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

1. Pengenalan

Dalam makalah ini, kriptosistem kunci awam baharu berasaskan masalah pemfaktoran diperkenalkan. Kriptosistem ini merupakan variasi daripada kriptosistem tersohor RSA (Rivest *et al*. 1978) yang hingga kini masih kebal dan diamalkan dengan meluas. Kriptosistem baharu ini diberi singkatan kriptosistem ESF yang merujuk kepada singkatan Inggeris *Easy Simple Factoring-based Cryptosystem.* Kriptosistem ESF mempunyai tiga kelebihan utama berbanding dengan versi asal RSA. Pertama, ia tidak memerlukan sebarang operasi songsangan modular semasa penjanaan kunci rahsia; keduanya, saiz mesej tersembunyi (*ciphertext*) yang lebih kecil dan yang ketiga, proses menyulit (*encryption*) dan menyahsulit (*decryption*) yang lebih pantas berbanding dengan RSA. Dengan ini secara heuristik, kriptosistem ESF lebih cekap berbanding dengan versi asal RSA jika dibangunkan atas sebarang platform perkakasan atau perisian. Sejak terciptanya RSA, banyak versi variasinya muncul dengan pelbagai dakwaan kelebihan masing-masing (Williams 1980; Fiat 1990; Quisquater & Couvreur 1982; Takagi 1997). Makalah ini hanya membandingkan antara kriptosistem ESF dengan RSA sahaja kerana versi asal RSA masih utuh ciri keselamatan dan kekebalannya. Makalah ini bermula dengan penerangan berkenaan kriptosistem RSA dan

diikuti dengan cadangan kriptosistem ESF. Selepas itu analisis kecekapan dan kekebalan ESF akan diberikan dan seterusnya perbandingan dengan RSA dilakukan. Makalah ini diakhiri dengan perbincangan dan kesimpulan.

2. Kriptosistem RSA

Sistem kunci awam RSA adalah yang pertama seumpamanya dicipta pada tahun 1978 sekaligus menyelesaikan masalah penyimpanan kunci oleh sistem kunci rahsia sebelum ini yang diutarakan oleh Diffie dan Hellman (1976). RSA dibangunkan dengan teras kekebalannya bergantung penuh kepada masalah memfaktorkan integer gubahan yang bersaiz besar yang masih belum dapat diselesaikan hingga sekarang kerana tiada penyelidik berjaya menemui alkhwarizmi masa polinomial meskipun usaha ke arah itu telah banyak dilakukan. Namun usaha itu tidak memberi impak serius kepada keutuhan RSA (Montgomery 1994; Peralta & Okamoto 1996; Lenstra 2000). Masalah pemfaktoran ini merupakan antara masalah tertua dalam bidang teori nombor. Sekarang diperlihatkan alkhwarizmi RSA.

2.1. *Parameter sistem*

(1) Pilih dua perdana p dan q bersaiz 1024-bit.
(2) Hitung modulus $n = pq$ dan fungsi fi-Euler $\phi(n) = (p-1)(q-1)$.

Parameter n dan $\{p, q, \phi(n)\}$ masing-masing disebut parameter awam dan parameter rahsia. Parameter awam akan disimpan dalam direktori awam untuk capaian sesiapa sahaja manakala parameter rahsia perlu disimpan kemas tanpa pengetahuan awam.

2.2. *Penjanaan kunci*

(1) Pilih kunci awam $e \in \{x : 1 \le x \le \phi(n), \text{pst}(x, \phi(n)) = 1\}$.
(2) Hitung kunci rahsia $d = e^{-1} \bmod \phi(n)$.

Simbol ‘pst’ menandakan pembahagi sepunya terbesar.

Integer e disebut kunci awam dan disimpan dalam direktori awam bersama n manakala integer d disebut kunci rahsia dan perlu disimpan rapi untuk pengetahuan penerima sahaja.

2.3. *Fasa menyulit*

Misalkan mesej sulit $m \in \{y : 1 \le y \le n, \text{pst}(y, n) = 1\}$ ingin dihantar. Penghantar menghitung

$$c = m^e \bmod n.$$

Mesej tersembunyi c akan dihantar terus kepada penerima.

2.4. *Fasa menyahsulit*

Sekarang penerima memperoleh mesej tersembunyi c yang dihantar. Untuk memperoleh kembali mesej sulit, penerima menghitung

$$c^d = m \bmod n.$$

Mesej sulit m akan diperoleh kembali.

