Aplikasi Steganografi Berbasis *Short Message Service* (SMS) pada Android

Skripsi

untuk memenuhi sebagian persyaratan
mencapai derajat S-1

Program Studi Teknik Informatika

Disusun oleh:

Abdur Rahman
NIM. 07650035

Kepada

PROGRAM STUDI TEKNIK INFORMATIKA
FAKULTAS SAINS DAN TEKNOLOGI
UIN SUNAN KALAIJAGA
YOGYAKARTA
2013

Universitas Islam Negeri Sunan Kalijaga FM-UINSK-BM-05-07/R0

PENGESAHAN SKRIPSI/TUGAS AKHIR

Nomor : UIN.02/D.ST/PP.01.1/299/2013

Skripsi/Tugas Akhir dengan judul : Aplikasi Steganografi Berbasis *Short Message Service* (SMS) pada Android

Yang dipersiapkan dan disusun oleh :
Nama : Abdur Rahman
NIM : 07650035
Telah dimunaqasyahkan pada : Rabu, 30 Januari 2013
Nilai Munaqasyah : A -

Dan dinyatakan telah diterima oleh Fakultas Sains dan Teknologi UIN Sunan Kalijaga

TIM MUNAQASYAH :

Ketua Sidang

M. Taufiq Nuruzzaman, M.Eng
NIP. 19791118 200501 1 003

Penguji I

Nurochman, M.Kom
NIP.19801223 200901 1 007

Penguji II

Bambang Sugiantoro, M.T
NIP. 19751024 200912 1 002

Yogyakarta, 7 Februari 2013
UIN Sunan Kalijaga
Fakultas Sains dan Teknologi
Dekan

KEMENTERIAN AGAMA FAKULTAS SAINS DAN TEKNOLOGI UIN SUNAN KALIJAGA YOGYAKARTA

Prof. Drs. H. Akh. Minhaji, M.A, Ph.D
NIP. 19580919 198603 1 002

SURAT PERSETUJUAN SKRIPSI/TUGAS AKHIR

Hal : Permohonan
Lamp : -

Kepada
Yth. Dekan Fakultas Sains dan Teknologi
UIN Sunan Kalijaga Yogyakarta
di Yogyakarta

Assalamu'alaikum wr. wb.

Setelah membaca, meneliti, memberikan petunjuk dan mengoreksi serta mengadakan perbaikan seperlunya, maka kami selaku pembimbing berpendapat bahwa skripsi Saudara:

Nama	: Abdur Rahman
NIM	: 07650035
Judul Skripsi	: **Aplikasi Steganografi *Berbasis Short Message Service* (SMS) pada Android**

sudah dapat diajukan kembali kepada Program Studi Teknik Informatika Fakultas Sains dan Teknologi UIN Sunan Kalijaga Yogyakarta sebagai salah satu syarat untuk memperoleh gelar Sarjana Strata Satu dalam Teknik Informatika.

Dengan ini kami mengharap agar skripsi/tugas akhir Saudara tersebut di atas dapat segera dimunaqsyahkan. Atas perhatiannya kami ucapkan terima kasih.

Wassalamu'alaikum wr. wb.

Yogyakarta, 21 Januari 2013
Pembimbing

M. Taufiq Nuruzzaman, M. Eng
NIP. 19791118 200501 003

HALAMAN PERNYATAAN KEASLIAN SKRIPSI

Yang bertanda tangan di bawah ini:

Nama	: Abdur Rahman
NIM	: 07650035
Program Studi	: Teknik Informatika
Fakultas	: Sains dan Teknologi

Menyatakan bahwa skripsi dengan judul "**Aplikasi Steganografi Berbasis *Short Message Service* (SMS) pada Android**" 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 orang lain, kecuali yang secara tertulis diacu dalam naskah ini dan disebutkan dalam daftar pustaka.

