



**PENGAMANAN AUTENTIKASI SISTEM INFORMASI  
AKADEMIK MENGGUNAKAN KRIPTOGRAFI  
*ONE TIME PAD***

**SKRIPSI**

**IQBAL ADHI SURACHMAN**

**1410511007**

**UNIVERSITAS PEMBANGUNAN NASIONAL “VETERAN” JAKARTA  
FAKULTAS ILMU KOMPUTER  
PROGRAM STUDI INFORMATIKA  
2019**



**PENGAMANAN AUTENTIKASI SISTEM INFORMASI  
AKADEMIK MENGGUNAKAN KRIPTOGRAFI  
*ONE TIME PAD***

**SKRIPSI**

**Diajukan Sebagai Salah Satu Syarat Untuk Memperoleh Gelar  
Sarjana Komputer**

**IQBAL ADHI SURACHMAN**

**1410511007**

**UNIVERSITAS PEMBANGUNAN NASIONAL “VETERAN” JAKARTA  
FAKULTAS ILMU KOMPUTER  
PROGRAM STUDI INFORMATIKA**

**2019**

## PERNYATAAN ORISINALITAS

Skripsi ini adalah hasil karya sendiri, dan semua sumber yang dikutip maupun yang dirujuk telah saya nyatakan dengan benar.

Nama : Iqbal Adhi Surachman

NIM : 1410511007

Tanggal : 21 Januari 2019

Bilamana di kemudian hari ditemukan ketidaksesuaian dengan pernyataan saya ini, maka saya bersedia dituntut dan diproses sesuai dengan ketentuan yang berlaku.

Jakarta, 21 Januari 2019

Yang Menyatakan,

  
  
(Iqbal Adhi Surachman)

## **PERNYATAAN PERSETUJUAN PUBLIKASI SKRIPSI UNTUK KEPENTINGAN AKADEMIS**

---

Sebagai civitas akademik Universitas Pembangunan Nasional “Veteran” Jakarta, saya yang bertanda tangan di bawah ini :

Nama : Iqbal Adhi Surachman

NIM : 1410511007

Fakultas : Ilmu Komputer

Program Studi : Informatika

Demi pengembangan ilmu pengetahuan, menyetujui untuk memberikan kepada Universitas Pembangunan Nasional “Veteran” Jakarta Hak Bebas Royalti Non eksklusif (*Non-exclusive Royalty Free Right*) atas karya ilmiah saya yang berjudul :

**Pengamanan Autentikasi Sistem Informasi Akademik Menggunakan  
Kriptografi *One Time Pad***

Beserta perangkat yang ada (jika diperlukan). Dengan Hak Bebas Royalti ini Universitas Pembangunan Nasional “Veteran” Jakarta berhak menyimpan, mengalih media/formatkan, mengelola dalam bentuk pangkalan data (*database*), merawat, dan mempublikasikan Skripsi saya selama tetap mencantumkan nama saya sebagai penulis/pencipta dan sebagai pemilik Hak Cipta.

Demikian pernyataan ini saya buat dengan sebenarnya.

Dibuat di : Jakarta

Pada tanggal : 21 Januari 2019

Yang menyatakan,



(Iqbal Adhi Surachman)

## PENGESAHAN

Dengan ini dinyatakan bahwa Tugas Akhir berikut:

Nama : Iqbal Adhi Surachman

NIM : 1410511007

Program Studi : Informatika

Judul Tugas Akhir : Pengamanan Autentikasi Sistem Informasi Akademik  
Menggunakan Kriptografi One Time Pad.

Telah berhasil dipertahankan di hadapan Tim Penguji dan diterima sebagai bagian persyaratan yang diperlukan untuk memperoleh gelar Sarjana Komputer pada Program Studi Informatika, Fakultas Ilmu Komputer, Universitas Pembangunan Nasional “Veteran” Jakarta.

Vini Indriasari, S.T., M.Sc., Ph.D.

Penguji 1

Ichsan Mardani, S.Kom., M.Sc.

Penguji 2

Henki Bayu Seta., S.Kom., M.T.I.

Pembimbing 1

Bayu Hananto, S.Kom., M.Kom.

Pembimbing 2



Dr. Ermatita, M.Kom.

Dekan

Anita Muliawati, S.Kom., M.T.I.

