American Journal of Applied Sciences 9 (3): 289-292, 2012
ISSN 1546-9239

Secure Hybrid Mode-Based Cryptosystem

[1]Ismail, E.S. and [2]S. Baharudin
[1]School of Mathematical Sciences, Faculty of Science and Technology,
Universiti Kebangsaan Malaysia, 43600 UKM Bangi, Selangor, Malaysia
[2]Department of Sciences and Mathematics,
College of Engineering, Universiti Tenaga Nasional,
43009 Kajang, Selangor, Malaysia

Abstract: Problem statement: A cryptosystem provides two parties; a sender and a receiver to communicate interactively via an insecure channel in which, the sender is able to send any confidential message, document or data in a disguised form to the intended receiver. Upon receiving the disguised message, the receiver converts it to the intelligible message using his secret key. The security of the existing cryptosystems was based on a single hard problem such as factorization, discrete logarithm, quadratic residue, or elliptic curve discrete logarithm. Although these schemes appear secure, one day in a near future they may be broken if one finds a solution of a single hard problem. **Approach:** To overcome the disadvantage of using a single hard problem, we developed a secure hybrid mode-based cryptosystem based on the two well-known hard problems; factoring and discrete logarithm. We inject the element of the hard problems into our encrypting and decrypting equations respectively in such a way that the former equation depends on two public keys whereas the latter depends on two corresponding secret keys. **Results:** The new cryptosystem is shown heuristically secure against various algebraic attacks. The efficiency analysis confirms that our scheme only needs $3T_{exp}+T_{hash}$ time complexity for encryption and $2T_{exp}$ time complexity for decryption and this magnitude of complexity is considered minimal for multiple hard problems-like cryptosystems. **Conclusion:** The newly developed hybrid mode based-cryptosystem provides greater security level than that schemes based on a single hard problem. The enemy or adversary has to solve the two problems simultaneously which is unlikely to happen in order to read any secret message.

Key words: Cryptology, cryptography, cryptosystem, hard problems

INTRODUCTION

The security of a cryptosystem depends heavily on a hard mathematical problem used in the system. Some novel hard problems that have been used in many cryptosystems were discrete logarithms (ElGamal, 1985), factoring (Rivest *et al*., 1978), elliptic curve discrete logarithm (Koblitz, 1987; Miller, 1986), residuosity (Rabin, 1979) and many other problems. Although such problems remain hard today, it is conjectured that one day in the future those problems could be easily solved. As soon as this occurs, cryptosystems based on such problems will no longer be secure. This scenario has led designers to create cryptosystems based on hybrid mode problems (Harn, 1994; Elkamchouchi *et al*., 2004; Baocang and Yupu, 2005; Ismail and Hijazi, 2011). The major advantage of doing this is that these types of schemes provide greater level of security than that the schemes based on only a single hard problem. As a result, an adversary needs a longer period of time in order to break the hybrid mode-based cryptosystems since it is very unlikely for the adversary to obtain the solutions of these problems simultaneously. Developing of such system is still a field in need of cultivation. It is always one aims to have system with the following criteria: (1) the system uses only one pair of public and private keys; (2) each user uses common arithmetic modulus; and (3) the system uses the most novel two hard mathematical problems for its security base.

In this study, we created a new hybrid mode-based cryptosystem using factoring and discrete logarithm problems. With the greater level of security confirmed, we showed that the performance of the scheme requires acceptable time complexity unit operations in both encryption and decryption algorithms, which makes the system implementable

Corresponding Author: Ismail, E.S., School of Mathematical Sciences, Faculty of Science and Technology,
Universiti Kebangsaan Malaysia, 43600 UKM Bangi, Selangor, Malaysia

for real world applications. Next, our new system also enjoys the three mentioned criteria.

Some notations and parameters: Throughout the study, we use the following notations and parameters unless otherwise specified:

- Two large strong random primes p and q which are safe primes (Gordon, 1984) and set the system modulus as $n = pq$
- A phi-Euler function $\phi(n) = (p-1)\ (q-1)$
- A primitive element, g in multiplicative group $Z_n^* = \{z|\gcd(z,n) = 1\}$ with order n satisfying $g^{n-1} = 1 \pmod n$ where gcd (a,b) denotes the greatest common divisor of a and b
- A cryptographic hash function h(.) (Schneier, 1996) whose maps an arbitrarily length of string to an output of a t-bit length and we assume here that $t = 128$

MATERIALS AND METHODS

We present a new cryptosystem based on hybrid-mode problems; factoring and discrete logarithms. The scheme is made up of three phases namely Initialization, Encryption and Decryption. In Initialization phase, the two pairs of public and private keys of users are calculated using the user's parameters n, $\phi(n)$ and g. The generated public keys will be then published in an accessible public key directory while the private keys are kept secret to the owners. In Encryption phase, an encrypted message is developed using the receiver's public key and sender's commitment of secret number. This is done by first get the message hashed using the appropriate cryptographic hash function h(.). This function determines a fixed length of output by hashing any arbitrarily length of input. The encrypted message is then sent to the legal receiver. In Decryption phase, upon obtaining the encrypted message, the receiver recovers the original message by using his own private keys and without these keys no one can learn the original message.

