SISTEM KOMUNIKASI BERDASARKAN ALGORITMA PENYULITAN AES

NUR SAIYIDATUL AFIFAH BINTI HALIM
HAFIZ MOHD SARIM

Fakulti Teknologi & Sains Maklumat, Universiti Kebangsaan Malaysia

ABSTRAK

Kriptografi ataupun lebih dikenali sebagai tulisan rahsia adalah salah satu alat yang lazim digunakan untuk mengawal sebarang ancaman serta gangguan yang diterima oleh komputer. Pembangunan sistem komunikasi ini dibangunkan adalah berdasarkan kepada algoritma penyulitan AES iaitu kriptografi simetri. Algoritma ini diiktiraf sebagai Advance Encryption Standard, AES pada masa kini. Algoritma ini terkenal dengan tahap keselamatan yang tinggi dan kemudahannya. Projek ini akan membincangkan tentang konsep, senibina ciri-ciri keselamatan yang dilaksanakan dalam Sistem Komunikasi Berdasarkan Algoritma Penyulitan AES (Crypt Chat) bagi mencapai komunikasi yang selamat dan mengekalkan kerahsiannya. Pembangunan sistem ini dibangunkan berasaskan laman web dan menggunakan rangka kerja pembangunan web terkini iaitu PHP dan data disimpan di dalam phpMyAdmin. Adalah diharapkan sistem komunikasi ini dicipta untuk membantu pengguna meningkatkan tahap keselamatan dan memastikan mod selamat dalam berkomunikasi antara dua pengguna. Secara keseluruhannya, pembangunan Sistem Komunikasi Berdasarkan Algoritma Penyulitan AES(Crypt Chat) ini berjaya dibangunkan.

PENGENALAN

Alat komunikasi telah banyak memudahkan kehidupan manusia dari segala aspek tidak kira dimana kita berada sama ada jarak jauh atau dekat. Komunikasi membolehkan perpindahan mesej dari satu pengguna kepada pengguna lain melalui pelbagai jenis media yang sudah menjadi kebiasaan pada masa kini. Pengiriman data atau mesej melalui jaringan elektronik ini memerlukan kepada suatu proses yang menjamin keselamatan serta kerahsiaan daripada pengguna yang mengirimkan maklumat tersebut.

Data atau maklumat tesebut seharusnya bersifat rahsia atau sulit selama mana proses pengiriman dijalankan dan juga seharusnya asli pada saat penerimaan berlaku. Sewaktu perpindahan data, data terdedah kepada pelbagai ancaman dari pencerobohan kecurian data. Kaedah penyulitan dan penyahsulitan yang dikenali sebagai kriptografi merupakan salah satu penyelesaian dalam proses pengiriman data atau mesej melalui jaringan elektronik pada masa kini.

Teknologi utama yang digunakan dalam pembangunan sistem ini ialah kriptografi. Kriptografi ini digunakan bagi mengelakkan pihak tertentu yang tidak berhak untuk memintas komunikasi sistem sehingga kerahsiaan sesuatu maklumat atau data dapat dilindungi. Dalam penyelidikan, kriptografi digunakan semasa mengirim dan menerima pesanan.

Penghasilan sistem komunikasi berdasarkan kriptografi penyulitan ini adalah bertujuan untuk membantu serta mengatasi masalah pengguna sewaktu berkomunikasi dengan pengguna lain secara rahsia dan selamat kerana ia menggunakan kaedah penyulitan data. Oleh itu, dengan adanya kemudahan penyulitan data, ia dapat membantu serta memberi keyakinan kepada pengguna dalam berkomunikasi dalam rangkaian Internet.

PENYATAAN MASALAH

Jaringan Internet dan rangkaian membolehkan perpindahan data dari satu komputer kepada suatu komputer yang lain. Pengiriman maklumat serta data melalui jaringan ini memerlukan kepada suatu mekanisme keselamatan agar data atau maklumat yang ingin disampaikan tidak dapat dibaca, diubahsuai atau dipalsukan.

