DESIGN OF NEW SECURITY ALGORITHM
USING HYBRID CRYPTOGRAPHY ARCHITECTURE

Manali J Dubal, Mahesh T R, Pinaki A Ghosh
Dept. of Computer Engineering & Information Technology,
Atmiya Institute of Technology & Science, Rajkot, Gujarat
E-mail: manali@dubbal.in, admin@maheshtr.in, pinaki@pinaki.in

Abstract— **A computer network is any set of computing nodes which has the ability of exchanging data by interacting with each other meaningfully, allowing resource sharing in a proper manner. The collection of computers is interconnected by communication channels, which need to be secure for better information exchange. This field of networking consists of specialist area of network security adopted by network administrator to prevent and monitor unauthorized access, modification and denial of computer network [10]. To combat the growing problem, security professionals are in search of better protection. Security Attacks compromises the security and hence various Symmetric and Asymmetric cryptographic algorithms have been proposed to achieve the security service in the proper manner, such as Authentication, Confidentiality, Integrity, Non-Repudiation and Availability. These algorithms are required to provide data security and users authenticity. To improve the strength of these security algorithms, a new security algorithm can be designed using combination of both symmetric and asymmetric cryptographic techniques [4]. This algorithm provides three cryptographic primitives such as integrity, confidentiality and authentication. This can be achieved by the combinatorial effect of Elliptic Curve Cryptography implemented by ECDH and ECDSA, Dual RSA and Hash algorithm implemented by Message Digest 5. This new security algorithm has been designed for better security with integrity using a combination of both symmetric and asymmetric cryptographic techniques.**

Keywords – Network Security; Elliptic Curve Cryptography; Dual RSA; Message Digest 5; ECDH; ECDSA

I. INTRODUCTION

Cryptography is the science which uses mathematics to encrypt and decrypt data. This science enables you to store sensitive information or transmit it across insecure networks so that it cannot be read by anyone except the intended recipient.

While cryptography is the science of securing data, cryptanalysis is the science of analyzing and breaking secure communication. The science of Classical cryptanalysis involves an interesting combination of analytical reasoning, application of mathematical tools, pattern finding, patience, and determination. Cryptanalysts are also called attackers. Cryptology embraces both cryptography and cryptanalysis.

Cryptography basically works on the principles of mathematics that generate different algorithms known as Cryptographic Algorithms.

A cryptographic algorithm, or cipher, is a mathematical function used in the encryption and decryption process.

A cryptographic algorithm works in combination with a key — a word, number, or phrase — to encrypt the plaintext. The same plaintext encrypts to different cipher text with different keys. The security of encrypted data is entirely dependent on two things: the strength of the cryptographic algorithm and the secrecy of the key [10].

A cryptographic algorithm, plus all possible keys and all the protocols that make it work comprise a cryptosystem. In conventional cryptography, also called *secret-key* or *symmetric-key* encryption, one key is used both for encryption and decryption. In asymmetric cryptography, the encryption and decryption keys are different on both the sides.

A key is used in conjunction with a cipher to encrypt or decrypt text. The key might appear meaningful, as would be the case with a character string used as a password, but this transformation is irrelevant, the functionality of a key lies in its being a string of bits determining the mapping of the plain text to the cipher text [10].

II. TYPES OF CRYPTOGRAPHIC ALGORITHMS

A. ECC (Elliptic Curve Cryptography)

While using **ECC**, we deal with various properties of points on curve, and functions. The only aim is to use elliptic curves as an encryption tool which converts the information *m* into the point P on the curve E [2]. Assuming that the data *m* is already in the integer or any ASCII format, we have a curve $E : y^2 = x^3 + ax + b \pmod p$. This will work only if $m^3 + am + b$ is a square modulo p. Since only half of the numbers modulo p are squares, we only have about half a chance of this occurring. Thus, we embed the information m into a value that is a square.

We assume some value K such that 1/2K is an acceptable failure rate for embedding the information into a point on the curve. Also, we make sure that for the value of K, $(m + 1) K < p$.

Now, let $xj = mK + j$ for $j = 0, 1, 2, \ldots, K - 1$, we compute $x3j + axj + b$. The square root yj (mod p) is calculated. If there is a square root, we let our point on E representing m be $P_m = (xj, yj)$. So, for each value of j we have a probability of about 0.5 that xj is a square modulo p [1].

978-1-4244-8679-3/11/$26.00 ©2011 IEEE

Thus, the probability that no xj is a square is about 1/2K, which was the acceptable failure rate. In this way, the rate of failure of embedding the information in E decreases.

B. ECDH – Elliptic Curve Diffie Hellman

Using **ECDH** in the hybrid algorithm generates the key which is far secured than any other algorithm. The key generated is kept as a shared key between two parties, such that, it can be used for the private key algorithms [2].

