Pemanfaatan Barisan Bilangan Fibonacci dalam Kriptografi dan Keamanan Data

Karina Imani - 13519166
Program Studi Teknik Informatika
Sekolah Teknik Elektro dan Informatika
Institut Teknologi Bandung, Jl. Ganesha 10 Bandung 40132, Indonesia
13519166@std.stei.itb.ac.id

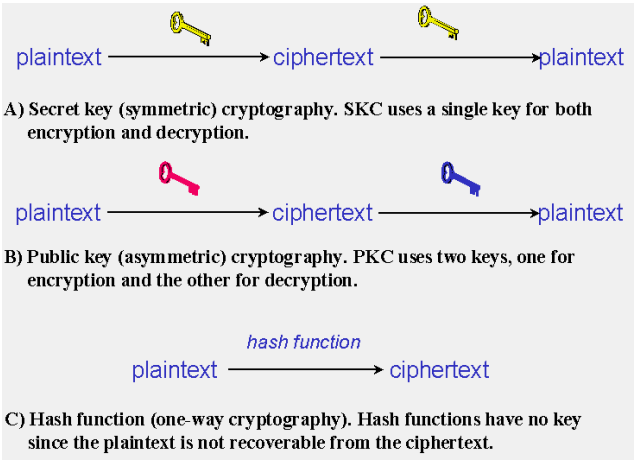
***Abstrak*—Di era teknologi ini, pentingnya keamanan data (*data security*) kian meningkat, mendorong munculnya pengembangan banyak metode kriptografi untuk melakukan enkripsi dan dekripsi data, dan dengan demikian menjaganya dari akses orang-orang tidak berwenang, kerusakan data, ataupun pencurian data. Salah satu metode kriptografi yang dapat digunakan memanfaatkan barisan bilangan Fibonacci, sebuah barisan bilangan istimewa yang merupakan fungsi rekursif. Adapun, metode yang dibahas pada makalah ini adalah modifikasi *Playfair Cipher* dan aplikasi matriks Fibonacci (*Qp-matrix*).**

***Kata kunci*—barisan bilangan Fibonacci, dekripsi, enkripsi, keamanan data, kriptografi.**

I. PENDAHULUAN

Kriptografi pada esensinya adalah tulisan yang dikodekan, yang telah digunakan untuk bertukar informasi rahasia sejak tahun 1900 SM, didokumentasikan pada penggunaan *hieroglyph* (huruf khas Mesir) non-standar pada suatu inskripsi. Sejak saat itu, bermunculan banyak penggunaan kriptografi lainnya, yang tersebar di berbagai waktu dan tempat.[1]

Karena fungsinya yang menyembunyikan pesan rahasia, tentunya dibutuhkan banyak cara mengubah pesan-pesan tersebut menjadi kode. Oleh karena itu, banyak pula metode mengubah suatu pesan menjadi kode (enkripsi) dan mengubah kode tersebut kembali menjadi pesan yang dapat dibaca penerimanya (dekripsi).



Gambar 1. Beberapa cara enkripsi dan dekripsi.
Sumber: *An Overview of Cryptography, Gary C. Kessler*.[6]

Salah satu cara enkripsi dan dekripsi adalah menggunakan kunci (key). Terdapat tiga cara enkripsi dan dekripsi yang akan dibahas, berdasarkan jumlah kunci yang digunakan.

Cara pertama adalah kriptografi kunci rahasia, yang menggunakan satu kunci, yaitu kunci yang sama untuk enkripsi dan dekripsi. Cara kedua adalah kriptografi kunci publik, yang memiliki dua kunci, yaitu kunci pertama yang tidak dirahasiakan untuk enkripsi, dan kunci kedua yang dirahasiakan untuk dekripsi. Metode lain untuk enkripsi adalah dengan hash function, atau fungsi tertentu yang mengubah pesan (*plaintext*) menjadi kode (*ciperthext*) menggunakan fungsi matematis tertentu. Karena kode pada metode ini tidak akan didekripsi, tidak dibutuhkan kunci.

Pada hakekatnya, kriptografi merupakan tameng dalam melakukan komunikasi melalui media yang tidak sepenuhnya terpercaya, dan media ini mencakup berbagai jaringan digital, termasuk Internet.

