BAB IV

HASIL DAN PENGUJIAN

IV.1. Tampilan Hasil

Aplikasi pengujian untuk membandingkan RSA dengan MD5 berdasarkan masing-masing metode yang dimiliki sebagai berikut :

1. Memberikan kemudahan dalam mengamankan pesan dengan metode RSA dan MD5.
2. Memberikan kemudahan dalam sistem mengamankan pesan melalui proses kerja dari masing-masing metode RSA dan MD5.

IV.1.1. Tampilan Menu Utama

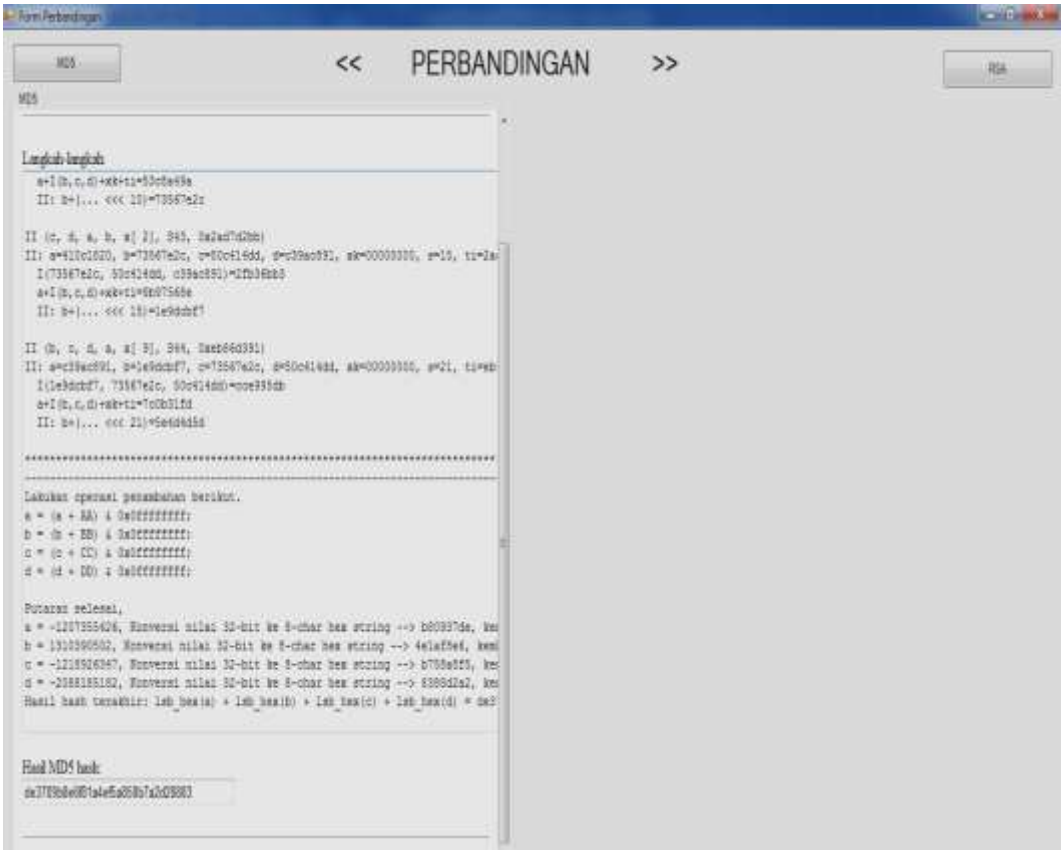
Tampilan menu utama terdiri dari beberapa menu yaitu algoritma dan profil dan keluar, untuk lebih jelasnya dapat dilihat pada gambar IV.1.

Gambar IV.1.Tampilan Menu Utama

Pada Gambar IV.1 menampilkan halaman utama yang terdiri dari beberapa menu, menu *file* digunaka untuk keluar dari aplikasi, menu algoritma untuk masuk kedalam form RSA dan MD5 yang digunakan.

IV.1.2. Tampilan Form MD5

Tampilan halaman form MD5 mempunyai dua tombol perbandingan yaitu tombol MD5 dan tombol RSA. Untuk menampilkan kalkulasi MD5, pengguna klik tombol MD5, untuk lebih jelasnya dapat dilihat pada gambar IV.2.



