Jurnal Teknologi, 37(C) Dis. 2002: 21–38

TRANSFORMASI POLIFUNGSI LUC DALAM SISTEM KRIPTOGRAFI

FARIDAH YUNOS, KAMEL ARIFFIN MOHD ATAN, & MOHAMAD RUSHDAN MD SAID

Abstrak. Katakan N adalah hasil daripada pendaraban dua nombor perdana berbeza yang besar saiznya iaitu p dan q , $N = pq$. Teks asal $P < N$ menghasilkan teks saifer C bermodulo N. Katakan $(P, N) = 1$. Andaikan kunci pengkriptan yang digunakan integer positif e sedemikian hingga $(e, N) = 1$, penterjemahan P menerusi transformasi Monofungsi LUC ditakrifkan sebagai

$$C \equiv N_e\,(P, 1)(mod\ N).$$

Pengkriptanan mesej P dikembangkan lagi melalui transformasi polifungsi sehingga menghasilkan mesej saifer. Penyelidikan ini membuktikan bahawa fungsi Lehmer Totient $S(N)$ sentiasa sama pada setiap transformasi bagi membolehkan pelaksanaan penghuraian mesej saifer.

Kata kunci: Teks saifer, Pengkriptanan, Penghuraian

Abstract. Let N be a product of two large distinct primes p and q , $N = pq$. The plaintext $P < N$ is encrypted to a cyphertext, C modulo N. Let $(P, N) = 1$. Assuming that the encrypting key is the positive integer e such that $(e, N) = 1$**,** translation of P through the LUC Monofunction transformation is defined by

$$C \equiv N_e\,(P, 1)(mod\ N).$$

The encrypted message P is extended via polyfunction transformation to produce a cyphertext. We show that the Lehmer Totient function $S(N)$ is always the same in each transformation, enabling us to carry out the decryption process.

Key words: Cyphertext, Encryption , Decryption

1.0 PENGENALAN

Dengan N dan P sebarang integer dan $n = 1, 2, 3\ldots$, jujukan Lucas dengan fungsi jadi semula linear berdarjah dua ditakrifkan sebagai

$$V_0 = 2, V_1 = P \quad \text{dan} \quad V_n(P,1) \equiv PV_{n-1}(P,1) - V_{n-2}(P,1)(mod\ N) \qquad (1)$$

atau

$$U_0 = 0, U_1 = 1 \quad \text{dan} \quad U_n(P,1) \equiv PU_{n-1}(P,1) - U_{n-2}(P,1)(mod\ N) \qquad (2)$$

[1] Jabatan Matematik, Fakulti Sains Dan Pengajian Alam Sekitar, Universiti Putra Malaysia, 43400 Serdang, Selangor, Malaysia.

Identiti lain bagi jujukan Lucas yang biasa dipraktikkan dalam sistem kriptografi LUC ialah

$$V_{2n}(P,1) \equiv V_n^2(P,1) - 2 (mod\ N) \tag{3}$$

$$V_{2n+1}(P,1) \equiv V_{n+1}(P,1)V_n(P,1) - P (mod\ N) \tag{4}$$

$$V_n^2(P,1) \equiv DU_n^2(P,1) + 4 (mod\ N) \tag{5}$$

$$V_{nm}(P,1) \equiv V_n\left(V_m(P,1)\right) (mod\ N) \tag{6}$$

$$2V_{n\pm m}(P,1) \equiv V_n(P,1)V_m(P,1) \pm DU_n(P,1)U_m(P,1) (mod\ N) \tag{7}$$

$$U_{2n}(P,1) \equiv U_n(P,1)V_n(P,1) (mod\ N) \tag{8}$$

$$U_{2n+1}(P,1) \equiv U_{n+1}(P,1)V_n(P,1) - 1 (mod\ N) \tag{9}$$

dengan pembeza layan $D = P^2 - 4$ dan $n, m = 1,2,3,\ldots$.

Berikut merupakan beberapa tatatanda dan takrif yang digunakan dalam kajian kita.

P merupakan nombor bersepadan dalam teks asal. Contohnya, jika nombor bersepadan bagi teks asal abjad R ialah 17 maka $P = 17$.

$C^{(t)}$ merupakan nombor bersepadan dengan teks saifer pada transformasi ke-t untuk $t = 1, 2, 3,\ldots$. $C^{(t)} = C$ apabila $t = 1$. Contohnya, jika nombor bersepadan teks saifer KX, iaitu 1023 terhasil daripada transformasi trifungsi maka $C^{(t)} = 1023$.

Katakan N hasil pendaraban dua nombor perdana berbeza p dan q, maka Fungsi Lehmer Totient bagi mesej asal P bermodulo N ialah $S(N) = g.s.k\left(p - \left(\frac{D}{p}\right), q - \left(\frac{D}{q}\right)\right)$ dengan pembezalayan $D = P^2 - 4$ sedemikian hingga (D, N) =1 supaya wujud nilai sama ada +1 atau –1 bagi simbol Legendre $\left(\frac{D}{p}\right)$ dan $\left(\frac{D}{q}\right)$. Fungsi Lehmer Totient bagi mesej $C^{(t)}$ bermodulo N ialah $S(N) = g.s.k\left(p - \left(\frac{D^{(t)}}{p}\right), q - \left(\frac{D^{(t)}}{q}\right)\right)$ dengan pembezalayan $D^{(t)} = \left(C^{(t)}\right)^2 - 4$ sedemikian hingga $\left(D^{(t)}, N\right) = 1$ supaya wujud nilai sama ada +1 atau –1 bagi simbol Legendre $\left(\frac{D^{(t)}}{p}\right)$ dan $\left(\frac{D^{(t)}}{q}\right)$ bagi setiap t = 1, 2, 3, ….

Sistem kriptografi menggunakan fungsi Lucas telah diperkenalkan pada tahun 1991 oleh P. Smith [6] berdasarkan idea daripada sistem RSA (R. Rivest, A. Shamir, L. Adleman [3]) dan beliau mendapati sistem LUC ini boleh mengatasi masalah sistem RSA yang berpunca daripada sifat homomorfismanya. Hasil daripada kajian oleh P. Smith [7], kita mengemukakan teorem di bawah.