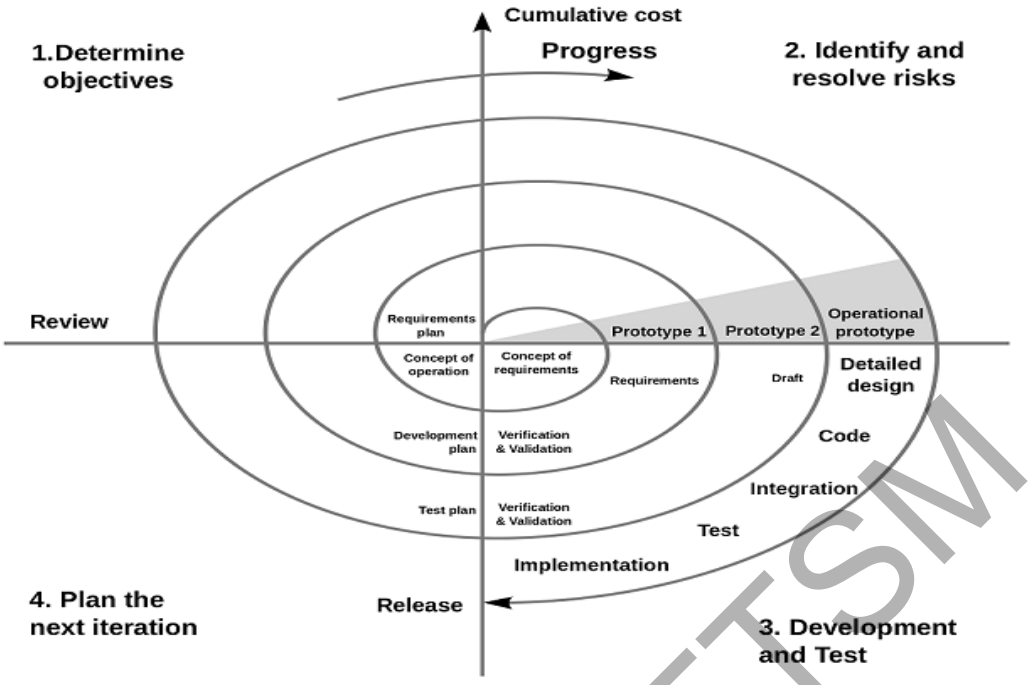
Perisian-perisian mesej ringkas dan mel elektronik awam sering terdedah kepada aktiviti pengintipan dan pencerobohan oleh pihak tertentu ketika dalam menyampaikan maklumat dan data. Selain itu, kecurian data-data penting seperti nombor kad pengenalan, nombor akaun bank dan alamat emel juga sering berlaku yang menyebabkan pengguna berasa ragu untuk berkongsi maklumat mahupun data rahsia menerusi rangkaian atau Internet.

OBJEKTIF KAJIAN

Objektif pembangunan sistem ini ialah untuk membangunkan satu sistem komunikasi antara dua pengguna bagi menyampaikan data dan maklumat secara selamat dan rahsia. Data dan maklumat disimpan menggunakan kaedah penyulitan data yang menjadi piawaian semasa. Konsep ini dapat meningkatkan lagi tahap keselamatan dan kerahsiaan dalam sesuatu perbualan.

METODOLOGI KAJIAN

Penggunaan model pembangunan yang sesuai penting untuk memasti perjalanan projek berjalan dengan lancar dan menjamin hasil kerja yang berkualiti. Bagi memastikan kajian berjalan dengan lancar, kajian ini menggunakan Pendekatan Pembangunan Spiral yang juga dikenali sebagai Model Kitar Hayat Spiral. Model ini adalah hasil daripada gabungan model prototaip dan model air terjun dalam pembangunan suatu sistem. Model Kitar Hayat Spiral adalah satu kaedah pembangunan sistem (SDLC) yang membantu pembangun sistem dalam mewujudkan perisian langkah demi langkah. Peringkat-peringkat dalam model kitar hayat spiral adalah seperti yang ditunjukkan dalam Rajah 1.



Rajah 1 Model Kitar Hayat Spiral

Sumber : ("Explain the Spiral Model - Testing" 2012)

Beberapa kebaikan dapat disenaraikan untuk penggunaan metadologi Model Air Terjun secara pratikal. Antaranya adalah seperti berikut :

i) Mengintegrasikan pembangunan dan penyenggaraan.
ii) Model ini memfokuskan perhatian terhadap penghapusan kesilapan pada peringkat awal.
iii) Model ini menghasilkan suatu rangka kerja untuk pembangunan perisian.

