# PENERAPAN ALGORITMA RSA DAN *STREAM CIPHER* RABBIT PADA APLIKASI *CHATTING*


**SKRIPSI**

**Disusun Sebagai Salah Satu Syarat**
**Untuk Memperoleh Gelar Sarjana Komputer**
**pada Jurusan Ilmu Komputer / Informatika**

**Disusun oleh:**

**Riyan Winangsih**

**J2F 008 067**

**JURUSAN ILMU KOMPUTER / INFORMATIKA**
**FAKULTAS SAINS DAN MATEMATIKA**
**UNIVERSITAS DIPONEGORO**

**2015**

# HALAMAN PERNYATAAN KEASLIAN SKRIPSI

Saya yang bertanda tangan di bawah ini :

Nama : Riyan Winangsih

NIM : J2F008067

Judul : Penerapan Algoritma RSA dan *Stream Cipher* Rabbit pada Aplikasi *Chatting*

Dengan ini saya menyatakan bahwa dalam tugas akhir/skripsi ini tidak terdapat karya yang pernah diajukan untuk memperoleh gelar kesarjanaan di suatu Perguruan Tinggi, dan sepanjang pengetahuan saya juga tidak terdapat karya atau pendapat yang pernah ditulis atau diterbitkan oleh orang lain, kecuali yang secara tertulis diacu dalam naskah ini dan disebutkan di dalam daftar pustaka.

**Semarang, 20 Agustus 2015**


**Riyan Winangsih**
**J2F008067**

# HALAMAN PENGESAHAN

Judul : Penerapan Algoritma RSA dan *Stream Cipher* Rabbit pada Aplikasi *Chatting*

Nama : Riyan Winangsih

NIM : J2F008067

Telah diujikan pada sidang tugas akhir pada 11 Agustus 2015 dan dinyatakan lulus pada tanggal 20 Agustus 2015.

Semarang, 20 Agustus 2015

Mengetahui,

| Ketua Jurusan Ilmu Komputer/Informatika<br>FSM UNDIP, | Panitia Penguji Tugas Akhir<br>Ketua, |
|---|---|
| Nurdin Bahtiar, S.Si., MT.<br>NIP. 19790720 200312 1 002 | Aris Sugiharto, M.Kom<br>NIP. 19710811 199702 1 004 |

# HALAMAN PENGESAHAN

Judul : Penerapan Algoritma RSA dan *Stream Cipher* Rabbit pada Aplikasi *Chatting*

Nama : Riyan Winangsih

NIM : J2F008067

Telah diujikan pada sidang tugas akhir pada tanggal 11 Agustus 2015.

Semarang, 20 Agustus 2015

Menyetujui,

| Pembimbing I, | Pembimbing II, |
| --- | --- |
| Drs. Eko Adi Sarwoko, M.Kom | Priyo Sidik Sasongko, S,Si M.Kom |
| NIP. 19651107 199203 1 003 | NIP. 19700705 199702 1 001 |

# ABSTRAK

Layanan *instant messaging* atau *chatting* digunakan untuk menunjang komunikasi antar pengguna melalui media internet secara *real-time*. Salah satu manfaatnya adalah untuk menunjang komunikasi antara pengunjung dengan *administrator* suatu *website* sebagai *customer service*. Kebanyakan layanan *chatting* saat ini didesain bukan berdasarkan aspek keamanan sebagai pertimbangan utama, melainkan aspek skalabilitas untuk menunjang jumlah pengguna yang besar. Salah satu aspek keamanan dapat dipenuhi dengan mengamankan data yang ditransmisikan dari penyadapan menggunakan kriptografi. Algoritma RSA dapat memberikan keamanan data, namun proses enkripsi dan dekripsinya sangat lambat dan rumit. Algoritma RSA dapat digunakan untuk pendistribusian kunci pengguna ketika pertama kali menggunakan aplikasi, kemudian proses enkripsi dan dekripsi pesan menggunakan *stream cipher* Rabbit. Kunci pengguna diproses menjadi *pseudo-random keystream* oleh algoritma Rabbit. Kunci yang berbeda tiap *session* (iterasi) dihasilkan dari *sifat real valued chaotic maps* algoritma Rabbit yang memiliki sensitivitas terhadap perubahan kecil sehingga perulangan *maps* menghasilkan sesuatu yang terlihat acak. Dengan menggabungkan kedua metode di atas, data yang ditransmisikan pada aplikasi *chatting* sudah dalam bentuk terenkripsi sehingga dapat mencegah penyadap memahami informasi dari data yang dikirimkan. *Response time* untuk proses mengirim dan menerima data 3.33 % dari *response time* pendistribusian kunci. Sehingga aplikasi *chatting* yang dikembangkan sedikit lambat ketika pendistribusian kunci, namun proses mengirim dan menerima data tetap terjadi secara *real-time*.