Teorem 1

Katakan $N = pq$. Secara bersimetri, jika $(U_e(P,1), N) = 1$ maka fungsi Lehmer Totient mempunyai nilai yang sama, sama ada dikira menggunakan P atau $V_e(P,1)$ bermodulo N.

Pembuktian

Katakan pembeza layan bagi mesej asal P ialah $D = P^2 - 4$ manakala pembeza layan bagi $V_e(P,1)$ ialah $D^{(1)} = V_e^2(P,1) - 4$.

Daripada identiti Lucas (5), $V_e^2(P,1) - 4 = DU_e^2(P,1)$ maka kita mendapati $\left(\frac{D^{(1)}}{p}\right) = \left(\frac{DU_e^2}{p}\right)$.

Jika $(U_e, p) = 1$ maka $\left(U_e^2\right)^{\frac{p-1}{2}} \equiv U_e^{p-1} \equiv 1 (mod\ p)$. Oleh yang demikian, $\left(\frac{D^{(1)}}{p}\right) = \left(\frac{D}{p}\right)$. Ini bermakna $\left(\frac{D}{p}\right) = \left(\frac{P^2-4}{p}\right) = \left(\frac{V_e^2(P,1)-4}{p}\right)$ begitu juga dengan $\left(\frac{D}{q}\right) = \left(\frac{P^2-4}{q}\right) = \left(\frac{V_e^2(P,1)-4}{q}\right)$. Oleh itu Fungsi Lehmer Totient akan sama, sama ada diperolehi daripada P atau $V_e(P,1)$ [5].

Hasil daripada perbincangan Teorem 1 digunakan dalam model perutusan mesej LUC sebagaimana digambarkan dalam Teorem 2 berikut:

Teorem 2

Katakan transformasi Pengkriptanan Monofungsi LUC ditakrifkan sebagai

$$C \equiv V_e(P,1) (mod\ N)$$

Jika $(U_e(P,1),N)=1$ dan $(e,S(N))=1$ dengan $D=P^2-4$ maka penghuraian teks saifer berbentuk

$$P \equiv V_d(C,1)(mod\ N)$$

dengan kunci penghurai d merupakan songsangan bagi e yang diperolehi daripada $de \equiv 1(mod\ S(N))$ dengan pembezalayan $D^{(1)}=C^2-4$.

Pembuktian

Katakan transformasi pengkriptanan P kepada C ditakrifkan sebagai

$$C \equiv V_e(P,1)(mod\ N) \tag{10}$$

Dari pada Teorem 1, jika $(U_e(P,1),N)=1$ maka Fungsi Lehmer Totient mempunyai nilai yang sama, sama ada dikira menggunakan P atau $V_e(P,1)(mod\ N)$. Andaikan Fungsi Lehmer Totient tersebut $S(N)$.

Jika $(e,S(N))=1$ maka wujud kunci penghurai d sedemikian hingga $ed \equiv kS(N)+1$ untuk sebarang integer k dan d diperolehi daripada algoritma Euklidan.

Daripada perkaitan (10), kita mendapati

$$\begin{aligned}
V_d(V_e(P,1),1) &\equiv V_{de}(P,1)(mod\ N) \\
&\equiv V_{kS(N)+1}(P,1)(mod\ N) \\
&\equiv V_{kS(N)}(P,1)-V_{kS(N)-1}(P,1)(mod\ N) \\
&\equiv PV_{kS(N)}(P,1)-\frac{1}{2}\Big[V_{kS(N)}(P,1)V_1(P,1) && \text{daripada (6)} \\
&\quad -DU_{kS(N)}(P,1)U_1(P,1)\Big](mod\ N) && \text{daripada (1)} \\
&\equiv 2P-\frac{1}{2}[2P-0](mod\ N) \\
&\equiv P(mod\ N) && \text{daripada (7)}
\end{aligned}$$

Jadi, kita telah membuktikan bahawa algoritma penghuraian C kepada P ialah

$$P \equiv V_d(C,1) mod\ N.$$

Untuk meningkatkan tahap keselamatan dalam sistem RSA, kajian berkaitan dengannya telah mengemukakan teknik transformasi polifungsi RSA (M. R. Schroeder

[5] m/s 123). Oleh kerana LUC digambarkan sebagai sistem yang lebih diberi kepercayaan berbanding RSA maka kita menggunakan teknik yang sama untuk mempraktikkannya ke dalam sistem LUC. Penelitian dimulai dengan transformasi dwifungsi, trifungsi dan seterusnya transformasi polifungsi dengan memperincikannya lagi kepada konsep pemecahan nombor-nombor bersepadan mesej asal kepada blok-blok mengandungi beberapa digit tertentu. Bagi tujuan keselamatan, apa yang perlu dirahsiakan selain daripada p, q dan d ialah bilangan transformasi t. Kajian turut membincangkan hubungan antara konsep kalaan fungsi Lucas dalam menetapkan syarat mesej asal tidak menyamai mesej saifernya. Akhir sekali kita akan menguji kekebalan sistem berasaskan beberapa faktor tertentu.

Transformasi pengkriptanan monofungsi LUC, iaitu $V_e(P,1) mod\ N$ akan menjadi objek kajian dengan mengekalkan ciri-ciri penting $N = pq$ dengan kunci-kunci rahsia p dan q nombor perdana berbeza yang besar saiznya, $(P < N, N) = 1$, $(D, N) = 1$ kunci awam $(e, N) = 1, (U_e(P,1), N) = 1, (e, S(N)) = 1$ dan $e^2 \not\equiv 1 (mod\,(S(N)))$ supaya $d \neq e$. Kunci rahsia d yang dimiliki oleh pengutus mesej berdasarkan analisis pembeza layan $D = P^2 - 4$. Oleh kerana individu penerima tidak mengetahui mesej asal dan dalam masa yang sama untuk menjaga kerahsiaannya daripada diketahui umum maka kunci d didapati daripada analisis pembeza layan $D^{(t)} = \left(C^{(t)}\right)^2 - 4$.