Ketua Program Studi

Ditetapkan di : Jakarta

Tanggal Ujian : 14 Januari 2019

**PENGAMANAN AUTENTIKASI SISTEM INFORMASI  
AKADEMIK MENGGUNAKAN KRIPTOGRAFI  
*ONE TIME PAD***

**Iqbal Adhi Surachman**

**Abstrak**

Sistem informasi akademik dibangun untuk memberikan kemudahan kepada para pelajar dalam kegiatan administrasi pendidikannya secara *online*. Setiap sistem informasi akademik pasti telah mempunyai sistem pengamanannya sendiri, namun dalam pengamanannya pasti mempunyai suatu kelemahan. Salah satu masalah yang dihadapi dalam keamanan pada sistem informasi akademik adalah bagaimana sistem dapat memastikan bahwa *user* yang mengakses data maupun informasi pada sistem tersebut adalah *user* yang benar-benar memiliki wewenang. Penelitian ini dilakukan untuk menambahkan keamanan pada sistem informasi akademik yaitu dengan kriptografi *one time pad* ini proses *login* akan di autentikasi terlebih dahulu dengan mengirimkan suatu *key* ke pemilik akun SIAKAD dengan begitu pemilik akan melewati 2 tahapan dalam login ke sistem informasi akademik.

**Kata Kunci** : Autentikasi, Sistem Informasi Akademik, Kriptografi, *One Time Pad*.

# **SECURITY AUTHENTICATION OF ACADEMIC INFORMATION SYSTEM USING CRYPTOGRAPHY ONE TIME PAD**

**Iqbal Adhi Surachman**

## **Abstract**

Academic information system is built to provide convenience to the students in their educational administration activities online. Each academic information system must have its own security system, but in its security must have a weakness. One of the problems encountered in the security of academic information systems is how the system can ensure that users who access data or information on the system are truly authorized users. This research is done to add security to academic information system that is with cryptography one time pad this process log in will in first authentication by sending a key to account owner SIAKAD so owner will pass 2 stages in login to academic information system.

**Keywords:** Authentication, Academic Information System, Cryptography, One Time Pad.

## KATA PENGANTAR

Puji dan syukur penulis panjatkan kehadirat Allah SWT atas segala karunia-Nya sehingga penelitian ini berhasil diselesaikan. Penelitian ini dilaksanakan sejak bulan Juli 2018 hingga Desember 2018 dengan Judul **Pengamanan Autentikasi Sistem Informasi Akademik Menggunakan Kriptografi *One Time Pad***. Dalam penulisan skripsi ini tentunya tidak lepas dari bantuan pembimbing, petunjuk dan dorongan baik secara materil maupun secara moril dari berbagai pihak. Dalam kesempatan ini, penulis bermaksud menyampaikan rasa terima kasih kepada :

1. Bapak Sarno dan Ibu Dwi Astuty sebagai kedua orang tua yang telah memberikan dukungan baik moril maupun materil, dan yang tentunya tidak pernah berhenti mendoakan kesuksesan dan kelancaran dalam penyusunan skripsi ini.
2. Ibu Dr. Ermatita, M.Kom. selaku Dekan Fakultas Ilmu Komputer Universitas Pembangunan Nasional “Veteran” Jakarta.
3. Ibu Anita Muliawati, S.Kom., M.T.I. sebagai Kepala Program Studi Informatika.
4. Bapak Henki Bayu Seta, S.Kom., M.TI. selaku Dosen Pembimbing I yang telah memberikan banyak bimbingan dan saran yang sangat bermanfaat.
5. Bapak Bayu Hananto, S.Kom., M.Kom. selaku Dosen Pembimbing II yang telah memberikan banyak bimbingan dan saran yang sangat bermanfaat.
6. Teman-teman BEMF-IK dan SMF-IK.
7. Teman-teman seperjuangan Program Studi S1 Informatika 2014.
8. dan dan teman-teman lainnya yang tentunya tidak dapat disebutkan satu persatu.



Penulis menyadari bahwa skripsi ini masih jauh dari sempurna, untuk itu penulis mengharapkan saran dan kritik yang bersifat membangun dalam menyempurnakan penelitian ini. Akhir kata dari penulis, semoga skripsi ini dapat bermanfaat bagi para pembaca khususnya mahasiswa Fakultas Ilmu Komputer Universitas Pembangunan Nasional "Veteran" Jakarta.

