

**IMPLEMENTASI TWO FACTOR AUTHENTICATION DAN**

**ALGORITMA RSA SEBAGAI METODE AUTENTIKASI**

**LOGIN PADA SI-ABKA (SISTEM AMAL BAKTI**

**KEMENTERIAN AGAMA)**

**SKRIPSI**

oleh

**Ahmad Choirul Mustaqim**

**NIM 152410101155**

**PROGRAM STUDI SISTEM INFORMASI**

**FAKULTAS ILMU KOMPUTER**

**UNIVERSITAS JEMBER**

**2019**



**IMPLEMENTASI TWO FACTOR AUTHENTICATION DAN**

**ALGORITMA RSA SEBAGAI METODE AUTENTIKASI**

**LOGIN PADA SI-ABKA (SISTEM AMAL BAKTI**

**KEMENTERIAN AGAMA)**

**SKRIPSI**

diajukan guna melengkapi tugas akhir dan memenuhi salah satu syarat untuk menyelesaikan pendidikan sarjana (S1) Program Studi Sistem Informasi Universitas Jember dan mendapat gelar Sarjana Komputer

oleh

**Ahmad Choirul Mustaqim**

**NIM 152410101155**

**PROGRAM STUDI SISTEM INFORMASI**

**FAKULTAS ILMU KOMPUTER**

**UNIVERSITAS JEMBER**

**2019**

# PERSEMBAHAN

**MOTTO**

# PERNYATAAN

Saya yang bertanda tangan di bawah ini:

Nama : Ahmad Choirul Mustaqim

NIM : 152410101155

Menyatakan dengan sesungguhnya bahwa karya ilmiah yang berjudul “Implementasi Two Factor Authentication Dan Algoritma Rsa Sebagai Metode Autentikasi Login Pada Si-Abka (Sistem Amal Bakti Kementerian Agama)”adalah benar-benar hasil karya saya sendiri, kecuali jika ada pengutipan substansi disebutkan sumbernya, belum pernah diajukan pada instansi manapun, dan bukti karya jiplakan. Saya bertanggung jawab atas keabsahan dan kebenaran isinya sesuai dengan sikap ilmiah yang harus dijunjung tinggi.

Demikian pernyataan ini saya buat dengan sebenarnya, tanpa adanya tekanan dan paksaan dari pihak manapun serta bersedia mendapat sanksi akademik jika dikemudian hari pernyataan ini tidak benar.

Jember, 20 Mei 2019

Yang menyatakan,

Ahmad Choirul Mustaqim

NIM 152410101155

**SKRIPSI**

**Implementasi Two Factor Authentication Dan Algoritma Rsa**

**Sebagai Metode Autentikasi Login Pada Si-Abka**

**(Sistem Amal Bakti Kementerian Agama)**

oleh

**Ahmad Choirul Mustaqim**

**NIM 152410101155**

Pembimbing

Pembimbing Utama : Dwiretno Istiyadi Swasono ST.,M.Kom.

Pembimbing Anggota : Yanuar Nurdiansyah ST,.M.Cs.

**PENGESAHAN PEMBIMBING**

Skripsi berjudul “Implementasi Two Factor Authentication Dan Algoritma Rsa Sebagai Metode Autentikasi Login Pada Si-Abka (Sistem Amal Bakti Kementerian Agama)”, telah diuji dan disahkan pada:

Hari tanggal : Jumat, 10 Mei 2019

Tempat : Program Studi Sistem Informasi Universitas Jember

Disetujui oleh:

|  |  |
| --- | --- |
| Pembimbing I,        Dwiretno Istiyadi Swasono ST.,M.Kom. NIP. 197803302003121003 | Pembimbing II,          Yanuar Nurdiansyah ST,.M.Cs. NIP. 19810123201021003 |

**PENGESAHAN PEMBIMBING**

Skripsi berjudul “Implementasi Two Factor Authentication Dan Algoritma Rsa Sebagai Metode Autentikasi Login Pada Si-Abka (Sistem Amal Bakti Kementerian Agama)”, telah diuji dan disahkan pada:

Hari tanggal : Jumat, 10 Mei 2019

Tempat : Program Studi Sistem Informasi Universitas Jember

Disetujui oleh:

|  |  |
| --- | --- |
| Pembimbing I,        Dwiretno Istiyadi Swasono ST.,M.Kom. NIP. 197803302003121003 | Pembimbing II,          Yanuar Nurdiansyah ST,.M.Cs. NIP. 19810123201021003 |

