GABUNGAN KRIPTOGRAFI LENGKUK ELIPTIK DAN SAIFER HILL DALAM PERUTUSAN IMEJ BERSKALA SAMAR (2)

Article · April 2023

CITATION
1

READS
45

2 authors, including:

Faridah Binti Yunos
Universiti Putra Malaysia
38 PUBLICATIONS **99** CITATIONS

SEE PROFILE

JURNAL

ASAS ILMU MATEMATIK

Jilid 1 Bilangan 4 Disember 2022

PENELAAHAN DAN PENEROKAAN BUDAYA BERMATEMATIK

JURNAL ASAS ILMU MATEMATIK
PP19700/01/2022 (035313) ISSN 2821-3459
Jilid 1 Bilangan 4 • DISEMBER 2022

PENERBIT
PUSTAKA ILMU MATEMATIK

JURNAL ASAS ILMU MATEMATIK

Jurnal Asas Ilmu Matematik (JAIM) ini ialah sebuah jurnal antarabangsa berwasit yang menerbitkan hasil penyelidikan yang asli dalam semua bidang matematik dan statistik untuk pelajar pada peringkat sekolah menengah hingga sarjana muda.

Pembaca Pruf: Noriah Mohamed, *Jurnal Kalam Enterprise, Malaysia*
Ilustrasi Kulit Jurnal: 'Arifa Zulfa As Sa'adah, *Institut Seni Indonesia, Yogyakarta, Indonesia*

Jurnal Asas Ilmu Matematik diterbitkan empat kali setahun pada bulan Mac, Jun, September, Disember oleh Pustaka Ilmu Matematik beralamat di Lot 3116, Jalan Pantai, Kampung Pengkalan Maras, Mengabang Telipot, 21030 Kuala Terengganu, Terengganu, Malaysia. Tel: 0122881074.

Jurnal ini dicetak oleh Sinaran Bros Sdn. Bhd, 5-3-18, The Promenade, Persiaran Mahsuri, 11950 Bayan Baru, Pulau Pinang, Malaysia. Tel: 046180541, 04-6180981; Faks: 046180421.

Jurnal ini dijual dengan harga MYR 30 (di dalam Malaysia) USD 30 (di luar Malaysia).

KANDUNGAN

HALAMAN

ISSN 2821-3459

AKADEMI SAINTIS SAINS MATEMATIK MALAYSIA
(MALAYSIAN ACADEMY OF MATHEMATICAL SCIENTISTS)

PENERBIT
PUSTAKA ILMU MATEMATIK

Jurnal Asas Ilmu Matematik

Jurnal Asas Ilmu Matematik 2022, 1(4): 68–81

GABUNGAN KRIPTOGRAFI LENGKUK ELIPTIK DAN SAIFER HILL DALAM PERUTUSAN IMEJ BERSKALA SAMAR

[1]Faridah Yunos dan [2]Muhammad Noor Akmal Buhari
[1]Jabatan Matematik dan Statistik, Fakulti Sains, Universiti Putra Malaysia
[1, 2]Institut Penyelidikan Matematik, Universiti Putra Malaysia
[2]Fakulti Sains, Universiti Teknologi Malaysia
[1]faridahy@upm.edu.my

Abstrak: Kriptografi Lengkuk Eliptik (ECC) ialah suatu penyulitan kunci asimetri yang kompleks, manakala Saifer Hill menggunakan penyulitan simetri yang mudah. Kajian terdahulu mendapati bahawa matriks kunci tersongsangkan kendiri yang dibina daripada domain parameter lengkuk eliptik di atas medan perdana telah diadaptasikan dalam meningkatkan keselamatan dan kecekapan perutusan mesej berskala samar melalui sistem gabungan ECC dan Saifer Hill. Makalah ini bertujuan memperkenalkan penggunaan lengkuk eliptik di atas medan dedua sebagai menggantikan peranan lengkuk eliptik jenis sebelumnya, terutamanya semasa proses penjanaan kunci. Seterusnya, ubahsuaian kaedah penyulitan dan penyahsulitan dilakukan terhadap Saifer Hill yang konvensional.

Kata Kunci: penyulitan, penyahsulitan, Saifer Hill, tersongsangkan kendiri, kriptografi

1. Pengenalan

Kriptografi berasal daripada dua patah perkataan Greek, iaitu *kryptos* dan *graphein*. *Kryptos* bermaksud tersembunyi manakala *graphein* bermaksud secara bertulis (Rathidevi *et al.*, 2017). Kriptografi bermula dari tahun 1400. Bidang ini didominasi oleh pengistilahan baharu untuk 450 tahun kemudian dengan setiap huruf digantikan oleh huruf yang lain (dipanggil saifer) bergantung pada jadual penggantian huruf tertentu (Davies, 1997). Beberapa dekad yang lalu, kriptografi telah dibuktikan digunakan secara meluas dalam sistem keselamatan komunikasi. Biasanya, kriptografi dimanfaatkan untuk melindungi kerahsiaan syarikat korporat, mendapatkan maklumat sulit dan melindungi maklumat peribadi daripada dicerobohi.

Terdapat dua klasifikasi dalam kriptografi, iaitu kunci kriptografi simetri dan asimetri. Kunci jenis yang pertama dibahagikan kepada kunci silam dan kunci moden. Di bawah kriptografi silam, kita ada saifer transposisi dan gantian, manakala saifer moden dibahagikan kepada saifer aliran dan saifer blok. Kriptografi kunci simetri menggunakan kunci rahsia yang sama untuk kedua-dua penyulitan teks asal dan penyahsulitan teks saifer. Kekunci mungkin sama ataupun mungkin terdapat beberapa penjelmaan mudah untuk memperoleh kunci penyulitan daripada kunci penyahsulitan. Saifer Hill ialah skim kunci simetri terkenal yang memberi kesan kepada penjelmaan linear pada ruangan mesej. Saifer Hill terdiri daripada vektor integer berdimensi m (Hill, 1929), yakni rentetan abjad berperingkat m dalam teks asal yang ditulis semula dalam bentuk vektor bagi Z_m (Overbey, 2005).

