ISSN:0975-9646

Design of New Security Protocol

K .Seena Naik (Ph.D)[1] , Dr G.A Ramachandra[2] , M V Bramhananda Reddy[3]

[1,2]*Dept Of CSE, S K University, Anantapur*
[3]*Dept Of CSE,Gitam University*

Abstract-A new security protocol for on- line- transaction can be designed using combination of both symmetric and asymmetric cryptographic techniques [1]. This protocol provides three cryptographic primitives – integrity, confidentiality and authentication. It uses Elliptic Curve Cryptography for encryption, RSA algorithm for authentication and MD-5 for integrity. Instead of ECC symmetric cipher (AES-Rijndael) can be used to encrypt, public key cryptography (RSA) to authenticate and MD-5 to check for integrity .The symmetric cryptographic algorithms are fast as compared to asymmetric cryptographic algorithms like RSA, Elliptic Curve Cryptography. Communication has a major impact on today's business. It is desired to communicate data with high security. At present, various types of cryptographic algorithms provide high security to information on controlled networks. These algorithms are required to provide data security and users authenticity. A new security protocol has been designed for better security using a combination of both symmetric and asymmetric cryptographic techniques.

1. Design of New Security Protocol.

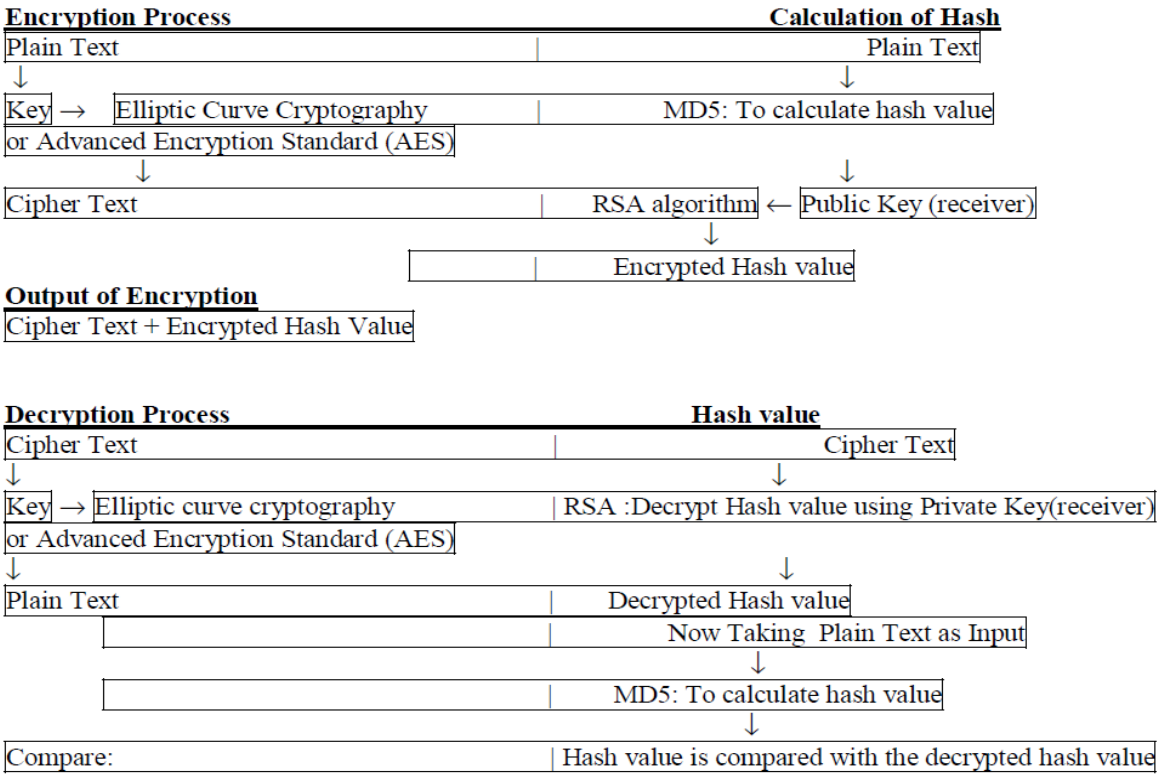
The encryption technique used in the protocol is a combination of both symmetric and asymmetric cryptographic techniques. It uses Elliptic Curve Cryptography for encryption, RSA algorithm for authentication and MD-5 for integrity. Instead of ECC symmetric cipher (AESRijndael) can be used to encrypt, t public key cryptography (RSA) to authenticate and MD-5 to check for integrity.

