SISTEM PENYULITAN DAN PENYAHSULITAN MAKLUMAT MENGGUNAKAN ALGORITMA RIVEST SHAMIR ADELMAN

UMMU SYAKIRAH BINTI ZULKEFLY
ZULKARNAIN MD ALI

Fakulti Teknologi & Sains Maklumat, Universiti Kebangsaan Malaysia

ABSTRAK

Projek ini adalah untuk membangunkan sebuah sistem penyulitan dan penyahsulitan maklumat berdasarkan algoritma Rivert-Shamir-Adelman (RSA) yang diperkenalkan pada tahun 1978 oleh Ronald R. Rivert, Adi Shamir dan Leonard M. Adelman. Proses penyulitan dan penyahsulitan yang dilakukan adalah ke atas maklumat dalam format *Text* (*.txt), *Rich Text Format* (*.rtf) dan format nombor. Algoritma RSA ialah suatu teknik dan langkah keselamatan piawai yang digunakan untuk menukar data kepada bentuk yang tidak difahami iaitu teks rahsia sebelum diberikan kepada individu lain. Projek ini secara amnya adalah kajian mengenai teknik penyulitan dan penyahsulitan data menggunakan algoritma RSA. Projek ini dibangunkan menggunakan bahasa pengatucaraan *C Sharp* menggunakan perisian *Microsoft Visual Basic 2010* dan pemprosesan pangkalan data iaitu *Microsoft Access*. Projek ini berdasarkan konsep mesra pengguna yang menggunakan persekitaran tetingkap.

1 PENGENALAN

Perkembangan teknologi kebelakangan ini tumbuh dengan sangat pesat. Perkembangan teknologi ini banyak melahirkan keuntungan yang mempermudah kelangsungan hidup manusia. Tapi seiring dengan berkembangnya teknologi, muncul pula masalah-masalah baru, mulai dari privasi, keamanan, hingga hak cipta. Keselamatan dalam menyimpan sesuatu maklumat adalah sangat penting bagi melindungi maklumat yang mempunyai data yang sulit. Secara umumnya maklumat ialah suatu bentuk penerangan yang dibuat berdasarkan sumber yang diperolehi dalam bentuk data hasil daripada pemprosesan, pengumpulan dan penganalisaan data yang kemudiannya dapat memberi manfaat dan menambah tahap pengetahuan kepada penerima maklumat tersebut. Maklumat boleh didefinisikan sebagai sistem yang menterjemahkan mesej supaya dapat disimpan, mendapatkan kembali dan kemudiannya dimanipulasikan dan akhirnya menjadi sumber akhir yang sedia untuk digunakan. Projek ini menggunakan teknik penyulitan dan penyahsulitan untuk menyembunyikan atau merahsiakan data supaya data tersebut tidak dapat dibaca secara langsung oleh pengguna yang tidak sah.

2 PENYATAAN MASALAH

Masalah pertama ialah kewujudan data disedari oleh pihak luar yang akan menyebabkan data boleh dicuri. Keadaan lebih membimbangkan apabila data dihantar tanpa proses penyulitan atau cara lain untuk menghilangkan kesan kewujudan data tersebut. Sebagai contoh, apabila individu menghantar mesej melalui rangkaian, pihak luar akan sedar penggunaan tersebut kerana sudah jelas apa yang dihantar adalah maklumat penting yang ingin disampaikan kepada penerima. Selain melalui rangkaian, maklumat yang disimpan dalam komputer juga boleh dibaca atau diceroboh oleh pihak lain. Ini seterusnya, mendedahkan data tersebut kepada risiko serangan sama ada untuk mendapatkan data atau mengubah data tersebut. Dengan pelbagai kepakaran pihak luar, kejadian ini tidak mustahil boleh berlaku terhadap maklumat pengguna.