Fasa Perancangan

Pada fasa ini, pengenalpastian pada tempoh waktu untuk pengendalian projek kajian ini dalam dua semester. Dengan pelan perancangan carta Gantt dibina untuk memastikan segala tindakan untuk projek kajian mampu dibangunkan dengan masa yang diberikan.

Fasa Analisis

Analisis pada pemahaman latar belakang, pengenalpastian masalah, skop, objektif, penyelesaian masalah dan metodologi yang perlu dilakukan dalam projek kajian ini berlaku di dalam fasa ini. Dengan itu, keperluan spesifikasi sistem dapat dilakukan dengan mudah apabila objektif untuk kajian ini telah jelas. Pemilihan reka bentuk dan pengimplementasi strategi juga turut dilakukan dengan merancang prototaip pertama pada fasa ini.

Fasa Reka Bentuk

Fasa ini adalah fasa yang penting dalam keseluruhan projek yang mana ia untuk memberi gambaran bagi memulakan fasa pembangunan sistem. Untuk menghasilkan Spesifikasi Rekabentuk Sistem , Keperluan Spesifikasi Sistem akan digunakan dalam mereka bentuk keperluan pengguna. Penghasilan reka bentuk perlu menepati ciri-ciri sistem komunikasi Crypt Chat yang akan dibangunkan. Oleh itu, fungsi utama yang dititikberatkan adalah penghantaran, penerimaan, penyulitan serta penyahsulitan mesej.

Fasa Pembangunan

Pada fasa ini, pembangunan sistem akan berpandukan Spesifikasi Rekabentuk Sistem dan Keperluan Spesifikasi Sistem. Pembangunan ini akan berasaskan laman web dan akan menggunakan bahasa pengaturcaraan PHP dan data disimpan di dalam phpmyAdmin.

Fasa Pengujian

Fasa ini bertujuan menguji fungsi kritikal dalam sistem. Penglibatan fungsi kritikal selaras dengan objektif projek. Kegagalan yang berlaku pada fungsi kritkal memberi impak yang besar pada projek ini. Sekiranya gagal mencapai objektif pada fasa perancangan pengulangan pertama, penyelarasan perlu dijalankan atau mengimbas kembali dengan merancangkan prototaip kedua pada fasa perancangan pengulangan kedua bergantung pada jenis kegagalan yang berlaku bagi membuat penambahbaikan kajian yang mendalam.

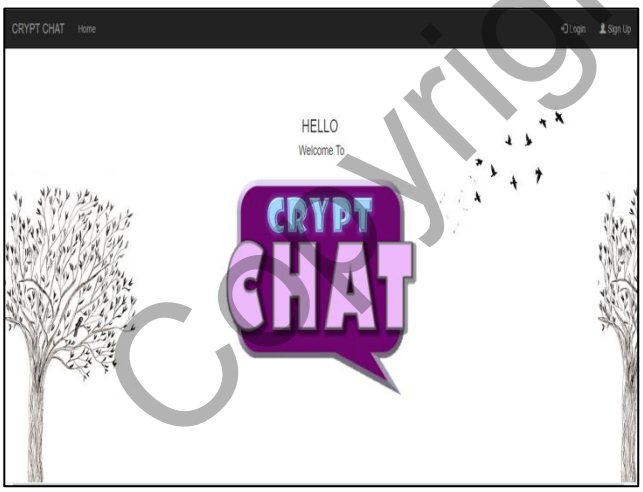
HASIL KAJIAN

Bahagian ini membincang hasil daripada proses pembangunan sistem komunikasi berdasarkan algoritma penyulitan AES. Penerangan secara keseluruhan tentang reka bentuk dan pembangunan sistem yang telah dihasilkan dalam projek ini diperihalkan. Sistem ini diberi nama Crypt Chat iaitu sistem komunikasi yang menggunakan kaedah penyulitan. Sistem Crypt Chat ini telah menggunakan kaedah penyulitan algoritma yang terkenal iaitu Advanced Encryption Standard(AES). Algoritma penyulitan ini menggunakan kunci rahsia untuk menyulit dan menyahsulit mesej bagi menjamin persekitaran komunikasi yang selamat dan rahsia. Fungsian penyulitan mesej ini merupakan fungsian yang paling utama yang ingin diketengahkan kerana ia melibatkan tahap keselamatan dan kerahsiaan sesuatu mesej. Beberapa pengujian perkataan dilakukan bagi mengenal pasti tahap keselamatan mesej iaitu nilai patah perkataan, teks dari segi abjad, nombor dan simbol seperti pada Rajah 2. Pengujian ini diambil kira dari segi keputusan penyulitan yang konsisten dan kebolehan dalam melakukan proses penyulitan dalam jumlah teks yang besar. Kemudian, kaedah ini diimplimentasikan ke dalam sistem Crypt Chat.