Di era teknologi ini, dimana keterhubungan melalui Internet terus meningkat, pentingnya keamanan data (*data security*) juga semakin meningkat. Keamanan data sendiri adalah praktek perlindungan informasi digital dari akses orang-orang yang tidak berwenang, kerusakan data, ataupun pencurian data selama masa keberadaannya di Internet. Hal ini mencakup keamanan digital maupun fisik, yang berarti *hardware* seperti *storage device* yang digunakan untuk menyimpan data, maupun *software* yang mengurus keamanan dalam bentuk logika atau algoritma program.[2]

Kriptografi banyak dikembangkan untuk mengenkripsi dan mendekripsi data penggunanya, untuk menjaga keamanan aktivitas mereka di Internet dan mencegah berbagai tindak kriminal. Pada karya tulis ini, metode enkripsi dan dekripsi yang akan dibahas adalah metode kriptografi yang menggunakan barisan bilangan Fibonacci.

II. LANDASAN TEORI

Sebelum membahas penggunaan Fibonacci dalam kriptografi, kita harus terlebih dahulu memahami barisan bilangan itu sendiri dan basis metode yang akan digunakan.

[1] Gary C. Kessler, "An Overview on Cryptography" (garykessler.net, 2020).

[2] "What Is Data Security?" (IBM, 2020).

1.1. Barisan Bilangan Fibonacci

Meskipun barisan bilangan Fibonacci sudah dipelajari dan digunakan sejak abad ke-450 SM, di berbagai naskah India dan Sansekerta, dunia Barat baru mengenal barisan bilangan tersebut pada abad ke-13, melalui seorang matematikawan Italia bernama Leonardo Bigollo Pisono, lebih dikenal dengan Leonardo Bonacci atau Fibonacci.

Dalam bukunya yang berjudul *Liber Abacci* (atau "Buku Perhitungan"), yang memperkenalkan bilangan-bilangan Arab (0, 1, 2, 3, …), Fibonacci mengemukakan suatu persoalan mengenai populasi kelinci yang ideal (secara matematika, bukan secara biologi), dirangkum menjadi pertanyaan demikian:

Jika pada suatu pulau terisolasi, satu pasang kelinci dilepaskan untuk berkembangbiak, berapa banyak pasangan kelinci yang ada setiap bulannya, dengan kondisi:

1. setiap pasang kelinci tidak dapat berkembangbiak hingga sebulan setelah kelahiran mereka
2. setiap bulan sepasang kelinci akan menghasilkan sepasang kelinci sebagai anaknya
3. jumlah kelinci tidak akan berkurang, atau kelinci yang sudah lahir tidak akan mati?[3]

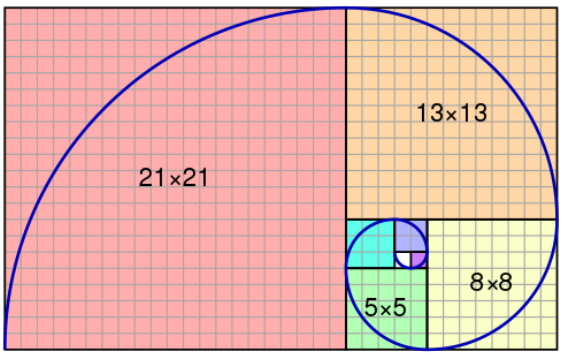
Solusi dari permasalahan ini adalah deret Fibonacci, yaitu 1, 1, 2, 3, 5, 8, …, sebuah barisan istimewa yang dapat diperoleh dari fungsi rekursif demikian:

$$f_n = \begin{cases} 0, & n = 0 \\ 1, & n = 1 \\ f_{n-1} + f_{n-2}, & n > 1 \end{cases}$$

Gambar 2. Fungsi rekursif Fibonacci.

Barisan bilangan Fibonacci merupakan barisan bilangan yang istimewa karena, di samping menjadi solusi persoalan perkembangbiakan kelinci, barisan bilangan ini muncul di berbagai aspek kehidupan kita, baik alami maupun buatan manusia.

Pada alam, bilangan Fibonacci dapat ditemukan pada jumlah mahkota bunga (1 pada *calla lily*, 3 pada *iris*, 5 pada *larkspur*, 8 pada *delphinium*, 13 pada *marigold*, dan seterusnya) serta spiral Fibonacci pada bunga matahari dan pinus.[4]



Gambar 3. Spiral Fibonacci.
Sumber: *Wikimedia Commons*.

Alasan munculnya Fibonacci pada alam masih diperdebatkan ilmuwan, namun salah satu penjelasan kemunculannya pada tumbuhan adalah optimisasi tatanan suatu tumbuhan untuk memaksimumkan sinar matahari yang diterimanya, ruang tumbuhnya cabang baru, dan sebagainya.[5] Ide dasarnya, setiap cabang baru suatu tumbuhan akan bertumbuh pada suatu sudut yang disebut *golden angle*, yaitu sebesar ~137.5 derajat.[6]

Sementara itu, kemunculan Fibonacci pada produk-produk buatan manusia dapat ditemukan pada kesenian seperti arsitektur, lukisan, dan musik, atau dalam matematika dan *programming*.[2]

Gambar 4. *Golden ratio* pada lukisan.
Sumber: *Wikimedia Commons*.