Kedua, masalah data yang tidak dilengkapi atau tiada langsung ciri-ciri keselamatan, berisiko tinggi untuk dibaca. Ini boleh berlaku apabila data tidak melalui proses penyulitan kriptografi sehingga pihak luar boleh terus membacanya tanpa halangan. Ini lebih berbahaya, jika ia melibatkan data penting peribadi seperti nombor akaun, senarai kata laluan, formula produk dan sebagainya. Kecurian data terbabit boleh mendatangkan kerugian dan sebagai contoh bagi data syarikat ia mungkin digunakan untuk meniru strategi, menilai prestasi atau mengganggu pelan syarikat. Syarikat akan kehilangan daya saing kerana maklumat penting diketahui oleh pihak lain, sehingga menimbulkan risiko jangka panjang iaitu kehilangan sumber pendapatan. Jika formula penting sesebuah syarikat dicuri maka, tiada produk yang boleh dihasilkan sehingga pendapatan masa depan turut terjejas. Kajian semula terpaksa dijalankan untuk menghasilkan formula baru atau masa dihabiskan untuk mencari pihak yang mencuri data syarikat.

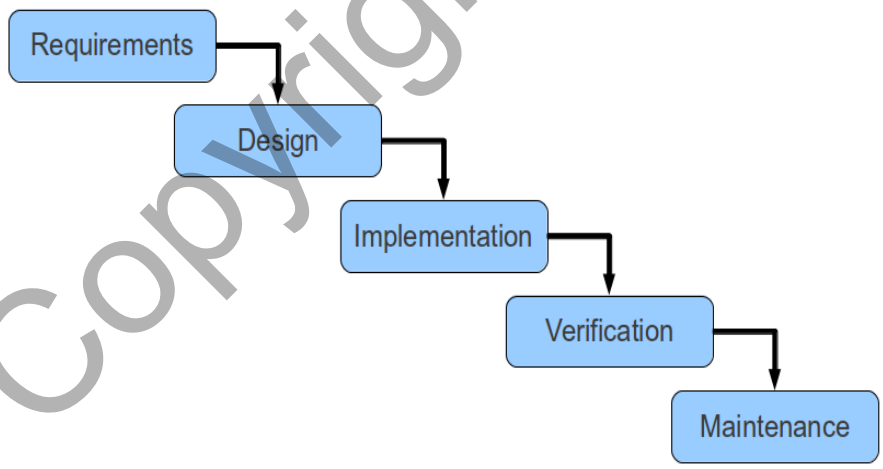
Perkembangan teknologi yang pesat meransang penceroboh menggunakan teknologi untuk mengambil kesempatan untuk mencuri maklumat tanpa izin pemilik maklumat. Oleh itu maklumat yang boleh diceroboh oleh pihak ketiga yang menyebabkan kebocoran maklumat yang seharusnya hanya penerima sahaja yang mengetahui tentang isi maklumat tersebut. Disebabkan itu, pihak ketiga berpotensi untuk menyebarkan maklumat ke seluruh media. Perkara ini tidak seharusnya berlaku jika pengguna memastikan keselamatan dalam komunikasi sebelum menghantar mesej kepada penerima.

3 OBJEKTIF KAJIAN

Projek ini bertujuan memperkenal sistem perlindungan terhadap data yang penting dari dicuri oleh pihak lain. Secara umum objektif kajian adalah menghasilkan sistem yang boleh menukarkan maklumat yang ingin dilindungi daripada orang lain kepada bahasa yang tidak difahami. Konsep ini dapat meningkatkan keselamatan data dari diceroboh oleh pengguna yang tidak dibenarkan. Kertas ini membincang tentang projek pembangunan sistem penyulitan dan penyahsulitan yang menggunakan algoritma RSA.

4 METOD KAJIAN

Penggunaan sistem pembangunan yang sesuai penting untuk memastikan perjalanan projek berjalan dengan lancar dan menjamin hasil kerja yang berkualiti. Sistem yang akan dibangunkan ini adalah berasakan kepada Modul Kitar Hayat Pembangunan Sistem (System Development Life Cycle) atau lebih dikenali sebagai Air Terjun (Waterfall Model). Model ini melibatkan beberapa fasa seperti fasa projek analisis sistem, rekabentuk, implementasi, pengujian dan penyelenggaraan. Model Kitar Hayat Pembangunan Sistem ini adalah seperti yang terdapat dalam Rajah 1.



