# SISTEM PENGHANTARAN MESEJ SELAMAT MENGGUNAKAN PERTUKARAN KUNCI DIFFIE-HELLMAN

SOFIYA ILYANA BINTI SAHROM

TS. DR. NAZHATUL HAFIZAH BINTI KAMARUDIN

*Fakulti Teknologi & Sains Maklumat, Universiti Kebangsaan Malaysia, 43600 UKM Bangi, Selangor Darul Ehsan, Malaysia*



## ABSTRAK

Dalam era digital yang pesat membangun, ancaman keselamatan siber seperti serangan orang tengah (MitM) telah menimbulkan persoalan penting mengenai perlindungan privasi komunikasi. Kajian ini bertujuan untuk membangunkan sistem penghantaran mesej yang selamat menggunakan protokol Pertukaran Kunci Diffie-Hellman. Protokol ini membolehkan penciptaan kunci rahsia bersama secara dinamik antara dua pihak tanpa mendedahkannya melalui saluran komunikasi yang mungkin tidak selamat. Kunci rahsia tersebut digunakan untuk mengenkripsi mesej, memastikan hanya penerima yang sah dapat mengakses kandungan mesej. Sistem ini direka berdasarkan seni bina Model-Paparan-Pengawal (MVC) dan menggunakan reka bentuk klien-pelayan yang mempermudah pelaksanaan fungsi utama seperti pendaftaran, log masuk, penghantaran mesej terenkripsi, dan penyahsulitan. Analisis keselamatan menunjukkan bahawa sistem ini mampu menahan serangan utama seperti MitM, menjadikannya lebih selamat dan efisien. Kajian ini menghasilkan sebuah teknologi komunikasi selamat yang berguna untuk tujuan pembelajaran, terutamanya dalam bidang keselamatan siber dan kriptografi. Projek ini dijangka memberi sumbangan penting kepada pembangunan teknologi komunikasi yang lebih terjamin serta meningkatkan kesedaran tentang kepentingan melindungi privasi dalam dunia digital.

Kata kunci: Protokol Diffie-Hellman, Penghantaran Mesej, Serangan Orang Tengah

## PENGENALAN

Dalam era digital yang serba canggih ini, masalah keselamatan dalam penghantaran mesej di Malaysia semakin menjadi perhatian disebabkan oleh peningkatan kes serangan siber dan pencerobohan data. Peningkatan penggunaan aplikasi pemesejan seperti WhatsApp, Telegram dan pelbagai platform komunikasi yang lain telah menjadi kaedah utama untuk berkomunikasi bagi individu dan organisasi, menyebabkan jumlah data yang dipertukarkan setiap saat semakin bertambah. Walau bagaimanapun, perkembangan ini turut membawa cabaran baru dalam aspek keselamatan, terutamanya dalam memastikan mesej yang dihantar kekal rahsia dan tidak dapat diakses oleh pihak yang tidak sah. Di Malaysia, insiden keselamatan siber termasuk serangan orang tengah (Man-in-the-Middle, MitM) telah menjadi ancaman besar terhadap integriti dan

privasi data dalam penghantaran mesej. CyberSecurity Malaysia melaporkan sebanyak 4,615 insiden siber dari Januari hingga Mei 2021, di mana kes pencerobohan yang sering dikaitkan dengan MitM menjadi penyumbang utama. Menteri Komunikasi dan Multimedia ketika itu, Datuk Saifuddin Abdullah, turut menyatakan bahawa tiga insiden tertinggi yang dilaporkan ialah penipuan (3,299 kes), pencerobohan (765 kes) dan kod berbahaya (256 kes).