Berasaskan kajian Christensen (2006), bentuk berangka bagi teks asal dalam Saifer Hill selalunya ditulis sebagai suatu matriks P. Matriks K dipilih untuk menjadi kunci utama yang dirahsiakan dan C ialah teks saifer. Ungkapan penyulitan P kepada C adalah seperti yang berikut:

$$C \equiv KP \bmod N$$

dengan N merupakan integer positif dan matriks yang terhasil yang dipadankan dengan huruf tertentu. Penyahsulitan daripada C kepada P pula dilakukan seperti yang berikut:

$$P \equiv K^{-1}C \bmod N$$

dengan K^{-1} merupakan songsangan bagi K dalam modulo N. Algoritma Saifer Hill ini mempunyai struktur yang mudah dan pengiraan yang pantas sekiranya K^{-1} mudah diperoleh. Jika kunci utama mempunyai songsangan, proses untuk menyahsulit teks saifer akan menjadi lebih sukar seiring dengan pertambahan bilangan dimensi kunci utama. Ini demikian kerana songsangan kunci ini harus dicari terlebih dahulu. Biasanya, kaedah operasi baris permulaan dan konsep songsangan pendaraban dalam aritmetik modulo digunakan untuk mendapatkan songsangan suatu matriks (Mollin, 2006; Bronson & Costa, 2007). Dengan mengambil faedah daripada penggunaan matriks tersongsangkan kendiri sebagai kunci rahsia Saifer Hill, proses mencari songsangan kunci utama sebelum melakukan proses penyahsulitan boleh dihapuskan. Acharya *et al.* (2007) telah membentangkan beberapa kaedah untuk menjanakan kunci yang sebegini bagi sebarang matra. Kaedah ini turut diguna pakai dalam sistem Saifer Hill yang diubahsuai seperti dalam kajian (Acharya *et al.*, 2009; Acharya *et al.*, 2010; Naveenkumar *et al.*, 2013; Dey, 2012; Dawahdeh *et al.*, 2018; dan Satapathy & Rajkumar, 2020).

Algoritma Saifer Hill mempunyai sistem keselamatan yang lemah kerana penghantar dan penerima perlu menggunakan dan berkongsi kunci peribadi yang sama dalam saluran yang mungkin tidak selamat. Bagi meningkatkan keselamatannya, Acharya *et al.* (2009) mengusulkan kaedah penjanaan tersongsangkan kendiri, terpilih atur dan lelaran semula kunci utama kerana skim ini dapat menghasilkan pola kunci yang berbeza untuk setiap blok penyulitan data.

Selain itu, Acharya *et al.* (2010) mencadangkan teknik daripada Sastry & Shankar (2008) untuk mendapatkan ciri-ciri biometrik dengan menggunakan Saifer Hill yang diubahsuai menggunakan kunci tersongsangkan kendiri dan sistem kripto yang mantap. Ini dapat menyelesaikan kelemahan Saifer Hill yang konvensional dengan menggunakan lelaran dan jalinan.

Kaedah penyulitan berasaskan imej digital meningkat dengan pesat seiring dengan peningkatan penggunaan rangkaian internet melalui media komunikasi. Perkongsian imej yang penting melalui saluran yang tidak selamat memberikan ruang imej tersebut digodam oleh penceroboh. Teknik penyulitan ialah kaedah yang sesuai untuk melindungi imej daripada serangan. Dey (2012) mencadangkan SD-AEI untuk penyulitan imej yang menggunakan teknik Saifer Hill yang diubahsuai dengan menggunakan matriks tersongsangkan kendiri. Matriks ini dijanakan oleh kata laluan yang sama yang digunakan dalam penyulitan sebelumnya untuk menjadikannya lebih selamat. Beliau juga menyatakan bahawa teknik ini boleh dikembangkan lagi dengan menambahkan manipulasi bit terhadap Saifer Hill untuk mengukuhkan algoritma penyulitan.

Naveenkumar *et al.* (2013) mencadangkan Saifer Hill dua peringkat yang merangkumi pemilihan blok persegi untuk memanipulasi matriks tersongsangkan kendiri. Ini bertujuan

untuk mengawal jumlah penyulitan bagi kadar penukaran piksel. Mereka menggunakan teknik Saifer Pesanan Persegi Latin untuk menjanakan blok asas bagi matriks tersongsangkan kendiri. Mereka juga membandingkan jumlah maklumat yang disulitkan antara Saifer Hill dua peringkat dan empat peringkat untuk meningkatkan kecekapan sesebuah kamera dan meningkatkan medan penggunaannya.

Kriptografi Lengkuk Elliptik (ECC) ialah suatu penyulitan kunci asimetri yang kompleks, manakala Saifer Hill menggunakan penyulitan simetri yang mudah. Teknik penyulitan imej yang menggabungkan ECC dengan Saifer Hill (ECCHC) telah dicadangkan dalam Dawahdeh *et al.* (2018) untuk menukar Saifer Hill daripada teknik simetri kepada asimetri dan meningkatkan keselamatan dan kecekapannya untuk menentang penggodam. Matriks kunci tersongsangkan kendiri berasal daripada parameter lengkuk eliptik $E_p: y^2 \equiv x^3 + ax + b \pmod{p}$ di atas medan perdana F_p digunakan untuk menjanakan penyulitan dan kunci rahsia penyahsulitan. Oleh itu, tidak perlu mencari matriks songsangan dalam proses penyahsulitan. Entropi, Isyarat Puncak kepada Nisbah Bunyi (PSNR) dan Intensiti Perubahan Purata Bersepadu (UACI) telah digunakan untuk menilai kecekapan penyulitan imej berskala samar dan membandingkan imej yang disulitkan dengan imej asal untuk menilai prestasi teknik penyulitan yang dicadangkan. Melalui ketiga-tiga kayu pengukur ini, kaedah ini dibuktikan lebih baik daripada sistem kripto sebelumnya yang dibangunkan oleh Panduranga & Naveen Kumar (2012) dan Naveen Kumar *et al.* (2012).

