J. Sains Dasar 2019 8 (1) 6 - 12

SISTEM KRIPTOGRAFI *STREAM CIPHER* BERBASIS FUNGSI CHAOS UNTUK KEAMANAN INFORMASI

STREAM CIPHER CRYPTOGRAPHY SYSTEM BASED ON CHAOTIC FUNCTION FOR INFORMATION SECURITY

Sahid[1], Atmini Dhoruri[1], Dwi Lestari[1,*)], Eminugroho Ratna Sari[1], Muhammad Fauzan[1]

[1]*Jurusan Pendidikan Matematika, Fakultas Matematika dan Ilmu Pengetahuan Alam, Universitas Negeri Yogyakarta, Yogyakarta, Indonesia*

*email korespondensi: sahid@uny.ac.id

Abstrak

Tujuan penelitian ini adalah menerapkan fungsi chaos *Logistic Map* dalam meningkatkan keamanan pengiriman informasi. Fungsi chaos memiliki tingkah laku yang sangat kompleks, *irregular* dan *random* di dalam sebuah sistem yang deterministik. Chaos mempunyai sifat yang kacau atau acak, perubahan sedikit saja akan membangkitkan bilangan yang berbeda, hal ini berguna dalam membangkitkan kunci. Fungsi chaos *Logistic Map* akan digunakan untuk membangkitkan kunci. Selanjutnya, digunakan fungsi *sinus* berosilasi tinggi untuk meningkatkan keacakan bilangan. Dalam menentukan pembangkit kunci akan digunakan protokol perjanjian kunci Stickel. Selanjutnya pembangkit kunci akan diproses menggunakan fungsi chaos *Logistic Map* dikombinasikan dengan fungsi *sinus* berosilasi tinggi dan akan diperoleh kunci yang akan digunakan untuk enkripsi serta dekripsi. Pada proses enkripsi dilakukan perhitungan dengan rumus $C_i = (K_i + P_i)$ mod 256, sedangkan proses dekripsi dilakukan perhitungan dengan rumus $C_i = (K_i - P_i)$ mod 256, dengan C_i adalah Ciphertext, P_i adalah Plaintext, serta K_i adalah Kunci. Dengan menggunakan *Logistic Map* dan fungsi *sinus* pada pembangkit kunci diperoleh sifat chaos yang tinggi untuk nilai parameter tertentu, bersifat chaos hanya pada beberapa iterasi awal, selanjutnya *error* berkaitan dengan nilai $x_i = 0$. Untuk nilai-nilai parameter yang lain diperoleh barisan kunci yang konvergen setelah beberapa iterasi.

Kata Kunci: Kriptografi, Fungsi Chaos, *Logistic Map*, fungsi *sinus*, keamanan informasi

Abstract

This research aims to apply Logistic Map as one of the chaotic functions for improving information transmission security. Chaotic function has a complex behavior, irregular, and random in the deterministic system. Chaotic with a little change will obtain a different number. It is useful for generating the key. Logistic map will be used to generate the key, then it will be combined with sine function to increase the chaos. In determining the key generator we will use the Stickel's protocol agreement. Furthermore, the key generator will be in process using chaos function of Logistic Map combined with high oscillating sine function and will get the key which will be used for encryption and decryption. The encryption process is done with the formula of $C_i = K_i + P_i$ *mod 256, while the decryption process is calculated by the formula of* $C_i = K_i - P_i$ *mod 256, with* C_i *is Ciphertext,* P_i *is Plain text, and* K_i *is the Key. Using the Logistic Map and sine function on the key generator, the chaotic properties are higher for certain parameter values, chaos only on some initial iterations, then an error is related to the value* $x_i = 0$ *. For other parameter values we get a converging key sequence after several iterations.*

Keywords: cryptography, chaotic function, logistic map, sine function, information security

Pendahuluan

Keamanan informasi merupakan hal yang penting. Informasi rahasia tidak boleh bocor ke publik atau segelintir orang yang tidak berkepentingan dalam informasi tersebut. Jika informasi bocor maka akan merugikan pihak pengirim ataupun penerima informasi. Seiring dengan perkembangan jaman, kemajuan teknologi semakin pesat. Seseorang yang tidak berkepentingan dalam informasi tersebut bisa dengan mudah mengetahui isi dari informasi. Pengirim informasi harus merahasiakan pesannya agar tidak mudah diketahui oleh orang luar. Pengamanan informasi bisa dilakukan dengan menyandikan pesan menjadi kode -kode yang rumit untuk diketahui, namun tidak menutup kemungkinan orang yang tidak bertanggung jawab

untuk bisa mengetahui isi pesan. Oleh sebab itu, dibutuhkan ilmu yang mempelajari keamanan informasi. Salah satu ilmu yang mempelajari sistem keamanan informasi adalah kriptografi.