Kajian mengemukakan beberapa takrif Pengkriptanan LUC di bawah sebagai penerusan daripada Takrif Pengkriptanan Monofungsi LUC sebelum ini untuk digunakan dalam perbincangan seterusnya.

Takrif 1

Katakan N adalah hasil daripada pendaraban dua nombor perdana berbeza yang besar saiznya, iaitu p dan q, $N = pq$. Teks asal $P < N$ menghasilkan teks saifer $C^{(t)}$ bermodulo N. Katakan $(P, N) = 1$ dan $\left(C^{(t)}, N\right) = 1$ bagi setiap $t = 1, 2, 3, \ldots$. Andaikan kunci pengkriptan yang digunakan integer positif e sedemikian hingga $(e, N) = 1$.

Algoritma pengkriptanan P ber*modulo* N pada transformasi pertama akan menghasilkan mesej $C^{(1)}$ ber*modulo* N melalui transformasi *Pengkriptanan Monofungsi LUC*

$$C^{(1)} \equiv V_e(P,1) (mod\ N).$$

Seterusnya mesej $C^{(1)}$ diterjemahkan kepada mesej saifer $C^{(2)}$ ber*modulo N* pada transformasi ke-2 melalui transformasi *Pengkriptanan Dwifungsi LUC*

$$C^{(2)} \equiv V_e\left(C^{(1)},1\right)(mod\ N).$$

Kemudian, mesej $C^{(2)}$ diterjemahkan kepada mesej saifer $C^{(3)}$ ber*modulo N* pada transformasi ke-3 menerusi transformasi *Pengkriptanan Trifungsi LUC*

$$C^{(3)} \equiv V_e\left(C^{(2)},1\right)(mod\ N).$$

Selanjutnya, transformasi pengitlakannya melalui transformasi *Pengkriptanan Polifungsi LUC*

$$C^{(t)} \equiv V_e\left(C^{(t-1)},1\right)(mod\ N).$$

Transformasi pengkriptanan di atas boleh diringkaskan sebagai

$$C^{(t)} \equiv V_{e^t}(P,1)(mod\ N).$$

2.0 TRANSFORMASI POLIFUNGSI LUC

Kita akan menggunakan transformasi Pengkriptanan Dwifungsi LUC $C^{(2)} \equiv V_{e^2}(P,1)(mod\ N)$ (*lihat* Takrif 1). Perhatikan bahawa bagi setiap transformasi, nilai $S(N)$ perlu dicari. Satu persoalan timbul, mungkinkah wujud nilai $S(N)$ yang sama, sama ada dianalisis daripada P atau pun $V_{e^2}(P,1)$? Ini penting bagi tujuan mendapatkan kunci penghurai d daripada perkaitan $ed \equiv 1\left(mod\ S(N)\right)$ dengan nilai $S(N)$ yang sama dan seterusnya menguji nilai d agar tidak menyamai e dengan perkaitan $e^2 \not\equiv 1\left(mod\ S(N)\right)$. Perlu diingat bahawa $S(N)$ berbeza menyebabkan d yang dimiliki oleh penerima mesej berbeza daripada d yang dimiliki oleh pengutus mesej. Keadaan ini menyebabkan penerima mesej gagal mengesan mesej asal.

Berikut adalah beberapa penegasan yang akan menghuraikan permasalahan tersebut.

Teorem 3

Katakan $N = pq$. Secara bersimetri, jika $\left(U_{e^2}(P,1),N\right)=1$ maka fungsi Lehmer Totient mempunyai nilai yang sama, sama ada dikira menggunakan $V_e(P,1)$ atau $V_{e^2}(P,1)$ bermodulo N.

Pembuktian

Katakan pembeza layan bagi $V_e(P,1)$ bernilai $D^{(1)} = V_e^2(P,1) - 4$ manakala pembeza layan bagi $V_{e^2}(P,1)$, $D^{(2)} = V_{e^2}^2(P,1) - 4$.

Daripada identiti Lucas (3), $V_{e^2}^2(P,1) - 4 = D^{(1)}U_{e^2}^2(P,1)$. Maka kita mendapati

$$\left(\frac{D^{(2)}}{p}\right) = \left(\frac{D^{(1)}U_{e^2}^2}{p}\right).$$

Jika $\left(U_{e^2}(P,1), N\right) = 1$ maka $\left(U_{e^2}^2\right)^{\frac{p-1}{2}} \equiv U_{e^2}^{p-1} \equiv 1 (mod\ p)$. Oleh itu $\left(\frac{D^{(2)}}{p}\right) = \left(\frac{D^{(1)}}{p}\right)$. Ini bermakna $\left(\frac{D^{(2)}}{p}\right) = \left(\frac{V_{e^2}^2(P,1)-4}{p}\right) = \left(\frac{V_e^2(P,1)-4}{p}\right)$ juga $\left(\frac{D^{(2)}}{q}\right) = \left(\frac{V_{e^2}^2(P,1)-4}{q}\right) = \left(\frac{V_e^2(P,1)-4}{q}\right)$. Jadi, Fungsi Lehmer Totient sentiasa sama tidak kira dianalisis daripada $V_e(P,1)$ atau pun $V_{e^2}(P,1)$.

Teorem 4

Katakan $N = pq$. Jika $\left(U_{e^2}(P,1), N\right) = 1$ maka Fungsi Lehmer Totient mempunyai nilai yang sama, sama ada diperoleh menggunakan P atau $V_{e^2}(P,1)$ bermodulo N.

Pembuktian

Daripada Teorem 1 dan Teorem 3, jika $\left(U_{e^2}(P,1), N\right) = 1$ maka $\left(\frac{D^{(2)}}{p}\right) = \left(\frac{D^{(1)}}{p}\right) = \left(\frac{D}{p}\right)$ juga $\left(\frac{D^{(2)}}{q}\right) = \left(\frac{D^{(1)}}{q}\right) = \left(\frac{D}{q}\right)$. Oleh itu, Fungsi Lehmer Totient mempunyai nilai yang sama, sama ada diperoleh menggunakan P atau $V_{e^2}(P,1)$.