1.1 AES – Algorithm

The Rijndael proposal for AES defined a cipher in which the block length and the key length can be independently specified to be 128, 192 and 256 bits[2]. AES algorithm contains the following four different stages: 1) Substitution bytes: Uses s_box (substitution box) to perform byte-to-byte substitution. 2) Shift rows: A simple permutation 3) Mix columns: A diffusion layer that makes use of Finite field arithmetic. 4) AddRoundKey: A simple bit wise XOR of the current block with the expanded key.

1.2 Encryption Technique

In the new security protocol, the sender uses 160 bits key size with Elliptic curve cryptography to encrypt the message. The hash value of the message is encrypted using RSA algorithm with 1028 bit public key of the receiver. The decryption is done using the Elliptic curvecryptography. The hash value is calculated from the original message using the hash function MD-5. RSA algorithm is used to encrypt the calculated hash value. On the receiving side RSA is used with 1028 bit private key of the receiver to decrypt the encrypted hash value. The calculated and decrypted hash values are compared to ensure integrity.



1.3 Security of Elliptic Curve Cryptosystems and Hash function – MD5

The security of Elliptic Curve Cryptosystems is based on the difficulty of computing discrete logarithms in the subgroup generated by the generator g. These can be computed if discrete logarithms in the full group of points on an elliptic curve over a finite field can be computed.

By solving the problem in all cyclic subgroups and then combining the results, the cryptosystem can be broken. The difficulty of the problem depends on the size of the largest prime divisor of the order of the group of points of the curve. For that reason, the values of parameters p and q in the Elliptic Curve Cryptosystem E (p, q) are usually chosen such that the sizes of p and q are close.

The hash function MD5 has the following characteristics: It uses a 128-bit digest size, MD5 uses 4 rounds of 16 steps, It uses initialized registers (32-bit) and chaining variables, MD5 uses a 512-bit block: 64 bits for the length of the block, 448 bits for data.

A successful attack consists of finding the values say s and t with the condition that s is notequal to t and the hashes of s and t are same. Hash functions can be attacked by birthday paradox attack.

1.4 Cryptanalysis of AES – Rijndael (The Square Attack)

Conventions used :

Intermediate text value used in round r after the MixColumn = m (r)

Intermediate text value used in round r after the Key addition = b (r) ,

Intermediate text value used in round r after the ShiftRow = t (r) ,

Sub key value in round r = K (r)

Equivalent sub key value that may be XORed into state before instead of after theMixColumn operation in round r = K (r)".

The attack starts by obtaining 256 encryptions that only differ in a single byte of m(1), and that take on all values for that particular byte. Instead of applying MixColumn and then adding in K (5), first add in K (5)" and then apply MixColumn. It is easy to see that any byte of b (4) depends on the cipher text, four bytes from K(6), and one byte from K (5)". These five key bytes can be guessed. Compute the value of b (4) byte

for 256 encryptions and check whether the sum is zero. For each group of 256 plain texts, it rejects 255/256 of all wrong key guesses. A total of nine key bytes are guessed, so 10 or more groups of 256 encryptions are needed to find the key. This attack can be extended to 7 rounds for 192 and 256-bit keys. The 16 bytes of the last round key can be guessed. This adds 128 bits to the key guessing.

CONCLUSIONS

A new security protocol has been designed for better security. It is a combination of both symmetric and asymmetric cryptographic techniques. It provides three cryptographic primitives– integrity, confidentiality and authentication. It makes use of Elliptic curve cryptography(ECC) to encrypt, RSA to authenticate and MD5 to check for integrity. Instead of ECC, symmetric cipher (AES –Rijndael) can be used to encrypt. The square attack on AES Rijndael can be extended to 7 rounds by guessing the 16 bytes of the last round key. To enhance the Encryption technique, security aspects of key management need to be looked into more detail.

REFERENCES:

[1] Ramaraj, E and Karthikeyan, S, " A Design of Enhanced Security Protocol for Wireless Communication using Hybrid Encryption Technique (AES – Rijndael and RSA)", Indian Journal of Computing Technology, pp 22-29, May, 2006.

[2] William Stallings, " Cryptography and Network Security – Principles and Practices", 3rd Edition, Pearson Education Asia – 2003.

[3] Arjen K. Lenstra, " Selecting Cryptographic Key Sizes", volume14, Issue4, Journal of Cryptography, http://www.springerlink.com/content/6d8hb94aenemfm5g, pp 255-293, 2002.

[4] James Nechvatal, Elaine Barker and Lawrence Bassham, "Report on the Development of the Advanced Encryption Standard (AES), Computer and Security Division National Institute of Standards and Technology (NIST), US Dept. of Commerce.

[5] Rivest, R., " The MD5 message-digest algorithm", RFC 1321, 1992.

AUTHORS:

K .Seena Naik (Ph.D)

Dr G.A Ramachandra

M.V.Bramahananda Reddy M.Tech(Ph.D)