Rajah 1. Modul Kitar Hayat Pembangunan Sistem (Model Air Terjun)

Pada peringkat analisis, segala maklumat projek yang akan dibangunkan hendaklah dikumpulkan dengan teliti bagi membolehkan projek disiapkan pada masa yang ditetapkan. Antara jangkaan yang perlu dibuat ialah seperti mengenal pasti tujuan dan objektif projek ini dibangunkan serta masalah yang timbul. Segala data yang berkaitan dengan projek ini akan

dikumpulkan untuk dianalisis dan disusun. Seterusnya perisian-perisian yang akan digunakan serta perkakasan yang akan digunakan dikenalpasti agar perisian-perisian dan alatan yang digunakan adalah bersesuaian dengan projek yang akan dibangunkan.

Fasa seterusnya ialah fasa rekabentuk. Pada peringkat ini, rekabentuk antara muka sistem ditetapkan. Contoh antara muka yang terlibat ialah seperti antara muka input dan antara muka output serta rekabentuk lain yang lebih terperinci. Rekabentuk antara muka haruslah direka dengan jelas agar interaksi pengguna dengan perjalanan sistem adalah lebih jelas dan tidak mengelirukan pengguna dan menyenangkan pengguna menggunakan sistem yang dibangunkan.

Seterusnya ialah fasa implementasi dimana pada peringkat ini sistem akan dibangunkan menggunakan perisian dan peralatan yang telah dipilih pada peringkat awal lagi. Sistem yang telah dibangunkan akan diuji bagi mengenalpasti masalah serta kelemahan sistem yang mungkin dapat diatasi. Peringkat ini dapat menentukan sama ada memenuhi skop dan objektif yang telah ditetapkan.

Pada peringkat pengujian pula sistem akan diuji oleh beberapa pengguna untuk menguji tahap pencapaian sistem yang telah dibuat penambahbaikkan. Pengguna akan mengikut langkah-langkah yang telah diarahkan untuk menguji sistem. Pemilihan perkakasan dan persisian yang tidak tepat boleh menjejas hasil projek. Spesifikasi keperluan perkakasan yang diguna untuk menghasil rekaan sistem adalah perkakasan asas sesebuah komputer. Senarai spesifikasi keperluan perkakasan yang dicadang untuk menghasil visualisasi sistem letak kereta automatik adalah seperti berikut:

i. Sistem Pengoperasian: Microsoft® Windows® XP Professional (SP3 atau ke atas)
ii. Pemproses Intel Core i3
iii. Ingatan capaian rawak 128 MB
iv. Papan kekunci dan Tetikus

Spesifikasi keperluan perisian yang diguna untuk membangunkan sistem penyulitan dan penyahsulit dengan menggunakan Microsoft Visual Studio. Visual Studio 2010 merupakan suatu peringkat yang dapat digunakan untuk pengembangan pelbagai aplikasi

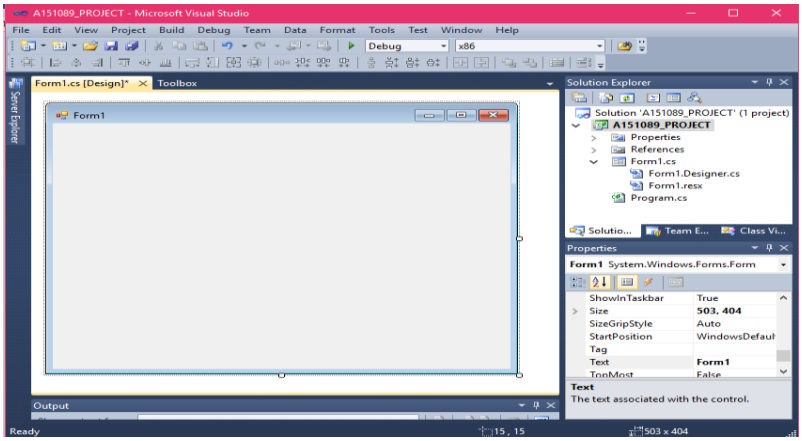
yang memiliki berbagai macam jenis. Antaranya aplikasi (Windows Form, CommandLine (Console)), Aplikasi Web, Windows Mobile (Poket PC).

