IJISET - International Journal of Innovative Science, Engineering & Technology, Vol. 2 Issue 4, April 2015.
www.ijiset.com
ISSN 2348 – 7968

Studying security protocol architecture based on cryptography algorithms

*Mohammad Trik[1,2], Sam Jabbehdari [3] Fardin Mohammadi Darvandi[1,2] and Azad shojaei [1,2]

[1,2]Young Researchers and Elite Club, Sardasht Branch, Islamic Azad University, Sardasht, Iran
[1,2]Young Researchers and Elite Club, Urmia Branch, Islamic Azad University, Urmia, Iran
[3] Computer Engineering Department, North Tehran Branch, Islamic Azad University, Tehran,Iran

Abstract

This research paper considers recent activities associated with hybrid encryption protocol and its functions in designing a hybrid protocol for hybrid encryption-based online interactions. A new security protocol for online transaction can be symmetric or asymmetric using a combination of encryption techniques; integrating these two techniques is known as hybrid or integrated encryption technique. This protocol considers three major principles in encryption including integrity, reliability, and biometric. Each encryption principle provided by symmetric or asymmetric encryption techniques. Symmetric encryption algorithms are faster than asymmetric encryption algorithms; so, once these two algorithms are properly applied in combination, it will be promising to provide high security and speed. This paper attempts to capsulate all applied developments in designing new security protocol for online transactions; however, it is extremely significant based on its major effect on today's occupations. Therefore, it is ideal to transfer data with high security and in a short time. Now, different encryption algorithms have proposed providing a high security for controlled networks data. These algorithms provide data security and user biometric. A new security protocol is also introduced for better security using a combination of both symmetric and asymmetric encryption algorithms.

Keywords: *Hybrid encryption, ECC, AES, RSA, binary, MD5*

1. Introduction

Cryptography is a science that uses mathematics for data encoding and decoding. This science allows you to store critical information and or transform it through networks (channels) that are not readable to individual unless it is the receiver of that data. In common cryptography, which is called symmetric-key or key-encryption, a key is used for encoding and decoding. In asymmetric cryptography, encoding and decoding keys are different in both sides.

Hybrid cryptography is a combination of symmetric and asymmetric techniques. Hybrid cryptography is extremely efficient in providing high security, as disregarding symmetric-key encryption techniques; it will be solved once a cryptography mechanism is used. Thus, when both types of algorithms apply in architecture protocol, the obtained new protocol architecture shows greater stability against errors such that providing a high security level [2].

Electronic commerce transactions and M-commerce are explosively growing. The success of such transactions is secured depending on how they are done. Primary requirements of e-commerce and m-commerce transactions include privacy, biometry, integrity, as well as redundancy [14]. Cryptography helps us to meet these requirements. Today, different developed encryption algorithms are used [7, 15].

2. Various cryptography algorithms

There are two cryptography algorithms: symmetric and asymmetric.The problem of symmetric-key cryptography techniques are solved using symmetric cryptography mechanism. Therefore, once both algorithms applied into architectural protocol, the new protocol architecture is more secured versus attacks i.e. providing a high-level of security [2]. Applied algorithms are as follows:

2.1 Elliptical Curve Cryptography

Different characteristics of curve points and functions are used for elliptical curve cryptography [11]. Thus, a common computing task when these curves are used, is finding an approach to transform information m to a point P on curve E as an encryption tool. Let information m are written in figures. There are many approaches, among which a simple one is placing letters as a=0 , b=1, and c=2.

Other methods like Ski can also be used. Now, if we have E:y2=x3+Ax+B(mod p). then we put m=x. However, this case only works when there m3+Am+B is a root module p. Since, only half of modules are square, there is 50% chance of occurrence. Therefore, we will try to integrate m data in a square-format value [9].

Pick some K such that 1I2K is an acceptable failure rate for embedding the information into a point on the curve. Also, make sure that (m + I)K < p. Let xj = mK + j for j = 0, 1, 2, ..., K - 1 Compute x3j + Axj + B. Calculate its square root yj (mod p), if possible. If there is a square root, we let our point on E representing m be Pm = (xj , yj) If there is no square root, try the next value of j[4,5].So, for each value of j we have a probability of about 1/2 that xj is

ISSN 2348 – 7968

a square modulo p. Thus, the probability that no xj is a square is about 1/2K, which was the acceptable failure rate [6]. In most common applications, many real problems may damage a message effort similar to computer error or electricity. Accepting 16 particular cases of an error (due to an uncontrollable phenomenon) caused to achieve an acceptable error rate from process for a controllable property. However, this particular process is not applied in our algorithm [1].