Yogyakarta, 21 Januari 2013

Yang Menyatakan

Abdur Rahman

07650035

KATA PENGANTAR

Alhamdulillah, segala puji bagi Allah *Subhanahu wa ta'ala* atas limpahan rahmat, hidayah, serta bimbingan-Nya. Shalawat serta salam semoga tercurah kepada Nabi Muhammad *Shallallohu 'alaihi wa sallam*. Akhirnya penulis dapat menyelesaikan penelitian Tugas Akhir yang berjudul **Aplikasi Steganografi *Short Message Service* (SMS) pada Android**. Oleh karena itu, dengan segala kerendahan hari pada kesempatan ini penulis mengucapkan banyak terima kasih kepada:

1. Prof. Drs. H. Akh. Minhaji, M.A.,Ph.D selaku Dekan Fakultas Sains dan Teknologi Universitas Islam Negeri Sunan Kalijaga.
2. Bapak Agus Mulyanto, S.Si, M.Kom. selaku Ketua Program Studi Teknik Informatika Fakultas Sains dan Teknologi Universitas Islam Negeri Sunan Kalijaga.
3. Bapak M Taufiq Nuruzzaman, M.Eng. selaku dosen pembimbing yang selalu sabar membimbing, mengarahkan, memberikan nasehat dan saran selama penyusunan skripsi.
4. Ibu, Ayah, kakak, dan adekku tercinta yang senantiasa mendoa'akan dan memberikan dukungan penuh bagi penulis.
5. Seluruh teman-teman keluarga besar Program Studi Teknik Informatika, khususnya angkatan 2007 yang telah banyak sekali memberi masukan, saran dan diskusi yang begitu berharga.

6. Serta semua rekan-rekan penulis di berbagai kegiatan maupun organisasi yang juga telah memberikan banyak sekali masukan dan kontribusi yang sangat berarti bagi penulis.

Penulis merasa masih banyak sekali kekurangan dan kelemahan dalam penelitian ini, oleh karena itu segala kritik dan saran senantiasa penulis harapkan dari para pembaca. Akhir kata, semoga penelitian ini dapat menjadi panduan serta referensi yang sangat berguna bagi pembaca dan dapat dimanfaakan sebaik-baiknya.

Yogyakarta, Januari 2013

Penulis

HALAMAN MOTTO

Jadi Diri Sendiri, Cari Jati Diri, And Dapetin Hidup Yang Mandiri

Optimis, Kaena Hidup Terus Mengalir Dan Kehidupan Terus Berputar

Sesekali Liat Ke Belakang Untuk Melanjutkan Perjalanan Yang Tiada Berujung

DAFTAR ISI

DAFTAR GAMBAR

DAFTAR TABEL

DAFTAR MODUL

Aplikasi Steganografi Berbasis *Short Message Service*(SMS) pada Android

ABBUR RAHMAN
07650035

INTISARI

Perkembangan pesat dalam teknologi ponsel baru-baru ini telah menyebabkan munculnya ponsel pintar dengan berbagai fitur, dan sistem operasi yang kompleks layaknya komputer. Salah satu sistem operasi terkenal untuk ponsel adalah Android. Kendati demikian, meskipun teknologi baru dari ponsel pintar ini memiliki banyak fitur, masyarakat tampaknya masih memiliki perhatian khusus ke layanan pesan singkat gaya lama, yaitu Short Message Service, lebih dikenal sebagai SMS. Sayangnya, fitur SMS saat ini masih memiliki keterbatasan. Terutama mengenai keamanan informasi rahasia. Dengan kata lain, kemampuan seseorang dalam mengirim informasi rahasia melalui SMS masih menjadi pertanyaan. Untuk mengatasi masalah seperti ini, penulis akan mencoba untuk membuat sebuah aplikasi yang mampu mengamankan pesan rahasia.

Sistem keamanan yang penulis tawarkan didasarkan pada dua model keamanan, yaitu keamanan enkripsi dan steganografi. Sebelum dikirim, pesan terlebih dahulu akan dienkripsi menggunakan algoritma *Caesar cipher*, dan kemudian dimasukkan ke dalam pesan teks SMS menggunakan algoritma *whitespace*. Selanjutnya, akses ke pesan dalam aplikasi tersebut harus diamankan dengan password, sehingga pesan akan aman dari pihak yang tidak berhak.

Metodologi penelitian yang digunakan dalam penelitian ini adalah pengembangan sistem operasi. Langkah-langkah penelitian dimulai dengan studi pustaka, identifikasi kebutuhan sistem, pengumpulan data, kebutuhan perangkat sistem, dan metode pengembangan sistem.