Dalam serangan MitM, pihak ketiga yang tidak sah boleh memintas komunikasi dengan tujuan mendapatkan akses kepada data sensitif atau mengubah mesej tanpa dikesan. Oleh itu, satu skema khas dicadangkan untuk penghantaran mesej rahsia yang selamat antara dua pihak. Mesej tersebut dienkripsi menggunakan kaedah enkripsi klasik, di mana kunci rahsia yang dihasilkan melalui protokol Pertukaran Kunci Diffie-Hellman. Pertukaran kunci Diffie Hellman ialah satu cara berkongsi kunci dengan selamat melalui rangkaian yang tidak selamat. Ia dinamakan sempena dua saintis Whitfield Diffie dan Martin Hellman (Mathew, 2021). Hal ini dikatakan demikian kerana, untuk memastikan hanya pihak yang dimaksudkan yang boleh memulakan dan menyelesaikan proses komunikasi. Kriptosistem ini menjalani analisis statistik, yang menunjukkan bahawa teks sifar secara konsisten lulus pelbagai ujian statistik, hal ini memberi keyakinan terhadap ketahanan enkripsi tersebut.Masalah utama yang dikenal pasti ialah ketidakamanan dalam penghantaran mesej melalui rangkaian awam, terutamanya apabila melibatkan maklumat sensitif dan rahsia. Kaedah enkripsi klasik yang digunakan kini sering terdedah kepada serangan seperti serangan orang tengah (MitM), di mana pihak ketiga boleh memintas komunikasi, mendapatkan kunci enkripsi, dan mengakses kandungan mesej tanpa dikesan. Kelemahan-kelemahan ini bukan sahaja mendedahkan maklumat sulit kepada pihak tidak bertanggungjawab, malah turut mengancam integriti komunikasi antara pengguna. Maka, terdapat keperluan mendesak untuk membangunkan sistem penghantaran mesej yang lebih selamat dan tahan terhadap serangan siber.

Objektif kajian ini adalah seperti berikut:

1. Membangunkan sistem penghantaran mesej yang selamat dengan mengimplementasikan algoritma Diffie-Hellman sebagai kaedah pertukaran kunci.
2. Menguji sistem yang dibangunkan agar mesej yang ingin dihantar dapat disampaikan dengan selamat dan tidak mudah diakses oleh pihak ketiga.

Skop kajian ini difokuskan kepada pelajar yang mempelajari mengenai keselamatan siber, kriptografi, dan pengembangan aplikasi, yang memerlukan pemahaman mendalam tentang teknik-teknik keselamatan dalam penghantaran maklumat. Tambahan lagi, ditujukan kepada pengguna akhir seperti individu yang ingin menghantar maklumat sensitif dengan selamat. Namun begitu projek ini tidak termasuk penyelesaian untuk masalah keselamatan lain yang tidak berkaitan dengan penghantaran mesej, seperti serangan siber yang lebih luas. Dengan skop ini, projek bertujuan untuk meningkatkan keselamatan dalam penghantaran mesej, memberikan pengguna alat yang lebih baik untuk melindungi maklumat mereka.

Projek ini penting kerana ia menawarkan pendekatan yang praktikal dan selamat untuk menyelesaikan isu keselamatan dalam komunikasi digital. Dengan menggunakan algoritma

pertukaran kunci Diffie-Hellman, sistem ini menyediakan kaedah selamat untuk menjana kunci rahsia yang hanya boleh diakses oleh pihak yang sah. Hasil daripada projek ini dijangka dapat menyumbang kepada pengetahuan dalam bidang keselamatan maklumat dan menjadi rujukan berguna dalam pembangunan sistem pemesejan selamat pada masa hadapan.

## METODOLOGI KAJIAN

Metodologi yang digunakan dalam pembangunan projek ini ialah model Waterfall yang menggunakan pendekatan pembangunan berfasa secara berurutan. Model ini dipilih kerana keperluan sistem dan objektif projek telah ditentukan dengan jelas sejak awal, membolehkan dokumentasi lengkap dan pelaksanaan sistematik dijalankan. Waterfall amat sesuai untuk projek ini yang melibatkan pembangunan sistem penghantaran mesej selamat dengan ciri enkripsi dan pengesahan masa, kerana ia memudahkan kawalan, semakan dan pengujian menyeluruh di setiap peringkat pembangunan.

### Fasa Analisis

Menganalisis keperluan sistem yang diperlukan oleh pengguna termasuk ciri-ciri yang ingin ditawarkan dalam sistem serta mengumpulkan data daripada pengguna untuk memahami keperluan mereka. Tambahan lagi, menyediakan dokumen spesifikasi keperluan dari awal dan jelas termasuk keperluan fungsian dan bukan fungsian.