Kata kunci : aplikasi *chatting*, *customer service*, algoritma RSA, *stream cipher* Rabbit

# ABSTRACT

Instant messaging or chat service supported real-time communications among all of connected users via internet. One of the benefits is to support communication between visitor and administrator of a website as a customer service. Nowadays, most of the chat services are not designed based on security aspect as the main consideration, except for scalability to support large number of users. One of security aspect can be fulfilled by securing transmitted data from eavesdropping use cryptography. RSA algorithm provides data security, but the encryption and decryption process was very slow and complex. RSA algorithm used for user key establishment at the first time using the application, and then encryption dan decryption process using Rabbit stream cipher. User key processed into pseudo-random keystream by Rabbit algorithm. Different key of each session (iteration) produced by the real valued chaotic maps habbit of Rabbit algorithm that had sensitify to small changes, so maps iteration produced something that looks random. By combined the two methods above, the data transmitted on the chat application was already in an encrypted form thus preventing eavesdroppers understand the information of the data being sent. Response time for sending and receiving data was 3.33% of the response time for key distribution. So the developed chatting application was slow when key distribution, but the process of sending and receiving data still occur in real-time.

Keywords : chat application, customer service, RSA algorithm, Rabbit stream cipher

# KATA PENGANTAR

Segala puji penulis ucapkan kehadirat Allah SWT yang telah melimpahkan rahmat dan hidayah-Nya sehingga penulis dapat menyusun tugas akhir yang berjudul "Penerapan Algoritma RSA dan *Stream Cipher* Rabbit pada Aplikasi *Chatting*" sehingga dapat memperoleh gelar sarjana strata satu Jurusan Ilmu Komputer / Informatika Fakultas Sains dan Matematika Universitas Diponegoro Semarang.

Dalam penyusunan tugas akhir ini, penulis mendapat bantuan dan dukungan dari banyak pihak. Atas peran sertanya dalam membantu dalam penyelesaian tugas akhir ini, penulis ingin mengucapkan terima kasih kepada :

1. Prof. Dr. Widowati, S.Si, M.Si selaku Dekan FSM UNDIP.
2. Nurdin Bahtiar, S.Si, M.T selaku Ketua Jurusan Ilmu Komputer / Informatika.
3. Drs. Eko Adi Sarwoko, M.Kom selaku dosen pembimbing I dan Priyo Sidik Sasongko, S.Si, M.Kom selaku dosen pembimbing II yang senantiasa membimbing, memberikan dukungan, semangat, serta masukan bagi penulis dalam menyelesaikan tugas akhir ini.
4. Indra Waspada, S.T, M.TI selaku Koordinator Tugas Akhir dan dosen wali yang memberikan arahan dalam bidang akademik, serta bapak / ibu dosen lainnya yang telah memberikan pelajaran yang sangat berharga kepada penulis.
5. Semua pihak yang telah membantu hingga selesainya tugas akhir ini, yang tidak dapat penulis sebutkan satu persatu.

Penulis menyadari masih banyak kekurangan dalam penyusunan laporan tugas akhir ini, untuk itu penulis mohon maaf dan mengharapkan saran serta kritik yang membangun dari pembaca. Semoga laporan tugas akhir ini dapat bermanfaat bagi pengembangan ilmu dan pengetahuan khususnya pada bidang informatika.