Kemudian, akhirnya, penelitian ini akan mampu menciptakan suatu aplikasi yang akan diinstal pada ponsel pintar berbasis Android. Aplikasi ini dapat melakukan proses enkripsi algoritma Caesar cipher, dan akan menyembunyikannya ke dalam pesan teks atau SMS. Hasil enkripsi dan steganografi terhadap pesan tersebut juga dapat didekripsi melalui aplikasi ini dengan memasukkan password sebelumnya.

Kata Kunci: enkripsi, steganografi, keamanan informasi, spasi, Caesar cipher.

Steganography Application Based Short Message Service (SMS) on Android

ABDUR RAHMAN
07650035

ABSTRACT

Rapid development in mobile phone technology recently has caused the emergence of smart phones with many different features, and a complex operating system just like a computer. One of well known operating system for mobile phones is android. Nonetheless, although these new technology of smart phones have many features, people seems still has a special attention to an old-fashioned text service, which is Short Message Service, better known as SMS. Unfortunately, SMS feature nowadays still has limitations. Especially regarding the safety of confidential information. In other word, the ability of someone in sending a confidential information through SMS is still in question. In order to solve this kind of problem, authors will try to create an application that capable to secure a confidential message.

Security system that author offered is based on two security models, namely encryption and steganography security. Before being sent, a message will firstly encrypted using the Caesar cipher algorithm, and then inserted into the SMS text messages using the algorithm whitespace. Next, an access to the message in the application must be secured with a password, so the message will be safe from unauthorized parties.

The research methodology used in this research is the development of the operation system. The research steps is begins with library study, identifying system requirements, data collection, system requirements, and system development methods.

Then, finally, this research will able to create an applications that will be installed on Android-based smart phones. This application can do the Caesar cipher encryption algorithm, and will hide it in a text message or SMS. The results of encryption and steganography process to the message is also can be decrypted through this application by entering a preceding password.

Keywords: encryption, steganography, information security, whitespace, Caesar cipher.

BAB I

PENDAHULUAN

1.1 Latar Belakang

Beberapa tahun terakhir ini terjadi perkembangan yang pesat pada teknologi, salah satunya adalah perkembangan telepon selular (*ponsel*). Salah satunya adalah mulai bermunculan *ponsel* pintar dengan berbagai fitur dan memiliki sistem operasi kompleks layaknya komputer. Berbagai sistem operasi untuk ponsel pun bermunculan, diantaranya yang cukup dikenal luas adalah android. Ponsel bersistem operasi android merupakan "ponsel cerdas" (*smart phone*) yang memiliki berbagai fungsi seperti *multimedia*, *multiplayer games*, *transfer* data, *video streaming* dan lain-lain. Berbagai perangkat lunak untuk mengembangkan aplikasi ponsel pun bermunculan.

Walaupun ponsel pintar memiliki berbagai fitur, fitur lama seperti Layanan Pesan Singkat atau lebih dikenal dengan SMS masih tetap ramai digunakan. SMS adalah sebuah layanan yang dilaksanakan dengan ponsel untuk mengirim maupun menerima pesan-pesan pendek. SMS sekarang ini menjadi salah satu layanan komunikasi yang sangat populer dikalangan masyarakat. Dengan SMS dapat memudahkan dalam komunikasi dengan waktu yang singkat dan biaya yang murah. SMS juga menjadi salah satu fitur utama dalam telepon seluler.

Namun dengan fasilitas SMS yang ada, timbul pertanyaan mengenai keamanan data SMS tersebut. Keamanan data SMS sangat diperlukan baik itu

dalam urusan pribadi maupun bisnis. Keamanan data SMS diperlukan untuk memberikan perlindungan isi SMS agar tidak bisa dibaca oleh orang lain yang tidak dikehendaki dan hanya orang tertentu saja yang bisa membaca SMS tersebut.

Berdasarkan permasalahan diatas, penulis akan membagun sebuah aplikasi SMS yang dapat menyembunyikan pesan rahasia dibalik pesan yang biasa agar sulit diketahui oleh orang lain dan hanya orang tertentu saja yang bisa membaca SMS tersebut.

1.2 Rumusan Masalah

Berdasarkan latar belakang di atas, rumusan masalah dalam penelitian ini adalah sebagai berikut : Bagaimana cara memanfaatkan layanan SMS yang mudah penggunaannya agar dapat juga dipakai untuk mengirim dan menerima pesan yang bersifat rahasia, dimana informasi atau isi dari pesan tersebut sulit diketahui oleh pihak yang tidak dikehendaki membacanya.