Kriptografi berasal dari dua kata, yaitu *cryptos* dan *graphein*. *Cryptos* berarti rahasia, dan *graphein* berarti tulisan, sehingga menurut bahasa, kriptologi berarti tulisan rahasia. Sementara itu, menurut definisi, kriptografi adalah ilmu yang mengkaji penyandian dan penguraian pesan rahasia [1]. Dalam kriptografi, pesan asli yang akan dikirim terlebih dahulu dikodekan, proses ini disebut Enkripsi. Enkripsi berguna untuk merahasiakan Pesan. Sementara itu, untuk mengembalikan ke bentuk pesan asli disebut Dekripsi. Pesan asli disebut *Plaintext* dan pesan yang sudah dirahasiakan disebut *Ciphertext*.

Proses enkripsi dan dekripsi membutuhkan kunci. Sistem kriptografi digolongkan menjadi dua macam, yaitu sistem kriptografi simetri dan asimetri. Perbedaan antara dua sistem kriptografi ini adalah kunci enkripsi dan dekripsi. Sistem kriptografi simetri, kunci yang digunakan untuk enkripsi dan dekripsi sama, dan dalam sistem kriptografi asimetri kunci yang digunakan untuk enkripsi dan dekripsi berbeda. Sistem kriptografi simetri mempunyai kelemahan yaitu kunci harus dikirim melalui jalur aman. Pengirim dan penerima harus menjaga kerahasiaan kunci ini. Sementara itu, untuk sistem kriptografi asimetri, kunci enkripsi tidak perlu dijaga kerahasiaanya yaitu berupa kunci publik, dan kunci dekripsi yang akan dirahasiakan dan diketahui oleh penerima saja.

Algoritma kriptografi simetri mengharuskan kunci terjaga rahasia dan kunci rawan diketahui pihak penyadap. Untuk meningkatkan keamanan dan kerumitan kunci dalam algoritma kriptografi digunakan fungsi chaos untuk membangkitkan kunci. Terdapat fungsi chaos yaitu *Logistic Map, Henon Map, Baker Map, Arnold Cat Map* dan *Circle Map* yang sensitif pada nilai awal, dimana perubahan sedikit dapat memunculkan bilangan yang berbeda. Dalam penelitian ini dibahas fungsi chaos Logistic Map yang dianalisa nilai parameter sifat chaosnya sehingga fungsi chaos berguna di dalam sistem kriptografi sebagai pembangkit kunci yang akan digunakan dalam proses enkripsi.

Aplikasi yang digunakan untuk membuat kunci dalam sistem kriptografi sudah dibahas sebelumnya dalam artikel ilmiah yang berjudul *Aplikasi Aljabar Min-Plus untuk Mengamankan Informasi rahasia* yang membahas tentang kegunaan Aljabar *Min-Plus* dalam menentukan kunci pada proses pengamanan informasi rahasia [2]. Dalam artikel lain telah dilakukan penelitian tingkat keacakan peta logistic menggunakan fungsi trigonometri osilasi tinggi [3]. Dalam artikel yang berjudul *Suatu Algoritma Kriptografi Stream Cipher Berdasarkan Fungsi Chaos* dijelaskan tentang fungsi chaos *logistic map* yang digunakan untuk menyandikan pesan [4]. Mina Mishra and Vijay H Mankar [5,6] mendiskusikan peran fungsi chaos dalam kriptografi. Dalam penelitian ini akan dibahas aplikasi fungsi chaos *Logistic Map* dikombinasikan dengan fungsi *sinus* berosilasi tinggi dalam kriptografi untuk keamanan informasi.

Fungsi chaos *Logistic Map* pertama kali digunakan dalam model matematika pertumbuhan populasi. Fungsi tersebut menunjukkan dinamika populasi yang ditemukan oleh ilmuwan Verhults. Fungsi ini memiliki periode, yaitu akan kembali ke bentuk semula pada saat jumlah iterasi tertentu. Fungsi chaos *Logistic Map* mempunyai keunggulan dalam kecepatan mengenkripsikan data. Sementara itu, fungsi *sinus* berosilasi tinggi akan dikombinasikan dengan fungsi *Logistic Map* sehingga diharapkan tingkat keacakannya lebih tinggi. Selanjutnya untuk simulasi digunakan program komputer OCTAVE [7].

