

# **ANALISIS DAN IMPLEMENTASI ALGORITMA SHA-1 DAN SHA-3 PADA SISTEM AUTENTIKASI GARUDA TRAINING COST**

## **SKRIPSI**

Untuk memenuhi sebagian persyaratan  
memperoleh gelar Sarjana Komputer

Disusun oleh:  
Firlhi Kurniawan  
NIM: 135150200111102



PROGRAM STUDI TEKNIK INFORMATIKA  
JURUSAN TEKNIK INFORMATIKA  
FAKULTAS ILMU KOMPUTER  
UNIVERSITAS BRAWIJAYA  
MALANG  
2017

# PENGESAHAN

ANALISIS DAN IMPLEMENTASI ALGORITMA SHA-1 DAN  
SHA-3 PADA SISTEM AUTENTIKASI GARUDA TRAINING COST

SKRIPSI

Diajukan untuk memenuhi sebagian persyaratan  
memperoleh gelar Sarjana Komputer

Disusun Oleh :  
Firlhi Kurniawan  
NIM: 1351502001111102

Skripsi ini telah diuji dan dinyatakan lulus pada  
30 Mei 2017  
Telah diperiksa dan disetujui oleh:

Dosen Pembimbing I

Dosen Pembimbing II

Ari Kusyanti, S.T, M.Sc  
NIK: 201102 831228 2 001

Heru Nurwarsito, Ir., M.Kom  
NIP: 196504021990021001

Mengetahui  
Ketua Jurusan Teknik Informatika

Tri Astoto Kurniawan, S.T, M.T, Ph.D  
NIP: 19710518 200312 1 001

## PERNYATAAN ORISINALITAS

Saya menyatakan dengan sebenar-benarnya bahwa sepanjang pengetahuan saya, di dalam naskah skripsi ini tidak terdapat karya ilmiah yang pernah diajukan oleh orang lain untuk memperoleh gelar akademik di suatu perguruan tinggi, dan tidak terdapat karya atau pendapat yang pernah ditulis atau diterbitkan oleh orang lain, kecuali yang secara tertulis disitasi dalam naskah ini dan disebutkan dalam daftar pustaka.

Apabila ternyata didalam naskah skripsi ini dapat dibuktikan terdapat unsur-unsur plagiasi, saya bersedia skripsi ini digugurkan dan gelar akademik yang telah saya peroleh (sarjana) dibatalkan, serta diproses sesuai dengan peraturan perundang-undangan yang berlaku (UU No. 20 Tahun 2003, Pasal 25 ayat 2 dan Pasal 70).

Malang, 30 Mei 2017

Firhi Kurniawan

NIM: 135150200111102

## KATA PENGANTAR

Puji dan syukur atas kehadiran Allah SWT atas limpahan rahmat dan karunia-Nya, sehingga penulis dapat menyelesaikan skripsi dengan judul “Analisis dan Implementasi Algoritma SHA-1 dan SHA-3 pada Sistem Autentikasi Garuda Training Cost”. Skripsi ini disusun untuk memenuhi sebagian persyaratan memperoleh gelar Sarjana Komputer.

Untuk menyelesaikan penulisan skripsi ini, penulis tidak lepas dari bantuan dari berbagai pihak yang telah banyak memberikan bantuan dan dukungan. Dalam kesempatan ini penulis ingin mengucapkan terima kasih kepada :

1. Ibu Ari Kusyanti, S.T, M.Sc selaku dosen pembimbing yang telah dengan sabar, tekun, tulus, dan ikhlas meluangkan waktu, tenaga, serta pikiran dalam memberikan arahan, bimbingan, motivasi dan saran-saran yang sangat berharga kepada penulis selama menyusun skripsi.
2. Bapak Heru Nurwarsito, Ir., M.Kom selaku dosen pembimbing yang telah dengan sabar, tekun, tulus, dan ikhlas meluangkan waktu, tenaga, serta pikiran dalam memberikan arahan, bimbingan, motivasi dan saran-saran yang sangat berharga kepada penulis selama menyusun skripsi.
3. Orang tua, keluarga, teman-teman dan seluruh orang yang telah banyak membantu dan mendoakan untuk penyelesaian skripsi ini.