1.3 Batasan Masalah

Adapun batasan masalah dalam penelitian ini adalah sebagai berikut:

1. Aplikasi ini dijalankan pada *ponsel* yang bersistem operasi android minimum versi 2.3. (*Gingerbread*)
2. Metode *Kriptografi* yang digunakan adalah *caesar cipher.*
3. Teknik *steganografi* yang digunakan adalah *whitespace*
4. Bahasa pemrograman yang digunakan adalah *Java*.
5. Panjang maksimal pesan media (pesan pembawa pesan rahasia) yang dikirimkan adalah 50 karakter.

6. Nomor tujuan hanya untuk satu nomor tujuan.
7. Password hanya berupa angka 0-95

1.4 Manfaat Penelitian

Hasil penelitian ini diharapkan dapat memberi manfaat sebagai berikut:

1. Memberi kemudahan bagi pengguna ponsel untuk mengirimkan informasi rahasia melalui SMS.
2. Seseorang dapat mengirimkan suatu informasi rahasia tanpa takut diketahui isi informasi tersebut oleh orang lain.
3. Dengan adanya penelitian ini, maka dapat dijadikan dasar pengembangan tentang aplikasi steganografi berbasis SMS bagi peneliti berikutnya.

1.5 Tujuan Penelitian

Tujuan yang ingin dicapai dari penelitian ini adalah menghasilkan suatu aplikasi pada *handphone* yang bersistem operasi android yang dapat digunakan untuk mengirim dan menerima pesan teks sekaligus memiliki fasilitas untuk mengamankan atau menyembunyikan informasi dari pesan yang dikirimkan.

1.6 Keaslian Penelitian

Penelitian yang berhubungan dengan aplikasi steganografi sudah pernah dilakukan. Penelitian yang terdahulu telah menggunakan berbagai macam tipe file sebagai media pembawa pesan tersembunyi seperti gambar, suara, video dan lain-lain. Kebanyakan hasil dari penelitian tersebut berupa aplikasi desktop, tetapi aplikasi steganografi yang memanfaatkan media SMS pada ponsel sebagai media pembawa pesan rahasia belum pernah dilakukan.

BAB VII

PENUTUP

7.1 Kesimpulan

Berdasarkan pengujian fungsional sistem yang telah dilakukan oleh penulis, hasilnya menunjukkan, bahwa sebagian besar pengguna menyatakan fungsional system berfungsi dengan baik. Hal ini dapat diketahui dari banyaknya koresponden yang mengisi questioner dengan jawaban "Ya".

Berdasarkan penelitian yang telah dilakukan penulis mengenai Aplikasi steganografi *Short Message Service* (SMS) Berbasis Android, maka dapat diambil kesimpulan bahwa penelitian ini telah berhasil membuat suatu aplikasi pada telepon selular yang dapat digunakan untuk mengirim dan menerima pesan teks sekaligus memiliki fasilitas untuk mengamankan atau menyembunyikan informasi dari pesan yang dikirimkan.

7.2 Saran

Penelitian yang dilakukan tentunya tidak lepas dari kekurangan dan kelemahan. Oleh karena itu, untuk pengembangan aplikasi lebih lanjut diperlukan perhatian terhadap beberapa hal, diantaranya:

1. Menggunakan kriptografi yang lebih modern agar pesan lebih aman.
2. Ditambah algoritma kompres sms agar pesan yang ditampung lebih banyak.
3. Menambah menu *draft* untuk menyimpan pesan.

DAFTAR PUSTAKA

Ariyus, Dony., 2006, *Kriptografi, Keamanan Data, dan Komunikasi*. Graha Ilmu, Yogyakarta.

Dharwiyanti, Sri, 2003. *Pengantar Unified Modeling Language (UML),* IlmuKomputer.Com.

Johnson, Neil F. dan Jajodia, Sushil. 1998. *Exploring Steganography: Seeing The Unseen*. George Mason University.

Junaedi, Moh, 2003. *Pengantar XML, kuliah umum ilmu komputer*, www.ilmukomputer.com.