Usulan 2.1. *Pertimbangkan suatu sistem RSA. Jika semua parameter* $\{p,q,n,\phi(n)\}$ *dan kunci* $\{e,d\}$ *dipilih dan dijana mengikut syarat dalam RSA, maka mesej sulit akan diperoleh kembali dalam fasa menyahsulit RSA.*

Pembuktian. Perhatikan bahawa, oleh kerana

$$d = e^{-1} \bmod \phi(n)$$

maka wujud suatu integer k sedemikian hingga

$$de = 1 + k\phi(n).$$

Seterusnya,

$$c^d = \left(m^e\right)^d = m^{1+k\phi(n)} = m\left(m^{\phi(n)}\right)^k = m(1)^k = m \bmod n$$

yang $m^{\phi(n)} = 1 \bmod n$ bertepatan dengan Teorem Euler (Rosen 2000) . □

Hastad (1986) dalam makalahnya membuktikan bahawa penggunaan eksponen kunci awam e yang rendah beserta syarat lain akan menyebabkan mesej sulit boleh diperoleh pihak musuh. Beliau menggunakan teori kekisi (Durfee 2002) sebagai alat utama dalam pembuktian beliau yang kini menjadi landasan kepada perkembangan kriptografi pasca-kuantum sekarang. Wiener (1990) dalam artikelnya pula membuktikan penggunaan eksponen rahsia $d < n^{0.25}$ yang rendah juga mengakibatkan mesej sulit mudah diperoleh musuh. Beliau menggunakan serangan pecahan berlanjar (Rosen 2000) dengan mengeskploitasi hubungan matematik di antara eksponen e dengan d. Coppersmith *et al*. (1996) seterusnya memperkenalkan kelas baharu serangan dengan membuktikan bahawa jika terdapat hubungan polinomial di antara mesej-mesej sulit dengan syarat eksponen kunci awam e dan modulus RSA yang sama digunakan maka mesej-mesej sulit tersebut boleh dihitung secara aljabar. Coppersmith (1997) juga membuktikan dengan eksponen RSA yang rendah, modulus RSA $n = pq$ boleh difaktorkan jika $(1/4)\log_2 n$-bit perdana p diketahui. Boneh dan Durfee (1999) menunjukkan yang batas $d < n^{0.25}$ tidak kuat dan membuktikan jika $d < n^{0.292}$ maka sistem tidak selamat dan berkonjektur bahawa batas $d < n^{0.5}$ boleh dicapai. Boneh (1999) mengulas dan menyimpulkan serangan RSA bermula pada tahun 1979 dan menyatakan bahawa semua serangan itu boleh dielak dan tidak bahaya jika pelaksanaan RSA dilakukan secara kemas dan rapi.

3. Kriptosistem ESF

Diperkenalkan kriptosistem ESF yang dasar pembinaannya bergantung berat kepada masalah memfaktorkan integer gubahan yang besar seperti versi asal RSA.

3.1. *Parameter sistem*

(1) Pilih dua perdana p dan q bersaiz 1024-bit dan anggap $p > q$.
(2) Hitung modulus $n = pq$.
(3) Cari integer r dan s yang r/s adalah bentuk termudah pecahan $(p-1)/(q-1)$.
(4) Hitung ω yang $\omega = s(p-1)+1 = r(q-1)+1$.

Parameter n dan $\{p,q,r,s,\omega\}$ masing-masing disebut parameter awam dan parameter rahsia. Parameter awam akan disimpan dalam direktori awam untuk capaian sesiapa sahaja manakala parameter rahsia perlu disimpan kemas tanpa pengetahuan awam.

3.2. *Penjanaan kunci*

(1) Cari integer u yang u membahagi ω.
(2) Hitung integer v yang $uv = \omega$.

Integer u disebut kunci awam dan disimpan dalam direktori awam bersama n manakala integer v disebut kunci rahsia dan perlu disimpan rapi untuk pengetahuan penerima sahaja.

3.3. *Fasa menyulit*

Misalkan mesej sulit $m \in \{y : 1 \le y \le n, \text{pst}(y,n) = 1\}$ ingin dihantar, maka proses berikut dilakukan: Hitung

$$c = m^u \bmod n.$$

Mesej tersembunyi c akan dihantar terus kepada penerima.

3.4. *Fasa menyahsulit*

Sekarang penerima memperoleh mesej tersembunyi c yang dihantar. Untuk memperoleh kembali mesej sulit, penerima melakukan proses berikut: Hitung

$$c^v = m \bmod n.$$

Mesej sulit m akan diperoleh kembali.

