# PENGGUNAAN ALGORITMA KRIPTOGRAFI ONE TIME PAD UNTUK PENYANDIAN DATA ALPHANUMERIK (STUDI KASUS PADA E-MAIL)

# THE USING OF ONE TIME PAD CRYPTOGRAPHICS ALGORITHM FOR ALPHANUMERIC DATA ENCODING (STUDY CASE BY E-MAIL)

**Palupi Ambarwati[1], Eddy Muntina Dharma[2], M. Zuliansya[3]**

[1]Teknik Informatika, Fakultas Teknik Informatika, Universitas Telkom

**Abstrak**

**Kerahasiaan data adalah hal yang penting dalam komunikasi data. Ada beberapa algoritma enkripsi yang biasa digunakan seperti, DES, Triple DES, Blowfish, IDEA, dsb. Algoritma-algoritma tersebut begitu rumit dan sulit dimengerti, memang itu alasannya, 'tampilan keamanan', semakin sulit suatu algoritma dimengerti, maka semakin aman. Namun, bagi para pemakai, mereka tidak memikirkan seberapa sulit algoritmanya, yang penting data mereka aman. Ada dua syarat keamanan suatu sistem enkripsi, yaitu true random bits dan key space yang sangat besar untuk algoritma enkripsi tersebut. Jika dua syarat tersebut dipenuhi, tidak masalah seberapa kompleks algoritma enkripsinya. Bahkan semakin sederhana semakin baik, karena semakin sederhana, maka semakin sedikit proses komputasinya, dan semakin sedikit waktu yang dibutuhkan untuk mengeksekusinya Tugas Akhir ini membahas algoritma One Time Pad (OTP), yang terkenal sederhana dan 'unbreakable', pada data yang bertipe alphanumerik serta bagaimana kemungkinan pengulangan kunci simetrik yang digenerate. Algoritma OTP ini dipadukan dengan algoritma RSA dan Md5 untuk keamanan kunci dan tanda tangan digital. Sistem pada Tugas Akhir ini dibangun pada sistem operasi Windows Server 2003, mail server Kerio versi 5.5.0 dan tools pembantu lainnya, serta dengan bahasa pemrograman Java. Sistem e-mail OTP yang dipadukan dengan RSA dan MD5 ini menawarkan kemudahan dan keamanan dengan key yang tidak berulang pada ukuran message tertentu**

**Kata Kunci : OTP, kriptografi, kerahasiaan data, e-mail**

**Abstract**

**Data secrecy is an important thing in data communication. There is some encryption algorithms that usually use like DES, Triple DES, Blowfish, IDEA, etc. Those algorithms is so complicative dan hard to be understand, that is the reason, 'security appearance', more difficult to be understand, more save. But, on the user side, they do not care how difficult the algorithm that they use, they just care their data safety. There is two security recuirements in an encyption system, true random bits and very big key space for that ancryption algorithm. If both recuirement fulfilled, no matter how complex the encryption algorithm. Even the simplier is better, because simplier an algorithm result in fewer computation process, and fewer time to execute. This Final Project disscuss about One Time Pad (OTP) algorithm, which has been known simple and 'unbreakable', on the alphanumerik data and also how the possibility of the generate key repetition. This algorithm fused with RSA algorithm and MD5 algorithm for key security and digital signature. The final project system is build on Windows Server 2003 operating system, Kerio Mail server version 5.5.0, and other supporting tool, and also with Java programming language. One Time Pad e-mail system which fused with RSA and MD5 offerring easy and secure mail system with 'one time' key on certain message sizes.**

**Keywords : OTP, cryptography, data secrecy, e-mail**

# BAB I
# PENDAHULUAN

## 1.1. Latar Belakang

Kerahasiaan dan keamanan saat melakukan pertukaran data adalah hal yang penting dalam komunikasi data, baik itu untuk tujuan keamanan bersama, maupun untuk privasi individu. Mereka yang menginginkan agar datanya tidak diketahui oleh pihak-pihak yang tidak berkepentingan akan berusaha menyiasati cara mengamankan informasi yang dikomunikasikannya. Perlindungan terhadap kerahasiaan data pun semakin meningkat. Salah satu caranya yakni dengan penyandian data atau enkripsi.

Enkripsi merupakan suatu proses pengubahan pesan asal menjadi karakter yang tidak dapat dibaca[9]. Ada beberapa algoritma kriptografi yang biasa digunakan antara lain DES, Triple DES, Blowfish, IDEA, dsb. Algoritma-algoritma tersebut begitu rumit dan sulit dimengerti, hal ini memang merupakan alasannya, semakin sulit suatu algoritma dimengerti, maka semakin aman. Namun, disisi pengguna, mereka mungkin tidak akan mau ambil pusing dengan apa yang ada dibalik aplikasi mereka, yang mereka inginkan adalah bagaimana aplikasi tersebut dapat memenuhi keinginan mereka, yakni menjaga kerahasiaan data.

