

**ANALISIS MODEL FRAKSIONAL PENYEBARAN INFEKSI
KODE MALICIOUS PADA JARINGAN KOMPUTER**

SKRIPSI



ROKHANA ETHA DAMAYANTI

**PROGRAM STUDI S-1 MATEMATIKA
DEPARTEMEN MATEMATIKA
FAKULTAS SAINS DAN TEKNOLOGI
UNIVERSITAS AIRLANGGA**

2016

**ANALISIS MODEL FRAKSIONAL PENYEBARAN INFEKSI
KODE MALICIOUS PADA JARINGAN KOMPUTER**

SKRIPSI



ROKHANA ETHA DAMAYANTI

**PROGRAM STUDI S-1 MATEMATIKA
DEPARTEMEN MATEMATIKA
FAKULTAS SAINS DAN TEKNOLOGI
UNIVERSITAS AIRLANGGA**

2016

ANALISIS MODEL FRAKSIONAL PENYEBARAN INFEKSI

KODE MALICIOUS PADA JARINGAN KOMPUTER

SKRIPSI

Sebagai Salah Satu Syarat Untuk Memperoleh

Gelar Sarjana Sains Bidang Matematika

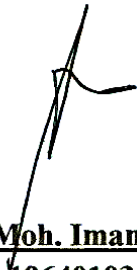
pada Fakultas Sains dan Teknologi


Universitas Airlangga

Disetujui oleh :

Pembimbing I,

Pembimbing II,


Dr. Moh. Imam Utoyo, M.Si.
NIP. 19640103 198810 1 001


Dr. Fatmawati, M.Si.
NIP. 19730704 199802 2 001

LEMBAR PENGESAHAN NASKAH SKRIPSI

Judul : Analisis Model Fraksional Penyebaran Infeksi Kode
Malicious Pada Jaringan Komputer

Penyusun : Rokhana Etha Damayanti

NIM : 081211232027

Pembimbing I : Dr. Moh. Imam Utoyo, M.Si.

Pembimbing II : Dr. Fatmawati, M.Si.


Tanggal Seminar : 27 Januari 2016

Disetujui oleh :

Pembimbing I,

Pembimbing II,




Dr. Moh. Imam Utoyo, M.Si.
NIP. 19640103 198810 1 001



Dr. Fatmawati, M.Si.
NIP. 19730704 199802 2 001

Mengetahui,

Ketua Departemen Matematika
Fakultas Sains dan Teknologi
Universitas Airlangga

Koordinator Program Studi Matematika
Fakultas Sains dan Teknologi
Universitas Airlangga



Badrus Zaman, S.Kom., M.Cs.
NIP. 19780126 200604 1 001


Dr. Moh. Imam Utoyo, M.Si.
NIP. 19640103 198810 1 001

PEDOMAN PENGGUNAAN SKRIPSI

Skripsi ini tidak dipublikasikan, namun tersedia di perpustakaan dalam lingkungan Universitas Airlangga, diperkenankan untuk dipakai sebagai referensi kepustakaan, tetapi pengutipan harus seizin penulis dan harus menyebutkan sumbernya sesuai kebiasaan ilmiah. Dokumen skripsi ini merupakan hak milik Universitas Airlangga.



SURAT PERNYATAAN TENTANG ORISINALITAS

Yang bertanda tangan di bawah ini, saya :

Nama : Rokhana Etha Damayanti
NIM : 081211232027
Program Studi : Matematika
Fakultas : Fakultas Sains dan Teknologi
Jenjang : Sarjana (S1)

Menyatakan bahwa saya tidak melakukan kegiatan plagiat dalam penulisan skripsi
sayang yang berjudul :

**Analisis Model Fraksional Penyebaran Infeksi Kode Malicious
Pada Jaringan Komputer**

Apabila suatu saat nanti terbukti melakukan tindakan plagiat, maka saya akan
menerima sanksi yang telah ditetapkan.

Demikian surat pernyataan ini saya buat dengan sebenar-benarnya.

Surabaya, 1 Februari 2016



Rokhana Etha Damayanti
NIM. 081211232027

KATA PENGANTAR



Alhamdulillahrabbi'l'amin. Segala puji syukur penulis panjatkan kepada Allah SWT karena hanya dengan rahmat dan karunia-Nya, sehingga proposal skripsi yang berjudul “Analisis Model Fraksional Penyebaran Infeksi Kode Malicious Pada Jaringan Komputer” ini dapat diselesaikan dengan baik. Shalawat serta salam bahagia semoga senantiasa tercurahkan kepada junjungan kita, Nabi Besar Muhammad SAW, pemimpin sekaligus sebaik-baiknya suri tauladan bagi kehidupan umat manusia.