Penulis menyadari bahwa dalam penyusunan proposal ini masih banyak terdapat kekurangan, sehingga penulis mengharapkan adanya saran dan kritik yang bersifat membangun demi kesempurnaan skripsi ini. Semoga skripsi ini dapat bermanfaat bagi semua dan berguna untuk pengembangan ilmu pengetahuan.

Malang, 30 Mei 2017

Penulis

firlhik@gmail.com

## ABSTRAK

Garuda Training Cost merupakan suatu aplikasi *web* perhitungan biaya pelatihan untuk pilot dan pramugari yang dikembangkan di Garuda Indonesia Training Center. Aplikasi ini menggunakan algoritma *hash function* SHA-1 untuk mengamankan *password* pengguna yang tersimpan di *database*. Tetapi, dikarenakan telah ditemukannya kelemahan dan kolisi pada algoritma ini, maka algoritma ini sudah kurang aman lagi. Maka dari itu, pada penelitian ini, penulis akan menggantikan algoritma SHA-1 tersebut dengan algoritma penerusnya, yaitu SHA-3. Algoritma SHA-3 diimplementasikan pada proses *login*, proses perubahan *password* pengguna dan proses penambahan pengguna. Setelah itu dilakukan pengujian dan analisis untuk mengetahui kinerja dari kedua algoritma tersebut. Ada tiga jenis pengujian yang dilakukan, yang pertama yaitu pengujian *brute-force*, yang kedua pengujian *avalanche effect* dan yang terakhir pengujian waktu pemrosesan. Dari pengujian *brute-force*, algoritma SHA-3 jauh lebih baik dari algoritma SHA-1. Ditunjukkan dengan 30 kali percobaan *brute-force* untuk *password* dengan 10 karakter, *hash* yang dihasilkan SHA-1 membutuhkan waktu rata-rata 14 jam 53 menit dan 51 detik untuk menemukan *plaintext*-nya. Sedangkan *hash* yang dihasilkan SHA-3 membutuhkan waktu rata-rata 4 hari 13 jam 6 menit dan 6 detik untuk menemukan *plaintext*-nya. Untuk pengujian *avalanche effect*, algoritma SHA-1 mendapatkan persentase perubahan sebesar 100% sedangkan SHA-3 mendapatkan 95%. Sedangkan untuk pengujian waktu pemrosesan, SHA-1 lebih baik karena kompleksitas algoritma SHA-3 yang lebih tinggi. Walaupun dua dari tiga pengujian tersebut SHA-1 lebih unggul, bukan berarti SHA-3 tidak lebih baik. Persentase minimum *avalanche effect* untuk sebuah algoritma agar dapat dikatakan baik adalah lebih dari 50%. Sedangkan waktu pemrosesan tersebut masih dalam satuan *millisecond*, sehingga pengguna tidak merasakan dampaknya secara langsung. Kesimpulannya, dari ketiga pengujian tersebut menunjukkan bahwa SHA-3 memiliki ketahanan yang lebih tinggi dari algoritma SHA-1.

**Kata Kunci:** aplikasi *web*, keamanan *password*, fungsi *hash*, kriptografi, algoritma SHA-1, algoritma SHA-3

## **ABSTRACT**

*Garuda Training Cost is a web application for calculating the training costs for pilots and flight attendants developed in Garuda Indonesia Training Center. This application use SHA-1 hash function algorithm to secure user password in database. However, the weakness and colisions have been found in this algorithm, makes this algorithm less secure. Therefore, in this research authors will replace the SHA-1 with the algorithm successor, SHA-3. This algorithm will be implemented in login process, password change process and adding users process. And then both algorithm will be tested and analyzed to determine the performance of the algorithm. There are three types of tests performed. The first is brute-force testing, second is avalanche effect testing and the final test is processing time testing. From the brute-force test result, SHA-3 algorithm much better than SHA-1. From the 30 times testing for 10-character password, the SHA-1 generated hash need average 14 hours 53 minutes and 51 seconds to find the plaintext. While SHA-3 generated hash need average 4 days 13 hours 6 minutes and 6 seconds to find the plaintext. For the avalanche effect testing, SHA-1 algorithm get a percentage change of 100%, while SHA-3 get 95%. For the processing time testing, SHA-1 algorithm is better because of SHA-3 higher complexity. Although two of three test SHA-1 is better, does not mean SHA-3 is not better. Minimum avalanche effect percentage for an algorithm is 50%. And that processing time is still in millisecond unit, so that user do not feel the impact directly. In conclusion, the three these tests show that the SHA-3 has a higher resistance than the algorithm SHA-1.*