Untuk melindungi imej berskala samar, Satapathy & Rajkumar (2020) memodifikasi sistem ECCHC dan menamakannya MECCHC. Saifer Hill dalam ECCHC memerlukan imej asal yang dipetakan kepada nilai berangka sebelum melaksanakan penyulitan tetapi untuk kes penyulitan imej dalam MECCHC, pesanan asal ialah piksel imej yang sudah wujud dalam bentuk berangka dan tidak memerlukan fungsi pemetaan. Analisis membuktikan bahawa masa pengiraan bagi penyulitan dan penyahsulitan imej lebih cepat berbanding dengan kaedah ECCHC. Penilaian kecekapan yang menggunakan Entropi, PSNR dan UACI pula menunjukkan kesan yang setara seperti ECCHC.

Sorotan kajian di atas memberikan tumpuan kepada penggunaan kunci tersongsangkan kendiri yang bertujuan mengurangkan masa untuk mendapatkan songsangan bagi kunci penyahsulitan, seterusnya meningkatkan kecekapan dan keselamatan sistem Saifer Hill dan kembangannya. Analisis terkini menunjukkan kesan yang positif apabila digabungkan ECC dan Saifer Hill. Persoalan timbul, adakah terdapat jenis lengkuk lain yang boleh menggantikan E_p dan mempunyai kelebihan yang sama?

Susunan makalah ini adalah seperti yang berikut: Seksyen 2 memberikan padanan beberapa istilah dalam bahasa Melayu dengan bahasa Inggeris. Seksyen 3 menerangkan pelaksanaan matriks tersongsangkan kendiri dalam Saifer Hill dan pelbagaiannya dengan beberapa kelebihan. Dalam Seksyen 4, diberikan penerangan ringkas tentang persamaan lengkuk eliptik yang akan digunakan dalam kajian. Seksyen 5 pula mengutarakan semula Algoritma Saifer Hill yang konvensional. Seksyen 6 mengusulkan sistem kripto yang menggabungkan antara ECC yang berasaskan lengkuk E dalam medan dedua dan Saifer Hill. Seksyen 6 diikuti pula dengan contoh pelaksanaannya dalam Seksyen 7. Bab terakhir mengandungi kesimpulan makalah.

2. Istilah

Istilah yang digunakan merujuk istilah Dewan Bahasa dan Pustaka di *Pusat Rujukan Persuratan Melayu* (PRPM). Beberapa istilah yang digunakan dalam makalah ini dipaparkan dalam Jadual 1.

Jadual 1: Istilah dalam bahasa Melayu dan bahasa Inggeris

Bahasa Melayu	Bahasa Inggeris		Bahasa Melayu	Bahasa Inggeris
Tersongsangkan kendiri	Involutory		Penyahsulitan	decryption
Saifer	Cypher		Aliran	stream
Penyulitan	Encryption			

3. Fungsi Lengkuk Eliptik

ECC ialah teknik penyulitan yang sesuai digunakan dalam peranti mudah alih dan sistem terbenam kerana ECC ini dapat menyediakan ciri-ciri keselamatan yang tinggi dengan saiz kunci yang lebih kecil dan kurang penggunaan memori dan kuasa (Dawahdeh *et al.*, 2018).

Lengkuk bukan supersingular E ke atas medan dedua $\mathbb{F}_{2^m}$ ditakrifkan oleh

$$E: y^2 + xy \equiv x^3 + ax^2 + b \bmod f(z)$$

dengan beberapa sifat seperti yang berikut:

(1) Identiti: $P + \infty = \infty + P = P$ untuk semua $P \in E(\mathbb{F}_{2^m})$.

(2) Negatif: Jika $P = (x, y) \in E(\mathbb{F}_{2^m})$, maka $(x, y) + (x, x + y) = \infty$. Titik $(x, x + y)$ dilambangkan dengan $-P$ dan dipanggil negatif P; perhatikan bahawa titik $-P$ berada di dalam $E(\mathbb{F}_{2^m})$. Juga, $-\infty = \infty$.

(3) Penambahan titik: Biarkan $P = (x_1, y_1) \in E(\mathbb{F}_{2^m})$ dan $Q = (x_2, y_2) \in E(\mathbb{F}_{2^m})$ manakala $P = \pm Q$. Seterusnya, $P + Q = (x_3, y_3)$ dengan

$$\lambda = \frac{y_1 + y_2}{x_1 + x_2}$$

$$x_3 = \lambda^2 + \lambda + x_1 + x_2 + a$$

dan

$$y_3 = \lambda(x_1 + x_3) + x_3 + y_1.$$

(4) Penggandaan titik: Biarkan $P = (x_1, y_1) \in E(\mathbb{F}_{2^m})$, manakala $P = -P$. Seterusnya $2P = (x_3, y_3)$ dengan

$$\lambda = x_1 + \frac{y_1}{x_1}$$

$$x_3 = \lambda^2 + \lambda + a = {x_1}^2 + \frac{b}{{x_1}^2}$$

dan

$$y_3 = {x_1}^2 + \lambda x_3 + x_3.$$

(5) Pendaraban skalar: Skalar bagi suatu integer k mengikut titik $Q = (x_1, y_1)$ yang terletak pada lengkuk E boleh ditakrifkan dengan mengulangi penambahan titik Q kepada dirinya sendiri sebanyak k kali sehingga menghasilkan titik R yang juga terletak pada lengkuk yang sama.