2.2 Advanced encryption standard algorithm (AES)

Rejdenal proposal for AES defines an encryption in which block and key length independently equal to 128, 192, and 256 bits [4].

AES algorithm has four different steps as follows:

1. Replacement bytes: S box (replacement box) is used for byte-to-byte replacement.
2. Shift rows: a simple hybrid
3. Combine columns: a diffusion layer that applies limited field mathematics.
4. Add round key: a simple inter-reverse XOR from current box with developed key [15].

2.3 RSA and binary RSA

RSA encryption computations can be done, in practice, in p and q; then, it will be combined to CRT theorem such that a z n optimal solution attain rather than direct computing of exponent in Z N. This leads to reduced decoding computations' costs through two ways. First, computations are in Z p, and Z p is much more efficient than Z N in computations, since it has smaller elements. Second, according to Lagrange theorem, it is possible to integrate hidden exponent d with dq=d Mod (q-1) for computation in Z p; this leads to reducing each exponent cost when d is larger than variable cost. It is common to consider dp and Q as CRT exponents. The first method of applying CRT for decoding was proposed by Coroner and Cozies Coir [3, 7].

Since this method requires p and q knowledge, the key algorithm must change (d, p, q) instead of (d, N) in order to send the main key to output. According to private key and encrypted script C Z N, CRT encryption algorithm is as follows:

1. Calculating Cp=Cdp mod p
2. Calculating Cq=Cd mod q
3. Calculating M0=(Cq-Cp).p-1 mod q
4. Calculating aggregated text M = Cp + MO. p.

This version of CRT decoding is the same as Garner algorithm for Chinese remainder theorem applying in RSA. If key production algorithm changes in to output (Dp, dq, p, q, p-1, mod q) for giving private key, CRT decoding computational cost determined by modular exponents in algorithm steps 1 and 2. When p and q are the same size (half of module size), decoding computational cost using CRT encryption (without parallelism) will be theoretically decoding cost using main method [8]. Applying RSA with CRT decoding, allowing fast encoding and decoding, algorithm standardization occurs four times faster than RSA [11].

2.4 Message Digest Algorithm (MD5)

MD5 embraces 64 cases of these operations categorized into four 16-operation classes. F is a nonlinear function; one function is used per round. MI is a 32-bit block of message input, and Ki is a 32-bit block of message unit, and Ki is also a 32-bit constant different in each operation. S is a shift value retrieving for each operation. MD5 is processing a message with variable length in an output with constant length of 128 bit. Input message divides into some classes of 128-bit blocks. This message integrated such that its length can be divided by 512 [6]. False records work as follows:

A singular bit, 1, initially added to the end of message. Next, there are many zero areas, which are necessary for extending message length to 64 bits and less than a multiple of 5. Remaining bits filled with 64-bit integer showing the main message length [5].

Main MD5 algorithm operates on a 128-bit state divided into 21-bit words symbolizing by A, B, C, and D. These values are initialized based on particular constants. Then, main algorithm applies in each 512-bit message block changing block status. Processing a message block contains 4 similar steps naming round; each round consists of 16 similar operations based on F nonlinear function that is used today. These functions include HMAC, MD2, MD4, SHA, and SHA-1. This paper focuses on MD5, which uses many digest functions [2].

3.Earlier security protocols architecture and associated issues

After searching IEEE Xplore, an experimental paper named Designing Security Protocol was achieved. In this protocol, experimental scholars proposed a new protocol for online transaction created by using a combination (hybrid) of both symmetric and asymmetric cryptography technique [1]. This protocol provides three principles of cryptography-integrity, reliability, and biometry. This approach uses elliptic curve cryptography method for encoding, RSA algorithm for biometry, and MD-5 for studying integrity. Symmetric cryptography algorithms are fast comparing asymmetric cryptography algorithms such as RSA and elliptic curve cryptography.

Today, conversation significantly influences occupations. Therefore, it is ideal to have high-secured conversational data. Now, there are several different types of cryptography algorithms providing high security for data of controlled networks. These algorithms meet data

ISSN 2348 – 7968

security and user biometry. A new security protocol is also designed for better security, which applies both symmetric and asymmetric cryptography techniques like hybrid cryptography.

The cryptography technique used in this protocol is a combination (hybrid) of symmetric and asymmetric cryptography techniques that uses elliptic curve cryptography method for encryption, RSA algorithm for biometry, and MD-5 for integrity.