Visual Studio 2010 memiliki lebih dari satu kompiler, SDK (Software Development Kid), dan Dokumentasi Tutorial (MSDN Library). Kompiler yang dimasukkan kedalam Visual Studio 2010 antara lain Visual Basic, Visual C#, Visual C++, Visual InterDev, Visual J++, Visual F#, dan Visual Source Safe, dan sebagainya. Semuanya itu sudah diperuntukkan kedalam platform .Net Framework 4.0 atau versi yang lebih tinggi.

Peringkat yang seterusnya ialah peringkat penyelenggaraan dimana ia merupakan peringkat yang terakhir dalam Model Kitar Hayat Pembangunan Sistem. Pada peringkat ini, semua maklumat dan hasil kerja semasa pembangunan sistem akan dikumpulkan dan akan diselenggara semula mengikut hasil dari pengguna yang telah diuji semasa menggunakan sistem ini.

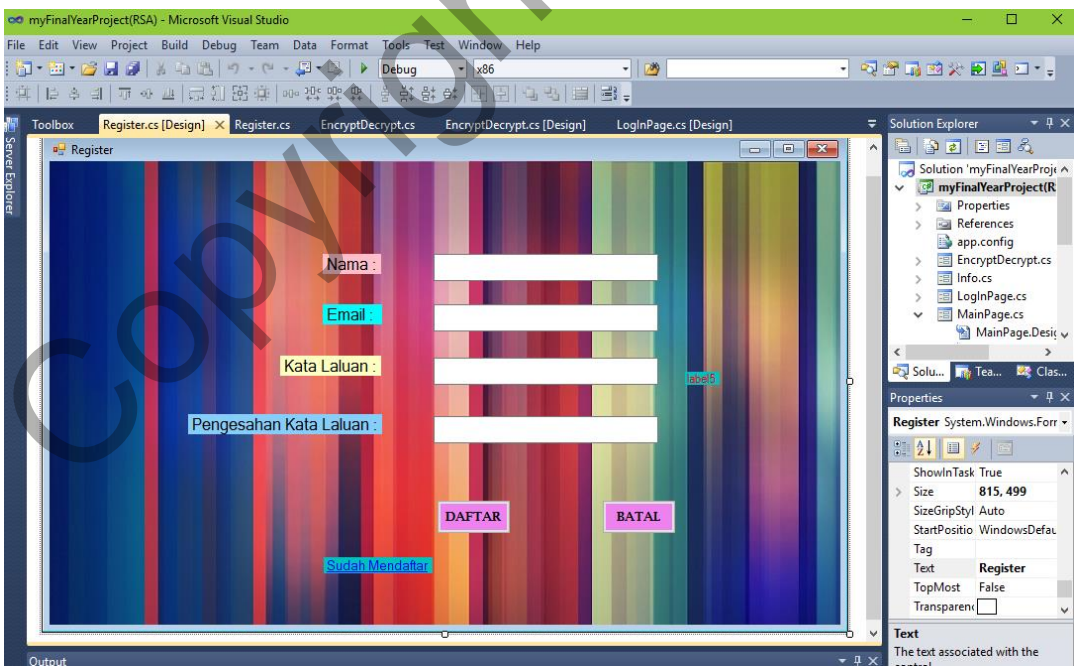
5 HASIL KAJIAN

Bahagian ini membincang hasil daripada proses pembangunan penyulitan dan penyahsulitan maklumat menggunakan algoritma RSA. Penerangan yang mendalam tentang reka bentuk antaramuka sistem penyulitan dan penyahsulitan maklumat. Fasa reka bentuk adalah fasa yang penting dalam pembangunan projek. Dalam projek ini, perisian Microsoft Visual Studio diguna untuk mereka bentuk antaramuka sistem penyulitan dan penyahsulitan maklumat. Antaramuka yang direka kemudiannya menjalankan reka bentuk dengan tujuan menunjukkan cara operasi