**Keyword:** *web application, password security, hash function, cryptography, SHA-1 algorithm, SHA-3 algorithm*

## DAFTAR ISI

PENGESAHAN .....	ii
PERNYATAAN ORISINALITAS .....	iii
KATA PENGANTAR.....	iv
ABSTRAK.....	v
ABSTRACT .....	vi
DAFTAR ISI.....	vii
DAFTAR TABEL.....	x
DAFTAR GAMBAR.....	xv
DAFTAR LAMPIRAN .....	xvii
BAB 1 PENDAHULUAN.....	1
1.1 Latar belakang.....	1
1.2 Rumusan masalah.....	2
1.3 Tujuan .....	2
1.4 Manfaat.....	2
1.5 Batasan masalah .....	2
1.6 Sistematika pembahasan .....	2
BAB 2 LANDASAN KEPUSTAKAAN .....	4
2.1 Kajian pustaka .....	4
2.2 Garuda Training Cost .....	5
2.3 Keamanan .....	6
2.4 Hash function.....	7
2.4.1 Secure Hash Algorithm-1 (SHA-1) .....	8
2.4.2 Secure Hash Algorithm-3 (SHA-3) .....	11
2.4.3 Perbandingan SHA-1 dengan SHA-3.....	13
2.5 Brute-force attack.....	13
2.6 Independent Samples t-Test.....	13
2.7 One-Way ANOVA .....	15
BAB 3 METODOLOGI .....	16
3.1 Studi literatur .....	16
3.2 Analisis kebutuhan.....	16

3.3 Perancangan dan implementasi sistem .....	17
3.3.1 Perancangan sistem .....	17
3.3.2 Desain tampilan .....	17
3.3.3 Implementasi sistem .....	17
3.4 Pengujian dan analisis.....	17
3.4.1 Parameter pengujian.....	17
3.4.2 Skenario pengujian.....	17
3.4.3 Hasil pengujian .....	17
3.4.4 Analisis pengujian.....	18
3.5 Kesimpulan.....	18
<b>BAB 4 PERANCANGAN DAN IMPLEMENTASI .....</b>	<b>19</b>
4.1 Analisis kebutuhan.....	19
4.1.1 Analisis permasalahan .....	19
4.1.2 Analisis data .....	22
4.1.3 Analisis keamanan data .....	22
4.2 Perancangan sistem .....	22
4.2.1 Flowchart sistem dengan SHA-1 .....	22
4.2.2 Flowchart sistem dengan SHA-3 .....	24
4.3 Desain tampilan .....	25
4.4 Implementasi sistem.....	28
4.4.1 Spesifikasi perangkat lunak dan perangkat keras.....	28
4.4.2 Implementasi pada proses login.....	28
4.4.3 Implementasi pada proses penambahan pengguna baru .....	30
4.4.4 Implementasi pada proses perubahan password pengguna ..	31
<b>BAB 5 PENGUJIAN DAN ANALISIS.....</b>	<b>32</b>
5.1 Parameter pengujian .....	32
5.2 Test vector .....	32
5.3 Skenario pengujian .....	33
5.4 Pengujian brute-force .....	34
5.4.1 Tujuan pengujian .....	34
5.4.2 Prosedur pengujian.....	34
5.4.3 Hasil pengujian.....	35



