Journal of Quality Measurement and Analysis *JQMA* 14(2) 2018, 81-89
Jurnal Pengukuran Kualiti dan Analisis

ESF: SUATU KRIPTOSISTEM MUDAH RINGKAS BERASASKAN MASALAH PEMFAKTORAN

(ESF: An Easy Simple Factoring-based Cryptosystem)

EDDIE SHAHRIL ISMAIL, MUHAMMAD ZAFREE ZAHARIDAN & FAIEZA SAMAT

ABSTRAK

Dalam makalah ini diperkenalkan kriptosistem baharu kunci awam ESF yang mudah lagi ringkas berasaskan masalah pemfaktoran. Sistem ini adalah variasi daripada kriptosistem tersohor RSA (Rivest, Shamir, Adleman) yang masih diamalkan sehingga kini. Kriptosistem baharu ini memiliki tiga kelebihan utama berbanding dengan RSA. Pertama, ia tidak memerlukan operasi modular songsangan yang sangat mahal apabila menjana kunci rahsia. Kedua, saiz dan nilai kunci rahsia yang lebih kecil jika kunci awam dan modulus dalam ESF dan RSA ditetapkan. Ketiga, saiz mesej tersembunyinya sentiasa lebih kecil jika kunci rahsia dan modulus dalam ESF dan RSA ditetapkan. Ini seterusnya menjadikan proses menyulit dan menyahsulit dalam kriptosistem ESF lebih cekap berbanding dengan RSA.

Kata kunci: kriptografi; RSA; masalah pemfaktoran

ABSTRACT

This paper introduces a new easy and simple ESF public key cryptosystem based on factoring problem. It is a variation from the novel RSA (Rivest, Shamir, Adleman) cryptosystem which is until now still practicable. The new proposed cryptosystem possesses three main advantages over RSA. Firstly, it requires no expensive inverse modular operation during secret key generation. Secondly, the size and value of secret key is smaller if one fixes the public key and modulus in ESF and RSA. Thirdly, the size and value of the ciphertext is always smaller if the secret key and modulus in ESF and RSA are fixed. Hence, the encryption and decryption processes in ESF are more efficient compared to RSA.

Keywords: cryptography; RSA; factoring problem

References

Aun H.G., Abu-Hasan Y. & Ismail E.S. 2001. Kriptosistem multi-RSA. *Jurnal Teknologi* **35**(C): 61-70.

Boneh D. 1999. Twenty years of attacks on the RSA cryptosystem. *Notices of the American Mathematical Society* (AMS) **46**(2): 203-213.

Boneh D. & Durfee G. 1999. Cryptanalysis of RSA with private key d less than $n^{0.292}$. *Proceedings Advances in Cryptology-EUROCRYPT'99, LNCS 1592,* Springer-Verlag, Berlin, pp. 1-11.

Coppersmith D. 1997. Small solutions to polynomial equations and low exponent RSA vulnerabilities. *Journal of Cryptology* **10**: 233-260.

Coppersmith D., Franklin M., Patarin J. & Reiter M. 1996. Low exponent RSA with related messages. *Proceedings Advances in Cryptology-EUROCRYPT'96, LNCS 1070* Springer-Verlag, Berlin, pp. 1-9.

Diffie W. & Hellman M. 1976. New directions in cryptography. *IEEE Transaction of Information Theory* **22**(6): 644-654.

Durfee G. 2002. Cryptanalysis of RSA using algebraic and lattice methods. PhD Thesis. Standford University.

Fiat A. 1990. Batch RSA. *Proceedings Advances in Cryptology-CRYPT0'89, LNCS 435* Springer-Verlag, Berlin, pp. 175-185.

Hastad J. 1986. On using RSA with low exponent in a public key network. *Proceedings Advances in Cryptology-CRYPTO'85, LNCS 218* Springer-Verlag, Berlin, pp. 403-408.

*Lenstra A.K. 2000. Integer factoring. Design, Codes and Cryptography **19**: 101-128.*

Lin H.F. & Chen C.Y. 1999. An extended RSA based generalised group oriented signature scheme. Unpublished.

Lin H.F., Hu C.Y., Chang C.C. & Chen C.Y. 1998. Sharing a secret using RSA cryptosystem. *Proceedings ICS98* Taipei, pp. 1490-1493.

Montgomery P.L. 1994. A survey of modern integer factorization algorithms. Quarterly 7(4): 337-365.

Peralta R. & Okamoto E. 1996. Faster factoring of integers of a special form. IEICE Trans. Fundamentals ***E79-A (4)****: 489-493.*

Quisquater J.-J. & Couvreur C. 1982. Fast decipherment algorithm for RSA public-key cryptosystem. Electronic Letters ***18****: 905-907.*

Rivest R.L., Shamir A. & Adleman L. 1978. A method for obtaining digital signatures and public-key cryptosystems. *Communications of the ACM* **21**(2): 120-126.

Rosen K.H. 2000. *Elementary Number Theory*. Ed. ke-4. New York: Addison Wesley Longman.

Takagi T. 1997. Fast RSA-type cryptosystem using n-adic expansion. Proceedings Advances in Cryptology-CRYPTO'97, LNCS 1294 Springer-Verlag, Berlin, pp. 372-384.

Williams H.C. 1980. A modification of the RSA public-key encryption procedure. *IEEE Transaction of Information Theory* **26**(6): 726-729.

Wiener M.J. 1990. Cryptanalysis of short RSA secret exponents. *IEEE Transaction of Information Theory* **36**(3): 553-558.

Pusat Pengajian Sains Matematik
Fakulti Sains dan Teknologi
Universiti Kebangsaan Malaysia
43600 UKM Bangi
Selangor DE, MALAYSIA
Mel-e: esbi@ukm.edu.my[*]

[*]Penulis untuk dihubungi