$$R = kQ = Q + Q + \cdots + Q.$$

Sebagai contoh, pengiraan $15Q$ boleh dilakukan menggunakan penambahan titik dan penggandaan titik seperti yang berikut:

$$15Q = 2(2(2Q + Q) + Q) + Q.$$

4. Algoritma Saifer Hill

Saifer Hill merupakan teknik blok saifer yang simetri yang diperkenalkan oleh ahli matematik Lester Hill pada tahun 1929. Kedua-dua pengirim dan penerima mesti berkongsi dan menggunakan kunci rahsia yang sama untuk melaksanakan proses penyulitan dan penyahsulitan. Rentetan huruf teks asal yang akan dikirim kepada penerima mestilah ditukar terlebih dahulu kepada nilai berangka yang sepadan, contohnya

$$A = 0, B = 1, C = 2, \ldots, Z = 25.$$

Kemudian, susunkan pesanan tersebut kepada bentuk matriks $P_{i\times j}$ yang bergantung pada saiz kunci rahsia. Contohnya, sekiranya kunci rahsia bersaiz 3×3, iaitu

$$K_{3\times 3} = \begin{bmatrix} 1 & 3 & 5 \\ 11 & 12 & 7 \\ 4 & 2 & 1 \end{bmatrix},$$

maka jujukan nombor bersepadan bagi teks asal

T R I G O N O M E T R I ialah 19 17 08 06 14 13 14 12 04 19 17 08

hendaklah disusun seperti

$$P_{3\times 4} = \begin{bmatrix} 19 & 17 & 08 & 06 \\ 14 & 13 & 14 & 12 \\ 04 & 19 & 17 & 08 \end{bmatrix},$$

dan proses penyulitan akan menghasilkan blok teks saifer dengan dua belas nilai berangka yang berbentuk

$$C_{3\times 4} \equiv \begin{bmatrix} 1 & 3 & 5 \\ 11 & 12 & 7 \\ 4 & 2 & 1 \end{bmatrix} \begin{bmatrix} 19 & 17 & 08 & 06 \\ 14 & 13 & 14 & 12 \\ 04 & 19 & 17 & 08 \end{bmatrix}.$$

$$\equiv \begin{bmatrix} 3 & 21 & 5 & 16 \\ 15 & 8 & 11 & 2 \\ 4 & 9 & 25 & 22 \end{bmatrix} \bmod 26.$$

Maka jujukan abjad yang bersepadan dengannya disusun seperti

D V F Q P I L C E J Z W.

Untuk menyahsulit mesej ini, penerima perlu mengira songsangan matriks bagi K sedemikian hingga $K \cdot K^{-1} = I$ dengan I merupakan matriks identiti. Kemudian, gunakan persamaan

$$P \equiv K^{-1}C \bmod 26$$

untuk memperoleh mesej asal P.

5. Perkaedahan

Dalam seksyen ini, kita mengemukakan kembali sebahagian daripada langkah penjanaan kunci, penyulitan dan penyahsulitan yang dibentangkan oleh Dawahdeh *et al.* (2018). Katakan pengirim (Pengguna A) mahu menghantar suatu imej kepada pihak lain (Pengguna B) melalui saluran yang tidak selamat. Pertama, mereka hendaklah bersetuju dengan fungsi

lengkuk eliptik E dan berkongsi domain parameter $a, b, f(z), G$, dan a, b ialah pekali dalam persamaan E, $f(z)$ ialah polinomial tak terturunkan dan G ialah titik penjana. Kemudian, setiap pihak perlu memilih kunci peribadinya secara rawak yang berdarjah kurang daripada darjah $f(z)$. Pemboleh ubah n_A dan n_B masing-masing untuk Pengguna A dan B bagi menjanakan kunci awam masing-masing, iaitu

$$P_A = n_A \cdot G \text{ dan } P_B = n_B \cdot G.$$

Setiap pengguna mendarabkan kunci peribadinya dengan kunci awam pengguna lain untuk mendapatkan kunci awal $K_I = (x, y)$ melalui

$$K_I = n_A \cdot P_B = n_B \cdot P_A = n_A \cdot n_B \cdot G = (x, y).$$

Seterusnya, mereka hendaklah mengira

$$K_1 = x \cdot G = (k_{11}, k_{12}) \text{ dan } K_2 = y \cdot G = (k_{21}, k_{22})$$

bagi menjanakan matriks kunci rahsia K_m. Namun demikian, songsangan matriks ini tidak selalu wujud. Untuk menyelesaikan masalah ini, matrik kunci tersongsangkan kendiri, iaitu $K_3 = K_3^{-1}$ akan dijana dan kunci yang sama akan digunakan untuk penyulitan dan penyahsulitan. Dalam kajian kita, pendekatan baharu ini akan dilaksanakan pada imej berskala samar bersaiz 256 x 256 piksel. Imej akan dibahagikan kepada blok bersaiz empat nilai piksel. Oleh itu, setiap pihak menghasilkan kunci K_3 bersaiz 4 x 4 dengan menggunakan kaedah yang dibentangkan oleh Acharya *et al.* (2007).