5.4.4	Analisis pengujian .....	77
5.5	Pengujian avalanche effect .....	79
5.5.1	Tujuan pengujian .....	79
5.5.2	Prosedur pengujian .....	79
5.5.3	Hasil pengujian .....	80
5.5.4	Analisis pengujian .....	80
5.6	Pengujian waktu pemrosesan .....	81
5.6.1	Tujuan pengujian .....	81
5.6.2	Prosedur pengujian .....	81
5.6.3	Hasil pengujian .....	82
5.6.4	Analisis pengujian .....	125
BAB 6	PENUTUP .....	127
6.1	Kesimpulan .....	127
6.2	Saran .....	127
DAFTAR	PUSTAKA .....	129
LAMPIRAN A	DATA HASIL PENGUJIAN .....	130
A.1	Data hasil pengujian brute-force .....	130
A.2	Data hasil pengujian waktu pemrosesan pada saat login .....	148

## DAFTAR TABEL

Tabel 2.1 Perbandingan penelitian penulis dengan penelitian terkait.....	4
Tabel 2.2 Tabel Levene’s Test for Equality of Variances untuk waktu.....	14
Tabel 2.3 Tabel t-test for Equality of Means untuk waktu .....	14
Tabel 2.4 Tabel One-way ANOVA untuk waktu .....	15
Tabel 5.1 Perintah yang digunakan dalam pengujian brute-force .....	34
Tabel 5.2 Hasil pengujian brute-force password 8 karakter lowercase .....	35
Tabel 5.3 Independent samples t-Test untuk pengujian brute-force password 8 karakter lowercase.....	37
Tabel 5.4 Hasil pengujian brute-force password 8 karakter lowercase dan angka .....	37
Tabel 5.5 Independent samples t-Test untuk pengujian brute-force password 8 karakter lowercase dan angka .....	39
Tabel 5.6 Hasil pengujian brute-force password 8 karakter lowercase, angka dan simbol.....	40
Tabel 5.7 Independent samples t-Test untuk pengujian brute-force password 8 karakter lowercase, angka dan simbol.....	42
Tabel 5.8 Hasil pengujian brute-force password 8 karakter lowercase, angka, simbol dan uppercase .....	42
Tabel 5.9 Independent samples t-Test untuk pengujian brute-force password 8 karakter lowercase, angka, simbol dan uppercase.....	44
Tabel 5.10 Hasil pengujian brute-force password 9 karakter lowercase .....	45
Tabel 5.11 Independent samples t-Test untuk pengujian brute-force password 9 karakter lowercase.....	47
Tabel 5.12 Hasil pengujian brute-force password 9 karakter lowercase dan angka .....	48
Tabel 5.13 Independent samples t-Test untuk pengujian brute-force password 9 karakter lowercase dan angka .....	49
Tabel 5.14 Hasil pengujian brute-force password 9 karakter lowercase, angka dan simbol.....	50
Tabel 5.15 Independent samples t-Test untuk pengujian brute-force password 9 karakter lowercase, angka dan simbol.....	52
Tabel 5.16 Hasil pengujian brute-force password 9 karakter lowercase, angka, simbol dan uppercase .....	53

Tabel 5.17 Independent samples t-Test untuk pengujian brute-force password 9 karakter lowercase, angka, simbol dan uppercase .....	54
Tabel 5.18 Hasil pengujian brute-force password 10 karakter lowercase .....	55
Tabel 5.19 Independent samples t-Test untuk pengujian brute-force password 10 karakter lowercase .....	57
Tabel 5.20 Hasil pengujian brute-force password 10 karakter lowercase dan angka .....	57
Tabel 5.21 Independent samples t-Test untuk pengujian brute-force password 10 karakter lowercase dan angka .....	59
Tabel 5.22 Hasil pengujian brute-force password 10 karakter lowercase, angka dan simbol .....	60
Tabel 5.23 Independent samples t-Test untuk pengujian brute-force password 10 karakter lowercase, angka dan simbol .....	62
Tabel 5.24 Hasil pengujian brute-force password 10 karakter lowercase, angka, simbol dan uppercase .....	62
Tabel 5.25 Independent samples t-Test untuk pengujian brute-force password 10 karakter lowercase, angka, simbol dan uppercase .....	64
Tabel 5.26 Independent samples t-Test untuk keseluruhan pengujian brute-force .....	65
Tabel 5.27 One-Way ANOVA untuk pengujian brute-force untuk password dengan karakter lowercase dari algoritma SHA-1 untuk semua jumlah karakter	66
Tabel 5.28 One-Way ANOVA untuk pengujian brute-force untuk password dengan karakter lowercase dikombinasikan dengan angka dari algoritma SHA-1 untuk semua jumlah karakter .....	67
Tabel 5.29 One-Way ANOVA untuk pengujian brute-force untuk password dengan karakter lowercase dikombinasikan dengan angka dan simbol dari algoritma SHA-1 untuk semua jumlah karakter .....	68
Tabel 5.30 One-Way ANOVA untuk pengujian brute-force untuk password dengan karakter lowercase dikombinasikan dengan angka, simbol dan uppercase dari algoritma SHA-1 untuk semua jumlah karakter .....	69
Tabel 5.31 One-Way ANOVA untuk pengujian brute-force untuk password dengan karakter lowercase dari algoritma SHA-3 untuk semua jumlah karakter	70
Tabel 5.32 One-Way ANOVA untuk pengujian brute-force untuk password dengan karakter lowercase dikombinasikan dengan angka dari algoritma SHA-3 untuk semua jumlah karakter .....	71
Tabel 5.33 One-Way ANOVA untuk pengujian brute-force untuk password dengan karakter lowercase dikombinasikan dengan angka dan simbol dari algoritma SHA-3 untuk semua jumlah karakter .....	73