Jakarta, 21 Januari 2019



Penulis

## DAFTAR ISI

HALAMAN JUDUL .....	i
PERNYATAAN ORISINALITAS.....	ii
PERNYATAAN PERSETUJUAN PUBLIKASI .....	iii
LEMBAR PERSETUJUAN .....	iv
ABSTRAK.....	v
<i>ABSTRACT</i> .....	vi
KATA PENGANTAR .....	vii
DAFTAR ISI .....	ix
DAFTAR TABEL .....	xii
DAFTAR GAMBAR .....	xiii
DAFTAR LAMPIRAN .....	xv
BAB 1 PENDAHULUAN	
1.1 Latar Belakang.....	1
1.2 Rumusan Masalah .....	3
1.3 Tujuan Penelitian .....	3
1.4 Manfaat Penelitian.....	3
1.5 Ruang Lingkup .....	4
1.6 Luaran Yang Diharapkan .....	4
1.7 Sistematika Penulisan .....	4
BAB 2 TINJAUAN PUSTAKA	
2.1 Konsep Dasar Sistem Informasi Akademik .....	6
2.1.1 Pengertian Sistem .....	6
2.1.2 Pengertian Informasi.....	6
2.1.3 Pengertian Sistem Informasi Akademik.....	6
2.2 Kriptografi.....	7
2.2.1 Sejarah Kriptografi .....	7
2.2.2 Definisi Kriptografi .....	8
2.2.3 Tujuan Kriptografi.....	8

2.2.4 Istilah Dalam Kriptografi .....	9
2.2.5 Jenis-Jenis Kriptografi .....	10
2.3 <i>One Time Pad</i> .....	11
2.3.1 Sejarah <i>One Time Pad</i> .....	11
2.3.2 Definisi <i>One Time Pad</i> .....	13
2.3.3 Proses Kerja <i>One Time Pad</i> .....	14
2.4 Konsep Dasar <i>Web</i> .....	18
2.4.1 Bahasa Pemrograman .....	18
2.4.1.1 PHP ( <i>Hypertext Preprocessing</i> ) .....	18
2.4.1.2 HTML ( <i>Hypertext Markup Language</i> ) .....	18
2.4.2 Basis Data .....	19
2.5 Penelitian Sejenis .....	19
<b>BAB 3 METODOLOGI PENELITIAN</b>	
3.1 Kerangka Berpikir.....	24
3.2 Tahapan Penelitian .....	25
3.3 Alat dan Bahan Penelitian.....	26
3.4 Jadwal Penelitian.....	27
<b>BAB 4 HASIL DAN PEMBAHASAN</b>	
4.1 <i>Flowchart</i> Sistem Informasi Akademik .....	28
4.2 Perancangan Aplikasi.....	31
4.2.1 <i>Use Case Diagram</i> .....	32
4.2.1.1 <i>Use Case Diagram</i> Pelajar .....	32
4.2.1.1 <i>Use Case Diagram</i> Admin .....	35
4.2.2 <i>Activity Diagram</i> . .....	36
4.2.2.1 <i>Activity Diagram</i> Pelajar .....	36
4.2.2.2 <i>Activity Diagram</i> Admin .....	40
4.2.3 <i>Sequence Diagram</i> .....	40
4.2.3.1 <i>Sequence Diagram</i> Pelajar .....	41
4.2.3.2 <i>Sequence Diagram</i> Admin .....	43
4.3 Perancangan <i>User Interface</i> .....	44
4.4 <i>Layout User Interface</i> .....	47
4.5 Implementasi Aplikasi.....	50

4.5.1 Aplikasi SIAKAD Dengan <i>One Time Pad</i> .....	50
4.5.2 Implementasi Algoritma <i>One Time Pad</i> .....	54
4.5.3 Pengujian Aplikasi .....	56
BAB 5 PENUTUP	
5.1 Kesimpulan.....	68
5.2 Saran.....	69
DAFTAR PUSTAKA	
RIWAYAT HIDUP	
LAMPIRAN	

## DAFTAR TABEL

Table 2.1 <i>Mod 26</i> .....	15
Table 2.2 Penelitian Sejenis .....	22
Table 3.1 Jadwal Penelitian .....	27
Table 4.1 <i>Use Case Diagram</i> Pelajar Registrasi <i>One Time Pad</i> .....	32
Table 4.2 <i>Use Case Diagram</i> Pelajar Autentikasi <i>One Time Pad</i> .....	33
Table 4.3 <i>Use Case Diagram</i> Pelajar Validasi Plainteks .....	34
Table 4.4 <i>Use Case Diagram</i> Pelajar Login SIAKAD .....	34
Table 4.5 <i>Use Case Diagram</i> Admin Aktivasi Akun <i>One Time Pad</i> .....	35
Table 4.6 <i>Mod 26</i> .....	55
Table 4.7 Kesesuaian Proses Enkripsi .....	56
Table 4.8 Hasil Ketepatan Data .....	57