Metode Penelitian

Penelitian ini termasuk dalam penelitian terapan dalam teori aljabar dan komputasi serta sistem kriptografi. Pada tahap awal, dibentuk persamaan dari fungsi chaos *Logistic Map* dengan memilih satu parameter tertentu yaitu μ. Kemudian dibentuk nilai awal menurut perjanjian kunci Stickel yang akan menjadi pembangkit kunci rahasia. Kunci rahasia dibentuk menggunakan fungsi *Logistic Map* dikombinasikan dengan fungsi *sinus* osilasi tinggi. Dilakukan proses enkripsi pesan plainteks menjadi cipherteks. Terakhir dilakukan proses dekripsi pesan cipherteks menjadi pesan semula yaitu plainteks. Pada tahap akhir, dilakukan simulasi menggunakan program komputer OCTAVE dengan memilih beberapa nilai awal yang berbeda sehingga diperoleh tingkat keacakan fungsi chaos yang digunakan.

Hasil dan Diskusi

Teori Chaos

Dalam buku Teori Chaos karya Yani Kusmarni [8] dijelaskan pada tahun 1880, seorang ahli matematika perancis bernama Henri Poincare adalah orang yang pertama merumuskan yang sekarang dikenal sebagai chaos. Henri Poincare menemukan bahwa terdapat orbit yang bersifat nonperiodik, yang berarti tidak bekerja secara

teratur. Awalnya gagasan Henri tidak terlalu dihargai oleh para ilmuwan, namun pada tahun 1898 Jacques Hadamard mempublikasikan teori yang hampir sama dengan Teori Henri.

Teori Chaos pertama kali dicetuskan oleh Edward Lorenz yang merupakan seorang ahli meteorologi AS pada tahun 1961. Edward menemukan teori chaos secara tidak sengaja saat melakukan peramalan cuaca dengan bantuan komputer. Dalam melakukan percobaan, Edward hanya mengambil 3 digit di belakang koma dari hasil yang didapatkan pada saat melakukan peramalan cuaca untuk dijadikan kondisi awal yang baru. Hasil yang didapatkan jauh berbeda. Data dari hasil percobaan dimasukkan dalam bentuk grafik maka tercipta efek kupu-kupu.

Teori Chaos berguna dalam membangkitkan bilangan secara acak, dan juga peka terhadap kondisi awal. Perubahan nilai awal sekecil 10^{-100} akan membangkitkan bilangan yang benar-benar berbeda. Hal ini sangat berguna dan dapat diterapkan di dalam kriptografi sebagai pembangkit kunci, yang selanjutnya digunakan untuk proses enkripsi serta dekripsi, maka dari itu dipilih Teori Chaos untuk diterapkan dalam kriptografi.

Logistic Map dalam Fungsi Sinus Berosilasi Tinggi

Berikut merupakan persamaan iteratif fungsi chaos logistic map dengan parameter μ.

$$x_{i+1} = \mu x_i(1-x_i), \quad 0 \le \mu \le 4, 0 \le x \le 1 \qquad (1)$$

Dalam penelitian ini dipilih fungsi chaos *Logistic Map* dikombinasikan dengan fungsi *sinus* osilasi tinggi karena fungsi tersebut memiliki perilaku sulit diprediksi pada parameter *x* yang dekat dengan nol. Oleh sebab itu hasil peta persamaan logistik dipilih dalam interval yang cukup dekat dengan nol yaitu [0,0.1] sehingga diharapkan kunci yang dibentuk semakin sulit ditebak. Adapun fungsi *sinus* osilasi tinggi yang dimaksud berbentuk sebagai berikut:

$$y = \sin\left(\frac{1}{x^3}\right). \qquad (2)$$

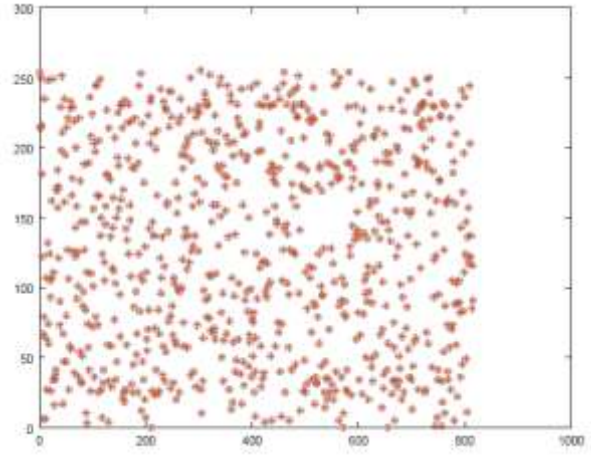
Penerapan pada Sistem Kriptografi

Langkah penerapan fungsi chaos dijelaskan pada bagan alir algoritma terlampir. Dimulai dengan memilih matriks berukuran $n \times n$ dengan entri bilangan bulat modulo prima. Selanjutnya matriks dipilih beserta sebarang bilangan asli oleh pihak 1 dan pihak 2 untuk melakukan protokol perjanjian kunci Stickel sehingga dihasilkan nilai awal yang sama untuk pihak 1 dan pihak 2. Setelah nilai awal diperoleh kemudian dioperasikan ke dalam fungsi chaos Logistic Map yang dikomposisikan dengan fungsi sinus berosilasi tinggi menghasilkan nilai iterasi yang digunakan sebagai barisan kunci untuk enkripsi.

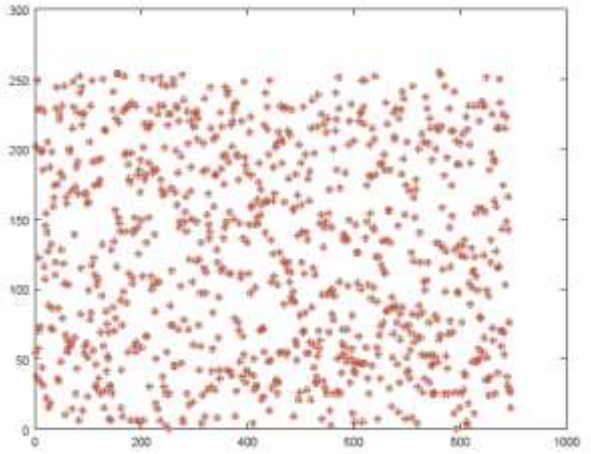
Proses enkripsi dilakukan setelah plainteks dikonversi ke dalam kode ASCII (digunakan modulo 256) sehingga dihasilkan cipherteks yang akan dikirim pihak 1 ke pihak 2. Selanjutnya pihak 2 melakukan hal yang sama untuk mendapatkan barisan kunci untuk proses dekripsi sehingga dihasilkan pesan dalam kode ASCII yang dikonversi menjadi pesan asli atau plainteks.

Hasil Simulasi Sifat Chaos parameter μ

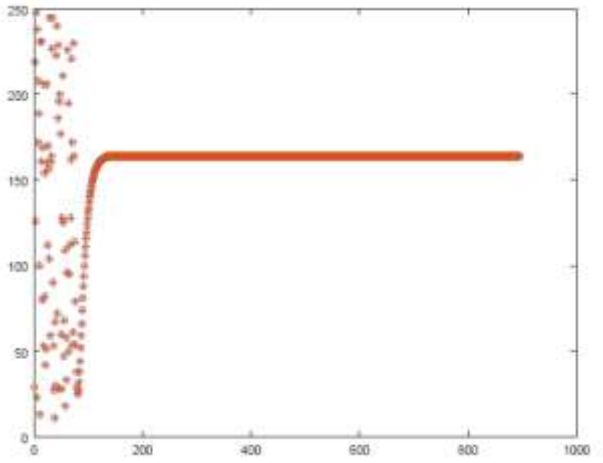
Untuk mendapatkan sifat chaos yang tinggi dilakukan analisa parameter μ. Gambar 1 hingga Gambar 12 menyajikan perilaku barisan kunci K_i yang dihasilkan untuk nilai-nilai parameter fungsi logistik μ yang berbeda-beda, dengan pesan sepanjang 895 karakter.