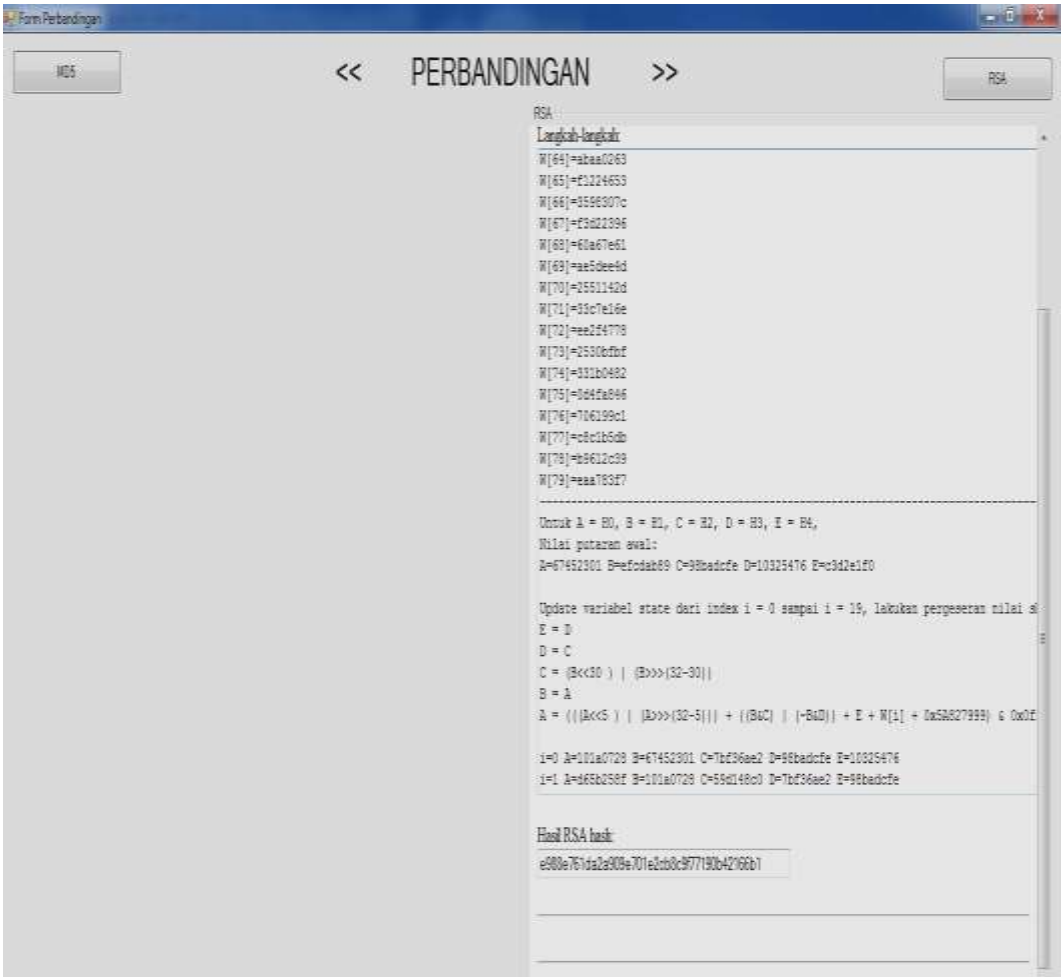
Gambar IV.2. Tampilan Kalkulasi MD5

Pada gambar IV.2 menampilkan pesan ke hash MD5 dengan melakukan langkah-langkah mengubah pesan kedalam bentuk bilangan HEX dengan

beberapa proses perputaran dari masing-masing blok FF, GG, HH, dan II, dengan menekan tombol kalkulasi MD5.

IV.1.3. Tampilan Form RSA

Tampilan halaman form RSA mempunyai dua tombol perbandingan yaitu tombol MD5 dan tombol RSA. Untuk menampilkan kalkulasi RSA, pengguna klik tombol RSA, untuk lebih jelasnya dapat dilihat pada gambar IV.2.