Katakan

$$K_3 = \begin{bmatrix} k_{11} & k_{12} & k_{13} & k_{14} \\ k_{21} & k_{22} & k_{23} & k_{24} \\ k_{31} & k_{32} & k_{33} & k_{34} \\ k_{41} & k_{42} & k_{43} & k_{44} \end{bmatrix}$$

ditulis semula sebagai

$$K_3 = \begin{bmatrix} K_{11} & K_{12} \\ K_{21} & K_{22} \end{bmatrix}.$$

Andaikan bahawa

$$K_{11} = \begin{bmatrix} k_{11} & k_{12} \\ k_{21} & k_{22} \end{bmatrix}$$

maka nilai bagi petak yang lain dalam K_3 diperoleh dengan menyelesaikan

$$K_{12} = I - K_{11},\ K_{21} = I + K_{11} \text{ dan } K_{11} + K_{22} = 0,$$

dengan I matriks identiti.

Sekarang, asingkan nilai piksel bagi imej kepada blok bersaiz empat. Setiap blok akan ditukar kepada vektor bersaiz 4 x 1 dengan (P_1, P_2, P_3, ...). Kemudian, darabkan K_3 kepada setiap vektor dengan mengambil modulo $f(z)$ untuk mendapatkan vektor saifer $(C_1, C_2, C_3, ...)$. Selepas itu, binakan semula imej saifer C daripada nilai-nilai dalam vektor saifer dan utuskannya kepada pihak lain. Pengiraan yang berikut diulang untuk setiap blok:

Katakan

$$P_1 = \begin{bmatrix} p_{11} \\ p_{21} \\ p_{31} \\ p_{41} \end{bmatrix}$$

maka

$$C_1 \equiv K_3 P_1 \equiv \begin{bmatrix} k_{11} & k_{12} & k_{13} & k_{14} \\ k_{21} & k_{22} & k_{23} & k_{24} \\ k_{31} & k_{32} & k_{33} & k_{34} \\ k_{41} & k_{42} & k_{43} & k_{44} \end{bmatrix} \begin{bmatrix} p_{11} \\ p_{21} \\ p_{31} \\ p_{41} \end{bmatrix} \equiv \begin{bmatrix} c_{11} \\ c_{21} \\ c_{31} \\ c_{41} \end{bmatrix} \mathrm{mod} f(z).$$

Proses penyahsulitan bermula setelah penerima menerima imej saifer C dengan memisahkan nilai piksel imej kepada blok bersaiz empat. Kemudian, setiap blok disusun ke bentuk vektor lajur empat baris. Selepas itu, darabkan K_3 kepada setiap vektor $(C_1, C_2, C_3, \ldots)$ dengan mengambil modulo $f(z)$ untuk mendapatkan vektor $(P_1, P_2, P_3, \ldots)$ yang memberikan imej asal. Pendekatan yang kita cadangkan dalam gabungan ECC yang berasaskan lengkuk E dalam medan dedua dan Saifer Hill ini disimbolkan sebagai ECCBHC:

Langkah 1: Penjanaan Kunci

1.1 Pengguna A selaku pengutus mesej hendaklah
- 1.1.1 memilih kunci peribadi, n_A yang berdarjah kurang daripada darjah polinomial tak terturunkan, $f(z)$.
- 1.1.2 mengira kunci awam $P_A = n_A \cdot G$
- 1.1.3 mengira kekunci awal $K_I = n_A \cdot P_B = (x, y)$
- 1.1.4 mengira $K_1 = x \cdot G = (k_{11}, k_{12})$ dan $K_2 = y \cdot G = (k_{21}, k_{22})$
- 1.1.5 menjanakan matriks kunci tersongsangkan kendiri K_3

1.2 Pengguna B selaku penerima mesej hendaklah
- 1.2.1 memilih kunci peribadi, n_B yang berdarjah kurang daripada darjah polinomial tak terturunkan, $f(z)$
- 1.2.2 mengira kunci awam $P_B = n_B \cdot G$
- 1.2.3 mengira kekunci awal $K_I = n_B \cdot P_A = (x, y)$
- 1.2.4 mengira $K_1 = x \cdot G = (k_{11}, k_{12})$ dan $K_2 = y \cdot G = (k_{21}, k_{22})$
- 1.2.5 menjanakan matriks K_3

Langkah 2: Penyulitan oleh pengguna A

2.1 Pisahkan nilai piksel imej asal kepada blok bersaiz empat.
2.2 Susun setiap blok kepada vektor lajur dengan empat baris (4 x 1).
2.3 Darabkan matriks kunci tersongsangkan kendiri K_3 dengan setiap vektor $(P_1, P_2, P_3, \ldots)$ dan ambil modulo $f(z)$ untuk setiap nilai $C_i \equiv K_3 P_i \bmod f(z)$.
2.4 Membina imej saifer C daripada nilai dalam vektor saifer $(C_1, C_2, C_3, \ldots)$.

Langkah 3: Penyahsulitan oleh pengguna B

3.1 Pisahkan nilai piksel bagi imej asal kepada blok bersaiz empat.
3.2 Susun setiap blok kepada vektor lajur dengan empat baris (4 x 1).

3.3 Gandakan matriks kunci tersongsangkan kendiri K_3 dengan setiap vektor $(C_1, C_2, C_3, ...)$ dan ambil modulo $f(z)$ untuk setiap nilai $P_i \equiv K_3 C_i \bmod f(z)$.