Daripada dua penegasan di atas, satu ketetapan dibuat untuk mendapatkan $S(N)$ hanya berdasarkan P dan sahaja $V_{e^2}(P,1)$.

Sebelum penghuraian teks saifer dilaksanakan, individu penerima mestilah mendapatkan pembeza layan bagi $C^{(2)}$, iaitu $D^{(2)} = \left(C^{(2)}\right)^2 - 4$, seterusnya mendapatkan nilai $S(N)$ dan kunci penghurai d daripada perkaitan $ed \equiv 1 \left(mod\, S(N)\right)$.

Berikut dibentangkan kaedah kriptografi berorientasikan transformasi Dwifungsi LUC.

Teorem 5

Katakan penterjemahan P kepada $C^{(2)}$ menerusi *transformasi Dwifungsi LUC*

$$C^{(2)} \equiv V_{e^2}(P,1)(mod\, N) \quad (lihat \text{ Takrif 1})$$

Jika $\left(U_{e^2}(P,1), N\right) = 1$ dan $\left(e, S(N)\right) = 1$ dengan $D = P^2 - 4$ maka algoritma penghuraian $C^{(2)}$ kepada mesej P berbentuk

$$C^{(1)} \equiv V_d\left(C^{(2)}, 1\right)(mod\, N)$$

$$p \equiv V_d\left(C^{(1)}, 1\right)(mod\, N)$$

Transformasi penghuraian di atas boleh kita ringkaskan seperti berikut

$$P \equiv V_d\left(V_d\left(C^{(2)}, 1\right)\right)(mod\, N)$$

$$\equiv V_{d^2}\left(C^{(2)}, 1\right)(mod\, N)$$

dengan kunci penghurai d merupakan songsangan bagi e yang diperolehi daripada $de \equiv 1\left(mod\, S(N)\right)$ dengan pembeza layan $D^{(2)} = \left(C^{(2)}\right)^2 - 4$.

Pembuktian

Daripada Teorem 4, jika $\left(U_{e^2}(P,1), N\right) = 1$ maka Fungsi Lehmer Totient mempunyai nilai yang sama, sama ada dikira menggunakan P atau $V_{e^2}(P,1)(mod\, N)$. Andaikan Fungsi Lehmer Totient tersebut $S(N)$.

Jika $\left(e, S(N)\right) = 1$ maka wujud kunci penghurai d sedemikian hingga $ed = kS(N) + 1$ untuk suatu integer k dan d diperolehi daripada algoritma Euklidan.

Katakan transformasi pengkriptanan P kepada $C^{(2)}$ ditakrifkan sebagai

$$C^{(2)} \equiv V_{e^2}(P,1)(mod\, N)$$

maka

$$
\begin{aligned}
V_{d^2}\left(C^{(2)},1\right) &\equiv V_{d^2}\left(V_{e^2}(P,1),1\right)(mod\ N) \\
&\equiv V_{d^2}\left(V_e\left(V_e(P,1)\right),1\right)(mod\ N) && \text{daripada (6)} \\
&\equiv V_{d^2}\left(V_e\left(C^{(1)},1\right)\right)(mod\ N) && \text{daripada Takrif 1} \\
&\equiv V_d\left(V_{ed}\left(C^{(1)},1\right)\right)(mod\ N) && \text{daripada (6)} \\
&\equiv V_d\left(C^{(1)},1\right)(mod\ N) && \textit{lihat} \text{ pembuktian Teorem 2} \\
&\equiv P\,(mod\ N) && \textit{lihat} \text{ pembuktian Teorem 2}
\end{aligned}
$$

Jadi, kita telah membuktikan bahawa algoritma penghuraian $C^{(2)}$ kepada P ialah

$$P \equiv V_{d^2}\left(C^{(2)},1\right)(mod\ N)$$

Penterjemahan mesej asal P ber*modulo* N kepada mesej saifer $C^{(2)}$ melalui transformasi Dwifungsi LUC $C^{(2)} \equiv V_{e^2}(P,1)(mod\ N)$ sebelum ini akan diteruskan lagi sehingga transformasi trifungsi menghasilkan mesej saifer $C^{(2)}$ ber*modulo* N. Kita akan menggunakan algoritma Pengkriptanan Trifungsi LUC

$$C^{(3)} \equiv V_{e^3}(P,1)(mod\ N) \quad \text{(lihat Takrif 1)}$$

Pengutus mesej perlu memastikan bahawa nilai $S(N)$ yang diperolehi daripada pemerhatian terhadap pembeza layan $D = P^2 - 4$ dan $D^{(3)} = V_{e^3}^2(P,1) - 4$ adalah sama. Ini penting agar penerima mesej boleh memperolehi kunci penghurai d sedemikian hingga $\left(e, S(N)\right) = 1$ seterusnya mengesan mesej asal. Justeru itu penerima mesej hanya akan mempertimbangkan pembeza layan bagi $C^{(3)}$ iaitu $D^{(3)} = \left(C^{(3)}\right)^2 - 4$ bagi mendapatkan nilai $S(N)$ seterusnya kunci songsangan d dengan mengabaikan pembeza layan bagi $C^{(2)}$ dan pembeza layan bagi $C^{(1)}$.

Teorem di bawah menjelaskan perbincangan di atas dengan mengambil $t = 3$.

Teorem 6

Sebagai keputusan daripada Teorem 1 dan Teorem 3 sebelum ini, dapat dilihat bahawa jika $\left(U_{e^t}(P,1), N\right) = 1$ maka Fungsi Lehmer Totient mempunyai nilai yang sama, sama ada dikira menggunakan P atau $V_{e^t}(P,1)$ bagi setiap $t = 1, 2, 3, \ldots$.

Seterusnya kita bentangkan kaedah kriptografi berorientasikan transformasi Trifungsi LUC seperti di bawah ini.

