipher with a fixed secret key. If the cipher text is described as a polynomial with unknown coefficients-of the plaintext, and if the degree of this polynomial is sufficiently low, then a limited number of plaintext-cipher text pairs are capable to completely determine the encryption function. Constructing this polynomial will not immediately yield the key. Actually this is a polynomial that emulates the encryption function. It produces valid cipher text from given plaintexts. It can be applied by constructing an implicit polynomial expression involving parts of the plaintext and the cipher text. Now, we can check the polynomial against another value that was not used in the construction to test it. If the polynomial produces the correct result, then we have guessed the key bits. This allows the cryptanalyst to encrypt and decrypt data for the unknown key without doing any key-recovery. This work describes the main parts of AES (RIJNDAEL) which consists of the individual transformations and AES S-box. We will introduce the interpolation attack with considering of the points of weakness and strength in AES S-box. Finally, we will discuss the manner of doing interpolation attack using the different representations of AES S-box.

Related work

Security of the system rests in part on the difficulty of factoring the published divisor, in cryptographic algorithm that can be used to protect electronic data. The AES algorithm is asymmetric block cipher that can encrypt (encipher) and decrypt (decipher) information. Encryption converts data to an unintelligible form called cipher text; decrypting the cipher text converts the data back into its original form, called plaintext. The AES algorithm is capable of using cryptographic keys of 128, 192, and 256 bits to encrypt and decrypt data in blocks of 128 bits. Data security has evolved rapidly since 1975. It have seen exciting developments in cryptography: public-key encryption, digital signatures, the Data Encryption Standard (DES), key safeguarding schemes, and key distribution protocols. It have developed techniques for verifying that programs do not leak confidential data, or transmit classified data to users with lower security clearances. It has found new controls for protecting data in statistical databases--and new methods of attacking these databases. It have come to a better understanding of the theoretical and practical limitations to security. An encryption method is presented with the novel property that publicly revealing an encryption key does not thereby reveal the corresponding decryption key. This has two important consequences: Couriers or other secure means are not needed to transmit keys, since a message can be enciphered using an encryption key publicly revealed by the indented recipient. Only he can decipher the message, since only he knows the corresponding decryption key.

A message can be "signed" using a privately held decryption key. Anyone can verify this signature using the corresponding publicly revealed encryption key. Signatures cannot be forged, and a signer cannot later deny the validity of his signature. This has obvious applications in "electronic mail" and "electronic funds transfer" systems. A message is encrypted by representing it as a number M, raising M to a publicly specified power, and then taking the remainder when the result is divided by the publicly specified product, n, of two large secret primer numbers p and q. Decryption is

***Corresponding author:** vpazhanisamy@yahoo.co.in*

similar; only a different, secret, power d is used, where e * d ≡ 1(mod (p - 1) * (q - 1)).

Proposed research work

A. **Key Encryption**

This file security using hybrid cryptosystem of RIJNDAEL cipher, designed by Daemen and Rijmen in 1998, is a successor of SQUARE. It was submitted to the US National Institute of Standards and Technology (NIST) in response to an open call for 128 bit block ciphers. It was, together with 14 other candidates, extensively evaluated during two years, before NIST announced in 2000 that RIJNDAEL would replace DES and become the new AES. Just as its predecessor SQUARE, RIJNDAEL was specifically designed to resist differential and linear cryptanalysis. In RIJNDAEL cipher, the individual transformations Sub Bytes, Shift Rows, Mix Columns, and Add Round Key process the state.

B. **The performing of interpolation attack over AES**

Using the interpolation attack, SHARK cryptosystem was analyzed by (Hacigumus *et al.,* 2002). This cryptosystem was designed by AES designers, whereas they had enough information about the interpolation attack. But this is not certain reason for resistance of SHARK against interpolation attack. In this cryptosystem, a carefully chosen S-box imposes most number of terms on the equations. Since in the polynomial representation of S-box, the all possible terms will be with hamming weights 7. With forming of the equation for one round cipher, we have:

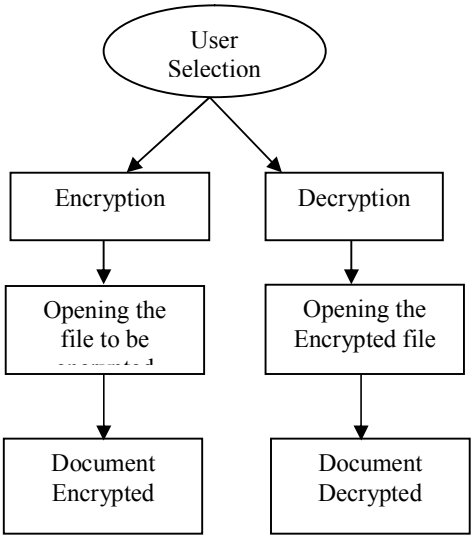
S(x + k1) + k2 = y (3)
x = Plaintext
y = Cipher text

Which x and y are known but, k1and k2 are unknowns. Using extension (3), we can find a polynomial in terms of x with 255 terms of degree 254, such that all possible powers of x appear in it. So, the interpolation attack is not possible. Since in the AES, S-box equation has the all possible terms with hamming weights 7, it can be seen that all terms appear in the representation of other rounds and the number of terms cannot be less than 2m, so the interpolation attack is impossible even on one round. Now, we can express this question: Is interpolation attack possible using S-box estimation? As an example, if we form the describer polynomial of one round using S85(x) estimation, then we will have 31 terms with nonzero coefficients instead of 255 terms, namely, we can get the coefficients with using 31 suitable texts instead of using 255 texts. Since the probability of truth for every pair is: are less than 255. The computational complexity of this attack is more than exhaustive key search attack, so it is not successful. Thus need (31×3 = 93) pairs of plaintext.

RESULTS AND DISCUSSION

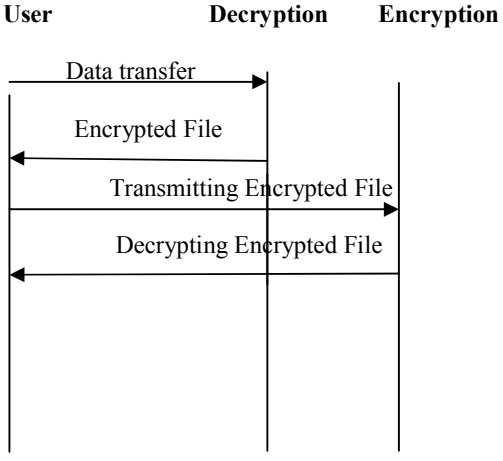
The Encryption work proposed Absolute wholeness of your protected files. Utmost safety of encrypted files and folders. Encrypted files cannot be accessed, read, modified and edited

C. **Architectural diagram**



Define abbreviations and acronyms the first time they are used in the text, even after they have been defined in the abstract. Abbreviations such as IEEE, SI, MKS, CGS, sc, dc, and rms do not have to be defined. Do not use abbreviations in the title or heads unless they are unavoidable. This work is to be used to protect the file from the unauthorized user and hackers, etc., This is to protect the document getting accessed, modified, editing by the unauthorized users. In this process the user Select the file to be encrypted in order to protect the data. The end user decrypts by the decrypting technique to view the original data that has been encrypted.

D. **Sequence Diagram**



User selects the encryption option for encrypting the file. The user specifies the file to be encrypted by clicking the encryption button to encrypt the document. The encrypted document transmitting to the decryption process. The receiver views the original file after the decryption process.

E. **Modules Description**

1. User Module

The user module is used to view two options Encryption and Decryption. The options are selected depends upon the user. If user want to encrypt the file select the encryption option. Otherwise select the decryption option.

2. Encryption Module

This module used to encrypt the document easily. First of all select the encryption option and then select the encrypting file. Finally click the encryption button. The file is to be encrypted.

3. Decryption Module

This module used to decrypt the document easily. First of all select the decryption option and then select the encrypted file. Finally click the decryption button. The file is to be decrypted.

F. Public Key Cryptography

In cryptography, RSA is an algorithm for public-key cryptography. It is the first algorithm known to be suitable for signing as well as encryption, and one of the first great advances in public key cryptography. RSA is widely used in electronic commerce protocols, and is believed to be secure given sufficiently long keys and the use of up-to-date implementations.