Rasio dari dua bilangan Fibonacci berturut-turut apapun, dengan bilangan yang lebih besar sebagai pembilang dan bilangan yang lebih kecil sebagai penyebut, cenderung mendekati bilangan ϕ = 1.6180339887, yang disebut sebagai *golden ratio*. Bilangan ini digunakan di berbagai lukisan dan arsitektur karena dianggap memiliki nilai estetika yang baik dipandang mata.[7]

Adapun, salah satu aplikasi Fibonacci pada dunia *programming* adalah sebagai salah satu metode enkripsi dan deskripsi pada kriptografi, pada kaitannya dengan keamanan data. Metode-metode yang dimaksud adalah modifikasi *Playfair Cipher* dan aplikasi matriks Fibonacci (*Qp-matrix*).

1.2. Playfair Cipher

Penggunaan *Playfair Cipher* pertama adalah di tahun 1854 oleh pencetusnya, Sir Charles Wheatstone. Metode kriptografi ini merupakan metode pertama yang memanfaatkan pasangan-pasangan alfabet dalam kriptografi. Aturan aingkat *Playfair Cipher* adalah sebagai berikut.[8]

[3] "Fibonacci's Liber Abacci (Book of Calculation)" (Utah, Amerika Serikat: The University of Utah, 2009).
[4] Sudipta Sinha, "The Fibonacci Numbers and Its Amazing Applications" (Research Gate, 2019).
[5] Robert Lamb, "How Are the Fibonacci Numbers Expressed in Nature?" (How Stuff Works, 2008).
[6] J.N. Ridley, "Packing Efficiency in Sunflower Heads" (Mathematical Biosciences, Volume 58 Issue 1, 1982).
[7] Rod Pierce, "Golden Ratio" (Math Is Fun, 2019).
[8] "Playfair Cipher" (Practical Cryptography, 2014).

Metode ini dimulai dengan membuat sebuah tabel 5x5 berisi alfabet unik yang dibuat dengan menentukan suatu kata kunci yang diketahui kedua belah pihak. Tabel akan diawali semua alfabet pada kata kunci tersebut, kemudian diikuti alfabet lainnya sesuai urutan abjad latin.

Sebagai contoh, menggunakan kata kunci "playfair" dapat membentuk tabel seperti demikian:

P	**L**	**A**	**Y**	**F**
I	**R**	B	C	D
E	G	H	K	M
N	O	Q	S	T
U	V	W	X	Z

Tabel 1. Contoh tabel untuk *Playfair Cipher*.

Karena terdapat 5x5 sel dalam tabel dan 26 alfabet, maka huruf I dan J ditulis dalam sel yang sama sebagai I. Selanjutnya, ambil pesan yang akan dienkripsi dan bagi menjadi pasangan-pasangan huruf. Sebagai contoh, kata "hebat" menjadi:

HE BA TX

Playfair Cipher memanfaatkan pasangan huruf, sehingga ketika huruf yang akan dienkripsi berjumlah ganjil, ditambahkan huruf X di akhir pesan tersebut. Dalam mengenkripsi suatu kalimat, hapus terlebih dahulu tanda baca dan spasi, serta ubah angka-angka menjadi ejaannya (misalnya angka 8 menjadi "delapan").

Selanjutnya, enkripsi pesan yang sudah diproses dapat dilakukan dengan tiga aturan berikut:

1. Jika pasangan huruf di kolom yang sama, geser setiap huruf sebanyak satu sel ke bawah.
2. Jika pasangan huruf di baris yang sama, geser setiap huruf sebanyak satu sel ke kanan.
3. Jika pasangan huruf di baris dan kolom yang berbeda, tukarkan baris kedua huruf dengan mempertahankan kolom tempat mereka berada.[8]

Beri perlakuan yang sama untuk setiap pasang kata yang diperoleh dari pembagian pesan yang akan dienkripsi.