proses menyulit dan menyahsulit data yang dimasukkan pengguna. Reka bentuk antaramuka sistem dihasilkan dalam bentuk tetingkap. Seterusnya pengujian terhadap reka bentuk sistem dijalankan untuk memasti hasil pembangunan adalah selaras dengan objektif yang ditetapkan sebelumnya. Antaramuka sistem dihasilkan dalam bentuk tetingkap dihasil dengan menggunakan perisian Microsoft Visual Studio. Secara umum, reka bentuk antaramuka sistem kepada dua bahagian utama, iaitu bahagian pendaftaran masuk sistem dan bahagian proses penyulitan dan penyahsulitan dijalankan. Antaramuka bagi reka bentuk sistem dirangkakan dalam bentuk tetingkap seperti yang ditunjukkan dalam Rajah 2. Antaramuka ini adalah gambaran permulaan sebelum meletakkan sebarang fungsian.



Rajah 2. Antaramuka bentuk tetingkap

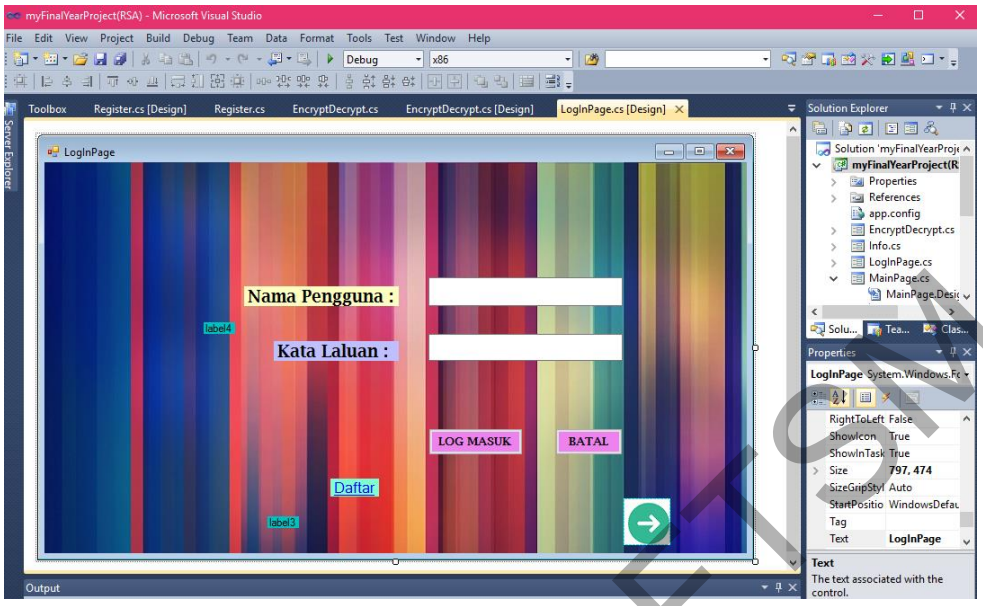
Reka bentuk antaramuka sistem ini ditunjukkan dalam Rajah 3. Kerja reka bentuk anatramuka sistem ini tidak memerlukan model atau protoaip untuk menyelesaikannya. Oleh itu, merekabentuk sistem ini tidak memerlukan masa yang panjang. Rajah 3 merupakan bahagian pendaftaran pengguna bagi pengguna yang belum mendaftar ke dalam sistem. Pendaftaran maklumat pengguna memerlukan nama, email, kata laluan dan pengesahan kata laluan. Kemudian maklumat tersebut akan direkod dalam pangkalan data sistem.