Ada dua syarat untuk mengimplementasikan suatu sistem enkripsi yang aman[6]. Pertama, *true random bits* (benar-benar hanya dihasilkan sekali) dan kedua, *key space* yang sangat besar untuk algoritma enkripsi tersebut. Jika dua syarat tersebut dipenuhi, tidak masalah seberapa kompleks algoritma enkripsinya. Bahkan semakin sederhana semakin baik, karena semakin sederhana suatu algoritma, maka akan semakin sedikit proses komputasinya dan semakin sedikit waktu yang dibutuhkan untuk mengeksekusinya. Kesederhanaan itulah yang ditawarkan oleh algoritma One Time Pad (OTP), algoritma kriptografi yang secara teori dan praktek aman dari tangan-tangan penyadap[3], dan juga dikenal dengan sebutan '*unbreakable algorithm*'[10].

Skema enkripsi yang akan dibangun pada Tugas Akhir ini menerapkan teknik pada kriptografi modern, dimana pada kriptografi modern yang dirahasiakan adalah kunci (key). Sehingga keamanan enkripsi tergantung pada key dan tidak tergantung apakah algoritmanya diketahui orang atau tidak[9]. Oleh karenanya, pada Tugas Akhir ini algoritma OTP dipadukan dengan algoritma kriptografi RSA, sebagai algoritma 'standar' pembuatan kunci publik, dan MD5, algoritma 'standar' untuk *signature*.

## 1.2. Rumusan Masalah

Semakin sulit suatu algoritma, semakin banyak proses komputasi yang diperlukan sehingga semakin banyak waktu yang dibutuhkan untuk mengeksekusinya. Sedangkan *user* tidak akan memikirkan seberapa sulit algoritma yang digunakan, yang penting kerahasiaan data mereka terjamin. Oleh karena itu, Tugas Akhir ini mencoba menggunakan algoritma kriptografi One Time Pad (OTP), suatu algoritma yang bisa dibilang sederhana namun handal.

## 1.3. Tujuan Pembuatan

Tujuan pembuatan Tugas Akhir ini yakni agar:

- Algoritma OTP ini dapat diketahui dan dianalisa sifat-sifatnya (kelebihan dan kekurangan) baik dalam aspek '*one time*' key dan kehandalan.
- Algoritma OTP ini dapat dipadukan dengan algoritma RSA dan MD5 sehingga dapat menjadi suatu alternatif sistem enkripsi yang lebih baik daripada sistem enkripsi yang hanya menggunakan algoritma OTP saja.
- Sistem ini dapat menjadi salah satu alternatif untuk penyandian data pada e-mail dengan kebutuhan proses dan waktu yang relatif singkat.

## 1.4. Batasan Masalah

Ruang lingkup permasalahan pada Tugas Akhir ini adalah:

- Data yang digunakan berupa data alphanumerik.
- Mail server yang digunakan adalah Kerio Mail Server versi 5.5.0.
- Penyandian data dilakukan di sisi web server.
- Pertukaran data dilakukan pada jaringan komputer lokal.
- Tidak membahas keamanan trafik pada jaringan, misalnya *cell loss*.
- Panjang publik key dan private key untuk algoritma RSA 1024 bit (128 byte).
- Modul RSA dan MD5 menggunakan Java Cryptography Extension (JCE) yang terintegrasi pada Java Software Development Kit 1.5.03.
- Mail Client dibangun menggunakan Java Mail API versi 1.3.3_01 dan JavaBean Activation Framework (JAF)1.0.2.

## 1.5. Metodologi Pembahasan

Metode yang akan digunakan dalam menyelesaikan Tugas Akhir ini adalah:

- Studi literatur

  Mempelajari literatur-literatur yang berkaitan dengan perumusan dan pemecahan masalah
- Analisa masalah dan perancangan perangkat lunak

  Mempelajari masalah untuk menemukan faktor-faktor yang mungkin maupun yang tidak mungkin dalam pemecahannya
- Implementasi perangkat lunak

  Mengimplementasikan ke dalam bentuk perangkat lunak
- Pengujian dan kesimpulan

  Melakukan pemeriksaan dan melakukan uji coba perangkat lunak
- Penyusunan laporan

  Mendokumentasikan keseluruhan hasil studi serta hal-hal pendukung lain yang berkaitan selama studi berlangsung.