Pembuktian ke arah kesahihan $c^v = m \bmod n$ adalah cetusan idea daripada fungsi yang ditakrifkan oleh Lin dan Chen (1999) dan Lin *et al*. (1998) serta telah digunakan oleh Aun *et al*. (2001) yang mencadangkan variasi pembangunan skema kriptografi RSA.

Usulan 3.1. *Pertimbangkan sistem ESF. Jika semua parameter* $\{p,q,n,r,s,\omega\}$ *dan kunci* $\{u,v\}$ *dipilih dan dijana mengikut syarat dalam ESF, maka mesej sulit akan diperoleh kembali dalam fasa menyahsulit ESF.*

Pembuktian. Perhatikan bahawa, oleh kerana $\omega = s(p-1)+1 = r(q-1)+1$ maka

$p-1$ dan $q-1$ membahagi $\omega-1$.

Dari Teorem Fermat (Rosen 2000) wujud suatu integer s dan r sedemikian hingga

$$m^{\omega} = m^{s(p-1)+1} = \left(m^{p-1}\right)^{s} m = 1^{s} m = m \bmod p$$

dan

$$m^{\omega} = m^{r(q-1)+1} = \left(m^{q-1}\right)^{r} m = 1^{r} m = m \bmod q$$

yang m tidak membahagi p dan q. Seterusnya oleh kerana p dan q perdana secara relatif, maka

$$m^{\omega} = m \bmod pq$$

atau setara dengan $c^{v} = m^{\omega} = m \bmod pq = m \bmod n$. □

4. Analisis Kecekapan dan Kekebalan

Dalam kedua-dua sistem RSA dan ESF, parameter awam yang boleh dicapai oleh pihak awam hatta musuh hanyalah modulus $n = pq$ dan kunci awam penerima, iaitu e dan u. Selagi tiada alkhwarizmi masa polinomial yang boleh memfaktorkan integer besar n ke dalam pembahagi perdana p dan q maka kunci rahsia d dan v masih kekal sukar untuk diperoleh walaupun dengan pengetahuan e dan u, seterusnya menjamin keutuhan dan kekebalan dua sistem ini.

Perhatikan bahawa untuk mengira kunci rahsia d dalam sistem RSA, songsangan modular diperlukan. Walau bagaimanapun, telah diketahui bahawa operasi ini sangat mahal dan menuntut tempoh yang lama untuk dilaksanakan. Berbanding dengan sistem ESF, pengiraan kunci rahsia v hanya memerlukan operasi pembahagian sahaja yang sangat efisien untuk dilaksanakan. Namun, pencarian integer u itu sendiri perlu diperhalusi. Untuk menentukan nilai u, satu daripada caranya adalah dengan mencari faktor atau pembahagi bagi ω. Perhatikan juga integer ω sentiasa ganjil. Pencarian pembahagi bagi ω jika $\omega = fg$ yang f, g perdana bersaiz 1024-bit pastilah sukar kerana ia berbalik semula kepada masalah pemfaktoran yang sukar diselesaikan itu dengan saiz ω sekarang adalah 2048-bit. Walau bagaimanapun, modulus $\omega = r(q-1)+1 = s(p-1)+1$ hanya bersaiz sekitar 1024-bit jika $r \ll q$ atau $s \ll p$. Justeru pembahagi bagi ω mudah untuk dicari. Tambahan lagi, $\omega = uv$ yang u, v bukan perdana maka pencarian pembahaginya tidaklah sesukar masalah pemfaktoran yang merupakan antara masalah tertua teori nombor.

Dalam proses menyahsulit bagi memperoleh semula mesej asal, penerima dalam RSA dan ESF masing-masing perlu mengira $m^{ed} \bmod n$ dan $m^{\omega} \bmod n$. Dengan mengandaikan m, n yang sama digunakan dalam kedua-dua sistem, boleh ditunjukkan bahawa pengiraan dalam ESF adalah lebih pantas. Hal ini benar apabila $\omega < ed$ seperti yang ditunjukkan dalam teorem berikut.

Teorem 4.1. *Pertimbangkan sistem RSA dan ESF. Jika* $\{e,d\}$ *dan* $\{u,v\}$ *adalah masing-masing pasangan kunci awam-rahsia maka* $uv = \omega < ed$.