Rajah 3. Antaramuka Pendaftaran Baru

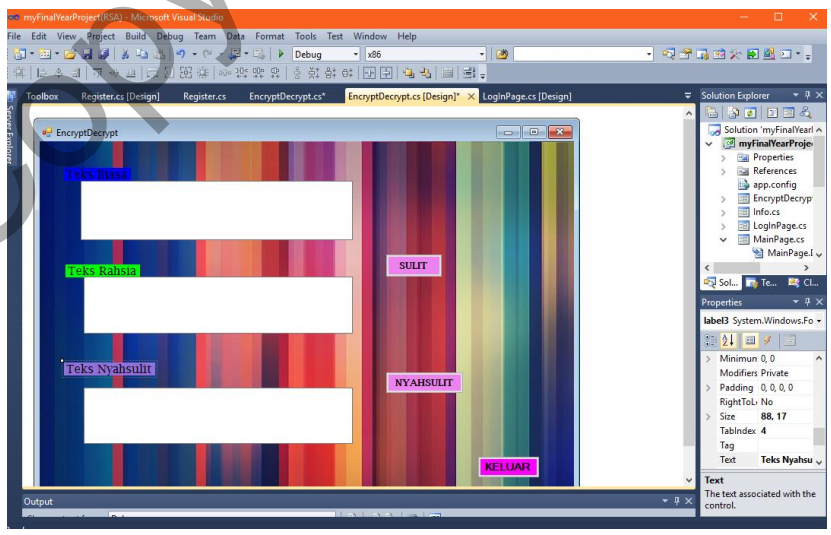
Reka bentuk antaramuka sistem yang seterusnya ini ditunjukkan dalam Rajah 4. Rajah 4 merupakan bahagian pengenalan identiti pengguna sistem. Pada bahagian ini memerlukan

maklumat pengguna iaitu email dan kata laluan yang telah didaftarkan. Bagi pengguna yang tidak berdaftar, tidak boleh menggunakan sistem ini.



Rajah 4. Antaramuka Pengenalan Identiti

Reka bentuk antaramuka bahagian akhir dalam sistem ini ditunjukkan dalam Rajah 5. Rajah 5 merupakan bahagian proses penyulitan dan penyahsulitan maklumat dilaksanakan. Pada ruang teks biasa adalah maklumat pengguna yang ingin ditukarkan kepada bahasa yang tidak difahami. Pada ruang teks rahsia adalah maklumat pengguna yang telah ditukarkan dalam kod rahsia. Pada ruang teks nyahsulit merupakan hasil proses penyahsulitan dari kod rahsia kepada bahasa yang difahami.



Rajah 5. Antaramuka Penyulitan dan Penyahsulitan

Persekitaran dihasil dengan menggunakan pelaksanaan algoritma rsa. Komponen yang melakukan pengendalian disusun pada di lokasi yang tepat selaras dengan reka bentuk yang bersesuaian. Rajah 6 menunjukkan hasil paparan tetingkap proses penyulitan maklumat bentuk teks.