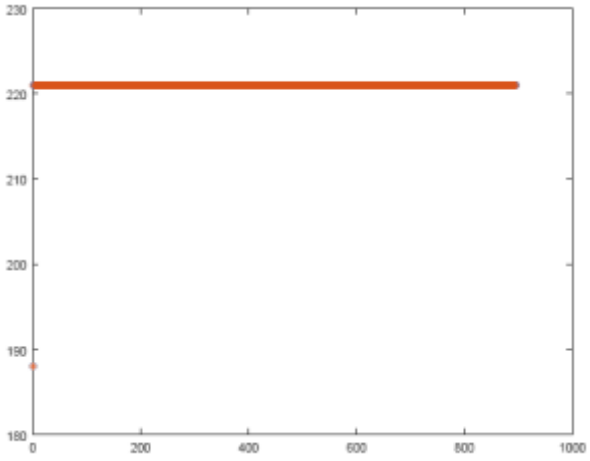
Gambar 1. Hasil barisan kunci K_i untuk $\mu = 0.75$.



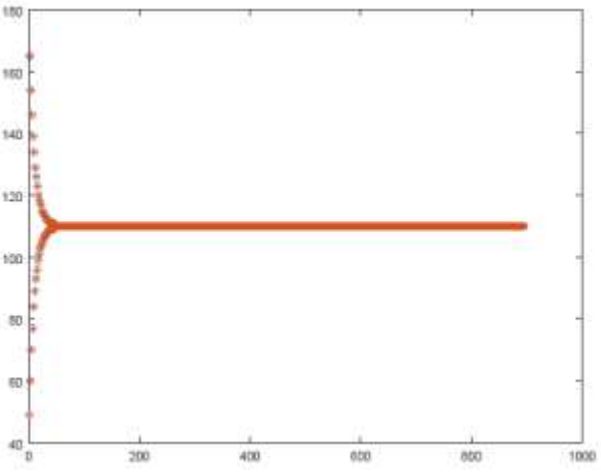
Gambar 2. Hasil barisan kunci K_i untuk $\mu = 1$



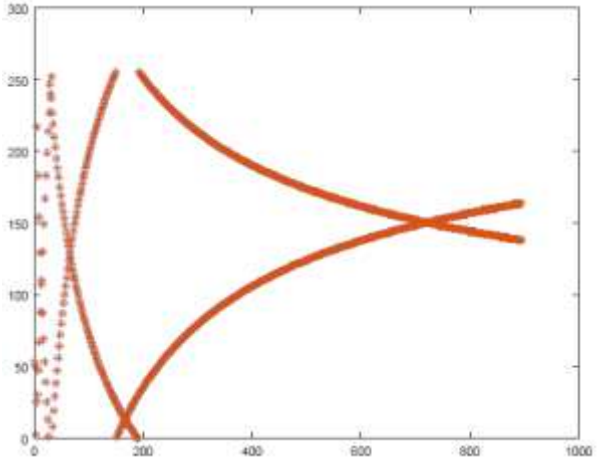
Gambar 3. Hasil barisan kunci K_i untuk $\mu = 1.1$



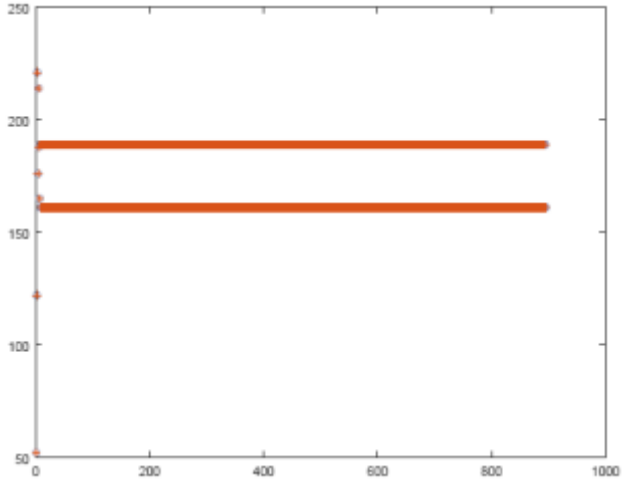
Gambar 4. Hasil barisan kunci K_i untuk $\mu = 2$