Teorem 7

Katakan penterjemahan P kepada $C^{(3)}$ menerusi transformasi pengkriptanan *Trifungsi LUC*

$$C^{(3)} \equiv V_{e^3}(P,1)(mod\ N) \quad (lihat \text{ Takrif } 1).$$

Jika $\left(V_{e^3}(P,1), N\right) = 1$ dan $\left(e, S(N)\right) = 1$ dengan $D = P^2 - 4$ maka algoritma penghuraian $C^{(3)}$ kepada mesej $C^{(2)}$ adalah berbentuk

$$C^{(2)} \equiv V_d\left(C^{(3)},1\right)(mod\ N).$$

Seterusnya mesej $C^{(2)}$ diterjemahkan kepada mesej $C^{(1)}$ melalui transformasi

$$C^{(1)} \equiv V_d\left(C^{(2)},1\right)(mod\ N).$$

Akhir sekali, kita akan mengesan mesej asal P melalui penghuraian $C^{(1)}$ dengan transformasi

$$P \equiv V_d\left(C^{(1)},1\right)(mod\ N).$$

Transformasi penghuraian tersebut boleh diringkaskan seperti berikut:

$$\begin{aligned} P &\equiv V_d\left(V_d\left(C^{(2)},1\right),1\right)(mod\ N) \\ &\equiv V_d\left(V_d\left(V_d\left(C^{(3)},1\right),1\right),1\right)(mod\ N) \\ &\equiv V_{d^3}\left(C^{(3)},1\right)(mod\ N). \end{aligned}$$

dengan kunci penghurai d merupakan songsangan bagi e yang diperolehi daripada $de \equiv 1\left(mod\ S(N)\right)$ dengan pembeza layan $D^{(3)} = \left(C^{(3)}\right)^2 - 4$.

Pembuktian

Daripada Teorem 6, jika $\left(U_{e^3}(P,1), N\right) = 1$ maka Fungsi Lehmer Totient mempunyai nilai yang sama, sama ada dikira menggunakan P atau $V_{e^3}(P,1)(mod\ N)$. Andaikan Fungsi Lehmer Totient tersebut $S(N)$.

Jika $(e,S(N))=1$ maka wujud kunci penghurai d sedemikian hingga $ed=kS(N)+1$ untuk sebarang integer k dan d diperolehi daripada algoritma Euklidan.

Katakan transformasi pengkriptanan P kepada $C^{(3)}$ ditakrifkan sebagai

$$C^{(3)} \equiv V_{e^3}(P,1)(mod\ N)$$

maka

$$\begin{aligned} V_{d^3}\left(C^{(3)},1\right) &\equiv V_{d^3}\left(V_{e^3}(P,1),1\right)(mod\ N) \\ &\equiv V_{d^3}\left(V_e\left(V_{e^2}(P,1)\right),1\right)(mod\ N) && \text{daripada (6)} \\ &\equiv V_{d^3}\left(V_e\left(C^{(2)},1\right)\right)(mod\ N) && \text{daripada Takrif 1} \\ &\equiv V_{d^2}\left(V_{ed}\left(C^{(2)},1\right)\right)(mod\ N) && \text{daripada (6)} \\ &\equiv V_{d^2}\left(C^{(2)},1\right)(mod\ N) && \textit{lihat} \text{ pembuktian Teorem 2} \\ &\equiv P(mod\ N) && \textit{lihat} \text{ pembuktian Teorem 5} \end{aligned}$$

Jadi, kita telah membuktikan bahawa algoritma penghuraian $C^{(3)}$ kepada P ialah

$$P \equiv V_{d^3}\left(C^{(3)},1\right)(mod\ N).$$

Secara am, katakan mesej saifer yang terhasil daripada pengkriptanan P pada transformasi ke-t dengan t = 1, 2, 3, … maka kita mengitlakkan teknik kriptografi berasaskan transformasi Monofungsi LUC kepada yang lebih umum, iaitu transformasi Polifungsi LUC 1 sepertimana digambarkan dalam Teorem 8 di bawah.

Teorem 8

Katakan penterjemahan P kepada $C^{(t)}$ menerusi transformasi pengkriptanan *Polifungsi LUC.*

$$C^{(t)} \equiv V_{e^t}(P,1)(mod\ N) \quad (\textit{lihat}\ \text{Takrif 1})$$

Jika $\left(U_{e^t}(P,1),N\right)=1$ dan $(e,S(N))=1$ dengan $D=P^2-4$ maka algoritma penghuraian $C^{(t)}$ kepada mesej asal P akan berbentuk

$$P \equiv V_{d^t}\left(C^{(t)},1\right)(mod\ N).$$

Dengan kunci penghurai d merupakan songsangan bagi e yang diperolehi daripada $de \equiv 1(mod\, S(N))$ dengan pembezalayan $D^{(t)} = \left(C^{(t)}\right)^2 - 4$.

(Teorem 8 di atas merupakan keputusan daripada Teorem 5 dan Teorem 7).

Contoh 1 di bawah merupakan ilustrasi daripada Teorem 8 di atas dengan mengambil $t = 3$.

Contoh 1

Katakan kita ingin mengutuskan mesej asal, iaitu $P = 12$. Kita memilih dua nombor perdana berbeza, iaitu $p = 23$ dan $q = 19$ maka $N = 437$ sedemikian hingga $P < N$ dan $(P, N) = 1$. Pembeza layan bagi mesej P ialah $D = 140$. Ia memenuhi syarat $(D, N) = 1$.

Simbol Legendre $\left(\frac{D}{p}\right) = 1$ dan $\left(\frac{D}{q}\right) = 1$ diperolehi terlebih dahulu sebelum mendapat Fungsi Lehmer Totient $S(N) = 198$. Seterusnya, kita pilih kunci pengkriptan $e = 7$ yang perdana relatif dengan N dan $S(N)$ juga $e^2 \not\equiv 1(mod\, S(N))$. Kunci penghurai $d = 85$ diperolehi daripada syarat $ed \equiv 1(mod\, S(N))$. Jelas $e \neq d$.