Krenn, J.R. 2004. *Steganography and Steganalysis*. *http://www.krenn.nl/univ/cry/steg/article.pdf.* diakses tanggal 20 Juni 2012

Mangarae, Aelphaeis. *2006. Steganography FAQ*. http://www.infosecwriters.com/text_resources/pdf/Steganography_AMangarae.pdf, diakses tanggal 28 Juni 2012.

Maulana, Ahmad Mansur. 2009. *Data Hiding Steganography Pada File Image Menggunakan Metode Least Significant Bit*. Skripsi Institut Teknologi Sepuluh November. Surabaya.

Menezes, dkk. 1996. *Handbook of Applied Cryptography*. CRC Press.

Munir, Rinaldi. 2006. *Kriptografi*. Penerbit Informatika, Bandung

Prayogo, Andika. 2007. *Aplikasi Steganografi Untuk Menyembuyikan Pesan Terenkripsi Pada Media Plain Text*. Skripsi Universitas Gajah Mada. Yogyakarta.

Priyanta, F, 2011. *Pemrograman Android Untuk Pemula*, Penerbit Cerdas Pustaka. Jakarta.

Purwanto, Heri dan Anny Kartika Sari. 2003. *Aplikasi Kompresi SMS Teks (Short Message Service) Dengan Menggunakan Algoritma Huffman Kononik dan LZW (Lempel-Ziv-Welch).* Yogyakarta : Jurusan Ilmu Komputer Inuversitas Gajah Mada.

Safaat H, Nazruddin, 2011. *Pemrograman Aplikasi Mobile Smartphone dan Tablet PC Berbasis Android*. Penerbit Informatika, Bandung.

Schneier, Bruce., 1996, *Applied Cryptography 2nd*. John Wiley & Sons, Ltd.

Tresnani, Dini Lestari, 2009. *Kode Huffman Untuk Kompresi SMS*. Skripsi Informatika Institut Teknologi Bandung. Bandung.

Tsani, Fahmi Aulia.2012. *Implementasi Steganografi dan Algoritma Kriptografi Vigenere Cipher pada Media Plain Text.* Skripsi Universitas Islam Negeri Sunan Kalijaga.Yogyakarta.

Wulandari, Ratna. 2010. *Pembuatan Aplikasi Steganografi pada File Audio Mp3 Dengan Metode Parity Coding Dan Enkripsi Rijndael*. Skripsi Institut Teknologi Sepuluh November. Surabaya.

LAMPIRAN SOURCE CODE

Class steganografi.java

```
public class steganografi {

	protected String getPesanAsli(String stegoSMS) {
		// TODO Auto-generated method stub
		int j=0;
		String pesanBawa =
		stegoSMS.substring(0,stegoSMS.indexOf("`.`"));
		char[] pesanBawaArray = pesanBawa.toCharArray();
		for(int p = 0; p < pesanBawa.length();p++){
			int temp = (int) pesanBawaArray[p];
			if(temp == 9){
				pesanBawaArray[j] = (char) 32;
					j++;
			}else {
				pesanBawaArray[j] = pesanBawaArray[p];
					j++;
			}
		}
		return new String(pesanBawaArray);
	}


	protected String ekstrak(String stegoSMS) {
		char[] stegoSMSArray = stegoSMS.toCharArray();
		String chiperBiner = ""; String chiperBiner2 = "";
		for(int z=0; z < stegoSMSArray.length; z++){
		int tempo = (int) stegoSMSArray[z];
		if(tempo == 32) {
			chiperBiner = chiperBiner + "0";
			chiperBiner2 = chiperBiner2 + "0";
			if((chiperBiner.length()%8)==0){
				chiperBiner2 = chiperBiner2 + "-";
			}
		}else if(tempo == 9){
			chiperBiner = chiperBiner + "1";
			chiperBiner2 = chiperBiner2 + "1";
			if((chiperBiner.length()%8)==0){
				chiperBiner2 = chiperBiner2 + "-";
				}
			}
		}

	String[] pecahBiner = chiperBiner2.split("-");
	char[] chiperTextArray = new char[pecahBiner.length];
	for(int k=0; k<pecahBiner.length; k++){
```

```
            chiperTextArray[k]= (char)
             Integer.parseInt(pecahBiner[k], 2);
      }
            return new String(chiperTextArray);
      }

      protected String stego(String pesan1, String pesan2) {
            // TODO Auto-generated method stub
            String full_biner ="";
            char[] pesanArray = pesan1.toCharArray();
            for(int i=0; i<pesanArray.length; i++)
            {
                  int temp = (int) pesanArray[i];
                  String temp1 = Integer.toBinaryString(temp);
                  String temp2 = "00000000" + temp1;

                  String biner = temp2.substring(temp2.length()-8);

                  full_biner = full_biner + biner;
            }

            String binerToChar = "";
            for(int a=0; a<full_biner.length(); a++) {
                  if (full_biner.charAt(a) == '1'){
                        binerToChar += '  ';    }
                  else if(full_biner.charAt(a) == '0')
                        {
                        binerToChar +=' ';}
            }

            int u=0; int p=full_biner.length();String pesanStego="";
            for(int s=0; s<pesan2.length();s++){
                  if(u<p){
                        if(pesan2.charAt(s) == ' '){
                              pesanStego += binerToChar.charAt(u);
                              u++;
                        }else{
                              pesanStego += pesan2.charAt(s);
                        }
                  }else{
                        pesanStego += pesan2.charAt(s);
                  }
            }

            pesanStego = pesanStego + "`.`";
            for(int e=u; e<p; e++ ){

                  pesanStego += binerToChar.charAt(e);
            }
                  return pesanStego;
      }
}
```