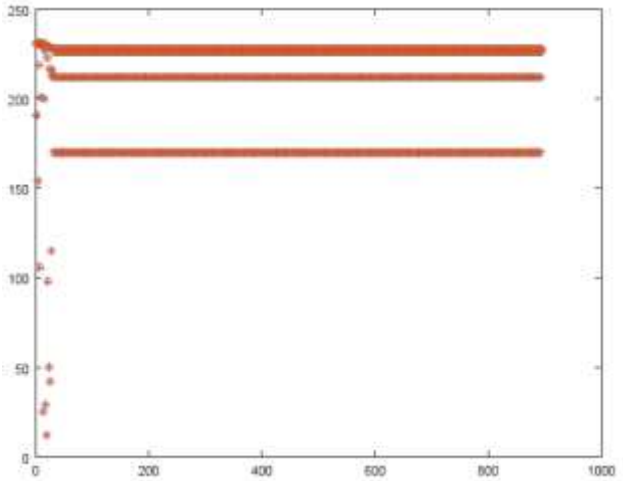
Gambar 5. Hasil barisan kunci K_i untuk $\mu = 2.9$



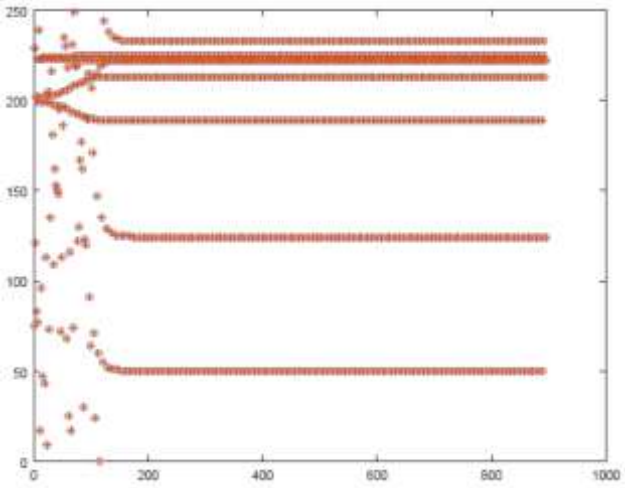
Gambar 6. Hasil barisan kunci K_i untuk $\mu = 3$



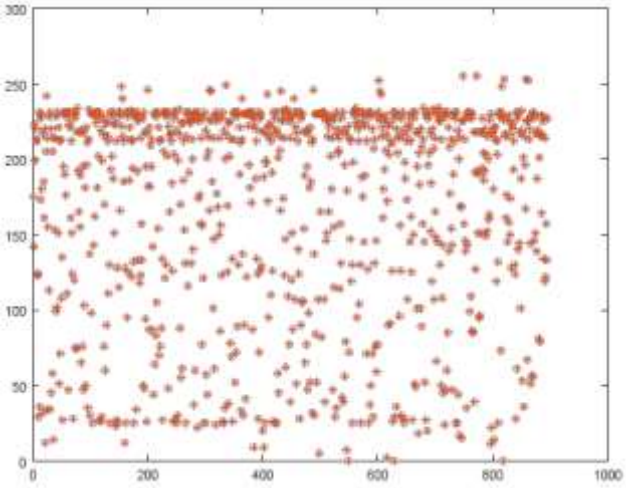
Gambar 7. Hasil barisan kunci K_i untuk $\mu = 3.25$



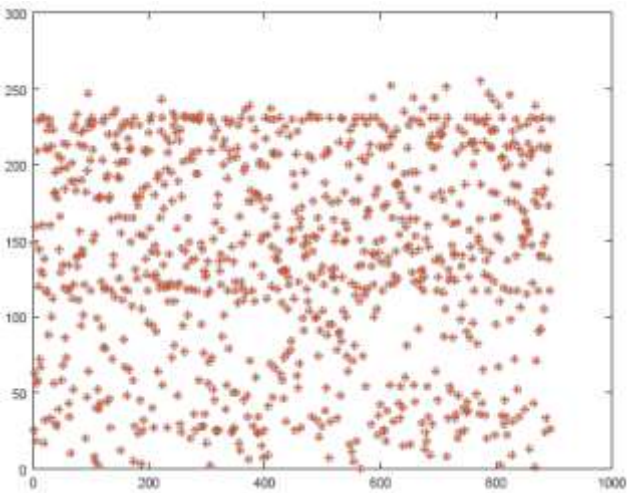
Gambar 8. Hasil barisan kunci K_i untuk $\mu = 3.5$