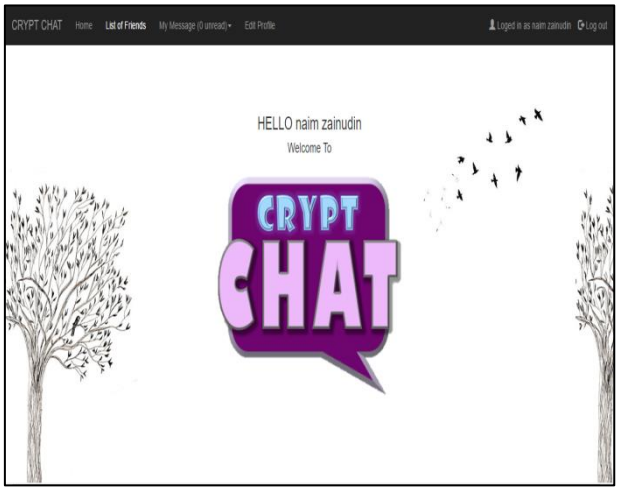
```
Plain Text     = Hello
Encrypted Text = VE5IbUVUUGxBL1pXdk8zWU45RWkzdz09


Plain Text     = Hello.My name is Alice. I am 22 years old. I love programming so much.
Encrypted Text = TVgrb201T1lGUzVXZ2dWbEU2eXNpR21GcE53MGJHQkZmaEhuZHp6QV1Q
                 LzJhTHF3eWwzQitsdWJHdEQ0bUpYYm5PRDZzOE1tWGozT1lXUFpuMnpuaXcybDhISVBpc3RzN
                 UpLcUJwNmpUQ1k9


Plain Text     = A
Encrypted Text = YkZtREhkWEpmTVIxSWZiR1h6a0loZz09


Plain Text     = a
Encrypted Text = dFJDM3pRSnVjdHRtdEFkRVBDMEFXdz09


Plain Text     = 45
Encrypted Text = RWlBMnRxT0hVK1poSUlSb0tLK1JJZz09


Plain Text     = #,?
Encrypted Text = K21IVG5HOHkrNW03S2o2U3BMUF1DUT09
```

Rajah 2 Hasil Pengujian Penyulitan AES

Rajah 3 merupakan antara muka menu hadapan sistem Crypt Chat sebaik sahaja pengguna mengakses sistem ini pada pelayar web. Manakala, selepas pengguna berjaya log masuk sistem, antara muka menu utama akan dipaparkan. Perbezaan kedua-dua laman menu ini adalah dari segi butang yang terdapat pada navigasi bar yang mana ia membolehkanpengguna pergi ke laman seterusnya. Rajah 4 menunjukkan antara muka menu utama sistem Crypt Chat.