P	L	A	Y	F
I	R	B	C	D
E	**G**	**H**	**K**	M
N	O	Q	S	T
U	V	W	X	Z

P	L	**A**	Y	F
I	R	**B**	C	D
E	G	**H**	K	M
N	O	Q	S	T
U	V	W	X	Z

P	L	A	Y	F
I	R	B	C	D

E	G	H	K	M
N	O	Q	**S**	**T**
U	V	W	**X**	**Z**

Tabel 2. Contoh penggunaan *Playfair Cipher*.
HE → KG; BA → HB; TX → ZS

Pada contoh di atas, HE menjadi KG, BA menjadi HB, dan TX menjadi ZS, sehingga kata "hebat" menjadi "kghbzs". Untuk dekripsi, dapat dilakukan kebalikan dari ketiga aturan di atas, selama kata kunci yang digunakan untuk tabel sama.

1.3. Matriks Fibonacci

Dalam topik barisan bilangan Fibonacci, dikenal matriks (p+1) (p+1) berbasis p bilangan Fibonacci (p = 0, 1, 2, 3, …), yang disebut dengan matriks Q_p (*Q_p-matrix*). Telah dibuktikan bahwa matriks demikian selalu memiliki determinan ±1.

Untuk mengerti penggunaan matriks Q_p, kita harus memulai dari bentuk paling sederhananya, yang disebut matriks Q atau Q^n. Matriks Q^n pertama kali didefinisikan pada tahun 1951 oleh Joel Brenner, dan merupakan matriks 2x2 dengan bentuk:

$$Q^n = \begin{bmatrix} F_{n+1} & F_n \\ F_n & F_{n-1} \end{bmatrix}$$

dengan masing-masing F_i sebagai bilangan Fibonacci.[9] Pada tahun 1960, King mengemukakan beberapa sifat matriks Q^n, yaitu:

$$|Q^n| = |Q|^n$$

$$\begin{bmatrix} F_{n+2} & F_{n+1} \\ F_{n+1} & F_n \end{bmatrix}\begin{bmatrix} F_{n+1} & F_n \\ F_n & F_{n-1} \end{bmatrix} = \begin{bmatrix} F_{2n+2} & F_{2n+1} \\ F_{2n+1} & F_{2n} \end{bmatrix}$$

$$Q^m Q^{n-1} = Q^{n+m-1}$$

$$\begin{bmatrix} F_{m+1} & F_m \\ F_m & F_{m-1} \end{bmatrix}\begin{bmatrix} F_n & F_{n-1} \\ F_{n-1} & F_{n-2} \end{bmatrix} = \begin{bmatrix} F_{m+n} & F_{m+n-1} \\ F_{m+n-1} & F_{n+n-2} \end{bmatrix}$$

Adapun, invers matriks Q^n dapat dituliskan sebagai berikut:

$$Q^{-n} = \begin{bmatrix} F_{n+1} & -F_n \\ -F_n & F_{n-1} \end{bmatrix}$$

Ide matriks Q dapat diaplikasikan ke matriks Q_p, yang merepresentasikan barisan bilangan Fibonacci-p. Matriks Q_p sendiri memiliki bentuk umum (p+1)(p+1) seperti demikian:

$$Q_p = \begin{bmatrix} 1 & 1 & 0 & \cdots & 0 & 0 \\ 0 & 0 & 1 & \cdots & 0 & 0 \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\ 0 & 0 & 0 & \cdots & 1 & 0 \\ 0 & 0 & 0 & \cdots & 0 & 1 \\ 1 & 0 & 0 & \cdots & 0 & 0 \end{bmatrix}$$

Kolom pertamanya memiliki angka 1 di awal dan di akhir,

[9] Eric W. Weisstein, "Fibonacci Q-Matrix" (MathWorld—A Wolfram Web Resource).

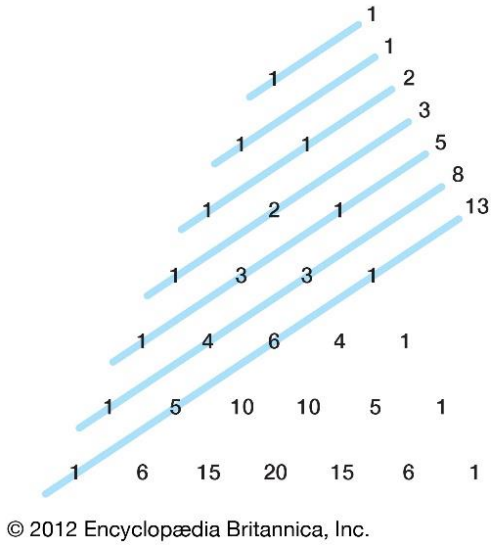
dan p–1 angka 0 mengisi sisanya. Baris terakhirnya diisi angka 0 selain 1 di awal. Selain itu, matriks (p)(p) di ujung kanan atasnya menyerupai matriks identitas. Determinannya adalah:

$$|Q_p| = (-1)^p$$

Selanjutnya, matriks Q_p dikembangkan dengan konsep matriks Q^n, menjadi matriks $Q_p{}^n$ yang merupakan "pangkat ke-n" dari matriks Q_p.