## 1.6. Sistematika Penulisan

Tugas Akhir ini disusun berdasarkan sistematika penulisan sebagai berikut:

**BAB I : Pendahuluan**

Berisi latar belakang, perumusan masalah, tujuan penelitian, batasan masalah, metodologi pembahasan, sistematika pembahasan, rencana penelitian, dan daftar pustaka.

**BAB II : Landasan Teori**

Berisi penjelasan singkat mengenai teori-teori yang digunakan untuk pembuatan Tugas Akhir ini.

**BAB III : Analisa dan Desain Sistem**

Berisi pembahasan tentang analisa masalah dan desain sistem yang akan dibangun dalam mengimplementasikan hasil analisa.

**BAB IV : Implementasi dan Pengujian**

Berisi penjelaskan implementasi sistem serta hasil pengujian setelah dievaluasi.

**BAB V : Penutup**

Berisi kesimpulan dari seluruh rangkaian pembuatan Tugas Akhir serta saran untuk pengembangan selanjutnya.

# BAB V
# KESIMPULAN DAN SARAN

## 5.1. Kesimpulan

Berdasarkan implementasi dan analisis data uji yang telah dilakukan, maka dapat ditarik beberapa kesimpulan sebagai berikut:

- Sistem ini mampu menghasilkan key sekali yang tidak berulang dengan kondisi tertentu (jumlah key antara 1 sampai 188 dengan panjang key $2^2$ sampai $2^{15}$).
- Generator key yang digunakan untuk pengujian ini menghasilkan key yang acak, karena tidak terdapat pengulangan karakter pada key hasil generate.
- Karena algoritma OTP memiliki karakteristik besar key sama dengan besar *message*, maka sistem ini memiliki keterbatasan akan ukuran *message*.
- Dalam penggunaannya sistem ini merupakan salah satu alternatif yang menawarkan bagi user yang menginginkan kemudahan dan keamanan dalam mengirim e-mail.
- E-mail yang dikirim dan dengan sengaja dienkrip menggunakan O-mail, atau dengan kata lain memilihi opsi pengiriman ‘Send With Encrypt’ masih dalam keadaan terenkripsi di jaringan.
- Mail client lain dapat menerima dan membuka e-mail yang dikirim dari O-mail, namun tidak dapat membaca pesan yang dienkrip. Hanya pesan yang tidak dienkrip saja yang bisa dibaca.
- Sistem OTP yang dipadukan dengan RSA+MD5 sebagai digital signature dan RSA untuk pengamanan kunci merupakan suatu sistem aman.

## 5.2. Saran

- Untuk password login, sebaiknya dipilih sesuatu yang unik, mudah diingat dan bersifat pribadi. Hindari password yang berasal dari literatur yang bersifat umum karena akan memiliki kemungkinan yang besar untuk ditebak.
- Untuk kedepannya, diharapkan Tugas Akhir ini dapat dikembangkan dan digunakan dan diterapkan pada bidang-bidang kehidupan yang lain.

# DAFTAR PUSTAKA


[1] Chambers, Josyanne and Carl Morgan. September, 2003. *COMS W4995 Introduction to Cryptography. Lecture 3: Introduction to Computational Security*.

[2] *Cryptography*. http://en.wikipedia.org/wiki/Cryptography

[3] Eisenman, Shane. September, 2003. *COMS W4995 Introduction to Cryptography, Lecture 2: Perfect Secrecy*.

[4] Faisal. April 2003. *Memahami Enkripsi*. Faisal WebSite, Fisika ITB.

[5] FAQ. 2005. Vadium Technology, Inc. http://www.ranum.com/security/computer_security/papers/otp-faq/

[6] http://www.topsecretcrypto.com

[7] Jack Febrian dan Farida Andayani. April 2002. *Kamus Komputer dan Istilah Teknologi Informasi*. Bandung: Informatika.

[8] Kerio http://www.kerio.com

[9] Kurniawan, Yusuf. April 2004. *Kriptografi Keamanan Internet dan Jaringan Telekomunikasi*. Bandung: Penerbit Informatika.

[10] Medeiros, Breno de. 2004. *Confidential Channels, Using encryption for network security*. Florida State University.

[11] One-Time Pad http://en.wikipedia.org/wiki/One-Time Pad

[12] One Time Pad Generator http://www.fourmilab.ch/onetime/otpjs.html

[13] Rubin, Frank. 1997. *One-Time Pad Cryptography*.

[14] Scheineier, Bruce. 1996. *Applied Cryptography Protocols, Algorithms, And Source Code In C*. Second Edition. USA: John Wiley & Sons, Inc.

[15] Wagner, Neal R. 2002. *The Laws of Cryptography: Perfect Cryptography: The One-Time Pad*.