Tabel 5.34 One-Way ANOVA untuk pengujian brute-force untuk password dengan karakter lowercase dikombinasikan dengan angka, simbol dan uppercase dari algoritma SHA-3 untuk semua jumlah karakter.....	74
Tabel 5.35 One-Way ANOVA untuk pengujian brute-force untuk password dengan semua jenis karakter dan semua jumlah karakter dari algoritma SHA-1	75
Tabel 5.36 One-Way ANOVA untuk pengujian brute-force untuk password dengan semua jenis karakter dan semua jumlah karakter dari algoritma SHA-3	76
Tabel 5.37 One-Way ANOVA untuk pengujian brute-force untuk password dengan semua jenis karakter dan semua jumlah karakter dari algoritma SHA-1 dan SHA-3.....	77
Tabel 5.38 Perbandingan keseluruhan pengujian brute-force untuk password dari algoritma SHA-1 dan SHA-3.....	78
Tabel 5.39 Hasil pengujian avalanche effect untuk algoritma SHA-1.....	80
Tabel 5.40 Hasil pengujian avalanche effect untuk algoritma SHA-3.....	80
Tabel 5.41 Hasil pengujian waktu pemrosesan password 8 karakter lowercase .	82
Tabel 5.42 Independent samples t-Test untuk pengujian waktu pemrosesan pada saat login password 8 karakter lowercase .....	84
Tabel 5.43 Hasil pengujian waktu pemrosesan password 8 karakter lowercase dan angka .....	85
Tabel 5.44 Independent samples t-Test untuk pengujian waktu pemrosesan pada saat login password 8 karakter lowercase dan angka .....	86
Tabel 5.45 Hasil pengujian waktu pemrosesan password 8 karakter lowercase, angka dan simbol .....	87
Tabel 5.46 Independent samples t-Test untuk pengujian waktu pemrosesan pada saat login password 8 karakter lowercase, angka dan simbol.....	89
Tabel 5.47 Hasil pengujian waktu pemrosesan password 8 karakter lowercase, angka, simbol dan uppercase.....	89
Tabel 5.48 Independent samples t-Test untuk pengujian waktu pemrosesan pada saat login password 8 karakter lowercase, angka, simbol dan uppercase .....	91
Tabel 5.49 Hasil pengujian waktu pemrosesan password 9 karakter lowercase .	92
Tabel 5.50 Independent samples t-Test untuk pengujian waktu pemrosesan pada saat login password 9 karakter lowercase .....	94
Tabel 5.51 Hasil pengujian waktu pemrosesan password 9 karakter lowercase dan angka .....	94
Tabel 5.52 Independent samples t-Test untuk pengujian waktu pemrosesan pada saat login password 9 karakter lowercase dan angka .....	96