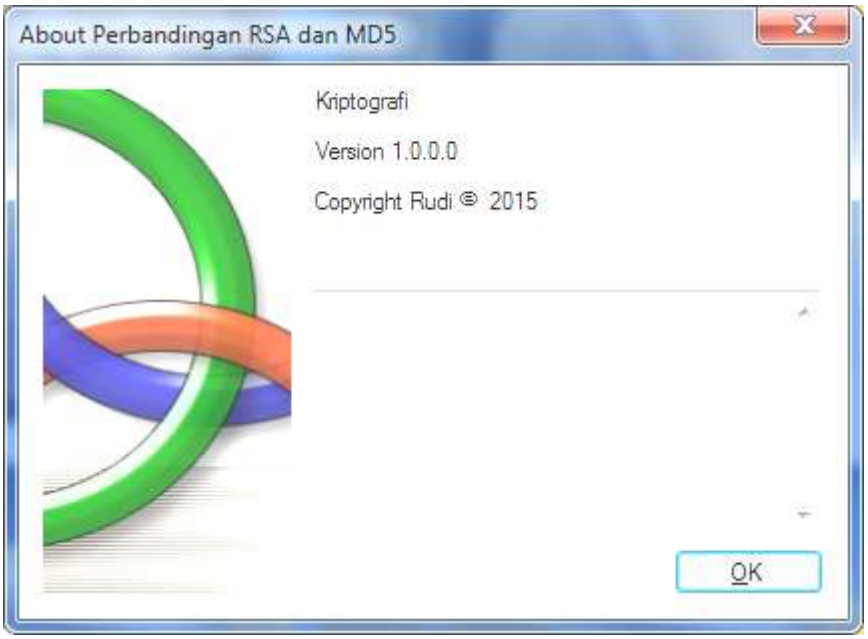
Gambar IV.3. Tampilan Kalkulasi RSA

Pada gambar IV.3 menampilkan pesan ke hash RSA dengan melakukan langkah-langkah mengubah pesan kedalam bentuk bilangan HEX dengan

beberapa proses perputaran dari masing-masing blok A, B, C, dan D dengan menekan tombol kalkulasi RSA.

IV.1.4. Tampilan *About*

Tampilan form *about* menampilkan identitas programmer dan program perbandingan keamanan data RSA dengan MD5, untuk lebih jelasnya dapat dilihat pada gambar IV.4.



Gambar IV.4. Tampilan *About*

Pada tampilan IV.4 ini memberikan informasi kepada pengguna untuk keluar dari form about ini pengguna klik tombol ok.

IV.2. Pengujian

Hasil aplikasi Sistem keamanan data dengan algoritma RSA dan MD5, aplikasi ini dibangun dengan menggunakan visual studio 2010 dan menggunakan

bahasa pemrograman C#. Aplikasi keamanan data dengan membandingkan RSA dan MD5 dengan berupa pesan, kemudian pesan tersebut di hashkan dengan melakukan kalkulasi terhadap kedua metode tersebut.

Dalam pengujian perbandingan antara RSA dan MD5 nantinya diketahui setelah melakukan kalkulasi terhadap kedua metode tersebut dimana perbedaan dari kedua metode tersebut berdasarkan langkah-langkahnya sampai menampilkan hasil dari masing-masing metode tersebut, adapun hasil dari pengujian dapat dilihat pada tabel IV.1.

Tabel IV.1. Daftar Pengujian Perbandingan RSA dan MD5

No	Metode	Kalkulasi ke Hash			
		Pesan	Putaran Akhir LSB	Kalkulasi Akhir Hash	Hasil Akhir
1.	MD5	penulis	a = -1207355426, Konversi nilai 32-bit ke 8-char hex string --> b80937de, kembalikan ke nilai hex LSB --> de3709b8	lsb_hex(a) + lsb_hex(b) + lsb_hex(c) + lsb_hex(d)	de3709b8e6f81a4ef5a858b7a2d28883
			b = 1310390502, Konversi nilai 32-bit ke 8-char hex string --> 4e1af8e6, kembalikan ke nilai hex LSB --> e6f81a4e00000000		
			c = -1218926347, Konversi nilai 32-bit ke 8-char hex string --> b758a8f5, kembalikan ke nilai hex LSB --> f5a858b700000000		
			d = -2088185182, Konversi nilai 32-bit ke 8-char hex string --> 8388d2a2, kembalikan ke nilai hex LSB --> a2d2888300000000		
2.	RSA	penulis	H0 = (H0 + A) & 0x0ffffffff; = -376903839, Konversi ke hex --> e988e761	cvt_hex(H0) + cvt_hex(H1) + cvt_hex(H2) + cvt_hex(H3) + cvt_hex(H4)	
			H1 = (H1 + B) & 0x0ffffffff; = -634744674, Konversi ke hex --> da2a909e		