$$Q_p = \begin{bmatrix} F_p(n+1) & F_p(n) & \cdots & F_p(n-p+2) & F_p(n-p+1) \\ F_p(n-p+1) & F_p(n-2) & \cdots & F_p(n-2p+2) & F_p(n-2p+1) \\ \vdots & \vdots & \vdots & \vdots & \vdots \\ F_p(n-1) & F_p(n-2) & \cdots & F_p(n-p) & F_p(n-p-1) \\ F_p(n) & F_p(n-1) & \cdots & F_p(n-p+1) & F_p(n-p) \end{bmatrix}$$

Matriks ini, menariknya, menghasilkan segitiga Pascal. Penjumlahan baris segitiga Pascal, sebaliknya, menghasilkan barisan bilangan Fibonacci-p. Untuk p = 0, barisan bilangan yang dihasilkan adalah bilangan pangkat 2 (penjumlahan garis horizontal), dan untuk p = 1, barisan bilangan yang dihasilkan adalah Fibonacci yang umum.[10]



Gambar 5. Fibonacci dalam segitiga Pascal.
Sumber: *Encyclopedia Britannica*.

Adapun, fungsi rekursif dari Fibonacci-p sebagai berikut:

$$f_p(n) = \begin{cases} 0, & n < 0 \\ 1, & n = 0 \\ f_p(n-1) + f_p(n-p-1), & n > 0 \end{cases}$$

Gambar X. Fungsi rekursif Fibonacci-p.

Sedangkan, determinan dari matriks $Q_p{}^n$ dapat dituliskan dengan persamaan sebagai berikut:

$$|{Q_p}^n| = ((-1)^p)^n = (-1)^{pn}$$

Dapat dilihat bahwa, seperti matriks Q^n dan Q_p, matriks $Q_p{}^n$ juga memiliki sifat unik, yakni determinan yang hanya dapat bernilai di antara ±1.

III. FIBONACCI DALAM KRIPTOGRAFI

Dalam bagian ini, akan dilakukan eksplorasi terhadap berbagai metode kriptografi menggunakan modifikasi *Playfair Cipher* dan aplikasi matriks Fibonacci (Q_p-*matrix*).

2.1. Playfair Cipher yang Dimodifikasi

Seperti yang telah dijelaskan di bab sebelumnya, pada metode *Playfair Cipher*, kata kunci dibagikan ke seluruh pihak yang memiliki akses ke informasi yang dirahasiakan. Kebocoran kata kunci ini tentunya dapat memunculkan masalah keamanan. Penentuan kata kunci menggunakan barisan bilangan Fibonacci dapat mencoba meningkatkan keamanan data.

Konsepnya sederhana, yaitu dengan menentukan satu angka (x) yang termasuk barisan bilangan Fibonacci, umumnya salah satu bilangan yang cukup kecil, serta satu lagi angka yang akan menentukan panjangnya kata kunci (y).

Misalkan x = 3 dan y = 7. Ambil 7 – 1 = 6 angka setelah 3 yang terletak dalam barisan bilangan Fibonacci, yakni 5, 8, 13, 21, 34, dan 55. Angka-angka ini akan dihitung modulusnya dengan 26 (jumlah abjad) dan dipetakan sesuai abjad yang berkorespondensi dengan angka tersebut, dimulai dari 0. Input x dan y dalam contoh di atas akan menghasilkan kata kunci berupa "dfinvlj".[11]

2.2. Matriks Fibonacci dalam Kriptografi

Penggunaan matriks $Q_p{}^n$, sebagaimana telah dibahas pada bagian sebelumnya, mengenkripsi pesan yang telah terlebih dahulu dibentuk menjadi matriks. Matriks yang akan dikodekan harus berupa matriks persegi, dan memiliki jumlah baris dan kolom genap.

Matriks ini dapat diperoleh dengan metode apapun, selama telah disepakati oleh pengirim dan penerima pesan, namun salah satu cara yang umum adalah dengan memilih suatu bilangan m dan mengkodekan matriks secara semikian:

A	B	C	D	E
m	m + 1	m + 2	m + 3	m + 4

F	G	H	I	…
m + 5	m + 6	m + 7	m + 8	…

Tabel 3. Metode mengenkripsi pesan menjadi matriks.[12]

Adapun, jika pesan dirasa terlalu panjang (sehingga sulit

[10] Kantaphon Kuhapatanakul, "The Fibonacci p-numbers and Pascal's triangle" (Cogent Mathematics Volume 3 No. 1, 2016).