Initialization phase: The user or receiver derives his public and private keys as follows:

- Select at random two integers $3 \le e, x < n$ from Z_n^*
- Calculate $d = e^{-1} \bmod \phi(n)$
- Compute $y = g^x \bmod n$

The public keys are formed by (e, y) and can be accessed in the public directory and the private keys are given by (d, x) and are kept secret by the receiver.

Encryption: The sender encrypts his original message, m as follows:

- Pick at random an integer $c < n$ from Z_n^*
- Hash the original message to obtain h(m)
- Computes $c_1 = h(m)^e + y^c \pmod n$
- Calculate $c_2 = g^c \pmod n$

Send the encrypted message (c_1,c_2) to the receiver.

We compute the first component of encrypted message, c_1 with two public keys e and y as if we disguise the original message 'twice' and this is one of the techniques to realize the hybrid mode-based cryptosystem.

Decryption: The receiver decrypts the obtained encrypted message (c_1,c_2) as below. Compute the following:

- $(c_1 - c_2^x)^d = h(m) \bmod n.$

RESULTS

We discuss our results according to the following criteria:

- Validation of the new cryptosystem
- Security analysis
- Efficiency performance

To validate the newly developed cryptosystem, we prove that the decrypting equation is always true for any corrected encrypted message (c_1, c_2).

For security consideration, we use a technique from heuristic security to show that the scheme is secure. We do this by delivering the scheme to the literature for attacks. We consider common possible attacks for cryptosystem by which an adversary (Adv) may try to take down the new scheme. In particular, we define each attack and give the corresponding analysis of why this attack would fail.

For efficiency performance, we evaluate the time complexity for both phases; encryption and decryption in terms of various operation units. Finally we compute the communication cost of overall performance of the scheme.

Validation: We validate our new scheme by proving the following theorem.

Theorem: If the algorithms of Initialization and Encryption run smoothly, then the decryption process of the encrypted message in decryption is correct.

Proof: The decrypting equation is true for all encrypted message (c_1, c_2) since

$$(c_1 - c_2^x)^d = (h(m)^e + y^c - g^{cx})^d = (h(m)^e + g^{xc} - g^{cx})^d$$
$$= h(m)^{ed} = h(m) \bmod n.$$

Security attack: We show that our scheme is heuristically secure by considering the following common algebraic attacks.

Attack 1: Adv tries to obtain the private keys from the corresponding public keys in the system. In this case, Adv needs to solve $ed = 1 \bmod \phi(n)$ and $y = g^x \bmod n$ for d and x respectively. This is impossible due to the hardness of solving factoring and discrete logarithms. The best way to factorize the modulus $n = pq$, is by using the number field sieve method (Lenstra *et al*., 1990). However, this method is just dependent on the size of modulus n and it is computationally infeasible to factor an integer of size 1024-bit and above. Next, to increase the security of our scheme, we must select strong primes (Diaz and Masque, 2005) to avoid attacks using special-purpose factorization algorithms. We also can achieve and maintain the same security level for discrete logarithm problem by selecting the modulus n = pq where (p-1)/2 and (q-1)/2 respectively are product of two 512-bit strong primes.

Attack 2: Say, the Adv collects t encrypted messages (c_{1i}, c_{2i}) where i=1,2,…,t. Adv then has the following system of equations $(c_{1i} - c_{2i}^x) = h(m_i)^e \bmod n$.

Note that, the above system contains t equations with t+1 variables; x and $h(m_i)$ and solving this gives us infinitely many solutions which is hardly to detect the true one.

Attack 3: Assume that the Adv successfully solves the factoring problem so that he knows the secret d. With this, he learns that $(c_1 - c_2^x) = h(m)^e \bmod n$.

From the above equation, to recover the original message h(m), one has to compute $(c_1\text{-}c_2^x)^d$ and this obviously can be done if one knows the secret number x. Since at this stage the discrete logarithm problem remains hard to solve then the Adv would fail.

Attack 4: Assume otherwise that the Adv is able to solve the discrete logarithm problem and hence obtain the secret integer x. He then recovers $h(m)^e$ via the relation $(c_1 - c_2^x) = h(m)^e \bmod n$.

It is clear that, Adv is only able to read the original message if he has the secret d.

Table 1: The performance of our new public key encryption scheme

Our new public key encryption scheme		
The number of keys	SK	2
	PK	2
Computational complexity	Encryption	$3T_{exp} + T_{hash}$
	Decryption	$2T_{exp}$
Communication cost	Encryption	2n
	Decryption	n

Efficiency performance: We now describe and determine the performance of our scheme in terms of number of keys used, computational complexity overhead and the communication costs. The measurement is determined using numbers or units. The following notations are used to analyse the performance of the developed scheme.