### Fasa Keperluan Spesifikasi

Fasa keperluan spesifikasi merupakan fasa yang menyediakan semua keperluan yang telah dianalisis dan didokumentasikan sebelum memulakan projek supaya projek dapat berjalan dengan lancar.

### Fasa Reka Bentuk

Fasa reka bentuk akan bermula selepas Fasa Analisis dan Fasa Spesifikasi diselesaikan. Membuat reka bentuk sistem dan aliran proses berdasarkan keperluan yang telah dikumpulkan. Ini termasuk merancang elemen-elemen enkripsi menggunakan algoritma Diffie-Hellman, dan antara muka pengguna yang mesra. Reka bentuk penghantaran mesej yang mesra pengguna serta algoritma Diffie-Hellman yang dihasilkan di fasa ini.

### Fasa Pembangunan

Pada fasa ini, proses pengaturcaraan dan pembangunan sistem berdasarkan reka bentuk yang telah dipersetujui akan dilaksanakan. Ini termasuk penulisan kod untuk implementasi algoritma Diffie-Hellman, pengesahan pengguna melalui cap waktu, dan pengujian fungsi-fungsi lain yang diperlukan untuk penghantaran mesej yang selamat. Pembangunan ini bersifat iteratif, di mana setiap komponen diuji dan disempurnakan sebelum berpindah ke fasa selanjutnya.

### Fasa Pengujian dan Integrasi

Setelah fasa pembangunan tamat, sistem penghantaran mesej akan digabungkan dengan algoritma pertukaran kunci Diffie-Hellman dan akan melalui fasa pengujian bagi memastikan

semua komponen berfungsi dengan baik dan memenuhi keperluan yang telah ditetapkan. Maklum balas daripada pengguna akan diambil di fasa ini untuk mengetahui sebarang masalah terhadap sistem yang dibangunkan dan maklum balas tersebut akan digunakan pada fasa penambahbaikan.

**Fasa Penyelenggaraan dan Pelancaran**

Setelah pengujianan dilakukan dan mendapat maklum balas daripada pengguna, sistem akan diselenggarakan dan diperbaiki berdasarkan maklum balas pengguna dan mengatasi sebarang masalah atau kelemahan yang mungkin timbul. Setelah itu, sistem penghantaran mesej selamat siap untuk dilancarkan.

Kaedah pengumpulan data dilakukan melalui soal selidik secara atas talian menggunakan Google Form. Soal selidik ini bertujuan untuk mengenal pasti tahap kesedaran dan kefahaman pengguna terhadap aspek keselamatan komunikasi serta konsep asas algoritma Diffie-Hellman. Seramai 35 responden telah mengambil bahagian dalam soal selidik ini. Maklum balas yang diperoleh membantu dalam memahami keperluan pengguna dan membentuk asas dalam mereka bentuk antara muka dan fungsi sistem.

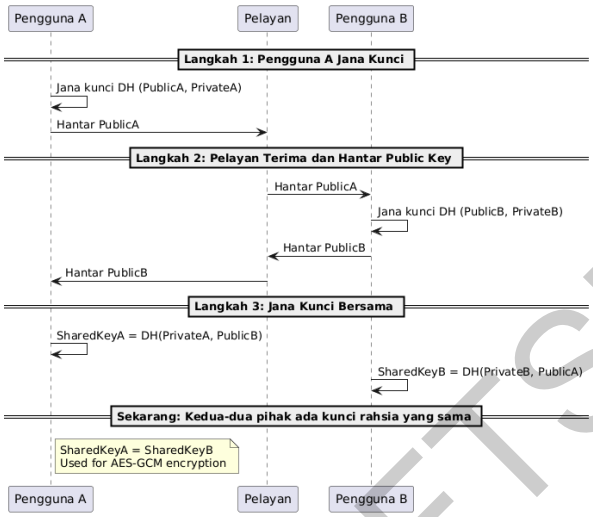
Data yang dikumpul melalui soal selidik dianalisis secara deskriptif menggunakan carta dan graf yang dijana secara automatik oleh Google Form. Analisis ini memberi gambaran umum terhadap kesedaran pengguna berkaitan penghantaran mesej selamat serta keperluan untuk sistem yang menyokong penyulitan dan perlindungan privasi. Pemahaman ini turut membantu dalam memastikan fungsi sistem dibangunkan selaras dengan keperluan pengguna.