[11] Mohd Vasim Ahmad et al., "An Improved Playfair Encryption Technique Using Fibonacci Series Generated Secret Key" (International Journal of Engineering & Technology Volume 7 No. 4.5, 2018).

[12] Sümeyra UçAr, Nihal Taş, dan Nihal Yilmaz Özgür, "A New Cryptography Model via Fibonacci and Lucas Numbers" (Cornell University, Computer Science: Cryptography and Security, arXiv: 1709.10355, 2017).

dilakukan enkripsi dan dekripsi), matriks pesan dapat dibagi menjadi beberapa matriks yang lebih kecil, selama pembagian menghasilkan matriks persegi dengan jumlah baris dan kolom genap. Jika jumlah huruf tidak sesuai dengan (m)(m), dapat diselingi angka 0 di antara kata atau di akhir suatu kalimat.

Setelah itu, matriks pesan tersebut dienkripsi menggunakan matriks Fibonacci dengan cara demikian:

$$E = (M)(Q_p{}^n)$$

Sebagai contoh, akan digunakan matriks 2x2 untuk mengenkripsi suatu pesan. Karena matriks yang digunakan sangat sederhana, hanya perlu digunakan matriks Q^n. Adapun, matriks pesan diibaratkan dengan:

$$M = \begin{bmatrix} m_1 & m_2 \\ m_3 & m_4 \end{bmatrix}$$

Selanjutnya, disepakati p = 1 dan n = 5. Matriks Q^n yang digunakan adalah:

$$Q^5 = \begin{bmatrix} 8 & 5 \\ 5 & 3 \end{bmatrix}$$

Menggunakan cara enkripsi yang telah dijelaskan sebelumnya, matriks M dikalikan dengan matriks Q^n.

$$E = \begin{bmatrix} m_1 & m_2 \\ m_3 & m_4 \end{bmatrix} \begin{bmatrix} 8 & 5 \\ 5 & 3 \end{bmatrix} = \begin{bmatrix} 8m_1 + 5m_2 & 5m_1 + 3m_2 \\ 8m_3 + 5m_4 & 5m_3 + 3m_4 \end{bmatrix}$$

Sebagai lapisan keamanan tambahan, matriks yang telah dienkripsi dapat di-"terjemahkan" menjadi alfabet kembali menggunakan sistem enkripsi sendiri, dan disajikan seperti *cipher* pada umumnya, berupa barisan huruf yang seolah-olah tidak beraturan.

Adapun, dekripsi dapat dilakukan dengan mengalikan matriks pesan yang sudah dienkripsi dengan invers dari matriks Q^n yang digunakan, yaitu sebagai berikut:

$$D = (E)(Q_p{}^{-n})$$

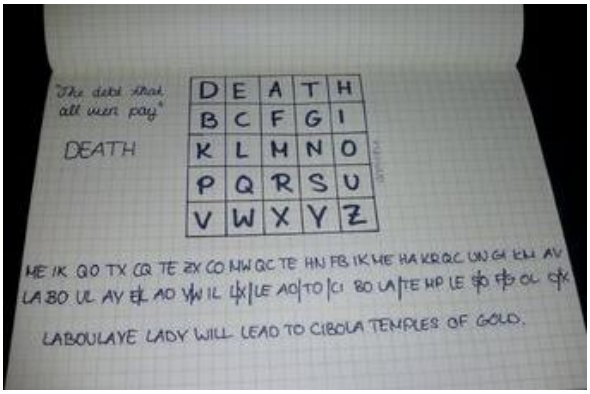
Yang berarti dalam contoh di atas, invers matriks Q^5, yaitu:

$$Q^5 = \begin{bmatrix} -3 & 5 \\ 5 & -8 \end{bmatrix}$$

Secara singkat, metode aplikasi matriks Fibonacci ini dapat digunakan dengan terlebih dahulu menentukan m (besar matriks pesan) yang harus berjumlah genap, dan n ("pangkat ke-n" matriks Q_p) dengan p = m, mengikuti aturan perkalian matriks yang harus memiliki jumlah kolom dan baris yang sama.[13]