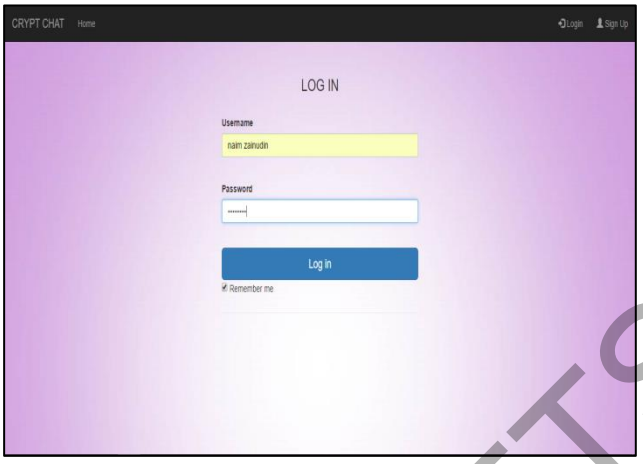


Rajah 3 Menu Hadapan Sistem Crypt Chat



Rajah 4 Menu Utama Crypt Chat

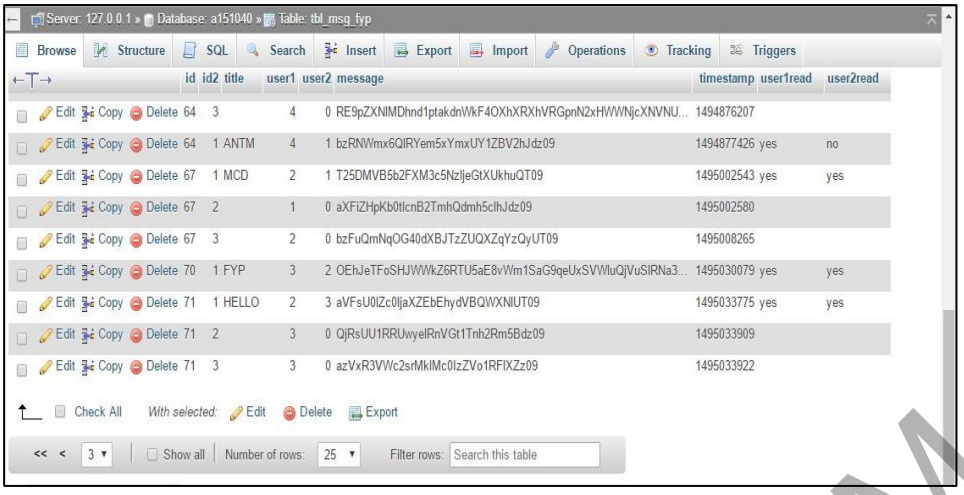
Pada fungsian pendaftaran, pengguna dapat mengisi borang pendaftaran pada laman tersebut dan ianya berjaya disimpan ke dalam pangkalan data maklumat pengguna. Rajah 5 menunjukkan antara muka bagi pendaftaran. Seterusnya, bagi memastikan pengguna dapat memasuki sistem, pengguna dikehendaki untuk log masuk ke sistem seperti pada Rajah 6. Fungsian log masuk dapat mengesahkan maklumat pengguna yang telah diisi.



Rajah 5 Pendaftaran Sistem Crypt Chat

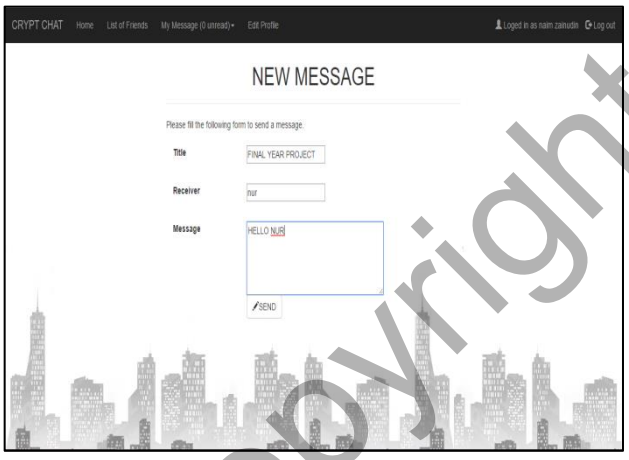
Rajah 6 Log Masuk Sistem Crypt Chat

Pada fungsian perbualan peribadi, fungsian ini melibatkan beberapa proses seperti menghantar dan menerima mesej dalam keadaan teks biasa. Dalam laman perbualan peribadi ini jugalah proses penyulitan dilakukan yang mana apabila pengguna menghantar mesej dalam teks biasa, mesej tersebut akan disulit dan kemudian disimpan ke dalam pangkalan data seperti yang ditunjukkan pada Rajah 7.