- SK and PK denote the number of private and public keys respectively
- T_{exp} is the time complexity taken for a modular exponentiation
- T_{mul} is the time complexity taken for a modular multiplication
- T_{hash} is the time complexity taken for performing a hash function and $|x|$ denotes the bit length of x

We neglect the time complexity for modular addition or subtraction and we assume that the probability of the bit being selected as 0 or 1 is 0.5. The efficiency of the new cryptosystem is summarized in Table 1.

From Table 1, the sender performs $720T_{mul} + T_{hash}$ time complexity for encryption and the receiver performs $480T_{mul}$ time complexity for decryption using the conversion $T_{exp} = 240T_{mul}$ (Koblitz *et al*., 2000). Finally the communication costs or size of parameters of the scheme is only $3|n|$.

DISCUSSION

The security of most of the designated cryptosystems was based on a single hard problem like factoring, discrete logarithm and elliptic curve discrete logarithm problems. These schemes are no longer secure if one day an enemy successfully finds a polynomial algorithm to solve the underlying problem. To prevent this, developing a scheme based on two hard problems is a good strategy. The enemy only can break this scheme if he can solve the two problems simultaneously and this is very unlikely to happen. If he manages to find a solution to one of the underlying hard problem, the scheme remains secure as the other problem remains hard to solve for at least another period of time. Our newly developed scheme is protected against the most common considering algebraic attacks. The performance analysis of the developed scheme requires only minimal and acceptable number of operations units in Encryption and Decryption phases and thus makes it very efficient.

CONCLUSION

We presented a secure hybrid mode-based cryptosystem using on factoring and discrete logarithms problems. The proposed scheme only requires $720T_{mul} + T_{hash}$ and $480T_{mul}$ respectively for encryption and decryption. Some possible algebraic attacks have also been considered and we showed that the scheme is heuristically secure from those attacks.

ACKNOWLEDGEMENT

We acknowledge the financial support received from University Kebangsaan Malaysia under the Research University Grant UKM-DLP-2011-028.

REFERENCES

Baocang, W. and H. Yupu, 2005. Public key cryptosystem based on two cryptographic assumptions. IEE Proc. Communi., 152: 861-865. DOI: 10.1049/ip-com:20045278

Diaz, R.D. and J.M. Masque, 2005. Optimal strong primes. Inform. Process. Lett., 93: 47-52. DOI: 10.1016/j.ipl.2004.09.015

ElGamal, T., 1985. A public key cryptosystem and a signature scheme based on discrete logarithms. Adv. Cryptol., 196: 10-18. DOI: 10.1007/3-540-39568-7_2

Elkamchouchi, H.M., M.E. Nasr and R. Esmail, 2004. New public key techniques based on double discrete logarithm problem. Proceedings of the 21th National Radio Science Conference, Mar. 16-18, IEEE Xplore Press, Cairo, Egypt, pp: 1-9. DOI: 10.1109/NRSC.2004.1321832

Gordon, J., 1984. Strong RSA keys. Elect. Letter, 20: 514-516. DOI: 10.1049/el:19840357

Harn, L., 1994. Public-key cryptosystem design based on factoring and discrete logarithms. IEE Proc. Comput. Digital Tech., 141: 193-195. DOI: 10.1049/ip-cdt:19941040

Ismail, E.S. and M.S. Hijazi, 2011. New cryptosystem using multiple cryptographic assumptions. J. Comput. Sci., 7: 1765-1769. DOI: 10.3844/jcssp.2011.1765.1769

Koblitz, N., 1987. Elliptic Curve Cryptosystems. Math. Comput., 48: 203-209.

Koblitz, N., A. Menezes and S. Vanstone, 2000. The state of elliptic curve cryptography. Design, Codes Cryptography, 19: 173-193. DOI: 10.1023/A:1008354106356

Lenstra, A.K., H.W. Lenstra, Jr., M.S. Manesse and J.M. Pollard, 1990. The number field sieve. Proceeding of the 22nd ACM Symposium on Theory of Computing, Baltimore, (TCB’ 90), Maryland, USA, 1990, pp: 564-572.

Miller, V.S., 1986. Use of elliptic curves in cryptography. Adv. Cryptol. Lecture Notes Comput. Sci., 218: 417-426. DOI: 10.1007/3-540-39799-X_31

Rabin, M.O., 1979. Digitalized signatures and public-key functions as intractable as factorization. Massachusetts Institute of Technology Cambridge, MA, USA. http://dl.acm.org

Rivest, R.L., A. Shamir and L. Adleman, 1978. A method for obtaining digital signatures and public-key cryptosystems. Mag. Commun. ACM, 21: 120-126. DOI: 10.1145/359340.359342

Schneier, B., 1996. Applied Cryptography: Protocols, Algorithms and Source Code in C. 2nd Edn., Wiley, New York, ISBN: 0471128457, pp: 758.