This architecture concerns properly selecting algorithms. As security risks are increasingly growing today; hence, it is necessary to update and upgrade protocol architecture in order to improve cryptography technique and consider, in detail, power levels of key management aspects.

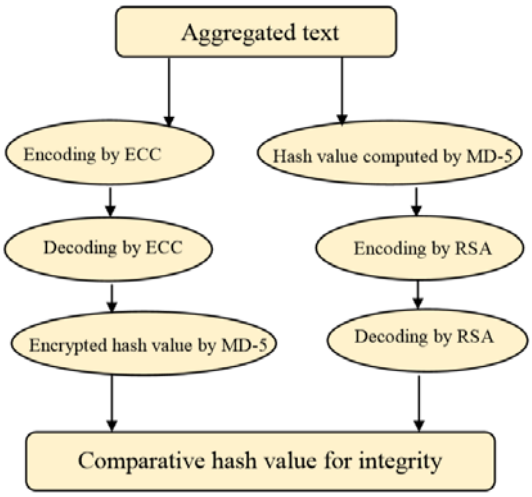

Fig 1: Basic structure of security protocol

To eliminate redundancies from this research paper, another paper named 'Designing a new security protocol through hybrid cryptography architecture' was also studied. The paper introduced a new better-secured protocol comparing to previous method designed as a combination of the two symmetric and asymmetric cryptography techniques.

This protocol provides three cryptography-integrity, reliability, and biometry principles obtained through elliptic curve cryptography, binary RSA algorithm, and digestive message MD-5. Elliptic curve cryptography is used for encryption, and binary RSA and MD-5 are applied for biometry and integrity, respectively.

The new security protocol design focuses on better security and integration through using a hybrid of symmetric and asymmetric cryptography techniques. The second research paper simply compared usual RSA and new binary RSA and used hybrid architecture to distinguish new security protocol design. This comparison demonstrates that binary RSA outperforms RSA in terms of computational costs and memory storage requirements. Moreover, this approach is called RSA-CRT, as it is applied in Chinese remainder theorem and CRT is used for decoding. Output shows that binary RSA leads to improved efficiency of RSA in terms of computational costs and memory storage requirements. Developed designing process of a security protocol is illustrated as follows.

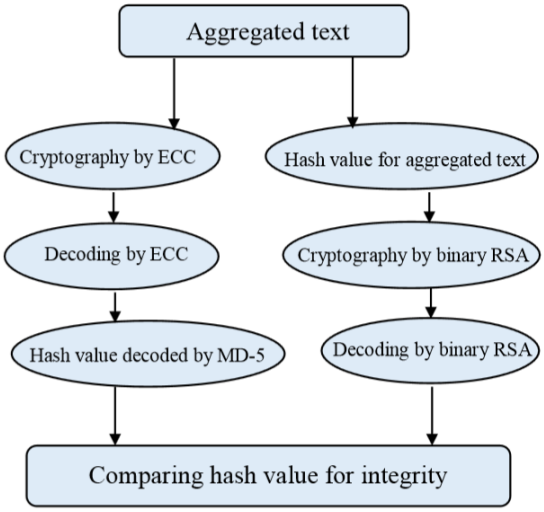

Fig 2: Recent security protocol architecture

In this way, parallelism value obtains. CRT decoding can be implemented ¼ times faster than original RSA. Therefore, once researcher intends to apply binary RSA in protocol architecture, a new security protocol emerges in comparison to previous research paper protocol [3].

4. Proposed architecture

The proposed hybrid security protocol is highly secured, especially for attacks, and is efficient in term of time. The aggregated text encrypted by help of AES (advanced encryption standard), and derived decoded text converses to destination through a secured channel. Hash value simultaneously converses by MD5 for that aggregated text decoded by AES. The hash value encrypted by binary RSA and decoded message of the hash value is also sent to destination. Now, hash value of encoded aggregated text is computed by MD5 at receiving end; then, it will be compared to hash value of aggregated text at sending end computed for integrity. Thus, it shows that whether original text can be changed through transferring medium or not.