Identiti $U_{7^3}(12,1) = 172$ jadi $\left(U_{7^3}(12,1), 437\right) = 1$ menyebabkan $S(N)$ daripada pemerhatian juga bernilai 198. Oleh itu, penerima mesej boleh mengesan mesej asal dengan menggunakan kunci penghurai.

Algoritma pengkriptanan $P = 12$ kepada mesej saifer $C^{(3)} = 88$ melalui transformasi trifungsi adalah seperti berikut:

$$C^{(1)} \equiv V_7(12,1) \equiv 124\,(mod\, 437)$$
$$C^{(2)} \equiv V_7(124,1) \equiv 339\,(mod\, 437)$$
$$C^{(3)} \equiv V_7(339,1) \equiv 88\,(mod\, 437)$$

atau boleh diringkaskan sebagai $C^{(3)} \equiv V_{7^3}(12,1) \equiv 88\,(mod\, 437)$.

Penerima mesej perlu mempertimbangkan $D^{(3)} = \left(C^{(3)}\right)^2 - 4 = 7740$ maka $\left(\frac{D^{(3)}}{p}\right) = \left(\frac{12}{23}\right) = 1$ dan $\left(\frac{D^{(3)}}{q}\right) = \left(\frac{7}{19}\right) = 1$ seterusnya $S(N) = 198$. Oleh itu, kunci penghurai $d = 85$ diperolehi daripada perkaitan $7d \equiv 1(mod\, 198)$. Proses seterusnya, iaitu menghuraikan $C^{(3)} = 88$ kepada mesej asal $P = 12$ menerusi algoritma berikut:

$$C^{(2)} \equiv V_{85}(88,1) \equiv 339 \,(mod\, 437)$$
$$C^{(1)} \equiv V_{85}(339,1) \equiv 124 \,(mod\, 437)$$
$$P \equiv V_{85}(124,1) \equiv 12 \,(mod\, 437)$$

atau boleh diringkaskan sebagai $P \equiv V_{85^3}(88,1) \equiv 12 \,(mod\, 437)$.

3.0 KONSEP KALAAN FUNGSI LUCAS DALAM PENETAPAN SYARAT MESEJ ASAL TIDAK MENYAMAI MESEJ SAIFER

Sekarang kita perhatikan bahawa walaupun penghantaran mesej memenuhi syarat $(D,N)=1$, $(e,N)=1$, $(e,S(N))=1$ dan $(P<N,N)=1$ tetapi setelah beberapa kali transformasi, kadangkala mesej asal P menyamai mesej saifer $C^{(t)} \equiv V_{e^t}(P,1)(mod\, N)$. Jadi perutusan mesej sebegini merupakan suatu yang sia-sia. Berikut adalah contoh pengkriptanan mesej yang menghasilkan mesej asalnya semula.

Katakan $P = 23$, $N = 187$, $e = 5$ dan $S(N) = 48$.

Maka $C^{(1)} = 45$ dan $C^{(2)} = 23$.

Punca mengapa keadaan ini berlaku kita bincangkan dengan lebih terperinci lagi dengan menggunakan konsep kalaan fungsi Lucas $V_{n+1} = PV_n - V_{n-1}$. Berpandukan $P = 23$ sama seperti di atas, kita memperolehi suatu jujukan, iaitu $V_0 = 2$, $V_1 = P = 23$, $V_2 = 153$, $V_3 = 130, \ldots$, $V_{23} = 23$, $V_{24} = 2 = V_0$, $V_{25} = 23 = V_1$, $V_{26} = 153 = V_2$, $V_{27} = 130 = V_3, \ldots$. Maka bilangan kalaan n bagi jujukan tersebut ialah 24 diilustrasikan daripada $V_n = V_0$ dan $V_{n+1} = V_1$. Jelas di sini bahawa

$$V_{e^2} \equiv P \,(mod\, N) \text{ maka } V_{25} \equiv 23 \,(mod\, 187)$$

dan

$$e^2 \equiv 1 \,(mod\, N) \text{ maka } 25 \equiv 1 \,(mod\, 24)$$

Seterusnya, pengkriptanan mesej yang sama, iaitu $P = 23$ untuk pusingan yang kedua menghasilkan

$$C^{(3)} = 45 \text{ dan } C^{(4)} = 23 = P.$$

Maka sekarang kita perhatikan bahawa

$$V_{e^4} \equiv P \,(mod\, N) \text{ maka } V_{652} \equiv 23 \,(mod\, 187)$$

dan

$$e^4 \equiv 1(mod\, n) \text{ maka } 625 \equiv 1(mod\, 24)$$

Bagi sebarang transformasi ke-t yang menyebabkan $P = C^{(t)}$ boleh diungkapkan secara ringkas sebagai $C^{(t)} = 1$ manakala perkaitan antara t dengan kalaan n yang menyebabkan keadaan ini berlaku diwakili oleh ungkapan $e^t \equiv 1(mod\, n)$. Kuasa t terkecil dinamai peringkat e modulo n. Integer t tidak melebihi bilangan kalaan n iaitu $t \leq n$. Ini kerana terdapat kemungkinan sebanyak n mesej berbeza atau kurang. Dari aspek pelaksanaan, peringkat yang kecil tidak begitu selamat. Akhir sekali, kita perhatikan bahawa $C^{(t)} \neq 1$ apabila $e^t \not\equiv 1(mod\, n)$. Misalnya jika bilangan transformasi $t = 3$ maka $5^3 \not\equiv 1(mod\, 24)$, oleh itu $C^{(3)} \neq P$.

4.0 KEKEBALAN SISTEM POLIFUNGSI LUC

Kita telah mengetahui beberapa ciri kekebalan sistem Monofungsi LUC misalnya kewujudan kunci awam N hasil daripada pendaraban dua nombor perdana berbeza p dan q yang besar, penggunaan Fungsi Lehmer Totient $S(N)$ yang agak kompleks iaitu $S(N) = g.s.k\left(p - \left(\frac{D}{p}\right), q - \left(\frac{D}{q}\right)\right)$ dan sifat homomorfisma sistem LUC. Ciri-ciri tersebut amat membantu pembinaan sistem Polifungsi LUC dalam kajian ini. Selain itu, struktur fungsi Lucas yang agak kompleks menyebabkan individu musuh sukar mengesan teks asal dengan menggunakan Teorem Baki Cina (akan diperjelaskan dalam bahagian seterusnya), tambahan pula apabila bilangan transformasinya bertambah.