Pembuktian. Perhatikan bahawa pasangan kunci awam-rahsia dalam RSA memenuhi

$$ed = 1 + k\phi(n) = 1 + k(p-1)(q-1)$$

yang k integer positif, $n = pq$ dan p,q perdana dengan $p > q$ serta ϕ ialah fungsi fi-Euler. Pasangan kunci awam-rahsia dalam ESF memenuhi

$$uv = \omega = r(q-1) + 1 = s(p-1) + 1$$

yang p,q perdana dan r/s adalah pecahan termudah bagi $(p-1)/(q-1)$. Oleh itu diperoleh $r < p-1$ dan $s < q-1$. Seterusnya, didapati $r(q-1) < (p-1)(q-1) < k(p-1)(q-1)$ kerana k integer positif yang seterusnya memberikan $r(q-1)+1 < k(p-1)(q-1)+1$ dan akhirnya diperoleh bahawa $\omega < ed$. □

Sekarang diberikan perbandingan berangka hasil darab kunci awam dan kunci rahsia di antara RSA dengan ESF seperti Jadual 1 apabila $u = e$.

Jadual 1: Perbandingan berangka hasil darab kunci awam dan rahsia antara RSA dengan ESF bagi beberapa pasangan nombor perdana *p* dan *q*

Nombor Perdana		RSA			ESF		
p	*q*	*e*	*d*	*ed*	*u*	*v*	$uv = \omega$
27449	17389	9178189	357949381	3285327071251009	9178189	13	119316457
48611	37813	70693897	919020673	64969152797932681	70693897	13	919020661
53441	42073	380299	1405205539	534398261276161	380299	739	281040961
58237	3413	2922077	149025941	435465274599457	2922077	17	49675309
59359	3581	44587	106253203	4737511562161	44587	2383	106250821
64453	52919	28903991	1705335527	49291002724388257	28903991	59	1705335469
70549	3571	149381	41976341	6270467794921	149381	281	41976061

Berdasarkan Jadual 1, terbukti bahawa nilai $uv = \omega$ sentiasa lebih kecil daripada nilai ed. Dalam proses menyulit pula, penghantar mengira $m^e \bmod n$ dan $m^u \bmod n$ masing-masing dalam RSA dan ESF. Daripada Teorem 4.1, diperoleh bahawa $uv < ed$ dan jika ditetapkan $u = e$ atau $v = d$ maka diperoleh $v < d$ atau $u < e$. Secara matematiknya, jika ini berlaku maka proses menyulit atau menyahsulit dalam ESF adalah lebih pantas berbanding dengan RSA. Sementara itu saiz mesej tersembunyi, c pula bergantung kepada saiz m^e atau m^u. Jika $m^e, m^u < n$ maka saiz c dalam ESF adalah lebih kecil berbanding dengan RSA dan ini benar sekiranya diambil $v = d$ dan seterusnya proses menyahsulit dalam ESF adalah lebih cekap berbanding dengan RSA. Perhatikan apabila $v = d$ maka $e > u$. Ini memberikan $m^e > m^u$, iaitu saiz mesej tersembunyi RSA lebih besar daripada ESF. Nisbah saiz mesej tersembunyi RSA dan ESF diberikan oleh

$$\frac{m^e}{m^u} = m^{d^{-1}(1+k(p-1)(q-1))-v^{-1}\omega} = m^{\frac{1+k(p-1)(q-1)-\omega}{d}} = \begin{cases} m^{k(p-1)-r}, & d = v \approx q-1 \\ m^{k(q-1)-s}, & d = v \approx p-1. \end{cases}$$

Oleh itu nisbah saiz mesej tersembunyi di antara RSA dengan ESF diberikan oleh $m^{k(p-1)-r}:1$ atau $m^{k(q-1)-s}:1$ jika $d \approx q-1$ atau $d \approx p-1$.

Jadual 2 pula menunjukkan perbandingan tempoh masa menyahsulit antara sistem RSA dan ESF dan diperoleh bahawa masa menyahsulit ESF adalah lebih pantas (menggunakan platform Python 3.7 Intel Core i5-6200U 2.3GHz 8GB RAM) daripada RSA dengan menetapkan nilai kunci awam $e = u$ dalam RSA dan ESF.