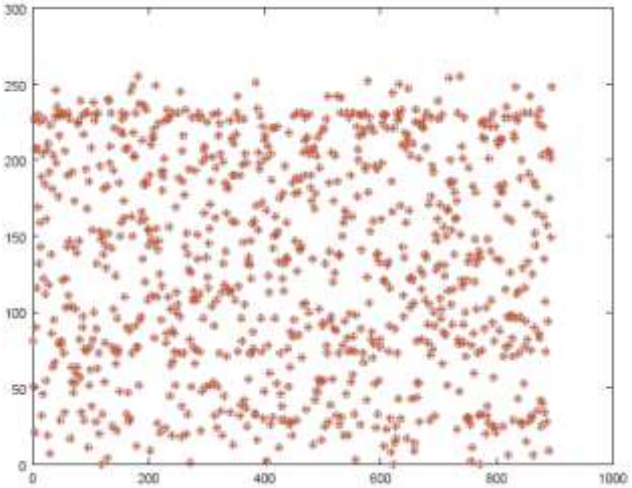
Gambar 9. Hasil barisan kunci K_i untuk $\mu = 3.55$



Gambar 10. Hasil barisan kunci K_i untuk $\mu = 3.6$



Gambar 11. Hasil barisan kunci K_i untuk $\mu = 3.89$



Gambar 12. Hasil barisan kunci K_i untuk $\mu = 4$

Berdasarkan simulasi dapat disimpulkan bahwa untuk $\mu = 1$ dan $3.75 \le \mu \le 4$ dihasilkan barisan kunci $\{K_i\}$ yang bersifat chaos, untuk $0 < \mu \le 0.75$ dihasilkan barisan kunci $\{K_i\}$ yang bersifat chaos hanya pada beberapa iterasi awal, serta *error* berkaitan nilai $x_i = 0$. Untuk nilai-nilai μ yang lain diperoleh barisan kunci yang konvergen setelah beberapa iterasi.

Simpulan

Dalam penelitian ini dapat disimpulkan penggunaan fungsi logistik Map yang dikombinasikan dengan fungsi sinus berosilasi tinggi dapat menghasilkan sifat chaos dimana untuk $\mu = 1$ dan $3.75 \le \mu \le 4$ dihasilkan barisan kunci $\{K_i\}$ yang bersifat chaos, untuk $0 < \mu \le 0.75$ dihasilkan barisan kunci $\{K_i\}$ yang bersifat chaos hanya pada beberapa iterasi awal, selanjutnya *error* berkaitan nilai $x_i = 0$. Untuk nilai-nilai μ yang lain diperoleh barisan kunci yang konvergen setelah beberapa iterasi. Perlu dipilih nilai parameter yang menghasilkan sifat chaos tinggi sehingga barisan kunci untuk proses enkripsi dan dekripsi memiliki sifat chaos tinggi yang berfungsi untuk tingkat keamanan informasi pengiriman pesan. Untuk penelitian selanjutnya dapat menggunakan fungsi chaos lain yang dikombinasikan dengan fungsi sinus osilasi tinggi. Selanjutnya dianalisa nilai parameter sifat chaosnya.

Ucapan Terima Kasih

Ucapan terima kasih peneliti sampaikan pada Fakultas Matematika dan Ilmu Pengetahuan Alam, Universitas Negeri Yogyakarta yang memberikan dana untuk mendukung terlaksananya penelitian DIPA Universitas Negeri Yogyakarta ini.

Pustaka

[1] Anton,Howard & Rorres,Chris.(2014). *Elementary Linear Algebra : Applications Version*. New Jersey:Wiley.

[2] Dimas Ridwan W. (2014).Aplikasi Aljabar Min-Plus untuk Mengamankan Informasi Rahasia. *Skripsi*. Yogyakarta : Universitas Negeri Yogyakarta.

[3] Achmad Dimas Noorcahyo. (2011). *Pendiskritan Pembangkit Bilangan Acak Peta Logistik Menggunakan Fungsi Trogonometri Osilasi Tinggi.* Artikel. Bandung: ITB.

[4] Dwi Lestari dan Zaki Riyanto. (2012). Suatu Algoritma Kriptografi Stream Cipher Berdasarkan Fungsi Chaos. *Prosiding,*Seminar Nasional. Yogyakarta : FMIPA UNY.