ISSN 2348 – 7968

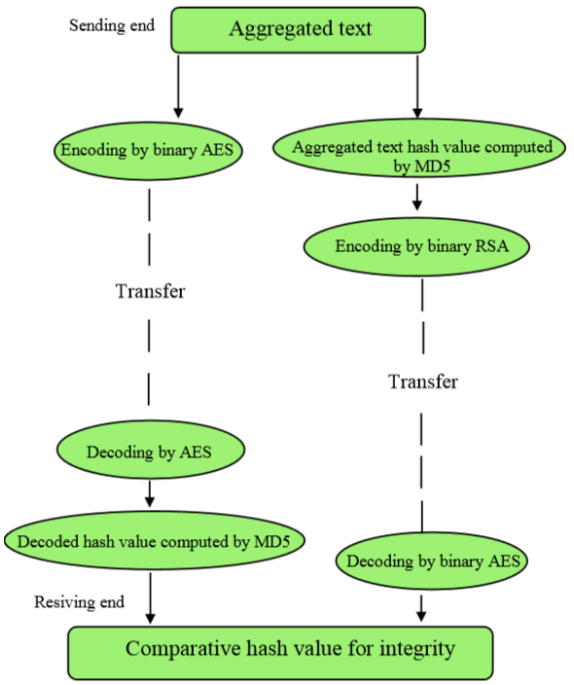

Fig 3: Proposed hybrid security protocol architecture

The attacker may try to hack original information of encoded messages. However, it is may be possible to trap both encrypted messages of original text and hash value, decoding messages (to get the original message) is impossible. Therefore, the message is highly secured conversed with destination. To evaluate the proposed architecture efficiency, both architectures of the security protocol are initially implemented by using Java 1.6; then, they run on a 5-core computer Windows 7. Standard dataset is an input for implementing both architectures.
Following table represents mean execution time of both implementations. More than a thousand samples of implemented security architecture are created through dividing total execution time followed by implementing the architecture by 1000.

Serial Number	Execution time (ms)	
	Recent architecture	Proposed architecture
1	**1306**	**642**

5.Results and conclusion

A new hybrid security protocol is designed for better security. Proposed hybrid security protocol is more secured against root, fundamental attacks, which is due to applying AES algorithm. Root attack on AES may last 7 rounds, and can guess round 16 in the last key. The proposed hybrid security algorithm may contain many problems about practical implementation with little response time, as well as efficient computation and powerful encoding systems.
AES desirability originates from providing better security level for smaller keys as well as reduced processing overhead. Advantage of this higher power includes higher speed and less energy consumption, reduced bandwidth, storage efficiency, and smaller acknowledgements per bit. Such advantages are practical in applications with limited bandwidth, computational capability, energy, and storage space. Hybrid protocol architecture can be easily upgraded; thus, it can be more secured and efficient against attacks.

References

[1] Ramaraj, E and Karthikeyan, S, " A Design of Enhanced Security Protocol for Wireless Communication using Hybrid Encryption Technique (AES - Rijndael and RSA)", India.
[2] Rivest, R., " The MDS message-digest algorithm", RFC 1321, 1992.
[3] Ravindra Kumar Chahar. Goutam Datta.Prof.Navin Rajpal. " Design of a new Security [Protocol". IEEE International Conference on Computational Intelligence and Multimedia Applications, pp 132 - 134, 2007.
[4] S.Subasree,N.K.Sakthivel,"Design of a new security protocol using hybrid cryptography algorithm",lJRRAS 2,feb 2010.
[5] William Stallings, " Cryptography and Network Security - Principles and Practices", 3rd Edition, Pearson Education Asia - 2009.
[6] Schneier, B., " Applied Cryptography", 2nd Edition, Wiley, 1996.
[5] Hung-Min Sun,. "Dual RSA and its Security Analysis", IEEE Transaction on Information Theory,Aug 2007, pp 2922 - 2933,2007
[9] Blake I, G. Seroussi and N. Smart (eds).Advances in Elliptic Curve Cryptography ,Cambridge University Press, 2005
[10] Certicom whitepaper, Remarks on the Security of the Elliptic Curve Cryptosystem .. September 2006.
[II] 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.
[12] R.Schoof,Elliptic curves over finite fields and the commutation of squareroots modp.Math.Comp. 1985,44: 483-494
[13] Rivest R L,Adleman L,Detrouzos M L On Data Banks and Privacy Homomorphism[M]. Demilio R .Fourldations of Secure Computation [C]. New York: Academin Press. 1978: 169-179.
[14] Domingo-Ferrer J, Herrera-Joancomarti J. New Privacy homomorphism and Applications. Information Processing Letters, 1996,60(5): 277-282 .
[15] Dabida G I,WelisD B,Kam J B.A database encryption system with subkeys[J].ACM Transaction on Database Systems, 1981,6 (2): 192-199.