Both ends have a key pair consisting of a private key d which is less than a random number n, and a public key Q = d * G, where G is the Generator point of the elliptic curve. Here, (dA, QA) is the private key - public key pair of A and (dB, QB) be the private key - public key pair of B [13]. The computation goes as,

1. The end A computes K = (xK, yK) = dA * QB
2. The end B computes L = (xL, yL) = dB * QA
3. Since dAQB = dAdBG = dBdAG = dBQA.
4. Hence the shared secret is xK

The security in encrypting the key is that is practically impossible to find the private key dA or dB from the public key K or L.

C. ECDSA – Elliptic Curve Digital Signature Algorithm

The **ECDSA** is known to be the variant of DSA, which sends a signed message from A to B, on the elliptic curve parameters [1]. For signing a message m by sender A, using A's private key dA

1. Calculate e = HASH (m)
2. Select a random integer k from [1, n − 1]
3. Calculate r = x1 (mod n), where (x1, y1) = k * G
4. Calculate s = k − 1(e + dAr) (mod n)
5. The signature is the pair (r, s)

D. DUAL RSA

The RSA decryption computations are performed in p and q and then combined via the Chinese Remainder Theorem (CRT) to obtain the desired solution in Z_N, instead of directly computing the exponentiation in Z_N. This decreases computational costs of decryption in two ways. First, computations in Zp and Zq are more efficient than the same computations in Z_N since the elements are much smaller. From Lagrange's Theorem, we can replace the private exponent d with dp = d mod (p - 1) for the computation in Zp and with dq = d mod (q - 1) for the computation in Zp, which reduce the cost for each exponentiation when d is larger than the primes. It is common to refer to dp and dq as the CRT-exponents [4].

Since the method requires knowledge of p and q, the key generation algorithm needs to be modified to output the private key (d, p, q) instead of (d, N). Given the private key (d, p, q) and a valid cipher text C ε Z_N, the CRTdecryption algorithm is as follows:

1) Compute $Cp = C^{dp} \bmod p$
2) Compute $Cq = C^{dq} \bmod q$
3) Compute $M_0 = (Cq - Cp).\ p^{-1} \bmod q$
4) Compute the plaintext $M = Cp + M_0 . p$

When the primes p and q are roughly the same size, the computational cost for decryption using CRT-decryption is theoretically 1/4 the cost for decryption using the original method [7]. Using RSA-Small-e along with CRT-decryption allows for extremely fast encryption and decryption that is at most four times faster than standard RSA.

E. MD5 Algorithm

MD5 consists of 64 of these operations, grouped in four rounds of 16 operations. F is a nonlinear function; one function is used in each round. Mi denotes a 32-bit block of the message input, and Ki denotes a 32-bit constant, different for each operation. s is a shift value, which also varies for each operation.

MD5 processes a variable length message into a fixed-length output of 128 bits. The input message is broken up into chunks of 512-bit blocks; the message is padded so that its length is divisible by 512. The padding works as follows: first a single bit, 1, is appended to the end of the message. The remaining bits are filled up with a 64-bit integer representing the length of the original message [5].

The main MD5 algorithm operates on a 128-bit state, divided into four 32-bit words, denoted A, B, C and D. These are initialized to certain fixed constants. The main algorithm then operates on each 512-bit message block in turn, each block modifying the state. The processing of a message block consists of four similar stages, termed rounds; each round is composed of 16 similar operations based on a non-linear function F, modular addition, and left rotation [12]. Many message digest functions have been proposed and are in use today. Here are just a few like HMAC, MD2, MD4, MD5, SHA, SHA-1. Here, we concentrate on MD5, one of the widely used digest functions.

III. HYBRID ALGORITHM ARCHITECTURE

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. This new security protocol has been designed for better security using a combination of both symmetric and asymmetric cryptographic techniques.

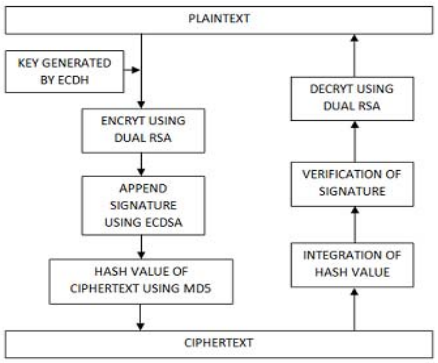

Figure 1. Hybrid Architecture for Cryptography

As shown in the figure, the Symmetric Key Cryptographic Techniques such as Advanced Elliptic Curve Cryptography and MD5 are used to achieve both the Confidentiality and Integrity. The Asymmetric Key Cryptography technique, Dual RSA used for Authentication.