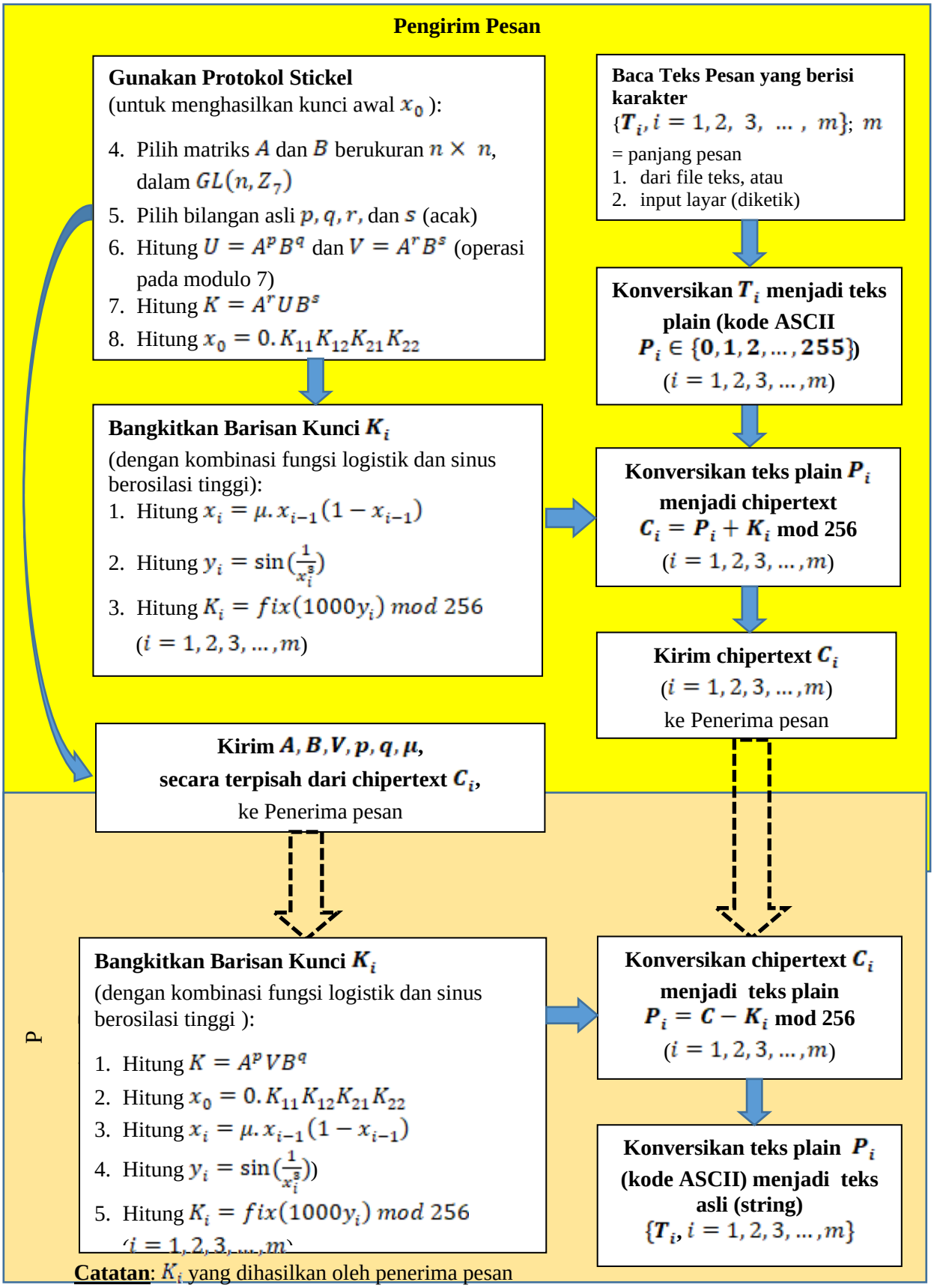
[5] Mina Mishra and Vijay H Mankar. 2011. Chaotic Encryption Scheme Using 1-D Chaotic Map. *Int.J.Communication Network and System Sciences.* 4, pp.452-455.

[6] Piyush Kumar Shukla, Ankur Khare, Murtaza Abbas Rizvi, Shalina Stalin, and Sanjay Kumar. 2015. Applied Cryptography Using Chaos Function for Fast Digital Logic-Based System in Ubiquitous Computing. *Entropy Journal* 17 pp: 1387-1410

[7] Eaton, J. W., Bateman, D.& Hauberg, S. (2007). *GNU Octave*.Boston: Free Software Foundation, Inc.

[8] Kusmarni, Yani. (2008). *TEORI CHAOS:Sebuah Keteraturan Dalam Keacakan*.Bandung:UPI.

Lampiran Bagan Alir Algoritma



Catatan: K_i yang dihasilkan oleh penerima pesan