3.4 Membina imej saifer C daripada nilai bersepadan dalam vektor saifer (P_1, P_2, P_3, ...).

Perubahan langkah kerja yang tertera di atas berlaku pada langkah 1.1.1, 1.2.1, 2.3 dan 3.3 sekiranya dibandingkan dengan Dawahdeh *et al.* (2018). Ini diakibatkan oleh penggantian lengkuk E_p dengan E. Matriks K_{11} yang menjanakan matriks segi empat sama K_3 ialah hasil daripada beberapa langkah pendaraban skalar di atas lengkuk E. Kajian terdahulu telah membuktikan bahawa kerahsiaan n_A dan n_B sangat sukar dibongkar kerana masalah diskrit log dalam pelaksanaan ECC. Oleh itu, kerahsiaan K_{11} turut terjamin. Seperti pengkaji terdahulu, sistem ECCBHC ini masih mengekalkan kelebihannya yang utama semasa pelaksanaan penyulitan dan penyahsulitan secara Saifer Hill, iaitu tidak perlu mendapatkan songsangan untuk K_3. Analisis untuk memperoleh K_3 yang tersongsangkan kendiri boleh dibuat melalui

$$K_{11} = \begin{bmatrix} k_{11} & k_{12} \\ k_{21} & k_{22} \end{bmatrix}$$

dengan mencuba sebanyak 4 kali 2^m kombinasi titik yang mematuhi E. Seterusnya, pencerobohan boleh dilakukan melalui penggunaan m yang kecil. Situasi pencerobohan ini boleh dikurangkan sekiranya pengguna memilih m yang perdana mengikut piawaian yang telah dikemukakan oleh FIPS PUB 186-4 dan boleh didapati di laman web NIST. Piawaian ini merupakan siri rasmi penerbitan yang keempat yang berkaitan dengan piawaian dan garis panduan yang diguna pakai dan termaktub di bawah peruntukan dalam Akta Maklumat Persekutuan Pengurusan Keselamatan, iaitu *The Federal Information Security Management Act* (FISMA) tahun 2002.

6. Contoh Pelaksanaan

Anggapkan bahawa pengguna A mahu mengutus imej M kepada pengguna B dan mereka bersetuju untuk menggunakan lengkuk eliptik $E: y^2 + xy = x^3 + z^3x^2 + (z^3 + 1) \bmod (z^4 + z + 1)$ ke atas medan dedua F_{2^4}. Unsur $a_3z^3 + a_2z^2 + a_1z + a_0$ dalam medan tersebut diwakili oleh rentetan bit $(a_3a_2a_1a_0)$ bersaiz empat; contohnya, (0101) mewakili $z^2 + 1$. Biarkan $a = z^3, b = z^3 + 1$. Semua titik yang melalui lengkuk E adalah seperti yang berikut:

∞	(0011,1100)	(1000,0001)	(1100,0000)
(0000,1011)	(0011,1111)	(1000,1001)	(1100,1100)
(0001,0000)	(0101,0000)	(1001,0110)	(1111,0100)
(0001,0001)	(0101,0101)	(1001,1111)	(1111,1011)
(0010,1101)	(0111,1011)	(1011,0010)	
(0010,1111)	(0111,1100)	(1011,1001)	

Salah satu titik yang terpilih, iaitu $G = (z^3, 1)$ merupakan titik penjana atau titik asas (Hankerson *et al.*, 2006). Oleh itu, domain parameter $a, b, f(z), G$ untuk E ialah $z^3, z^3 + 1, z^4 + z + 1, (z^3, 1)$. Sebelum Pengguna A mengutuskan imej berskala samar, perkara pertama yang perlu dilakukan adalah mendapatkan nilai berangka yang sepadan dengan warna merah, hijau, biru (RGB) bagi setiap piksel untuk imej berwarna, contohnya *Angry Birds* bersaiz 128 x 128 piksel dalam Rajah 1. Objek yang kita pilih untuk kajian ini ialah objek yang tidak realistik atau nyata berbanding dengan imej Lena yang biasa dijadikan sebagai perbandingan oleh pengkaji terdahulu.

Rajah 1: Imej berskala warna *Angry Birds* bersaiz 128 x 128 piksel

Berikut ini merupakan sebahagian daripada nilai berangka yang sepadan dengan Rajah 1:

$$\begin{bmatrix} & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \\ \dots & 243 & 119 & 8 & 2 & 66 & 129 & 129 & 53 & \dots \\ \dots & 243 & 119 & 8 & 2 & 49 & 96 & 96 & 40 & \dots \\ \dots & 243 & 120 & 9 & 3 & 10 & 16 & 16 & 9 & \dots \\ \dots & 5 & 5 & 84 & 196 & 251 & 251 & 251 & 251 & \dots \\ \dots & 5 & 5 & 62 & 145 & 186 & 186 & 186 & 186 & \dots \\ \dots & 6 & 6 & 11 & 25 & 30 & 30 & 30 & 30 & \dots \\ & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \end{bmatrix} \quad (1)$$

Jika Pengguna A mahu menghantar imej berskala samar, iaitu *Angry Birds* bersaiz 128 x 128 piksel kepada Pengguna B seperti dalam rajah yang berikut:

Rajah 2: Imej berskala samar Angry Birds bersaiz 128 x 128 piksel

maka kedua-dua pengutus dan penerima imej perlu menuruti langkah berikut:

Langkah 1: Penjanaan kunci

1.1 Pengguna A selaku pengutus mesej

1.1.1 memilih kunci rahsia, $n_A = z^2 + 1$.

1.1.2 mengira kunci awam $P_A = n_A \cdot G = (z^3 + z + 1, z)$

1.1.3 mengira kunci awal $K_I = n_A \cdot P_B = (z^3 + z^2, z^3 + z^2) = (x, y)$

1.1.4 mengira $K_1 = x \cdot G = z^3(z^3,1) + z^2(z^3,1) = (z^3,1) = (k_{11}, k_{12})$ dan
$K_2 = y \cdot G = z^3(z^3,1) + z^2(z^3,1) = (z^3,1) = (k_{21}, k_{22})$

1.1.5 menggunakan $K_{11} = \begin{bmatrix} z^3 & 1 \\ z^3 & 1 \end{bmatrix}$ untuk menjanakan kunci tersongsangkan kendiri

$$\begin{bmatrix} z^3 & 1 & z^3+1 & 1 \\ z^3 & 1 & z^3 & 0 \\ z^3+1 & 1 & z^3 & 1 \\ z^3 & 0 & z^3 & 1 \end{bmatrix}$$

1.2 Pengguna A selaku pengutus mesej

1.2.1 memilih kunci rahsia, $n_B = z^2 + z + 1$.