Ucapan terima kasih disampaikan kepada :

1. Universitas Airlangga yang telah memberikan kesempatan kepada penulis untuk menuntut ilmu.
2. Badrus Zaman, S.Kom., M.Cs. selaku Ketua Departemen Matematika Fakultas Sains dan Teknologi Universitas Airlangga.
3. Dr. Moh. Imam Utoyo, M.Si selaku dosen wali sekaligus dosen pembimbing I yang selalu memberikan masukan inspirasi dalam perkuliahan dan senantiasa penuh kesabaran, ketelitian, keramahan, dalam memberikan bimbingan berupa ilmu, arahan, waktu, serta semangat.
4. Dr. Fatmawati, M.Si selaku dosen pembimbing II yang senantiasa penuh kesabaran, ketelitian, keramahan, dalam memberikan bimbingan berupa ilmu, arahan, waktu, serta semangat.

5. Yang Tercinta Kedua orang tuaku Yamyuni dan Basori serta saudari-saudariku Gita, Rofa, dan Flora yang selalu memberikan dukungan, semangat, doa dan kasih sayangnya.
6. Teman-teman mahasiswa jurusan Matematika angkatan 2012 atas dukungan dan kebersamaannya selama ini.

Penulis berharap semoga proposal ini dapat bermanfaat sebagai bahan pustaka dan penambah informasi khususnya bagi mahasiswa Universitas Airlangga. Penulis menyadari bahwa dalam penulisan skripsi ini, kemungkinan masih terdapat kekurangan sehingga saran dan kritik yang membangun sangat diharapkan untuk penulisan berikutnya.

Surabaya, Januari 2016

Rokhana Etha Damayanti

Rokhana Etha Damayanti, 2016, **Analisis Model Fraksional Penyebaran Infeksi Kode Malicious Pada Jaringan Komputer**. Skripsi ini dibimbing oleh Dr. Moh. Imam Utoyo, M.Si. dan Dr. Fatmawati, M.Si., Departemen Matematika, Fakultas Sains dan Teknologi, Universitas Airlangga, Surabaya.

ABSTRAK

Perkembangan teknologi komputer yang sangat pesat, tidak hanya memberikan manfaat yang besar tapi juga memberikan kerugian bagi penggunanya. Kode *malicious* merupakan perangkat lunak yang mengganggu dan merusak operasi normal sistem komputer atau perangkat lunak lain, dan mengeksekusi tanpa persetujuan penggunanya. Model matematika penyebaran infeksi kode *malicious* diperlukan untuk mengurangi banyaknya komputer yang terserang *malicious*. Dinamika penyebaran infeksi kode *malicious* ini mirip dengan penyebaran infeksi virus biologi pada umumnya, sehingga dapat didekati dengan Sistem Persamaan Diferensial Biasa (SPDB) nonlinier.

Dalam skripsi ini dibahas mengenai modifikasi Sistem Persamaan Diferensial Fraksional (SPDF) nonlinier penyebaran infeksi kode *malicious* pada jaringan komputer dari Sistem Persamaan Diferensial Biasa (SPDB) nonlinier. Cara memodifikasinya yaitu dengan mengganti turunan pertamanya dengan turunan fraksional. Metode yang digunakan untuk menyelesaikan SPDF ini adalah Metode Analisis Homotopi (HAM). Solusi analitik yang diperoleh berupa deret tak hingga. Selanjutnya solusi numerik diperoleh dengan pemotongan empat suku pertama dari deret. Berdasarkan hasil simulasi, besarnya nilai orde sebanding dengan besarnya penurunan pada populasi komputer rentan, populasi komputer terekspos dan populasi komputer *removed*, serta sebanding pula dengan besarnya peningkatan pada populasi komputer terinfeksi dan populasi komputer antidotal.

Kata kunci : Model Matematika, Kode *Malicious*, Orde fraksional, Metode Analisis Homotopi.

Rokhana Etha Damayanti, 2016, **Fractional Model Analysis for Spreading of Malicious Codes Infection in Computer Network**. This final project is under advice by Dr. Moh. Imam Utoyo, M.Si. dan Dr. Fatmawati, M.Si., Mathematics Department, Science and Technology Faculty, Airlangga University, Surabaya.

ABSTRACT

The development of computer technology is not only providing great advantage but also many disadvantages. The malicious code is software that disrupts and damages the normal operation of a computer system or other software and execute without user consent. Mathematical model of spreading of malicious codes infection is required to reduce the number of infected computers that attacked by malicious code. The dynamics of the spread of malicious codes infection is similar to the spreading of biology virus infection in general, so we can approximate it by Ordinary Differential Equation System (ODEs).

In this final project, we discuss analytical solution by modifying the nonlinear Fractional Differential Equation System (FDEs) from nonlinear ODEs. It is modified by replacing the first derivative with the fractional derivative. We develop HAM to solve FDEs. The analytic result is infinite series. The numerical result is obtained with the truncations on the first four parts of the series. According to the simulation result, the value of the order is proportional to the decreasing of the susceptible computers population, exposed computers population and removed computers population, and proportional to the increasing of infected computers population and antidotal computers population.