IV. TAMBAHAN: A GAME OF SHADOWS

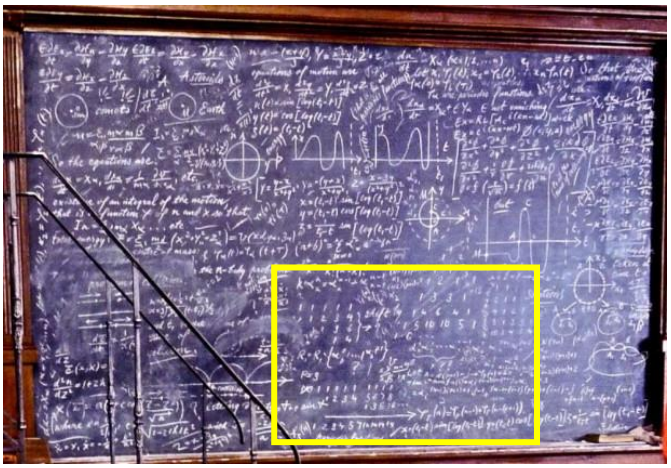
Kriptografi banyak digunakan dalam dunia perfilman, khususnya film-film dengan tema-tema misteri. Sebagai contoh, Playfair Cipher yang dijelaskan pada landasan teori digunakan pada film *National Treasure 2* yang dibintangi Nicholas Cage.



Gambar 6. Catatan *Playfair Cipher* di *National Treasure 2*. Sumber: *Walt Disney Pictures*.

Barisan bilangan Fibonacci pada kriptografi juga digunakan pada film 2011, *Sherlock Holmes: A Game of Shadows*.

Pada musim panas tahun sebelumnya, *the Oxford Centre for Collaborative Applied Mathematics* (OCCAM) mendapat panggilan dari Warner Bros. untuk mengisi sebuah properti lokasi syuting, yakni 'papan tulis Moriarty', dengan coretan-coretan yang dianggap matematis dan sesuai dengan latar film tersebut, yakni Eropa tahun 1890-an. Namun, seiring berjalannya waktu, tugas tersebut merambah ke menulis kode rahasia dan menyusun ceramah yang akan diberikan Moriarty pada berbagai adegan film.[14]



Gambar 6. Papan tulis Moriarty yang dapat dilihat di film *Sherlock Holmes: A Game of Shadows*. Penggunaan matriks Fibonacci dalam kriptografi ditandai persegi kuning. Sumber: *Warner Bros*.

Kode rahasia yang dibuat, dapat ditebak, merupakan salah satu metode kriptografi yang memanfaatkan Fibonacci. Kode tersebut berbasis segitiga Pascal dan memiliki tiga elemen utama, kunci, rumus kodifikasi, dan *cipher*. Kunci dalam

[13] Balasaheb Tarle dan G. Prajapati, "On the information security using Fibonacci series" (International Conference and Workshop on Emerging Trends in Technology 2011, ICWET 2011, 2011).

[14] Alain Goriely dan Derek E. Moulton, "The Mathematics Behind Sherlock Holmes: A Game of Shadows" (SIAM News Volume 45 No. 3, 2012).

metode kriptografi ini bersifat publik, sehingga tergolong kriptografi kunci publik atau kriptografi asimetris.

Untuk menggunakan kode ini, setiap huruf dari pesan yang ingin dirahasiakan pertama-tama diubah menjadi sejumlah pasangan angka (dua digit), berdasarkan isi sebuah buku hortikultura yang dimiliki Moriarty. Setiap pasang angka berkorespondensi dengan halaman, baris, dan huruf.

Deretan sejumlah pasangan angka ini kemudian dienkripsi lebih lanjut dengan segitiga Pascal, berdasarkan kunci publik bilangan bulat p. Setiap bilangan bulat p akan dikembangkan barisan bilangan Fibonacci-p, disebut berbasis segitiga Pascal karena dapat dibentuk dengan menjumlahkan barisan-barisan dalam segitiga Pascal, seperti yang telah dicontohkan pada bab sebelumnya.

Setelah kunci publik p dipilih, setiap bilangan dua digit N yang diperoleh sebelumnya dapat direpresentasikan sebagai penjumlahan bilangan Fibonacci-p. Sebagai contoh, jika dipilih kunci publik 3 dan dari tahap pertama bilangan-bilangan yang diperoleh adalah:

23 10 10 05 03 20
23 17 04 18 33 12

dikodekan menjadi hasil dari penjumlahan baris bilangan Fibonacci-3. Sebagai contoh, 23 merupakan penjumlahan baris ke-4 dan ke-9, yaitu 4 + 19 = 23, sehingga 23 dienkripsi menjadi 0409. Hal yang sama dilakukan ke setiap angka, sampai pesan sebelumnya menjadi:

0409 07 07 05 03 0109
0409 0308 04 0408 0610 0207

Selanjutnya, kunci publik diberikan Moriarty kepada rekan-rekannya melalui ceramah yang diberikannya, yakni melalui nilai suatu variabel di papan tulisnya yang sebelumnya telah disepakati.