Bagi menilai keberkesanan sistem yang dibangunkan, instrumen pengukuran digunakan merangkumi aspek fungsional seperti kebolehan sistem untuk menjana dan bertukar kunci secara automatik menggunakan algoritma Diffie-Hellman, serta tahap kejayaan penyulitan dan penyahsulitan mesej. Pemerhatian dilakukan terhadap tindak balas sistem, ketepatan hasil mesej, dan keselamatan semasa simulasi serangan seperti serangan orang tengah (MitM). Keberkesanan sistem turut diuji melalui penjejakan komunikasi menggunakan Wireshark bagi memastikan tiada pertukaran kunci peribadi berlaku secara terbuka dalam rangkaian

## KEPUTUSAN DAN PERBINCANGAN

Sistem penghantaran mesej selamat *RahsiaSelamatDH* telah berjaya dibangunkan sebagai satu aplikasi web masa nyata yang menekankan keselamatan komunikasi antara pengguna. Sistem ini membolehkan dua pengguna bertukar mesej yang telah disulitkan, dan setiap sesi komunikasi dilindungi melalui mekanisme pertukaran kunci rahsia menggunakan algoritma Diffie-Hellman. Proses pertukaran kunci rahsia dilaksanakan secara automatik di latar belakang sebaik sahaja dua pengguna bersetuju untuk memulakan komunikasi. Setiap pengguna akan menjana pasangan kunci awam dan peribadi secara rawak, dan hanya kunci awam akan ditukar melalui sambungan selamat menggunakan Socket.io. Setelah pertukaran berlaku, kedua-dua pihak menjana kunci rahsia bersama yang digunakan untuk proses penyulitan dan penyahsulitan mesej secara tempatan menggunakan algoritma simetri. Rajah

proses pertukaran kunci menggunakan algoritma Diffie-Hellman seperti berikut.

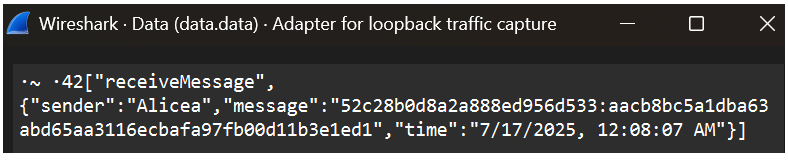



Rajah 1 Proses Pertukaran Kunci Diffie-Hellman

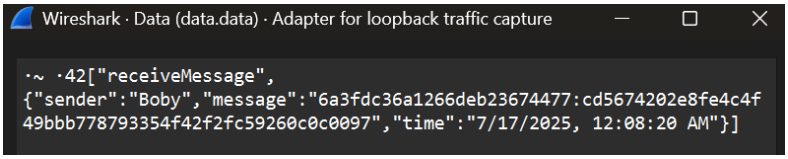
Dari sudut teknikal, sistem dibangunkan menggunakan Node.js bersama Express.js untuk membina pelayan aplikasi, manakala Socket.io digunakan untuk menyokong komunikasi masa nyata antara pengguna. Maklumat pengguna serta mesej yang telah disulitkan disimpan dalam pangkalan data MySQL, yang diuruskan melalui antaramuka phpMyAdmin. Tiada kunci rahsia atau mesej asal yang disimpan dalam bentuk teks jelas bagi menjamin keselamatan maklumat.

Bagi menguji keberkesanan keselamatan sistem, simulasi serangan orang tengah (MitM) telah dijalankan menggunakan Wireshark. Berdasarkan hasil penangkapan trafik, mesej yang dihantar tidak dapat dibaca oleh pihak ketiga kerana disulitkan dan tiada kunci rahsia yang dapat diperoleh sepanjang sesi. Tangkap layar ujian melalui Wireshark turut disertakan dalam laporan ini sebagai bukti bahawa mesej berada dalam bentuk tersulit sepanjang penghantaran.