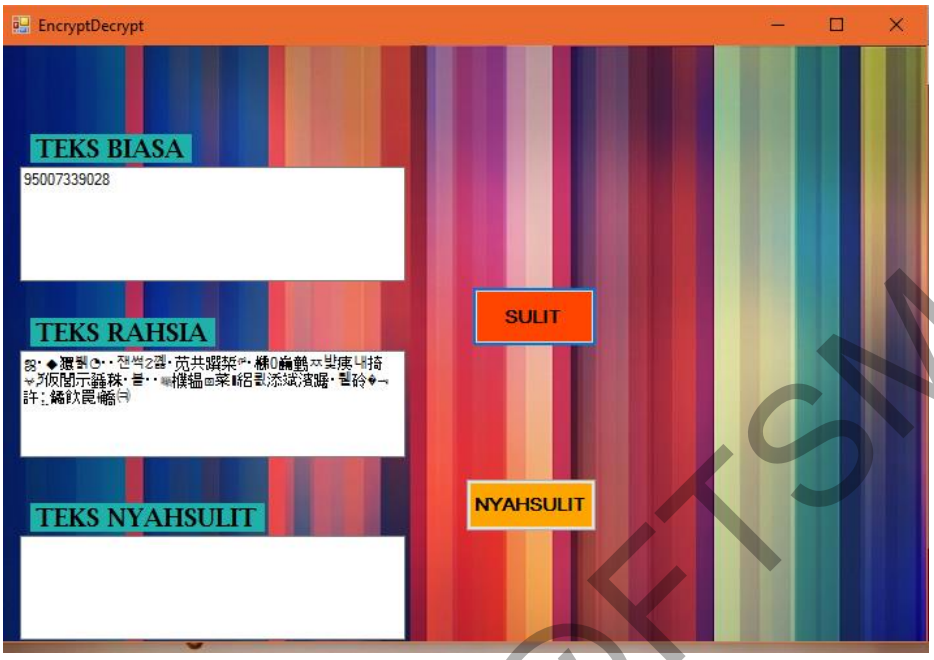
Rajah 6. Hasil paparan tetingkap proses penyulitan (teks)

Persekitaran dihasil dengan menggunakan pelaksanaan algoritma rsa. Komponen yang melakukan pengendalian disusun pada di lokasi yang tepat selaras dengan reka bentuk yang bersesuaian. Rajah 7 menunjukkan hasil paparan tetingkap proses penyahsulitan maklumat bentuk teks. Pertukaran dalam bentuk teks rahsia kepada maklumat asal.

Rajah 7. Hasil paparan tetingkap proses penyahsulitan (teks)

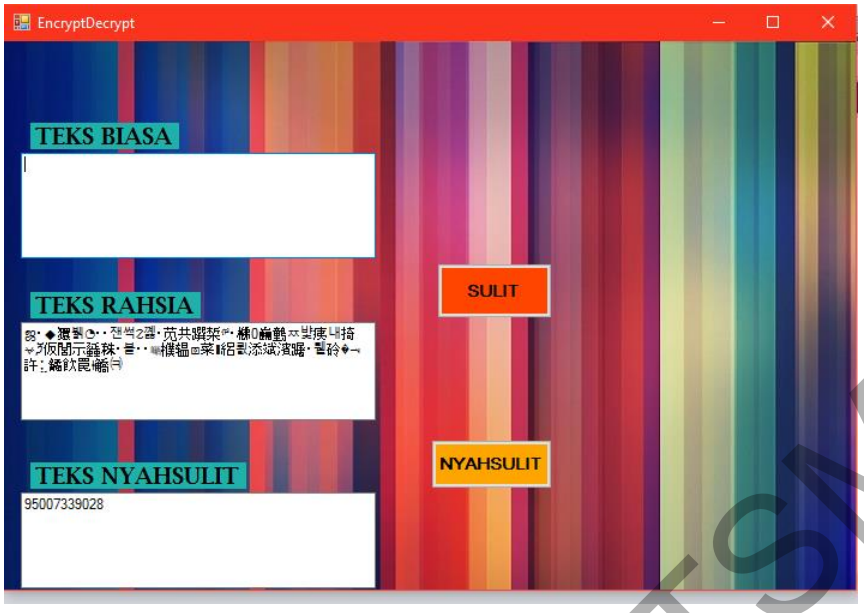
Rajah 8 menunjukkan hasil paparan tetingkap proses penyulitan maklumat bentuk nombor. Pada bahagian ini proses penyulitan bagi maklumat format nombor kepada bahasa

yang tidak difahami. Dengan cara ini, pengguna tidak perlu bimbang jika mahu menyimpan nmaklumat nombor yang penting sama ada dalam bentuk salinan keras atau salinan lembut.