Class caesar_cipher.java

```
package maman.oblo;

public class caesar_chiper {

	//mengenkripsi pesan
	protected String encrip(String psnRhs, int psswd) {
		// TODO Auto-generated method stub
		char[] charArray=psnRhs.toCharArray();
		for(int i=0;i<charArray.length;i++){
			char a = charArray[i];
			if(a >= 32 && a <= 127){
				int temp =  a - 32;
				temp  = (temp + psswd) % 96;
			charArray[i] = (char) (temp + 32);
			}
		}
		return new String(charArray);
	}

	//mendekripsi pesan
	protected String decrip(String psnRhs, int psswd) {
		// TODO Auto-generated method stub
		char[] charArray=psnRhs.toCharArray();
		for(int i=0;i<charArray.length;i++){
			char a = charArray[i];
			if(a >= 32 && a <= 127){
				int temp =  a - 32;
				temp  = (temp - psswd) % 96;
				if(temp < 0){
					temp += 96;
				}
			charArray[i] = (char) (temp+32);
			}
		}
		return new String(charArray);
	}
}
```

LAMPIRAN

ANGKET PENGUJIAN SISTEM

Aplikasi Steganografi Berbasis *Short Message Service*(SMS) pada Android

NAMA : .....

PEKERJAAN : .....

INSTANSI : .....

Berikanlah tanda centang (√) pada isian yang terlampir

Pengujian Fungsional Sistem

No	Pertanyaan	Ya	Tidak
1	Pesan dapat disampaikan dan diterima dengan baik		
2	Isi pesan yang dikirimkan sama dengan yang diterima		
3	Apliksi dapat menyaring pesan masuk khusus untuk pesan steganografi		
4	Aplikasi dapat menyimpan pesan masuk dan pesan terkirim		
5	Aplikasi dapat mengekstrak kembali pesan rahasia		
6	Apakah pesan dapat membalas sms setelah membaca pesan rahasia		
7	Pesan peringatan untuk validasi tiap-tiap form berfungsi dengan baik		
8	Jika password salah maka pesan rahasia yang ditampilkan bukanlah pesan rahasia yang asli		
9	Format pesan mudah dipahami		
10	Nomor pengirim bias diketahui oleh penerima		

DAFTAR RIWAYAT HIDUP

Nama	: Abdur Rahman
Tempat Tanggal Lahir	: Palembang, 12 Juni 1990
Alamat Asal	: Tegalkuning, RT 01, RW 02, Kec. Banyuurip, Kab. Purworejo
No HP	: +6285725812163 / +6285228050190
Email	: oblo.maman@gmail.com / maman_anteg@yahoo.com
Orang Tua	: Ayah : Parino Ibu : Isbandiyah

Pendidikan Formal :

- SD Negeri Tegalkuning (1995 - 2001)
- SLTP Negeri 1 Purworejo (2001 - 2004)
- SMA Negeri 6 Purworejo (2004 - 2007)
- UIN Sunan Kalijaga Yogyakarta (Angkatan 2007)