1.2.2 mengira kunci awam $P_B = n_B \cdot G = (z^3 + z + 1, z^3 + 1)$

1.2.3 mengira kunci awal $K_I = n_B \cdot P_A = (z^3 + z^2, z^3 + z^2) = (x, y)$

1.2.4 mengira $K_1 = x \cdot G = z^3(z^3,1) + z^2(z^3,1) = (z^3,1) = (k_{11}, k_{12})$ dan
$K_2 = y \cdot G = z^3(z^3,1) + z^2(z^3,1) = (z^3,1) = (k_{21}, k_{22})$.

1.2.5 menggunakan $K_{11} = \begin{bmatrix} z^3 & 1 \\ z^3 & 1 \end{bmatrix}$ untuk menjana kunci tersongsangkan kendiri

$$\begin{bmatrix} z^3 & 1 & z^3+1 & 1 \\ z^3 & 1 & z^3 & 0 \\ z^3+1 & 1 & z^3 & 1 \\ z^3 & 0 & z^3 & 1 \end{bmatrix}$$

Langkah 2: Penyulitan oleh Pengguna A

2.1 Peta unsur pemasukan dalam matriks (1) kepada nombor yang sepadan dengan imej berskala samar melalui formula $Y = 0.299R + 0.587G + 0.114B$. Penggunaan formula ini sangat popular dalam kalangan penyelidik terdahulu dan telah dikaji dari segi kesesuaiannya berbanding dengan beberapa formula lain (Nguyen & Brown, 2017).

$$\begin{bmatrix} \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \\ \dots & 243 & 119 & 8 & 2 & 50 & 97 & 97 & 40 & \dots \\ \dots & 243 & 119 & 8 & 2 & 50 & 97 & 97 & 40 & \dots \\ \dots & 243 & 119 & 8 & 2 & 50 & 97 & 97 & 40 & \dots \\ \dots & 5 & 5 & 63 & 147 & 188 & 188 & 188 & 188 & \dots \\ \dots & 5 & 5 & 63 & 147 & 188 & 188 & 188 & 188 & \dots \\ \dots & 5 & 5 & 63 & 147 & 188 & 188 & 188 & 188 & \dots \\ & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \end{bmatrix} \quad (2)$$

diikuti pula dengan menukarkan matriks (2) ke bentuk polinomial seperti yang berikut:

$$\begin{bmatrix} & \vdots & \vdots & \vdots & \\ \dots & z^7+z^6+z^5+z^4+z+1 & z^6+z^5+z^4+z^2+z+1 & z^3 & \dots \\ \dots & z^7+z^6+z^5+z^4+z+1 & z^6+z^5+z^4+z^2+z+1 & z^3 & \dots \\ \dots & z^7+z^6+z^5+z^4+z+1 & z^6+z^5+z^4+z^2+z+1 & z^3 & \dots \\ \dots & z^2+1 & z^2+1 & z^5+z^4+z^3+z^2+z+1 & \dots \\ \dots & z^2+1 & z^2+1 & z^5+z^4+z^3+z^2+z+1 & \dots \\ \dots & z^2+1 & z^2+1 & z^5+z^4+z^3+z^2+z+1 & \dots \\ & \vdots & \vdots & \vdots & \end{bmatrix} \quad (3)$$

Seterusnya, turunkan setiap polinomial tersebut dalam modulo (z^4+z+1), iaitu

$$\begin{bmatrix} & \vdots & \vdots & \vdots & \\ \dots & 1 & z^3+z^2+z & z^3 & \dots \\ \dots & 1 & z^3+z^2+z & z^3 & \dots \\ \dots & 1 & z^3+z^2+z & z^3 & \dots \\ \dots & z^2+1 & z^2+1 & z^3+z & \dots \\ \dots & z^2+1 & z^2+1 & z^3+z & \dots \\ \dots & z^2+1 & z^2+1 & z^3+z & \dots \\ & \vdots & \vdots & \vdots & \end{bmatrix} \quad (4)$$

2.2 Pisahkan matriks (4) menjadi blok $P_1, P_2, P_3, \dots$ yang masing-masing merupakan vektor bersaiz 4x1:

$$P_1 = \begin{bmatrix} 1 \\ 1 \\ 1 \\ z^2+1 \end{bmatrix}, P_2 = \begin{bmatrix} z^3+z^2+z \\ z^3+z^2+z \\ z^3+z^2+z \\ z^2+1 \end{bmatrix}, P_3 = \begin{bmatrix} z^3 \\ z^3 \\ z^3 \\ z^3+z \end{bmatrix}, \dots.$$