Semarang, Agustus 2015

Penulis

# DAFTAR ISI

Hal

# DAFTAR GAMBAR

Hal

# DAFTAR TABEL

Hal

# DAFTAR KODE

Hal

# BAB I
# PENDAHULUAN

Bab ini menyajikan latar belakang masalah, rumusan masalah, tujuan dan manfaat, ruang lingkup, dan sistematika penulisan tugas akhir mengenai Penerapan Algoritma RSA dan *Stream Cipher* Rabbit pada aplikasi *Chatting*.

## 1.1. Latar Belakang Masalah

Layanan *instant messaging* atau *chatting* digunakan untuk menunjang komunikasi antar pengguna melalui media internet secara *real-time*. Salah satu manfaatnya adalah untuk menunjang komunikasi antara pengunjung dengan *administrator* suatu *website* sebagai *customer service* melalui *live chatting*. Kebanyakan layanan *instant messaging* saat ini didesain bukan berdasarkan aspek keamanan sebagai pertimbangan utama, melainkan aspek skalabilitas untuk menunjang jumlah pengguna yang besar. Layanan *instant messaging* publik seperti *Yahoo Messenger*, *Windows Live Messenger* dan beberapa aplikasi *live chatting* kurang aman untuk digunakan karena data yang ditransmisikan dapat dibaca oleh penyadap. Aspek keamanan menjadi sangat penting, terutama jika informasi yang dipertukarkan bersifat sensitif dan rahasia (Karhendana, 2006).

Penyadapan informasi sulit untuk dideteksi. Namun, penyadapan dapat dicegah dengan mengamankan informasi menggunakan kriptografi. Kriptografi adalah ilmu penulisan rahasia dengan tujuan menyembunyikan arti dari pesan (Paar & Pelzl, 2010). Dalam prosesnya, kriptografi memerlukan algoritma dan kunci. Algoritma dan kunci digunakan untuk penyandian (enkripsi) dan untuk menerjemahkannya (dekripsi). Kriptografi dibagi menjadi kriptografi simetris dan asimetris berdasarkan jumlah kunci yang digunakan.

Kriptografi simetris menggunakan kunci yang sama untuk proses enkripsi dan dekripsi, sedangkan kriptografi asimetris menggunakan kunci yang berbeda. Kriptografi simetris memberikan keamanan pada pesan, namun memiliki masalah dalam pendistribusian kunci. Sedangkan kriptografi asimetris dapat memberikan keamanan pada pesan dan pendistribusian kunci, namun proses enkripsi dan dekripsinya sangat lambat dan rumit (Paar & Pelzl, 2010). Sehingga kriptografi

simetris dan asimetris dapat digunakan bersama untuk mendapatkan keamanan dan menjaga kecepatan pemrosesan.

Algoritma kriptografi yang pernah diusulkan untuk aplikasi *chatting* adalah *RSA (Rivest-Shamir-Adelman)* dan IDEA (*International Data Encryption Algorithm*) (Prasetyawan, 2008), AES (*Advanced Encrytion Standard*) (Kusumah, 2012), dan WAKE (*Word Auto Key Encryption*) (Maulana, 2012). Algoritma simetris yang pernah diusulkan dapat memberikan keamanan pada pesan, namun keamanannya tergantung pada kunci yang digunakan. Jika kunci yang dibangkitkan mengalami perulangan, maka algoritma tersebut dapat terpecahkan. Terdapat algoritma simetris yang dapat membangkitkan kunci yang berbeda setiap *session* (iterasi) yaitu *stream cipher* Rabbit.

Algoritma RSA adalah algoritma kriptografi asimetris yang kuncinya didapatkan dengan memfaktorkan bilangan-bilangan prima yang besar menjadi faktor prima (Caroline, 2011). Algoritma RSA mempunyai karakteristik algoritma kunci asimetris. Sehingga algoritma RSA dapat dimanfaatkan untuk pendistribusian kunci pengguna dalam aplikasi *chatting*. Proses enkripsi dan dekripsi pesan dapat menggunakan *stream cipher* Rabbit untuk mendukung keamanan dan kecepatan proses.