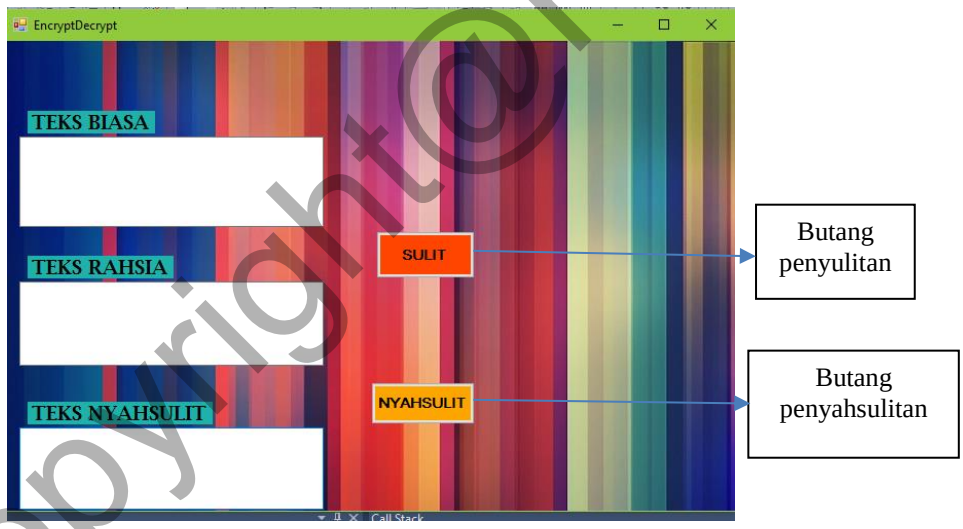


Rajah 8. Hasil paparan tetingkap proses penyahsulitan (nombor)

Rajah 9 menunjukkan hasil paparan tetingkap proses penyahsulitan maklumat bentuk maklumat yang tidak difahami. Pada bahagian ini proses penyahsulitan bagi maklumat format nombor kepada maklumat. Oleh itu, pengguna boleh mendapatkan semula maklumat yang mereka lindungi. Rajah 10 pula menunjukkan hasil paparan tetingkap dimana proses penyulitan dan penyahsulitan maklumat beroperasi. Pada bahagian ini menunjukkan pengendalian bagi butang sulit dan nyahsulit dalam melaksanakan proses penyulitan dan penyahsulitan tersebut.



Rajah 9. Hasil paparan tetingkap proses penyahsulitan (nombor)



Rajah 10. Pengendalian butang sulit dan nyahsulit

Pengujian sistem perlu dijalankan selepas pembangunan sistem untuk memasti aplikasi berfungsi dengan baik dan menepati speksifikasi yang ditetapkan. Antara pengujian yang diuji adalah dari segi kebolehan penyulitan dan penyahsulitan dijalankan berdasarkan maklumat yang pengguna masukkan.

6 KESIMPULAN

Sistem penyulitan dan penyahsulitan maklumat yang menggunakan algoritma rsa ini dijangka dapat membantu meningkat keselamatan pengguna dalam melindungi maklumat dari pihak yang tidak bertanggungjawab. Sistem ini memain peranan penting di negara yang sedang membangun dengan pelbagai teknologi yang boleh disalahguna bagi orang yang tidak perisian proses Penyulitan dan Penyahsulitan Maklumat dengan Menggunakan Algoritma RSA ini telah dibangunkan mengikut keperluan yang diinginkan. Perkasa asas yang diperlukan telah berjaya dipenuhi. Namun sekiranya terdapat penambahan fungsian, ia perlu melakukan beberapa kajian terlebih dahulu supaya fungsian tersebut tidak menggangu atau tidak memberi kesan terhadap fungsian yang telah sedia ada. Diharapkan dengan menggunakan sistem ini, masalah pencerobohan maklumat dapat dikurangkan dan dapat memberi manfaat kepada semua pihak yang menggunakannya. Fungsi yang mesra pengguna dalam perisian Microsoft Visual Studio dapat mencepat dan memudah pembangunan kerja reka bentuk. Akibat kekurangan pengalaman dalam penggunaan perisian ini, pelbagai tutorial dan latihan dijadikan rujukan bagi menyempurna projek ini.