www.ijecs.in
International Journal Of Engineering And Computer Science ISSN:2319-7242
Volume 3 Issue 11 November, 2014 Page No. 9169-9171

A New Design Of A Hybrid Encryption Algorithm

Jan Mohammad Najar[1], Shahid Bashir Dar[2]

[1]Bells Institute Of Management and Technology,
Knowledge City, Mehli, 171013, Shimla, India
Najarjan202@gmail.com

[2]Bells Institute Of Management and Technology,
Knowledge City, Mehli, 171013, Shimla, India
Darshahid9@gmail.com

Abstract*: In today's world where the data and sensitive information is distributed over the networks, secure and strong cryptographic techniques should be employed to maintain integrity, authentication, and privacy of data. The aim of this paper is to propose a new design for a hybrid encryption algorithm by making use of both symmetric-key and asymmetric-key algorithms. We will use RSA, AES, and SHA-1 for this scheme.*

Keywords: RSA, AES, SHA-1, encryption.

1. Introduction

The communication between two parties over the network needs to be protected from enemies and intruders. Data integrity, authentication, and secrecy of exchanged data should be made while they are in communication. The data should be efficiently encrypted at the sender site and only the intended recipient(s) should be able to interpret the encrypted message. The encryption algorithms that has been used for this purpose can be either symmetric-key or asymmetric-key algorithms. The symmetric-key algorithm uses the single private key for encryption as well as for decryption. The message of the sender called as the plain text is converted into an unreadable form, called as cipher text. The cipher text is transmitted over the network to the receiver, who decrypts it into original message using the same private key. This scheme is having the problem of key distribution. DES (Data Encryption Standard) and AES(Advanced Encryption Standard) are two most important asymmetric-key algorithms. Asymmetric-key algorithm also called as public-key algorithm uses two pair of keys, private key and public key pair. One pair is used at the sender site and the other pair is used at the receiver site. This scheme efficiently solves the problem of key distribution. RSA (Rivest, Shamir, Adleman) algorithm is an example of public-key algorithm. The authentication of data is determined by the presence or absence of digital signatures. Various hash functions like MD5 (Message Digest 5) and SHA-1 (Secure Hash Algorithm 1) are used to digitally signature the data. The aim of this paper will be to use symmetric-key algorithms, symmetric-key algorithms, and hash functions in a single encryption technique. The proposed scheme gathers their features to a common place, and develops a hybrid encryption algorithm that is secure, efficient, and proves data authenticity.

2. Methodologies

2.1 AES

Advanced Encryption Standard (AES) is a symmetric-key cryptographic technique. Unlike its predecessor DES, the structure of AES does not resemble to that of Feistel Structure. AES has a fixed block size of 128-bit and the key length must be 128, 192, or 256 bits. A 128-bit key thus gives a key space of 2^{128} keys. Number of rounds in AES is determined by the key size used in the process. Number of rounds will be 10, 12, 14 for key sizes of 128, 192, 256 bits respectively. First n-1 rounds contain four distinct transformations: Substitute Bytes, Shift Rows, Mix Columns, and Add Round Key. The final round contains only three transformations: Substitute Bytes, Shift Rows, and Add Round Key. AES offers a very high security and performance.

2.2 RSA

RSA is a public-key cryptographic technique that uses private key and public key. Messages are encrypted by using the public key of specific receiver and decryption is done by using the private key of receiver. The steps involved in the process are:

- Choose two distinct large primes, p and q.
- Compute n = p*q.
- Compute z = (p-1)*(q-1).
- Choose a number relatively prime to z and call it d.
- Find e such that e*d = 1 mod z.

The pair (e, n) forms our public key and the pair (d, n) forms our private key. To compute cipher text (C) of message (M) uses the following equation.

$$C = M^{e} \pmod{n} \quad (1)$$

To decrypt the cipher text (C), use the following equation.

$$P = C^{d} \pmod{n} \quad (2)$$

2.3 SHA-1

Secure Hash Algorithm (SHA-1) is a major message digest function developed by NSA. SHA-1 processes the data blocks of 512-bit and generates a message digest of 160-bit.The message digest is produced on similar principles used in MD4 and MD5, but SHA-1 has more conservative design. SHA-1 is used in several widely used protocols and security applications like TLS, SSL, PGP, SSH, S/MIME, and IPSEC. Secure Hash

Algorithms comes in various flavors like SHA224, SHA256, SHA384, and SHA512.