Keywords: Mathematical Model, Malicious Code, Fractional Order, Homotopy Analysis Method.

DAFTAR ISI

	Halaman
HALAMAN JUDUL	i
LEMBAR PERSETUJUAN	ii
LEMBAR PENGESAHAN NASKAH SKRIPSI.....	iii
PEDOMAN PENGGUNAAN SKRIPSI	iv
SURAT PERNYATAAN TENTANG ORISINALITAS	v
KATA PENGANTAR	vi
ABSTRAK	viii
ABSTRACT.....	ix
DAFTAR ISI.....	x
DAFTAR TABEL.....	xii
DAFTAR GAMBAR.....	xiii
DAFTAR LAMPIRAN.....	xiv
BAB I PENDAHULUAN	
1.1 Latar Belakang	1
1.2 Rumusan Masalah	4
1.3 Tujuan.....	4
1.4 Manfaat.....	5
1.5 Batasan Masalah.....	5
BAB II TINJAUAN PUSTAKA	
2.1 Definisi Kode Malicious dan Cara Penyebarannya.....	6
2.2 Cara Pencegahan Penyebaran Infeksi Kode Malicious.....	7

2.3 Model Matematika Untuk Penyebaran Infeksi Kode Malicious	8
2.4 Sistem Persamaan Diferensial Orde Fraksional Untuk Penyebaran Infeksi Kode Malicious.....	13
2.5 Homotopy Analysis Method (HAM).....	16
BAB III METODE PENELITIAN	19
BAB IV PEMBAHASAN	
4.1 Model Matematika Penyebaran Infeksi Kode Malicious pada Jaringan Komputer Orde Fraksional	22
4.2 Solusi Model Penyebaran Infeksi Kode Malicious pada Jaringan Komputer dengan Menggunakan Metode Analisis Homotopi.....	23
4.3 Simulasi Numerik Sistem Persamaan Diferensial Fraksional Penyebaran Infeksi Kode Malicious pada Jaringan Komputer	31
BAB V PENUTUP	
5.1 Kesimpulan.....	39
5.2 Saran.....	40
DAFTAR PUSTAKA	41
LAMPIRAN	

DAFTAR TABEL

No.	Judul	Halaman
2.1	Notasi dan Deskripsi Parameter Penyebaran Infeksi Kode Malicious pada Jaringan Komputer	10
4.1	Nilai Parameter Model Penyebaran Infeksi Kode Malicious pada Jaringan Komputer	31



DAFTAR GAMBAR

No.	Judul	Halaman
2.1	Diagram Transmisi Model Matematika Penyebaran Infeksi Kode Malicious pada Jaringan Komputer	11
4.1	Simulasi Numerik SPDB Nonlinier Penyebaran Infeksi Kode Malicious pada Jaringan Komputer	32
4.2	Simulasi Numerik SPDF $\mu_1 = 1$ Penyebaran Infeksi Kode Malicious pada Jaringan Komputer	33
4.3	Perbandingan Simulasi Numerik SPDB Nonlinier dengan SPDF $\mu_i = 1$ pada Populasi Komputer	33
4.4	Dinamika Populasi Komputer untuk $\mu_1 = \mu_2 = \mu_3 = 1$, $\mu_1 = \mu_2 = \mu_3 = 0.75$, $\mu_1 = \mu_2 = \mu_3 = 0.5$, $\mu_1 = \mu_2 = \mu_3 = 0.25$ dan $\mu_4 = \mu_5 = 1$	35
4.5	Dinamika Populasi Komputer untuk $\mu_4 = \mu_5 = 1$, $\mu_4 = \mu_5 = 0.75$, $\mu_4 = \mu_5 = 0.5$, $\mu_4 = \mu_5 = 0.25$ dan $\mu_1 = \mu_2 = \mu_3 = 1$	37

DAFTAR LAMPIRAN

No.	Judul Lampiran
1	Perhitungan Bentuk Umum $\mathcal{R}S_m(\vec{S}_{m-1}(t))$, $\mathcal{R}E_m(\vec{E}_{m-1}(t))$, $\mathcal{R}I_m(\vec{I}_{m-1}(t))$, $\mathcal{R}R_m(\vec{R}_{m-1}(t))$, dan $\mathcal{R}A_m(\vec{A}_{m-1}(t))$
2	Kode Program Perbandingan Simulasi Numerik SPDB Nonlinier dengan SPDF $\mu_i = 1$ pada Populasi Komputer
3	Kode Program μ_1 , μ_2 , μ_3 , dan μ_4 Terhadap Dinamika Populasi Komputer