Rajah 2 Mesej antara Alicea dan Boby




Rajah 3 Kandungan mesej Alicea yang dinyahsulit




Rajah 4 Kandungan mesej Boby yang dinyahsulit

Maklumat ini membuktikan bahawa sistem telah menjalankan penyulitan di sisi klien sebelum penghantaran mesej. Nilai dalam medan "message" merupakan mesej yang telah disulitkan, yang terdiri daripada rentetan cipher dan nilai IV (Initialization Vector), dipisahkan oleh titik bertindih (:). Format ini merupakan amalan standard dalam penyulitan simetri seperti AES, dan menunjukkan bahawa kandungan sebenar mesej tidak dihantar dalam bentuk teks biasa (plaintext), tetapi dalam bentuk ciphertext yang tidak dapat difahami tanpa kunci rahsia.

Pengesanan waktu yang sepadan dengan waktu mesej dihantar dalam antaramuka pengguna mengesahkan bahawa mesej tersebut berjaya diproses dan dihantar dalam bentuk tersulit. Ini membuktikan keberkesanan mekanisme penyulitan sistem RahsiaSelamatDH dalam melindungi kerahsiaan komunikasi antara pengguna.

Selain itu, semua ujian fungsian sistem telah dijalankan, termasuk pengesahan pengguna, proses sambungan antara pengguna, pertukaran kunci, penyulitan dan penyahsulitan mesej, serta pemutusan sambungan secara automatik selepas komunikasi tamat. Kesemua ujian fungsian ini telah lulus dan membuktikan sistem berfungsi seperti yang dirancang dari segi logik dan keselamatan.

Jadual 1 Hasil Pengujian Kes Guna

| ID Pengujian | Jangkaan Pengujian | Hasil Sebenar Pengujian | Status Pengujian |
|---|---|---|---|
| P01 | Berjaya daftar masuk dan sistem meminta untuk log masuk | Berjaya daftar masuk dan sistem meminta untuk log masuk | Berjaya |
| P02 | Berjaya log masuk dan memaparkan halaman utama. | Berjaya log masuk dan memaparkan halaman utama. | Berjaya |
| P03 | Pengguna berjaya berhubung, sistem memaparkan status “The shared key is successful. You can connect..” menandakan komunikasi berjaya dibuat. | Pengguna berjaya berhubung, sistem memaparkan status “The shared key is successful. You can connect..” menandakan komunikasi berjaya dibuat. | Berjaya |
| P04 | Sistem Berjaya menghantar mesej kepada pengguna lain | Sistem Berjaya menghantar mesej kepada pengguna lain | Berjaya |
| P05 | Sistem berjaya menghantar dan memaparkan mesej kepada penerima. | Sistem berjaya menghantar dan memaparkan mesej kepada penerima. | Berjaya |
| P06 | Sistem berjaya menghantar mesej bersekalikan jejak masa terkini. | Sistem berjaya menghantar mesej bersekalikan jejak masa terkini. | Berjaya |
| P07 | Sistem berjaya mendaftar keluar pengguna dan memaparkan halaman log masuk. | Sistem berjaya mendaftar keluar pengguna dan memaparkan halaman log masuk. | Berjaya |

Secara keseluruhannya, pembangunan sistem *RahsiaSelamatDH* telah memenuhi objektif utama iaitu menyediakan platform komunikasi yang selamat dan interaktif, di samping memperkenalkan prinsip keselamatan siber melalui pengalaman penggunaan yang mesra pengguna.

**Cadangan Penambahbaikan**

Bagi memperkukuhkan sistem *RahsiaSelamatDH* pada masa hadapan, beberapa penambahbaikan dicadangkan. Antaranya ialah penggunaan rangkaian sebenar untuk membolehkan ujian dijalankan dalam persekitaran dunia sebenar, penambahan fungsi notifikasi atau log keselamatan bagi memaklumkan pengguna tentang aktiviti berkaitan keselamatan, serta integrasi enjin pengesahan lebih kuat seperti pengesahan dua faktor (2FA) atau OTP. Selain itu, penambahbaikan antaramuka agar lebih responsif dan mesra peranti mudah alih juga dicadangkan. Penambahbaikan ini dijangka dapat menjadikan sistem lebih selamat, berdaya saing dan mudah digunakan.

## KESIMPULAN

Secara keseluruhannya, sistem penghantaran mesej selamat *RahsiaSelamatDH* telah berjaya dibangunkan berdasarkan objektif dan keperluan yang telah ditetapkan. Sistem ini menggunakan algoritma Diffie-Hellman bagi pertukaran kunci secara automatik serta penyulitan mesej di sisi klien, sekaligus memastikan mesej tidak dihantar dalam bentuk asal.