The above discussed three primitives can be achieved with the help of this Security Protocol Architecture. The Architecture is as shown in the **Figure 1**. As shown in the figure, the Symmetric Key Cryptographic Techniques such as Elliptic Curve Cryptography and MD5 are used to achieve both the Confidentiality and Integrity. The Asymmetric Key Cryptography technique, Dual RSA used for Authentication. The new Security Protocol has been designed for better security. It is a combination of both the Symmetric and Asymmetric Cryptographic Techniques. It provides the Cryptographic Primitives such as Integrity, Confidentiality and Authentication.

The given plain text can be encrypted with the help of key that is generated by the type Elliptic Curve Cryptography, i.e., ECDH. The encryption algorithm used is Dual RSA, which takes as the original information and the key. The derived cipher text is appended with the digital signature for more authentication, generated by the ECDSA algorithm. Simultaneously, the hash value of this encrypted cipher text is taken through the Message Digest 5 algorithm. Now the generated cipher text and the signature can be communicated to the destination through any secured channel. On the other side, i.e., on decryption end, the hash value is first evaluated and integrated. This is compared with the signature, for the verification of the digital signature appended at the end of message. Thereafter, the decryption of cipher text is done by Dual RSA. Hence, the plaintext can be derived.

The intruders may try to hack the original information from the encrypted messages. He may be trapped both the encrypted messages of plain text and the hash value and he will try to decrypt these messages to get original one. He might get the hash value and it is impossible to extract the plain text from the cipher text, because, the hash value is derived from the Dual RSA and appended signature, and the plain text is encrypted with Dual RSA, with the key generated by ECDH algorithm. Hence, the message can be communicated to the destination with highly secured manner.

The new hash value is calculated with MD5 for the received originals messages and then it is compared with decrypted hash message for its integrity. By which, we can ensure that either the original text being altered or not in the communication medium. This is the primitive feature of this hybrid protocol.

CONCLUSION

In this paper, we proposed a robust and lightweight protocol that has security function using blind factor and ECC scheme. Our tag lightweight protocol may solve several problems as practical implement, short response time and efficient computation and the strength of cryptosystem.

The attractiveness of ECC, compared to RSA, is that it appears to offer better security for a smaller key size, thereby reducing processing overhead. The benefits of this higher-strength per-bit include higher speeds, lower power consumption, bandwidth savings, storage efficiencies, and smaller certificates. These advantages are particularly beneficial in applications where bandwidths, processing capacity, power availability or storage are constrained.

The new Hybrid Public Key Cryptographic algorithm has been developed for better performance in terms of computation costs and memory storage requirements. From the output, it is noted that Dual-RSA and ECC, improved the performance of algorithm in terms of computation cost and memory storage requirements.

ACKNOWLEDGMENT

The authors are grateful to the principal and management of Atmiya Institute of Technology & Science for extending all the facilities and constant encouragement for carrying out this research work. Also they heartily thank the IACSIT organization for giving me an opportunity to present the paper.

REFERENCES

[1] Darrel Hankerson, Julio Lopez Hernandez, Alfred Menezes, *Software Implementation of Elliptic Curve Cryptography over Binary Fields*, 2000, Available at http://citeseer.ist.psu.edu/hankerson00software.html

[2] Certicom, Standards for Efficient Cryptography, *SEC 2: Recommended Elliptic Curve Domain Parameters, Version 1.0*, September 2000, Available at http://www.secg.org/download/aid-386/sec2_final.pdf

[3] E. Jochemsz and A. May, "A polynomial time attack on standard RSA with private CRT-exponents", 2007.

[4] M. J. Hinek, "Another look at small RSA exponents," in *Topics in Cryptology-CT-RSA 2006*, ser. Lecture Notes in Computer Science, D. Pointcheval, Ed. New York: Springer, 2006, vol. 3860, pp. 82–98.

[5] Ravindra Kumar Chahar and et.al., " Design of a new Security Protocol", IEEE International Conference on Computational Intelligence and Multimedia Applications, pp 132 – 134, 2007.

[6] S. D. Galbraith, C. Heneghan, and J. F. McKee, "Tunable balancing of RSA", 2005. Updated version of ACISP 2005.

[7] D. Bleichenbacher and A. May, "New attacks on RSA with small CRTexponent in Public Key Cryptography", PKC 2006, volume 3968 of Lecture Notes in Computer Science, pages 1–13. Springer-Verlag, 2006.

[8] B. den Boer and A. Bosselaers, "Collisions for the compression function of MD5", Advances in Cryptology, Eurocrypt „07, pages 293-304, Springer-Verlag, 2007.

[9] N. Gura, A. Patel, A. Wander, H. Eberle, and S.C. Shantz, "Comparing Elliptic Curve Cryptography and RSA on 8-bit CPUs". Proceedings of Workshop on Cryptographic Hardware and Embedded Systems (CHES 2004), 6th International Workshop, pages 119–132, 2004.

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

[11] Schneier, B., " Applied Cryptography", 2nd Edition, Wiley, 1996.

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

[13] D. Johnson, "ECC, Future Resiliency and High Security Systems," Certicom White Paper, March 1999.