Pada alur film, metode kriptografi ini nantinya akan dipecahkan Holmes setelah mengunjungi ceramah Moriarty dan menyadari adanya perubahan salah satu variabel di papan tulisnya, ketika dibandingkan dengan papan tulis di kantornya saat dikunjungi Holmes beberapa hari sebelumnya.

Selanjutnya, ia mendeduksi bahwa kunci dari kode tersebut berasal dari buku hortikultura Moriarty setelah memperhatikan bunga dalam vas yang diletakkan di kantor Moriarty yang tampak layu.

V. KESIMPULAN

Terdapat banyak metode kriptografi yang memanfaatkan barisan bilangan Fibonacci, seperti beberapa yang telah dicontohkan di atas yaitu modifikasi *Playfair Cipher*, aplikasi matriks Qp, dan metode yang digunakan pada *Sherlock Holmes: A Game of Shadows* yang menggunakan kodifikasi buku dan segitiga Pascal.

Dalam implementasinya dalam kehidupan nyata, baik tertulis maupun *programming*, tentu harus memperhatikan metode yang paling cocok digunakan dan yang memiliki tingkat keamanan tertinggi berdasarkan situasi, kondisi, dan kebutuhan.

Adapun, dapat dilakukan eksplorasi lebih lanjut mengenai pembuatan metode kriptografi lainnya yang memanfaatkan barisan bilangan, misalnya, barisan bilangan Lucas.

REFERENSI

[1] Kessler, Gary C. (2020). *An Overview on Cryptography*. Diakses pada 7 Desember 2020, dari: https://www.garykessler.net/library/crypto.html.

[2] IBM. (2020). *What is Data Security?* Diakses pada 7 Desember 2020, dari: https://www.ibm.com/topics/data-security.

[3] University of Utah. (2009). *Fibonacci's Liber Abaci (Book of Calculation)*. Utah, Amerika Serikat.

[4] Sinha, Sudipta. (2019). *The Fibonacci Numbers and Its Amazing Applications*. Research Gate.

[5] Lamb, Robert. (2008). *How Are Fibonacci Numbers Expressed in Nature?* How Stuff Works. Diakses pada 6 Desember 2020, dari: https://science.howstuffworks.com/math-concepts/fibonacci-nature.htm.

[6] Ridley, J.N. (1982). *Packing Efficiency in Sunflower Heads*. Mathematical Biosciences, Volume 58 Issue 1.

[7] Pierce, Rod. (2019). *Golden Ratio*. Math Is Fun. Diakses pada 6 Desember 2020, dari: http://www.mathsisfun.com/numbers/golden-ratio.html.

[8] (2014). *Playfair Cipher*. Practical Cryptography. Diakses pada 9 Desember 2020, dari: http://practicalcryptography.com/ciphers/playfair-cipher/.

[9] Weisstein, Eric W. *Fibonacci Q-Matrix*. MathWorld—A Wolfram Web Resource. Diakses pada 10 Desember 2020, dari: https://mathworld.wolfram.com/FibonacciQ-Matrix.html

[10] Vasim Ahmad, Mohd et al. (2018). *An Improved Playfair Encryption Technique Using Fibonacci Series Generated Secret Key*. International Journal of Engineering & Technology Volume 7 No. 4.5.

[11] Kuhapatanakul, Kantaphon. (2016). *The Fibonacci p-numbers and Pascal's triangle*. Cogent Mathematics Volume 3 No. 1.

[12] UçAr, Sümeyra, Taş, Nihal, dan Özgür, Nihal Yilmaz. (2017). *A New Cryptography Model via Fibonacci and Lucas Numbers*. Cornell University, Computer Science: Cryptography and Security, arXiv: 1709.10355, 2017).

[13] Tarle, Balasaheb dan Prajapati, G. (2011). *On the information security using Fibonacci series*. International Conference and Workshop on Emerging Trends in Technology 2011, ICWET 2011. Diakses pada 11 Desember 2020, dari: https://www.researchgate.net/publication/220902441_On_the_information_security_using_Fibonacci_series.

[14] Goriely, Alain dan Moulton, Derek E. (2012). *The Mathematics Behind Sherlock Holmes: A Game of Shadows*. SIAM News Volume 45 No. 3.

PERNYATAAN

Dengan ini saya menyatakan bahwa makalah yang saya tulis ini adalah tulisan saya sendiri, bukan saduran, atau terjemahan dari makalah orang lain, dan bukan plagiasi.

Bandung, 3 Desember 2020

Karina Imani – 13519166