Tabel 5.53 Hasil pengujian waktu pemrosesan password 9 karakter lowercase, angka dan simbol .....	97
Tabel 5.54 Independent samples t-Test untuk pengujian waktu pemrosesan pada saat login password 9 karakter lowercase, angka dan simbol.....	99
Tabel 5.55 Hasil pengujian waktu pemrosesan password 9 karakter lowercase, angka, simbol dan uppercase.....	99
Tabel 5.56 Independent samples t-Test untuk pengujian waktu pemrosesan pada saat login password 9 karakter lowercase, angka, simbol dan uppercase .....	101
Tabel 5.57 Hasil pengujian waktu pemrosesan password 10 karakter lowercase .....	102
Tabel 5.58 Independent samples t-Test untuk pengujian waktu pemrosesan pada saat login password 10 karakter lowercase .....	104
Tabel 5.59 Hasil pengujian waktu pemrosesan password 10 karakter lowercase dan angka .....	104
Tabel 5.60 Independent samples t-Test untuk pengujian waktu pemrosesan pada saat login password 10 karakter lowercase dan angka .....	106
Tabel 5.61 Hasil pengujian waktu pemrosesan password 10 karakter lowercase, angka dan simbol .....	107
Tabel 5.62 Independent samples t-Test untuk pengujian waktu pemrosesan pada saat login password 10 karakter lowercase, angka dan simbol.....	109
Tabel 5.63 Hasil pengujian waktu pemrosesan password 10 karakter lowercase, angka, simbol dan uppercase.....	109
Tabel 5.64 Independent samples t-Test untuk pengujian waktu pemrosesan pada saat login password 10 karakter lowercase, angka, simbol dan uppercase .....	111
Tabel 5.65 Independent samples t-Test untuk keseluruhan pengujian waktu pemrosesan pada saat login .....	112
Tabel 5.66 One-Way ANOVA untuk pengujian waktu pemrosesan untuk password dengan karakter lowercase dari algoritma SHA-1 untuk semua jumlah karakter .....	113
Tabel 5.67 One-Way ANOVA untuk pengujian waktu pemrosesan untuk password dengan karakter lowercase dikombinasikan dengan angka dari algoritma SHA-1 untuk semua jumlah karakter .....	114
Tabel 5.68 One-Way ANOVA untuk pengujian waktu pemrosesan untuk password dengan karakter lowercase dikombinasikan dengan angka dan simbol dari algoritma SHA-1 untuk semua jumlah karakter .....	115
Tabel 5.69 One-Way ANOVA untuk pengujian waktu pemrosesan untuk password dengan karakter lowercase dikombinasikan dengan angka, simbol dan uppercase dari algoritma SHA-1 untuk semua jumlah karakter.....	117

Tabel 5.70 One-Way ANOVA untuk pengujian waktu pemrosesan untuk password dengan karakter lowercase dari algoritma SHA-3 untuk semua jumlah karakter .....	118
Tabel 5.71 One-Way ANOVA untuk pengujian waktu pemrosesan untuk password dengan karakter lowercase dikombinasikan dengan angka dari algoritma SHA-3 untuk semua jumlah karakter .....	119
Tabel 5.72 One-Way ANOVA untuk pengujian waktu pemrosesan untuk password dengan karakter lowercase dikombinasikan dengan angka dan simbol dari algoritma SHA-3 untuk semua jumlah karakter .....	120
Tabel 5.73 One-Way ANOVA untuk pengujian waktu pemrosesan untuk password dengan karakter lowercase dikombinasikan dengan angka, simbol dan uppercase dari algoritma SHA-3 untuk semua jumlah karakter.....	121
Tabel 5.74 One-Way ANOVA untuk pengujian waktu pemrosesan untuk password dengan semua jenis karakter dan semua jumlah karakter dari algoritma SHA-1 .....	122
Tabel 5.75 One-Way ANOVA untuk pengujian waktu pemrosesan untuk password dengan semua jenis karakter dan semua jumlah karakter dari algoritma SHA-3 .....	123
Tabel 5.76 One-Way ANOVA untuk pengujian waktu pemrosesan untuk password dengan semua jenis karakter dan semua jumlah karakter dari algoritma SHA-1 dan SHA-3.....	124
Tabel 5.77 Perbandingan keseluruhan pengujian waktu pemrosesan untuk password dari algoritma SHA-1 dan SHA-3.....	126