Seiringan dengan itu, suatu kunci rahsia T perlu dikongsikan bersama penerima mesej. Katakan $M_1 = [m_{i1}]$ dan $P_1 = [p_{i1}]$ masing-masing daripada matriks (3) dan (4) untuk $i = 1,2,3,4$. Unsur pemasukan kedua-dua matriks tersebut boleh dihubungkan dengan perkaitan $p_{i1} = m_{i1} - t_{i1}(z^4+z+1)$ dengan t_{i1} merupakan kunci rahsia ahli kepada T. Dengan menggunakan kaedah pembahagian panjang, (iaitu Algoritma Euklidan), nilai $t_{11} = t_{21} = t_{31} = 1$ dan $t_{41} = 0$ boleh dicari. Secara umum, kunci

$$T = [t_{ij}] = \begin{bmatrix} & \vdots & \vdots & \vdots & \\ \dots & 1 & z^2+z+1 & 0 & \dots \\ \dots & 1 & z^2+z+1 & 0 & \dots \\ \dots & 1 & z^2+z+1 & 0 & \dots \\ \dots & 0 & 0 & z+1 & \dots \\ \dots & 0 & 0 & z+1 & \dots \\ \dots & 0 & 0 & z+1 & \dots \\ & \vdots & \vdots & \vdots & \end{bmatrix}$$

diperoleh melalui hubungan $p_{ij} = m_{ij} - t_{ij}f(z)$

2.3 Pendaraban K_3 kepada vektor P_1 akan menghasilkan vektor saifer C_1

$$C_1 \equiv K_3 \cdot P_1 \equiv \begin{bmatrix} z^3 & 1 & z^3+1 & 1 \\ z^3 & 1 & z^3 & 0 \\ z^3+1 & 1 & z^3 & 1 \\ z^3 & 0 & z^3 & 1 \end{bmatrix} \begin{bmatrix} 1 \\ 1 \\ 1 \\ z^2+1 \end{bmatrix} \equiv \begin{bmatrix} z^2+1 \\ 1 \\ z^2+1 \\ z^2+1 \end{bmatrix} \bmod (z^4+z+1)$$

dan proses yang sama diulang untuk memperoleh blok $C_2, C_3, \dots$.

pengiraan kunci penyahsulitan dalam sistem Saifer Hill yang asal juga turut dipercepat dengan kunci yang tersongsangkan kendiri. Namun begitu, analisis sebenar untuk mengira masa larian algoritma penyulitan dan penyahsulitan belum dilakukan lagi. Begitu juga dengan analisis Entropi, PSNR dan UACI. Keempat-empat analisis ini perlu dilakukan pada masa hadapan bagi menguji sejauhmana tahap keberkesanannya jika dibandingkan dengan sistem terdahulu.

Rujukan

Acharya, B., Patra, S. K. & Panda, G. 2009. Involutory, permuted and reiterative key matrix generation methods for Hill cipher system. *International Journal of Recent Trends in Engineering*, 1(4), 106.

Acharya, B., Rath, G., Patra, S. & Panigrahy, S. K. 2007. Novel methods of generating self-invertible matrix for Hill cipher algorithm. *International Journal of Security*, 06.

Acharya, B., Sharma, M. D., Tiwari, S. & Minz, V. K. 2010. *Privacy protection of biometric traits using modified Hill cipher with involutory key and robust cryptosystem*. Proceedings of the International Conference and Exhibition on Biometrics Technology. Procedia Computer Science, 2, 242–247. https://www.sciencedirect.com/science/article/pii/S1877050910003613

Bronson, R. & Costa, G. B. 2007. *Linear algebra: An introduction*. Academic Press.

Christensen, C. 2006. *Cryptography of the vigenere cipher*. Proceedings of Computer Sciences Corporation, 1–18.

Davies, D. 1997. A brief history of cryptography. *Information Security Technical Report*, 2(2), 14–17.

Dawahdeh, Z. E., Yaakob, S.N. & Othman, R.R. 2018. A new image encryption technique combining elliptic curve cryptosystem with Hill cipher. *Journal of King Saud University – Computer and Information Sciences*, 30, 349–355.

Dey, S. 2012. *SD-AEI: An advanced encryption technique for images*. Second International Conference on Digital Information Processing and Communications (ICDIPC), IEEE, 68–73.

Hankerson, D., Menezes, A. J. & Vanstone, S. 2006. *Guide to elliptic curve cryptography*. Springer Science & Business Media.

Hill, L. S. 1929. Cryptography in an algebraic alphabet. *The American Mathematical Monthly*, 36(6), 306–312. https://doi.org/10.1080/00029890.1929.11986963

Mollin, R. A. 2006. *An introduction to cryptography*. Chapman and Hall/CRC.

Naveen Kumar, S. K., Panduranga, H. & Kiran. 2013. *Partial image encryption for smart camera*. Proceedings of the 2013 IEEE International Conference on Recent Trends in Information Technology (ICRTIT), 126–132.

Naveen Kumar, S. K., Sharath Kumar, S.H. & Panduranga, H. T. 2012. Encryption approach for images using bits rotation reversal and extended Hill cipher techniques. *J. Comp. App.*, 59, 10–14.

Nguyen, R. M. & Brown, M. S. 2017. *Why you should forget luminance conversion and do something better*. Proceedings of the IEEE conference on computer vision and pattern recognition, 6750–6758.

Overbey, J. Traves, W. & Wojdylo, J. 2005. On the keyspace of the Hill cipher. *Cryptologia*, 29(1), 59–72.

Panduranga, H. T. & Naveen Kumar, S. K. 2012. Advanced partial image encryption using two-stage Hill cipher technique. *J. Comp. App.*, 60.

Pusat Rujukan Persuratan Melayu (PRPM). Dewan Bahasa dan Pustaka Malaysia.

https://prpm.dbp.gov.my/

Rathidevi, M., Yaminipriya, R. & Sudha, S. 2017. *Trends of cryptography stepping from ancient to modern.* International Conference on Innovations in Green Energy and Healthcare Technologies (IGEHT). IEEE, 1–9.

Satapathy, S. & Rajkumar, S. 2020. Image encryption using modified elliptic curve cryptography and Hill cipher. *Smart Intelligent Computing and Applications*, 675–683.

Sastry, V. & Shankar, N. R. 2008. Modified Hill cipher for a large block of plaintext with interlacing and iteration. *Journal of Computer Science*, 4(1), 15–20.