Jadual 2: Perbandingan berangka masa menyahsulit (dalam saat) antara RSA dengan ESF bagi beberapa pasangan nombor perdana *p* dan *q*

p	*q*	*e* = *u*	Mesej, *m*	Masa menyahsulit (RSA)	Masa menyahsulit (ESF)
10000002403	10000004039	54225323643641	3	0.01696	0.01396
99999999947	99999999977	536947	23154364635423	0.01565	0.01548
99999999769	100000000003	178757776758779	402090	0.01562	0.01544
69999994741	69999999997	434908456335809	12423145	0.01562	0.01545
20000000089	20000003767	16667059	55635234	0.01495	0.01217
29999999993	30000000001	32634708817173109	93565	0.01401	0.01067
451346952449	451346953807	180277939908872862493	7654	0.01411	0.01319
851346952429	851346955379	224796937887937931	3	0.01496	0.01096
571346952353	571346954771	54406223557239248186507	3563254232553	0.01496	0.01181
381346952381	381346957919	8931292883	94762452	0.01302	0.01169

5. Perbincangan dan Kesimpulan

Dalam kajian ini, versi baharu RSA yang dinamai ESF diperkenalkan. Perbezaan ketara ESF dengan variasi RSA yang lain adalah ESF amat mirip dengan RSA dengan perbezaan hanyalah pada kaedah penjanaan kunci awam dan rahsianya sahaja manakala variasi RSA yang lain berbeza ketara pada proses menyulit dan menyahsulit. Namun, struktur alkhwarizmi bagi proses menyulit dan menyahsulit dalam ESF adalah serupa seperti dalam RSA dan inilah sebab mengapa perbandingan ESF hanya dilakukan dengan RSA dan bukan dengan variasi RSA yang lain.

Kunci awam dan kunci rahsia RSA dijana melalui hubungan $ed = 1 + k(p-1)(q-1)$ yang p, q adalah nombor perdana bersaiz 1024-bit dan k adalah integer. Bagi pelaksanaan secara praktikal, saiz perdana mestilah paling minimum 512-bit supaya strategi serangan musuh sentiasa gagal. Dalam persamaan ini, hanya nilai e yang diketahui musuh manakala nilai perdana p, q hanya boleh diketahui jika wujud alkhwarizmi masa polinomial bagi menyelesaikan pemfaktoran modulus $n = pq$. Kos bagi mencari nilai d memerlukan operasi songsangan modular yang mahal apabila dilaksanakan dalam perkakasan komputer.

Dalam ESF pula, kunci awam dan kunci rahsia terkait melalui persamaan $uv = \omega = r(q-1)+1 = s(p-1)+1$ yang r, s adalah integer dengan $r/s = (p-1)/(q-1)$ adalah dalam bentuk pecahan termudah dan hanya nilai u yang diketahui oleh musuh. Bagi menentukan nilai v, operasi songsangan modular tidak diperlukan tetapi hanya melalui penguraian ω kepada pemfaktoran perdananya sahaja.

Dibuktikan seterusnya bahawa $uv < ed$. Jika ditetapkan $u = e$ maka diperoleh $v < d$ dan ini jelas menunjukkan proses menyahsulit ESF memerlukan masa yang lebih singkat daripada RSA manakala jika $v = d$ maka diperoleh $u < e$ dan ini jelas sekali lagi menunjukkan bahawa masa proses menyulit ESF adalah lebih pantas berbanding dengan RSA. Dalam hal ini, saiz mesej tersembunyi ESF juga lebih kecil daripada RSA dengan nisbah $1: m^{k(p-1)-r}$ atau $1: m^{k(q-1)-s}$. Kesimpulannya, skema ESF adalah lebih cekap berbanding dengan RSA atau dengan kata lain ESF adalah lebih mudah dan ringkas merujuk kepada saiz kunci, saiz mesej sulit atau mesej tersembunyi yang jauh lebih kecil serta masa menyulit atau menyahsulit yang lebih singkat.

Sistem ESF yang dicadangkan ini boleh sahaja diperluaskan menggunakan dua kunci rahsia v dan λ yang dijana melalui persamaan Diophantine, $uv + \gamma\lambda = \omega$ dengan u, γ adalah kunci awam yang sepadan. Proses mengkrip seterusnya menghasilkan mesej tersembunyi $\left(c_1 = m^u \bmod n, c_2 = m^\gamma \bmod n\right)$ dan proses menyahkrip menghasilkan mesej asal, m melalui $c_1^v c_2^\lambda = m \bmod n$ yang n adalah modulus sistem ESF. Peluasan ini ada kelebihan dan kekurangannya, antaranya penjanaan kunci akan lebih cekap tetapi saiz mesej tersembunyi menjadi dua kali ganda daripada sistem sebelumnya. Namun, peluasan ini banyak manfaat lain yang boleh diterokai sebagai penyelidikan masa hadapan.

Penghargaan

Penulis merakamkan penghargaan kepada Universiti Kebangsaan Malaysia atas sokongan dan pemberian dana penyelidikan GUP-2017-089 untuk penyelidikan ini.

Rujukan

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