Sistem RahsiaSelamatDH menonjol dari aspek keselamatan komunikasi antara pengguna. Antara kekuatan utama sistem ini ialah keupayaannya untuk menyulitkan mesej di sisi pengguna serta penggunaan algoritma Diffie-Hellman untuk pertukaran kunci secara selamat. Selain itu, sistem berjaya mengesan dan menghentikan komunikasi apabila simulasi serangan MitM dikesan, membuktikan kecekapan dalam perlindungan kerahsiaan mesej.

Namun, pembangunan sistem turut menghadapi beberapa kekangan. Antaranya ialah ujian hanya dijalankan dalam persekitaran tempatan, kekangan masa untuk menambah fungsi lanjutan seperti pengesahan dua faktor, serta kerumitan dalam memahami dan melaksanakan teknik kriptografi. Kekangan lain termasuk keperluan pengendalian data sulit secara berhati-hati dan kekurangan bimbingan daripada pakar keselamatan siber.

Kesimpulannya, kajian ini telah berjaya membangunkan sistem penghantaran mesej selamat iaitu RahsiaSelamatDH, yang menggunakan algoritma Diffie-Hellman bagi penghasilan kunci rahsia bersama antara pengguna. Sistem ini mampu menyulitkan mesej di sisi klien dan memastikan mesej tidak dihantar dalam bentuk asal, sekaligus melindungi komunikasi daripada serangan pihak ketiga. Hasil pengujian menunjukkan mesej disulitkan dengan berkesan dan sistem berjaya mengesan serta menggagalkan serangan orang tengah (MitM). Secara keseluruhan, objektif kajian telah dicapai dan sistem menunjukkan potensi untuk dikembangkan dengan ciri keselamatan tambahan pada masa hadapan.

## PENGHARGAAN

Penulis kajian ini ingin ucapkan setinggi-tinggi penghargaan dan jutaan terima kasih kepada Ts. Dr. Nazhatul Hafizah, penyelia penulis kajian ini yang telah memberi tunjuk ajar serta bimbingan untuk menyiapkan projek ini dengan jayanya.

Penulis kajian ini juga ingin mengucapkan terima kasih kepada semua pihak yang membantu secara langsung mahupun tidak langsung dalam menyempurnakan projek ini. Segala bantuan yang telah dihulurkan amatlah dihargai kerana tanpa bantuan mereka, projek ini tidak dapat dilaksanakan dengan baik. Semoga tuhan merahmati dan memberikan balasan yang terbaik.

## RUJUKAN

Adrian, & Adrian. (2023, October 29). *Understanding Secure key Exchange Protocols: An expert guide*. CERTAURI.

Alsmadi, I., & Zarour, M. (2022). Evaluating Software Requirements: The Impact of Non-functional Aspects on Security and Usability. Computers, 11(1), 13.

Mathew, J., P., Thomas, J., Sarthik, J., & A. (2021). *Secure Text Transfer Using Diffie-Hellman Key Exchange Based On Cloud*. *International Journal of Advances in Engineering and Management (IJAEM)*, *3*, 998.

GeeksforGeeks. (2024, July 3). *Implementation of DiffieHellman Algorithm*. GeeksforGeeks.

Kara, M., Laouid, A., AlShaikh, M., Bounceur, A., & Hammoudeh, M. (2021). Secure Key *Exchange Against Man-in-the-Middle Attack: Modified Diffie-Hellman Protocol. Jurnal Ilmiah Teknik Elektro Komputer Dan Informatika*, *7*(3), 380.

Rustagi, P. (2015). MVC ARCHITECTURE AND IT'S APPLICATION [Thesis]. In *Major project report*. Jaypee University of Information Technology.

Senarath, U. S. (2021). *Waterfall Methodology, Prototyping and Agile Development*.

*Sofiya Ilyana Binti Sahrom (A195223)*
*Ts. Dr. Nazhatul Hafizah Kamarudin*
Fakulti Teknologi & Sains Maklumat
Universiti Kebangsaan Malaysia