			H2 = (H2 + C) & 0x0ffffffff; = 1881025720, Konversi ke hex --> 701e2cb8		e988e761da2a909e701e2cb8c9f77190b42166b1
			H3 = (H3 + D) & 0x0ffffffff; = -906530416, Konversi ke hex --> c9f77190		
			H4 = (H4 + E) & 0x0ffffffff; = -1272879439, Konversi ke hex --> b42166b1		

Metode MD5 kalkulasi pesan tidak habis dibagi 4 dan sisa pesanya sebagai *byte padding* lalu nilai *buffer* sebagai penyimpanan putaran AA,BB,CC dan DD lalu Panjang pesan 264 bit jika lebih maka hanya 64 bit yang dimasukan dan diikuti dengan nilai konstanta kemudian melakukan 16 operasi setiap putarannya, putaran CLS ada 4 putaran yaitu FF,GG,HH dan II dengan rumus a = b + ((a + F(b,c,d) + X[k] + T[i]) <<< s) setelah putaran ke 4 di jumlahkan ke a+AA,b+BB,c+CC,d+DD dan terakhir menghasilkan 128 *bit message*.

Sedangkan metode RSA kalkulasi pesan tidak habis dibagi 4 dan sisa pesanya sebagai *byte padding* lalu nilai *buffer* sebagai penyimpanan putaran A, B, C dan D lalu Panjang pesan 960 bit dan diikuti dengan nilai konstanta kemudian panjang menampung array CLS maksimum 79, putaran CLS ada 4 putaran yaitu Putaran $0 \leq t \leq 19$, Putaran $20 \leq t \leq 39$, Putaran $40 \leq t \leq 59$, Putaran $60 \leq t \leq 79$ dan setelah putaran ke 79 di jumlahkan ke H0+A,H1+B,H2+C,H3+D dan terakhir menghasilkan 160 *bit message*.

IV.3. Hasil Perbandingan Antara MD5 dan RSA

Beberapa perbedaan mendasar antara RSA dan MD5 dapat dijabarkan sebagai berikut :

Tabel IV.2. Perbandingan Antara RSA dan MD5

RSA	MD5
Panjang *Message digest* adalah 160 bit.	Panjang *Message digest* adalah 128 bit.
RSA memiliki lima putaran	MD5 memiliki empat putaran
Pesan dengan panjang 448 tetap harus ditambahkan *bit* sehingga panjangnya akan menjadi 960 *bit*	Pesan dengan panjang 448 tetap harus ditambahkan *bit* sehingga panjangnya akan menjadi 264 *bit*
Proses setiap perputaran, rumus yang digunakan berbeda	Proses setiap perputaran, rumus yang digunakan tetap

Sedangkan, ada beberapa kesamaan antara MD5 dan RSA adalah :

1. Konversi setiap 4 *byte* kedalam *word*
2. Menggunakan nilai konstanta.
3. Menggunakan operasi perkalian modulo.

IV.4. Kelebihan Dan Kekurangan Sistem Yang Dirancang

Sistem yang dirancang mempunyai beberapa kelebihan dan kekurangan ketika diterapkan diantaranya :

1. Kelebihan dari sistem yang dirancang :
    a. RSA dan MD5 berfungsi sebagai pendeteksi perubahan pesan ke *hash*
    b. Pesan ke hash tahan terhadap *collision* akibat terjadi penyerangan terhadap pesan.
    c. Sangat lebih detail dalam perubahan data sekecil apapun.

2. Kekurangan dari sistem yang dirancang :
   a. Pada saat proses kalkulasi pesan ke hash RSA sangat lambat jika dibandingan dengan metode RSA.
   b. Putaran CLS RSA sangat panjang dalam array bila dibandingkan dengan MD5.
   c. Nilai konstanta RSA lebih unik jika dibandingkan dengan MD5 karena nilai konstanta awal dalam bentuk HEX.