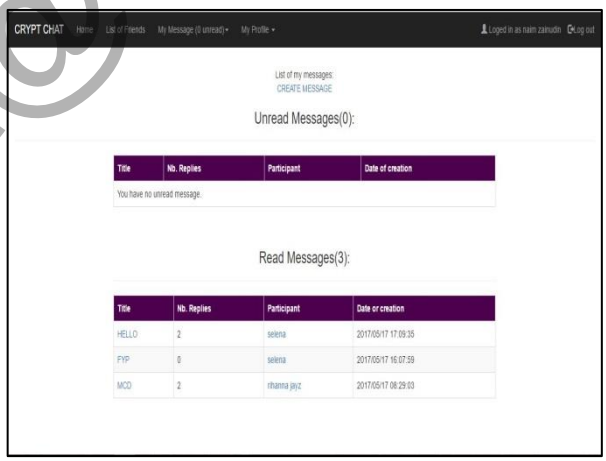


Rajah 7 Pangkalan Data Mesej Crypt Chat

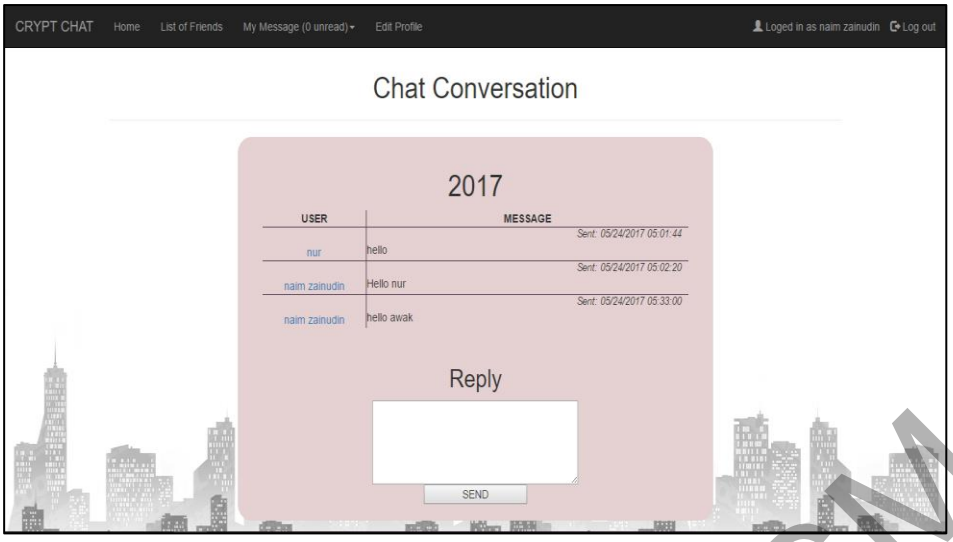
Sebelum pengguna menerima mesej, mesej teks sulit dari pangkalan data mengalami proses penyahsulitan telah berjaya dilakukan yang menyebabkan pengguna menerima mesej dalam keadaan teks biasa semula. Berikut merupakan laman yang terlibat dalam mencapai fungsian perbualan peribadi.



Rajah 8 Laman Cipta Mesej Crypt Chat



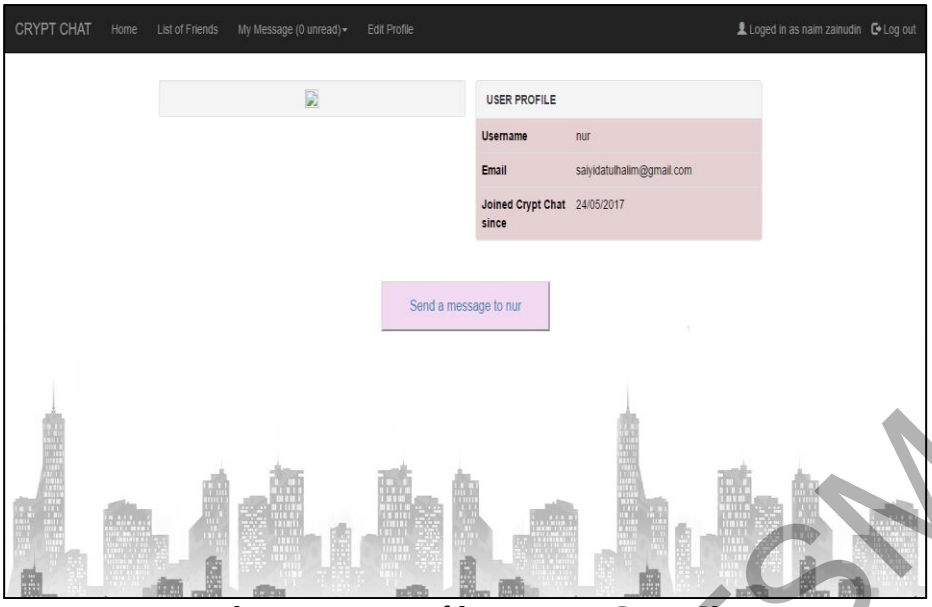
Rajah 9 Laman Senarai Perbualan Mesej Crypt Chat