Mengesahkan

Dekan Fakultas Ilmu Komputer,

Prof. Saiful Bukhori,ST., M.Kom

NIP. 196811131994121001

RINGKASAN

PRAKATA

## DAFTAR ISI

HALAMAN JUDUL ........................................................................................ i

PERSEMBAHAN ............................................................................................ ii

PERNYATAAN ............................................................................................. iii

PENGESAHAN PEMBIMBING..................................................................... iv

PENGESAHAN ............................................................................................. vi

RINGAKASAN

PRAKATA

DAFTAR ISI

DAFTAR GAMBAR ....................................................................................... x

DAFTAR TABEL ............................................................................................ xiii

BAB 1 . PENDAHULUAN .............................................................................. 1

1.1 Latar Belakang ............................................................................ 1

1.2 Rumusan Masalah ....................................................................... 2

1.3 Tujuan ............................................................................. 3

1.4 Manfaat ........................................................................... 3

1.5 Batasan Masalah ......................................................................... 4

BAB 2 . TINJAUAN PUSTAKA ..................................................................... 7

2.1 Password dan username ......................................................... 7

2.1 Otentikasi ......................................................... 7

2.1 One time password ......................................................... 7

2.2 Time-based OTP ................................................................ 7

2.4 Algoritma RSA ........................................................................... 10

2.5 Penelitian terdahulu .................................................................... 11

BAB 3 . METODOLOGI PENELITIAN ......................................................... 24

|  |  |
| --- | --- |
|  | viii |
| 3.1 Jenis Penelitian ........................................................................... | 24 |
| 3.2 Alur Penelitian ............................................................................ | 24 |
| 3.3.1 Tahap Pengumpulan Data ............................................... | 25 |
| 3.3.2 Tahap Perancangan ......................................................... | 26 |
| 3.3.3 Tahap Implementasi ........................................................ | 27 |
| 3.3.4 Tahap Pengujian ............................................................. | 27 |
| 3.3.5 Tahap Penyusunan Skripsi .............................................. | 28 |
| BAB 4 . DESAIN DAN PERANCANGAN SISTEM ..................................... | 29 |
| 4.1 Analisis Kebutuhan Perangkat Lunak ......................................... | 29 |
| 4.2 Usecase Diagram ........................................................................ | 30 |
| 4.3 Skenario ...................................................................................... | 32 |
| 4.4 *Activity Diagram* ......................................................................... | 41 |
| 4.5 *Sequence Diagram* ...................................................................... | 54 |
| 4.6 *Class Diagram* ............................................................................ | 68 |
| 4.7 *Entity Relation Diagram* ............................................................. | 71 |
| 4.8 Implementasi Perancangan ......................................................... | 73 |
| 4.9 Pengujian .................................................................................... | 73 |
| BAB 5 . HASIL DAN PEMBAHASAN .......................................................... | 79 |
| 5.1 *E-Learning* Universitas Jember .................................................. | 79 |
| 5.2 Hasil Implementasi *Mobile* *Learning* ......................................... | 80 |
| 5.2.1 Tampilan *Splash Screen* .................................................. | 80 |
| 5.2.2 Tampilan *Login* ............................................................... | 81 |
| 5.2.3 Tampilan Halaman Utama .............................................. | 81 |
| 5.2.4 Tampilan Menu Utama ................................................... | 81 |
| 5.2.5 Tampilan Menu *Course* .................................................. | 82 |
| 5.2.6 Tampilan Aktivitas Perkuliahan ..................................... | 82 |
| 5.2.7 Tampilan Detail Aktivitas Perkuliahan ........................... | 83 |
| 5.2.8 Tampilan Menu *Broadcast* ............................................. | 84 |
| 5.2.9 Tampilan *Pop-Up Notification* ....................................... | 85 |
|  | ix |
| 5.2.10 Tampilan Detail Pemberitahuan ................................... | 85 |
| 5.3 Hasil Implementasi AES-128 pada *mobile* *learning* .................. | 86 |
| BAB 6 . PENUTUP .......................................................................................... | 94 |
| 6.1 Kesimpulan ................................................................................. | 94 |
| 6.2 Saran ........................................................................................... | 94 |
| DAFTAR PUSTAKA ...................................................................................... | 95 |
| LAMPIRAN ............................................................................................. | 97 |

DAFTAR GAMBAR

DAFTAR TABEL