## DAFTAR GAMBAR

Gambar 2.1 Operasi SHA-1 .....	10
Gambar 4.1 Skema global sistem Garuda Training Cost.....	19
Gambar 4.2 Skema global algoritma SHA-1 .....	20
Gambar 4.3 Skema global algoritma SHA-3 .....	21
Gambar 4.4 Flowchart sistem dengan SHA-1 .....	23
Gambar 4.5 Flowchart sistem dengan SHA-3 .....	24
Gambar 4.6 Desain tampilan halaman login.....	25
Gambar 4.7 Desain tampilan halaman penambahan pengguna baru .....	26
Gambar 4.8 Desain tampilan halaman perubahan password pengguna .....	27
Gambar 4.9 Screenshot halaman login .....	29
Gambar 4.10 Screenshot halaman penambahan pengguna baru .....	30
Gambar 4.11 Screenshot halaman perubahan password pengguna.....	31
Gambar 5.1 Perbandingan waktu pengujian brute-force password 8 karakter lowercase .....	36
Gambar 5.2 Perbandingan waktu pengujian brute-force password 8 karakter lowercase dan angka.....	39
Gambar 5.3 Perbandingan waktu pengujian brute-force password 8 karakter lowercase, angka dan simbol .....	41
Gambar 5.4 Perbandingan waktu pengujian brute-force password 8 karakter lowercase, angka, simbol dan uppercase .....	44
Gambar 5.5 Perbandingan waktu pengujian brute-force password 9 karakter lowercase .....	46
Gambar 5.6 Perbandingan waktu pengujian brute-force password 9 karakter lowercase dan angka.....	49
Gambar 5.7 Perbandingan waktu pengujian brute-force password 9 karakter lowercase, angka dan simbol .....	51
Gambar 5.8 Perbandingan waktu pengujian brute-force password 9 karakter lowercase, angka, simbol dan uppercase .....	54
Gambar 5.9 Perbandingan waktu pengujian brute-force password 10 karakter lowercase .....	56
Gambar 5.10 Perbandingan waktu pengujian brute-force password 10 karakter lowercase dan angka.....	59

Gambar 5.11 Perbandingan waktu pengujian brute-force password 10 karakter lowercase, angka dan simbol .....	61
Gambar 5.12 Perbandingan waktu pengujian brute-force password 10 karakter lowercase, angka, simbol dan uppercase .....	64
Gambar 5.13 Perbandingan waktu pemrosesan untuk password 8 karakter lowercase .....	83
Gambar 5.14 Perbandingan waktu pemrosesan untuk password 8 karakter lowercase dan angka.....	86
Gambar 5.15 Perbandingan waktu pemrosesan untuk password 8 karakter lowercase, angka dan simbol .....	88
Gambar 5.16 Perbandingan waktu pemrosesan untuk password 8 karakter lowercase, angka, simbol dan uppercase .....	91
Gambar 5.17 Perbandingan waktu pemrosesan untuk password 9 karakter lowercase .....	93
Gambar 5.18 Perbandingan waktu pemrosesan untuk password 9 karakter lowercase dan angka.....	96
Gambar 5.19 Perbandingan waktu pemrosesan untuk password 9 karakter lowercase, angka dan simbol .....	98
Gambar 5.20 Perbandingan waktu pemrosesan untuk password 9 karakter lowercase, angka, simbol dan uppercase .....	101
Gambar 5.21 Perbandingan waktu pemrosesan untuk password 10 karakter lowercase .....	103
Gambar 5.22 Perbandingan waktu pemrosesan untuk password 10 karakter lowercase dan angka.....	106
Gambar 5.23 Perbandingan waktu pemrosesan untuk password 10 karakter lowercase, angka dan simbol .....	108
Gambar 5.24 Perbandingan waktu pemrosesan untuk password 10 karakter lowercase, angka, simbol dan uppercase .....	111



## DAFTAR LAMPIRAN

LAMPIRAN A DATA HASIL PENGUJIAN .....	130
A.1 Data hasil pengujian brute-force.....	130
A.2 Data hasil pengujian waktu pemrosesan pada saat login .....	148