3. Literature Review

Komal Rege et.al [4] proposed a hybrid encryption scheme for Bluetooth communication security, using AES and RSA. The key of 128-bit is encrypted using RSA algorithm, similarly the message of sender is encrypted using AES cipher. Both encrypted AES-key and cipher text of message is used to generate a complex message, which is transmitted over the network. The decryption is exactly the reverse process of encryption algorithm. Palanisamy et.al [5] proposes a hybrid cryptography technique using RSA and AES algorithms. RSA algorithm uses a key size of 128-bytes. It uses two pairs of keys: public key and private key. One pair is used at sender site for encryption/decryption and the other one at receiver's site. Ali E. Taki El_Deen [3] has proposed a hybrid encryption algorithm using AES and Blowfish. Plaintext of 64-bit is encrypted using Blowfish algorithm generating 64-bit cipher text which is again encrypted using same algorithm, thus generating a new 64-bit cipher text. The two outputs 64+64=128-bit cipher text is now given as an input to AES algorithm, generating the final 128-bit cipher text. Blowfish and AES algorithms make use of 32-bit and 128-bit key size respectively for their rounds. A statistical comparison of AES, DES, RSA, and Blowfish algorithms has been also provided. Ritu Pahal et.al [6] proposes an efficient implementation of AES. Instead of conventional 128-bit input, 200-bit input is copied into an array of 5*5 matrixes. The first nine rounds are same consisting of four transformations: Substitute Bytes, Shift Rows, Mix Columns, and Add Round Key, but in the final (10th) round transformation Mix Columns is not used. The results of proposed scheme are compared with 128-bit, 192-bit, and 256-bit AES techniques at the end.

4. Ideas and Processes of Proposed Hybrid Scheme

The proposed scheme consists of two processes, encryption process and decryption process. Both processes make use of RSA, AES and SHA1. The reason we have selected these particular algorithms is discussed as:

RSA a public-key algorithm can be used for encryption as well in digital signature processes. The key management is an essential feature of RSA algorithm. The security of the method used in RSA is based on the difficulty of factoring large numbers.

AES is not only a secure cipher but it offers a very high performance and makes better use of resources. It is strong enough to be certified for use by the US government for top secret information Encryption Process [3]. Not a single successful brute-force attack on AES has been found till date, the only possible known attack against AES.

SHA-1 a message digest function with a block size of 512-bit generates 160-bit message digest. It has a very conservative design and is used in various protocols like SSL, TLS, and PGP.

So all the essential features of these algorithms are made available in our proposed hybrid algorithm. Better encryption of AES, most efficient key management by RSA along with the digital signature by making use of SHA-1 are included in a single hybrid system.

4.1 Encryption Process

- An AES key 'K' of 128-bit, 192-bit or 256-bit is chosen.
- Encrypt message (M) using AES algorithm and above selected key K.

  eM = AES-encryption(M)
- AES key K is encrypted by making use of RSA algorithm.

  eK = RSA-encryption (K)
- The cipher text (eM) is fed to SHA1 algorithm which generates a message digest of 160-bit.

  mD = SHA1 (eM)
- The message digest is signed by RSA algorithm using private key of sender.

  DS = RSA-sign (mD)
- The encrypted message (eM), digital signature (DS) and AES encrypted key (eK) is transmitted to the user over a network.

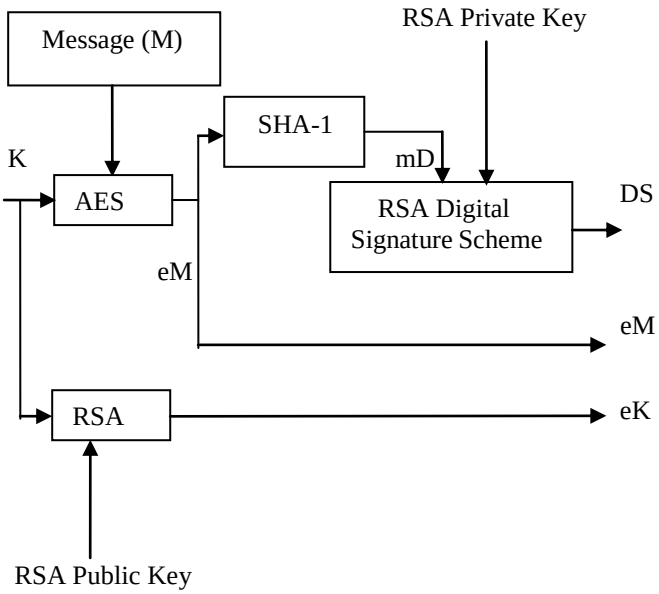

Figure 1: Encryption Process

4.2 Decryption Process

This process is the reverse of encryption process and is having following steps:

- The encrypted AES key (eK) is decrypted with RSA algorithm.

  K = RSA-decryption (eK)
- Similarly the encrypted message (eM) is decrypted by AES algorithm using key K.

  M = AES-decryption (eM)
- The message digest of encrypted message (eM) is computed using SHA1.

  mD = SHA1 (eM)
- The digital signature is verified by RSA algorithm by employing use of public key of sender.

  DS = RSA-verify (mD)
- Thus we get message (M) of sender in step-2 which is verified by digital signature DS.

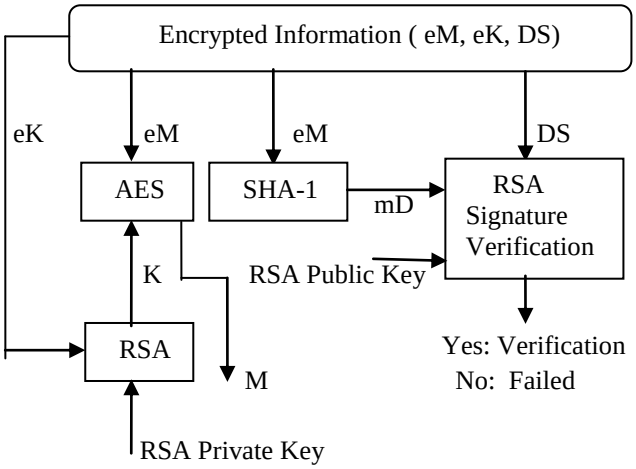

Figure 2: Decryption Process

5. Advantages of Proposed Scheme

- Keys are transmitted over the network in encrypted form along with data, not separately.
- Offers a very high security, performance and better key management.
- Makes use of digital signatures for message authentication.

6. Conclusion

A hybrid cryptographic algorithm based on RSA, AES, and SHA-1 techniques is proposed. Different features of these algorithms are made available in a single package. The proposed technique is secure, tough, and efficient due to the use of AES cipher, is having better key management due to the use of RSA technique, and makes use of digital signatures due to the use of SHA-1.

References

- Andrew S. Tenanbaum, "Computer Networks", Fourth Edition, Pearson Education, 2003.
- William Stallings, "Network Security Essentials: Applications and Standards", Prentice Hall, 4th edition, 2011.
- Ali E. Taki El_Deen , "Design and Implementation of Hybrid Encryption Algorithm", International Journal of Scientific & Engineering Research, Volume 4, Issue 12, December-2013.
- Komal Rege, Nikita Goenka, Pooja Bhutada, Sunil Mane, " Bluetooth Communication using Hybrid Encryption Algorithm based on AES and RSA", International Journal of Computer Applications (0975 – 8887) Volume 71– No.22, June 2013.
- Palanisamy, V. and Jeneba Mary, A., "HYBRID CRYPTOGRAPHY BY THE IMPLEMENTATION OF RSA AND AES", International Journal of Current Research Vol. 33, Issue, 4, pp.241-244, April, 2011.
- Ritu Pahal, Vikas kumar," Efficient Implementation of AES", International Journal of Advanced Research in Computer Science and Software Engineering, Volume 3, Issue 7, July 2013.

Author Profile

Jan Mohammad Najar received the B-TECH degree in Computer Science and Engineering from Islamic University of Science and Technology, Kashmir in 2012.He is now pursuing M-TECH in Computer Science and Engineering from Himachal Pradesh Technical University, India.

Shahid Bashir Dar received the B-TECH degree in Electronics and Communication Engineering from Islamic University of Science and Technology, Kashmir in 2013. He is now pursuing M-TECH in Computer Science and Engineering from Himachal Pradesh Technical University, India.