Untuk meningkatkan tahap keselamatan sistem Polifungsi LUC ini, kita merahsiakan bilangan transformasi t daripada pengetahuan umum tetapi kita perlu memastikan terlebih dahulu bahawa mesej asal tidak menyamai mesej saifer pada transformasi ke-t. Penterjemahan mesej asal kepada mesej saifer sehingga menyamai mesej asalnya semula dianggap sebagai satu kalaan. Katakan $C^{(10)} = P$ maka 1 kalaan bersamaan 10 transformasi. Jadi, kita tidak dibenarkan sama sekali mengkriptan dengan $t = 10$. Pengkriptanan dengan $t > 10$ hanya akan mengulang algoritma pengkriptanan. Ini adalah sia-sia. Manakala pengkriptanan dengan $t < 10$ dianggap tidak selamat kerana pihak musuh hanya perlu menghurai teks saifer sebanyak tidak lebih 9 transformasi. Bagaimanakah cara untuk kita mengetahui 1 kalaan bersamaan dengan beberapa transformasi masih di peringkat kajian. Kita mencadangkan pelaksanaan sistem dengan 1 kalaan bersamaan sebilangan transformasi yang besar. Oleh yang demikian, kebarangkalian untuk mendapat mesej asal sebenar sangat tipis.

Tafsiran terhadap mesej asal hanya akan terjadi sekiranya pihak musuh dapat memecah kerahsiaan kunci penghurai *d* dan mengetahui pola sistem kriptografi yang sedang digunakan. Oleh kerana dua nombor perdana berbeza *p* dan *q* turut dirahsiakan maka pihak musuh tidak mungkin memperolehi nilai Fungsi Lehmer Totient bagi mesej saifer. Jadi, amat mustahil untuk mendapatkan *d* daripada perkaitan $ed \equiv 1(mod\, S(N))$.

Wujudnya satu algoritma pengkriptanan yang agak panjang dianggap seolah-olah satu kelemahan memandangkan masa untuk mendapatkan mesej saifer terlalu lama sekiranya subskrip pengkriptanan besar. Kita misalkan mesej asal *P* ingin diterjemahkan kepada mesej saifer $C^{(1)}$ melalui transformasi monofungsi $V_e(P,1)(mod\, N)$. Langkah pengiraan V_e ini adalah menggunakan identiti Lucas $V_{2n} = V_n^2 - 2$ dan $V_{2n+1}V_n = V_{n+1} - P$ dengan $V_1 = P$. Bilangan langkah yang diperlukan sebanyak 3 langkah sekiranya e = 3, jika e = 7 maka terdapat 5 langkah, jika e = 100 akan memberikan 50 langkah pengiraan seterusnya jika nilai e yang agak besar, iaitu $e = 10^{100}$ memerlukan lebih kurang $\log_2 10^{100} = 332$ langkah (*lihat* [2] m/s 110). Bilangan atur cara akan meningkat dengan pertambahan bilangan transformasi. Misalnya t = 10 transformasi maka sebanyak 10(332) = 3320 langkah yang merupakan sejumlah angka yang agak besar untuk dianalisis. Namun begitu dengan adanya kemajuan sistem perisian komputer masa kini yang kita ketahui 16 kali lebih cekap berbanding 10 tahun yang lampau maka tidak mustahil individu pengutus mesej dapat mengkriptan mesej dalam masa yang singkat. Pada kelazimannya, subskrip pengkriptan merupakan satu integer yang jauh lebih kecil berbanding subskrip penghurai. Ini bertujuan untuk mengurangkan sekurang-kurangnya separuh bilangan langkah pengkriptanan. Walau bagaimanapun, kita tidak dapat mengawal sepenuhnya nilai subskrip penghurai. Contoh pemilihan kunci pengkriptan *e* yang dianggap sesuai iaitu nombor perdana 65,537. Ini kerana terdapat 15 bit yang sifar daripada 17 bit (*lihat* [6] m/s 48). Bilangan bit yang mengandungi banyak sifar akan memudahkan proses pengiraan yang melibatkan *e,* seterusnya mengurangkan bilangan langkah pengkriptanan.

5.0 PENGESANAN MESEJ ASAL DENGAN TEOREM BAKI CINA DALAM SISTEM LUC

Dalam rangkaian komunikasi, kita tidak semestinya mengutuskan maklumat rahsia kepada seorang individu atau kelompok sahaja. Kita mungkin akan mengutuskan maklumat yang sama kepada beberapa entiti berlainan. Dengan demikian, kita memerlukan sistem kriptografi yang selamat agar kerahsiaan mesej terpelihara. Dalam bahagian ini, kita meninjau sejauh manakah sistem kriptografi berorientasikan sistem LUC dalam kajian kita akan kebal daripada teknik pengesanan teks asal ini.

Struktur fungsi Lucas yang agak kompleks menyebabkan individu musuh sukar mengesan teks asal dengan menggunakan Teorem Baki Cina tambahan pula apabila bilangan transformasi bertambah.

Ambil kunci awam $e = 3$. Mesej P akan diutuskan kepada dua individu berbeza, iaitu individu $g = 1,2$. Katakan mesej saifernya ialah C_g bermodulo N_g dengan N_1 dan N_2 perdana relatif antara satu sama lain.

Andaikan model pengkriptanan sistem LUC yang digunakan ialah

$$C_g \equiv V_3(P,1)\left(mod\, N_g\right)$$

Daripada Teorem Baki Cina dan Algoritma Gauss, kita akan memperolehi penyelesaian unik

$$x \equiv \sum_{k=1}^{g} C_k R_k S_k \,(mod\, G)$$

dengan $R_k = \dfrac{G}{N_k}$, $S_k \equiv R_k^{-1}\left(mod\, N_k\right)$, x sebarang integer positif dan $G = N_1 N_2$.