Rajah 10 Laman Perbualan Crypt Chat

Selain itu, terdapat beberapa fungsian tambahan lain yang dilaksanakan seperti membuat pengubahsuaian terhadap maklumat diri pengguna seperti nama, emel dan kata laluan. Di samping itu, antara fungsian lain yang terlibat ialah paparan profil yang mana pengguna dapat melihat profil pengguna lain. Walau bagaimanapun, dalam fungsian ini sistem tidak dapat memaparkan gambar profil pengguna kerana terdapat masalah dalam memuat naik gambar pada pangkalan data.

Rajah 11 Laman Pengubahsuaian Maklumat Crypt Chat



Rajah 12 Laman Profil Pengguna Crypt Chat

Secara keseluruhannya, hampir kesemua fungsian Sistem Crypt Chat berjaya diuji serta memenuhi objektif kajian sistem ini dan hanya fungsian tambahan sahaja gagal dilaksanakan.

KESIMPULAN

Sistem Komunikasi Berdasarkan Penyulitan Kriptografi (Crypt Chat) adalah sebuah sistem yang dibangunkan bagi menjaga tahap keselamatan serta kerahsiaan sesuatu mesej ketika berkomunikasi atau berbual melalui jaringan Internet. Sistem ini berupaya untuk membuat proses penyulitan terhadap mesej yang disimpan dengan menggunakan kaedah penyulitan piawai semasa dan mesej tersebut hanya diketahui antara komunikasi dua pengguna sahaja. Oleh demikian, sistem ini berjaya dibangunkan walau bagaimanapun pada masa awal pembangunan terdapat masalah berlaku ketika ingin membuat pemilihan tentang kaedah penyulitan yang digunakan serta rangka kerja pembangunan web yang sesuai. Pengaturcaraan bagi sistem ini sedikit rumit kerana masih baru mempelajari cara pengekodan tersebut. Oleh itu, kebanyakan masa terbahagi kepada pemahaman terhadap proses penyulitan dan bahasa pengaturcaraan dan pembangunan tetapi dengan penyelidikan dan kajian terperinci, sistem ini akhirnya berjaya dibangunkan.

RUJUKAN

Gary C. Kessler. 2017. An Overview of Cryptography. http://www.garykessler.net/library/crypto.html [13 May 2017].

Yuniati, V., Indriyanta, G. & Rachmat, A. 2009. ENKRIPSI DAN DEKRIPSI DENGAN ALGORITMA AES 256 UNTUK SEMUA JENIS FILE *id*(12). Retrieved from https://www.researchgate.net/profile/Antonius_Rachmat/publication/265364513_ENKRIPSI_DAN_DEKRIPSI_DENGAN_ALGORITMA_AES_256_UNTUK_SEMUA_JENIS_FILE/links/54b520400cf28ebe92e4c3c5/ENKRIPSI-DAN-DEKRIPSI-DENGAN-ALGORITMA-AES-256-UNTUK-SEMUA-JENIS-FILE.pdf

Alfred J.Menezes, Paul C.van Oorschot, S. A. V. 2012. Handbook of Applied Cryptography : Alfred J. Menezes, Paul C. van Oorschot, Scott A. Vanstone : Free Download & Streaming : Internet Archive. https://archive.org/details/HandbookOfAppliedCryptography

Saxena, R. P. 2006. Governments of the Future in the ICT Era - Rajiv Prakash Saxena - Google Books. https://books.google.com.my/books?id=6ey6SoEeCvoC&pg=PA146&lpg=PA146&dq=public+key+era+after+private+key&source=bl&ots=v-70dLVVbl&sig=gLTZdrfngg9-rX-5GEg2GMLERHo&hl=en&sa=X&redir_esc=y#v=onepage&q=public key era after private key&f=fals

Explain the Spiral Model - Testing. 2012. http://www.careerride.com/testing-spiral-model.aspx