*Stream cipher* Rabbit melakukan proses enkripsi terhadap masing-masing bit pesan (*plaintext*) dengan *pseudo-random keystream* yang dihasilkan oleh algoritma Rabbit. Dari hasil pengujian serta analisis keamanan yang dilakukan oleh Cryptico, algoritma Rabbit terbukti kuat secara kriptografis dan resistan terhadap metode-metode kriptanalisis yang ada. Algoritma Rabbit memiliki sifat acak *real valued chaotic maps* yang memiliki sensitivitas terhadap perubahan kecil sehingga perulangan dari *maps* menghasilkan sesuatu yang terlihat acak (Adwitya, 2006).

Algoritma RSA dan *stream cipher* Rabbit digunakan untuk mengamankan pesan yang dikirimkan melalui aplikasi *chatting*. Algoritma RSA untuk pendistribusian kunci pengguna aplikasi *chatting* dan *stream cipher* Rabbit untuk proses enkripsi dan dekripsi pesan.

## 1.2. Rumusan Masalah

Berdasarkan uraian latar belakang masalah, dapat dirumuskan permasalahan yang dihadapi, yaitu bagaimana menerapkan algoritma RSA dan *stream cipher* Rabbit pada aplikasi *chatting*.

## 1.3. Tujuan dan Manfaat

Tujuan dari penelitian ini adalah untuk menghasilkan sebuah aplikasi *chatting* yang menerapkan algoritma RSA dan *stream cipher* Rabbit untuk mengamankan data yang ditransmisikan. Adapun manfaat yang diharapkan adalah informasi dari pesan yang ditukarkan antara dua pengguna aplikasi *chatting* dapat tersampaikan tanpa diketahui oleh penyadap.

## 1.4. Ruang Lingkup

Dalam penyusunan tugas akhir ini, diberikan ruang lingkup yang jelas agar pembahasan lebih terarah. Ruang lingkup penerapan algoritma RSA dan *stream cipher* Rabbit pada aplikasi *chatting* adalah :

1) Pengamanan diterapkan pada *live chatting* sebagai *customer service* antara pengujung *website* dengan *administrator website*.
2) Aplikasi *chatting* ini terdiri atas Aplikasi *Chat Client* dan Aplikasi *Chat Server* yang berbasis *web*. Aplikasi *Chat Client* dibedakan menjadi Aplikasi *Dashboard Client* dan Aplikasi *Widget Client*.
3) Aplikasi *Dashboard Client* digunakan oleh *administrator website* untuk melihat pesan yang dikirimkan pengunjung *website* dan memberikan pesan respon.
4) Aplikasi *Widget Client* digunakan oleh pengunjung *website* untuk mengirimkan pesan kepada *administrator website*. Aplikasi *Widget Client* ditampilkan setelah pengunjung *website* memilih *link* aplikasi *Widget Client* yang dipasang pada *website* yang dikunjungi.
5) Data yang diamankan berupa teks atau *string* dengan panjang maksimal 128 karakter.
6) Pertukaran kunci pengguna menggunakan algoritma RSA.
7) Pembentukan *keystream*, proses enkripsi, dan dekripsi menggunakan *stream cipher* Rabbit.
8) Bentuk implementasinya menggunakan Node.js dan basis data MongoDB.

9) Model proses yang digunakan adalah *Unified Process*.

## 1.5. Sistematika Penulisan

Sistematika yang digunakan dalam penulisan tugas akhir ini adalah :

BAB I : Merupakan pendahuluan yang berisi latar belakang, rumusan masalah, tujuan dan manfaat, ruang lingkup serta sistematika penulisan.

BAB II : Merupakan teori-teori penunjang yang berisi tentang kriptografi, kriptografi asimetris, algoritma RSA, algoritma Rabbit, *unified process*, *unified modelling language*, Node.js, MongoDB, dan *Local Storage*.

BAB III : Merupakan proses pengembangan perangkat lunak pada tahap kebutuhan, analisis dan perancangan, dengan hasilnya berupa desain dan perancangan perangkat lunak yang dikembangkan.

BAB IV : Membahas hasil pengembangan perangkat lunak pada tahap implementasi dan menerangkan rincian pengujian sistem.

BAB V : Merupakan penutup yang berisi kesimpulan berkaitan dengan perangkat lunak yang dikembangkan dan saran-saran untuk pembuatan perangkat lunak lebih lanjut.