## DAFTAR GAMBAR

Gambar 2.1 <i>Scytale</i> .....	7
Gambar 2.2 Mesin Enigma .....	8
Gambar 2.3 Hubungan Kriptologi, Kriptografi, dan Kriptanalisis.....	10
Gambar 2.4 Skema Kriptografi Simetris .....	10
Gambar 2.5 Skema Kriptografi Asimetris .....	11
Gambar 3.1 Kerangka Berpikir .....	24
Gambar 4.1 <i>Flowchart</i> Autentikasi <i>Login One Time Pad</i> .....	28
Gambar 4.2 <i>Use Case</i> Diagram Pelajar .....	32
Gambar 4.3 <i>Use Case</i> Diagram Admin .....	35
Gambar 4.4 <i>Activity</i> Diagram Registrasi <i>One Time Pad</i> .....	36
Gambar 4.5 <i>Activity</i> Diagram Autentikasi <i>One Time Pad</i> .....	37
Gambar 4.6 <i>Activity</i> Diagram Validasi Plainteks .....	38
Gambar 4.7 <i>Activity</i> Diagram Sistem Informasi Akademik .....	39
Gambar 4.8 <i>Activity</i> Diagram Aktivasi Akun <i>One Time Pad</i> .....	40
Gambar 4.9 <i>Sequence</i> Diagram Registrasi <i>One Time Pad</i> .....	41
Gambar 4.10 <i>Sequence</i> Diagram Autentikasi <i>One Time Pad</i> .....	41
Gambar 4.11 <i>Sequence</i> Diagram Validasi Plainteks .....	42
Gambar 4.12 <i>Sequence</i> Diagram Sistem Informasi Akademik .....	42
Gambar 4.13 <i>Sequence</i> Diagram Aktifasi Akun <i>One Time Pad</i> .....	43
Gambar 4.14 Rancangan Tampilan Halaman Autentikasi <i>One Time Pad</i> .....	44
Gambar 4.15 Rancangan Tampilan Halaman Registrasi <i>One Time Pad</i> .....	45
Gambar 4.16 Rancangan Tampilan Halaman Validasi Plainteks .....	45
Gambar 4.17 Rancangan Tampilan Halaman Utama .....	46
Gambar 4.18 Rancangan Tampilan Halaman Siswa .....	46
Gambar 4.19 Tampilan Halaman Autentikasi <i>One Time Pad</i> .....	47
Gambar 4.20 Tampilan Halaman Registrasi <i>One Time Pad</i> .....	48
Gambar 4.21 Tampilan Halaman Validasi Plainteks .....	48

Gambar 4.22 Tampilan Halaman Utama .....	49
Gambar 4.23 Tampilan Halaman Siswa .....	49
Gambar 4.24 Halaman Awal Sistem Informasi Akademik.....	50
Gambar 4.25 Pelajar Registrasi Akun.....	51
Gambar 4.26 Pelajar Mendapatkan Cipherteks.....	51
Gambar 4.27 Tampilan Gagal Registrasi .....	52
Gambar 4.28 Admin Mengaktifkan Akun <i>One Time Pad</i> Pelajar .....	52
Gambar 4.29 Pelajar <i>Login One Time Pad</i> .....	52
Gambar 4.30 Tampilan Gagal Login .....	53
Gambar 4.31 Pelajar <i>Input Challenge</i> .....	53
Gambar 4.32 Pelajar <i>Login SIAKAD</i> .....	54
Gambar 4.33 Pelajar Telah Masuk Ke SIAKAD .....	54
Gambar 4.34 Tampilan Aplikasi Wireshark .....	59
Gambar 4.35 Tampilan Traffic Jaringan .....	60
Gambar 4.36 Tampilan Login SIAKAD .....	60
Gambar 4.37 Tampilan Halaman Pelajar Setelah Login .....	61
Gambar 4.38 Traffic Jaringan Yang Menggunakan Website .....	61
Gambar 4.39 Wireshark Melihat Data Login .....	62
Gambar 4.40 Tampilan Aplikasi Wireshark .....	62
Gambar 4.41 Tampilan Traffic Jaringan .....	63
Gambar 4.42 Pelajar Login One Time Pad .....	63
Gambar 4.43 Pelajar Input Challenge .....	64
Gambar 4.44 Pelajar Login SIAKAD .....	64
Gambar 4.45 Pelajar Berhasil Login SIAKAD .....	65
Gambar 4.46 Traffic Jaringan .....	65
Gambar 4.47 Wireshark Merekam Data Login OTP .....	66
Gambar 4.48 Wireshark Merekam Data Challenge .....	66
Gambar 4.49 Wireshark Merekam Data Login SIAKAD .....	67

## **DAFTAR LAMPIRAN**

Lampiran 1. Data Pelajar Yang Memiliki Akun One Time Pad

Lampiran 2. Data Pelajar Yang Memiliki Akun Sistem Informasi Akademik

Lampiran 3. Laporan Hasil Pengujian