G. Operation

The RSA algorithm involves three steps. They are,

- key generation
- encryption and
- decryption

1) Key generation

RSA involves a public key and a private key. The public key can be known to everyone and is used for encrypting messages. Messages encrypted with the public key can only be decrypted using the private key. The keys for the RSA algorithm are generated the following way:

1. Choose two distinct prime numbers p and q. For security purposes, the integer's p and q should be chosen uniformly at random and should be of similar bit-length. Prime integers can be efficiently found using a Primality test.

2. Compute n = pq.
   - n is used as the modulus for both the public and private keys
3. Compute the totient
4. Choose an integer e such that, and e and share no divisors other than 1 (i.e. e and are co-prime).
   - e is released as the public key exponent.
   - Choosing e having a short addition chain results in more efficient encryption. Small public exponents (such as e=3) could potentially lead to greater security risks.
5. Determine d (using modular arithmetic) which satisfies the congruence relation .
   - Stated differently, ed − 1 can be evenly divided by the totient (p − 1)(q − 1).
   - This is often computed using the Extended Euclidean Algorithm.
   - d is kept as the private key exponent.
   -

The public key consists of the modulus n and the public (or encryption) exponent e. The private key consists of the modulus n and the private (or decryption) exponent d which must be kept secret.

2) Encryption

Alice transmits her public key (n, e) to Bob and keeps the private key secret. Bob then wishes to send message M to Alice. Alice first turns M into an integer $0 < m < n$ by using an agreed-upon reversible protocol known as a padding scheme. He then computes the cipher text c corresponding to. This can be done quickly using the method of exponentiation by squaring. Bob then transmits c to Alice.

3) Decryption

Alice can recover m from c by using her private key exponent d by the following computation. Given m, she can recover the original message M by reversing the padding scheme.

4) Working example

Here is an example of RSA encryption and decryption. The parameters used here are artificially small, but one can also use Open's to generate and examine a real key pair.

1. Choose two prime numbers
   p = 61 and q = 53
2. Compute n = pq
3. Compute the totient
4. Choose e > 1 coprime to 3120
   e = 17
5. Compute d such that e.g., by computing the modular multiplicative inverse of e modulo :
   d = 2753.

   Since 17 · 2753 = 46801 = 1 + 15 · 3120.

The public key is (n = 3233, e = 17). For a padded message m the encryption function is: The private key is (n = 3233, d = 2753). The decryption function is:

For example, to encrypt m = 123, we calculate
To decrypt c = 855, we calculate

Both of these calculations can be computed efficiently using the square-and-multiply algorithm for modular exponentiation. In real life situations the primes selected would be much larger, however in our example it would be relatively trivial to factor n, 3233, obtained from the freely available public key back to the primes p and q. Given e, also from the public key, we could then compute d and so acquire the private key.

Conclusion

This work using Rijndael cryptography symmetric algorithm used to data encryption/decryption and RSA cryptography asymmetric algorithm for Rijndael key's encryption/decryption. The encryption and decryption of any data has a secure key, which is used for data encryption. For this purpose asymmetric key is used. This work securing the data key using RSA algorithm. Here RSA key size is 128-bytes. This work also generating two pairs of keys; public and private key. Using Public key it encrypts the data key and other one is public and private key pair ,which will send to other person, so that opposite person can decrypt the encrypted key using his public and private key. This work described the interpolation attack against AES cryptosystem which utilized from algebraic properties of AES. We also introduced the version of AES which was resistant against interpolation attack. Finally we illustrated the new directions for the future research. We can develop the derivatives of interpolation attack.

****

REFERENCES

[1] Dr. Brian Gladman, Rijndael (by Joan Daemen & Vincent Rijmen), "*A Specification for the AES Algorithm*". 15 April 2003.

[2] Shafi Goldwasser, Mihir Bellare, "*Lecture Notes on Cryptography*", July 2008.

[3] William Stallings, "*Cryptography and Network Security"*, Fourth Edition, June 3, 2010.

[4] Tom Davis, "*RSA Encryption"*, October 10, 2003.

[5] PekkaRiikonen, "*RSA Algorithm"*, http://iki.fi /riikone/docs/ rsa.pdf. Sep 2003.

[6] Alexander W. Dent, "*Hybrid Cryptography"*. 2005