Daripada identiti Lucas (1), kita tuliskan

$$x \equiv V_3(P,1) \equiv PV_2 - P \equiv P\left(PV_1 - 2\right) - P \equiv P^3 - 3P\left(mod\, G\right)$$

maka $P^3 - 3P - x \equiv 0\left(mod\, G\right)$.

Seterusnya, lakukan proses pemfaktoran polinomial bermodulo G bagi memperolehi P (*lihat* [1] m/s 36).

Contoh 2 menunjukkan bagaimana suatu sistem LUC Monofungsi boleh dicerobohi oleh pihak musuh.

Contoh 2

Tujuan utama penggunaan Teorem Baki Cina dalam contoh ini adalah untuk mengesan mesej asal $P = 8$. Katakan $e = 3$, $g = 1,2$, $N_1 = 91$, $N_2 = 323$ maka $G = 29393$. Katakan mesej saifer diutuskan kepada dua individu tertentu dan digambarkan seperti berikut:

$$P\,? \begin{cases} \longrightarrow C_1 \equiv 33\,(mod\, 91) \\ \longrightarrow C_2 \equiv 165\,(mod\, 323) \end{cases}$$

Dengan Teorem Baki Cina dan Algoritma Gauss, kita memperolehi penyelesaian unik $x \equiv 488\left(mod\, 29393\right)$.

Oleh itu, $P^3 - 3P - 488 \equiv 0 \pmod{29393}$

$$(P-8)\left(P^2+8P+61\right) \equiv 0 \pmod{29393}$$

Daripada $P - 8 \equiv 0 \pmod{29393}$, kita menyelesaikan dua persamaan kongruen serentak berikut

$$P - 8 \equiv 0 \pmod{91} \quad \text{dan} \quad P - 8 \equiv 0 \pmod{323}$$

untuk mengesan mesej asal $P = 8$.

Atau daripada $P^2 + 8P + 61 \equiv 0 \pmod{29393}$, pihak musuh cuba menyelesaikan dua persamaan kongruen serentak berikut

$$P^2 + 8P + 61 \equiv 0 \pmod{91}$$

$$\text{dan } P^2 + 8P + 61 \equiv 0 \pmod{323}.$$

Namun demikian, kita tidak dapat menentukan sama ada terdapat penyelesaian bagi P ataupun tidak dengan menggunakan simbol Legendre $\left(\frac{D}{N_1}\right)=\left(\frac{184}{91}\right)$ dan $\left(\frac{D}{N_2}\right)=\left(\frac{184}{323}\right)$ kerana nilai kedua-duanya lain daripada 1 dan –1. Ini menjamin kerahsiaan P. Namun begitu, pada hakikatnya modulo N_g yang digunakan dalam contoh ini terlalu mudah difaktorkan bagi memperolehi dua nombor perdana berbezanya seterusnya mendapatkan kunci penghurai bagi setiap C_g untuk tujuan mengenal pasti mesej asal.

Pemfaktoran trinomial bermodulo G di atas masih dianggap mudah disebabkan nilai e kecil. Namun begitu, nilai e yang besar akan menyebabkan darjah polinomial bertambah seterusnya merumitkan proses pemfaktoran. Sistem perutusan mesej akan menjadi lebih selamat sekiranya kita menggunakan transformasi Polifungsi LUC. Ini kerana, pihak musuh terpaksa mendapatkan mesej asal dengan pemfaktoran polinomial berdarjah e^t.

6.0 KESIMPULAN

Kajian kita telah membina beberapa model perutusan mesej berasaskan transformasi Pengkriptanan Monofungsi LUC $C^{(1)} \equiv V_e(P,1) \pmod{N}$. Sistem tersebut kemudiannya dilanjutkan kepada dua sistem kriptografi berikut:

(i) *Transformasi Dwifungsi LUC*

$$C^{(2)} \equiv V_{e^2}(P,1)(mod\ N)$$

$$P \equiv V_{d^2}\left(C^{(2)},1\right)(mod\ N) \qquad (\textit{lihat}\ \text{Teorem 5})$$

dan

(ii) *Transformasi Trifungsi LUC*

$$C^{(3)} \equiv V_{e^3}(P,1)(mod\ N)$$

$$P \equiv V_{d^3}\left(C^{(3)},1\right)(mod\ N) \qquad (\textit{lihat}\ \text{Teorem 7}).$$

Untuk membolehkan sistem perutusan mesej menjadi lebih selamat dengan bilangan transformasi t dirahsiakan daripada pengetahuan umum maka kita telah mengitlakkan sistem LUC kepada sistem Polifungsi LUC

$$C^{(t)} \equiv V_{e^t}(P,1)(mod\ N)$$

$$P \equiv V_{d^t}\left(C^{(t)},1\right)(mod\ N) \qquad (\textit{lihat}\ \text{Teorem 8}).$$

BIBLIOGRAFI

[1] Cohen, H. 1993. *A Course in Computational Algebraic Number Theory*. New York: Spinger-Verlag.

[2] Riesel, H. 1994. *Prime Numbers and Computer Methods for Factorization*. Boston: 2nd edition, Birkhauser.

[3] Rivest, R., A. Shamir, L. Adleman. 1978. *A method for obtaining digital signatures and public key cryptosystem.* Communications of the ACM, 120-126.

[4] Said, M. R. 1997. *Applications of Reccurence Relations to Cryptography.* Tesis Ph.D., *Macquarie University*. Sydney: New South Wales.

[5] Schroeder, M. R. 1986. *Number Theory in Science and Communication.* 2nd edition, Spinger-Verlag, Berlin Hidelberg, New York, Tokyo.

[6] Smith, P. 1993. *LUC Public-key Encryption: A secure alternative to RSA*. Dr. Dobb's Journal, 44-48.

[7] Smith, P. dan Michael Lennon. 1993. *Luc: A new public key system.* Kertaskerja ini ditulis di *University of Auckland*. New Zealand.