KONSEP KEBOLEHLAKSANAAN ALGORITMA KRIPTOGRAFI PASCA-KUANTUM DALAM SISTEM TANDATANGAN DIGITAL

NURUL SYAFIQAH BINTI NORIHSAN

AZANA HAFIZAH BINTI MOHD AMAN

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

ABSTRAK

Kemajuan teknologi kuantum semakin memberi tekanan terhadap keselamatan algoritma kriptografi tradisional seperti RSA dan ECDSA yang digunakan secara meluas dalam infrastruktur kekunci awam (PKI). Sebagai langkah pencegahan, komuniti keselamatan digital memberi perhatian lebih kepada algoritma kriptografi pasca-kuantum (PQC) yang mampu bertahan daripada ancaman komputer kuantum. Antara algoritma PQC yang telah diluluskan oleh NIST ialah CRYSTALS-Dilithium dan SPHINCS+, seperti yang diumumkan dalam pusingan ketiga dalam pemilihan algoritma PQC oleh NIST pada 2022 (NIST, 2022). Oleh itu, projek ini bertujuan untuk membangunkan satu platform bukti konsep (PoC) dalam bentuk aplikasi web menggunakan Java Spring Boot, pustaka Bouncy Castle dan Bootstrap. Sistem ini menyokong algoritma RSA, ECDSA, Dilithium, dan SPHINCS+ untuk penjanaan pasangan kunci, penandatanganan fail, dan pengesahan tandatangan digital. Antara muka sistem membolehkan pengguna memilih algoritma, menandatangani fail, dan menyemak status tandatangan dengan pantas. Pengujian tanda aras juga turut disediakan bagi mengukur masa penjanaan pasangan kunci, masa penjanaan dan pengesahan tandatangan dan saiz tandatangan bagi setiap output daripada algoritma yang diuji. Hasil kajian menunjukkan bahawa integrasi algoritma PQC dalam sistem sijil digital adalah tidak mustahil untuk dilaksanakan secara teknikal dan mempunyai potensi untuk meningkatkan keselamatan jangka panjang dalam era pasca-kuantum.

Kata kunci: RSA, ECDSA, CRYSTALS-Dilithium, SPHINCS+, PQC

PENGENALAN

Pengesahan tandatangan digital merupakan elemen penting dalam infrastruktur kekunci awam (PKI) yang memastikan integriti, keaslian, dan terhadap data digital. Ia digunakan secara meluas dalam pelbagai sektor seperti komunikasi digital, kewangan digital, e-dagang, perbankan serta sistem kerajaan. Namun begitu, kemajuan dalam bidang pengkomputeran kuantum yang semakin menjadi bualan dunia kriptografi telah menimbulkan kebimbangan terhadap keselamatan algoritma kriptografi tradisional seperti *Rivest–Shamir–Adleman*, RSA dan *Elliptic Curve Digital Signature Algorithm,* ECDSA. Ini kerana komputer kuantum mampu

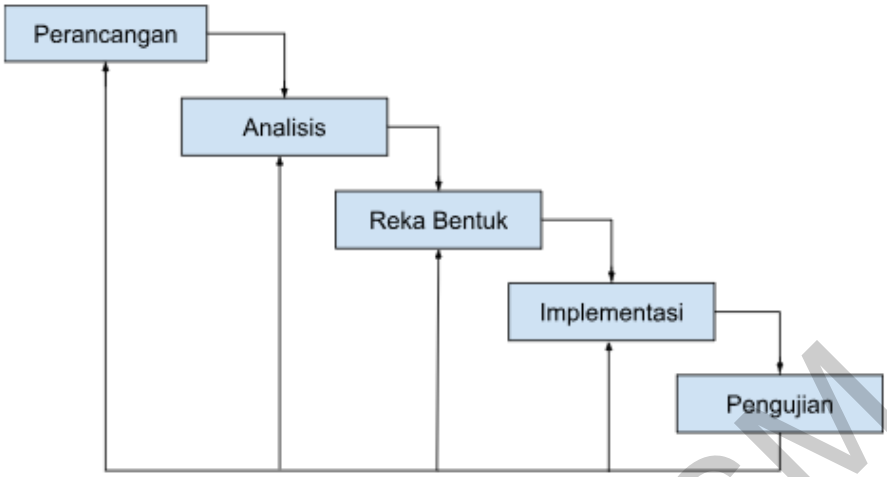
memecahkan algoritma tersebut dengan menggunakan algoritma Shor, yang membolehkan pemfaktoran nombor perdana dilakukan dalam pengiraan polinomial (Academy 2024). Oleh itu, keselamatan sistem PKI konvensional dijangka akan terjejas secara serius apabila komputer kuantum berskala besar menjadi kenyataan.

Sebagai respons terhadap ancaman tersebut, pihak yang berkenaan seperti Institut Piawaian dan Teknologi Nasional (NIST) telah menjalankan beberapa kajian dan proses penilaian algoritma kriptografi pasca-kuantum (PQC). Pada tahun 2022, NIST telah mengumumkan dan memilih algoritma seperti CRYSTALS-Dilithium dan SPHINCS+ sebagai algoritma utama yang akan digunakan dalam sistem yang tahan ancaman kuantum ("NIST Announces First Four Quantum-Resistant Cryptographic Algorithms" 2022).

Sehubungan dengan itu, kajian ini memberi tumpuan kepada pembangunan satu platform bukti konsep (Proof of Concept, PoC) dalam bentuk sistem web yang menerapkan algoritma kriptografi pasca-kuantum (PQC) bagi tujuan penandatanganan dan pengesahan digital dokumen. Pelaksanaan ini dijalankan menggunakan bahasa pengaturcaraan Java dengan rangka kerja Spring Boot, pustaka kriptografi Bouncy Castle, serta antaramuka pengguna berasaskan Bootstrap. Sistem ini menyokong algoritma RSA, ECDSA, CRYSTALS-Dilithium (Dilithium3), dan SPHINCS+ untuk penjanaan kunci, tandatangan digital dan pengesahan. Kajian ini turut menilai aspek kebolehlaksanaan teknikal dan prestasi setiap algoritma dari segi masa penjanaan kunci, masa tandatangan, masa pengesahan, serta saiz kunci dan saiz tandatangan. Dapatan ini diharapkan dapat menjadi rujukan awal ke arah penyesuaian sistem keselamatan maklumat yang lebih bersedia untuk menghadapi ancaman era pasca-kuantum.

METODOLOGI KAJIAN

Pendekatan metodologi projek ini menggunakan model Air Terjun (Waterfall) berdasarkan kitaran hidup pembangunan perisian atau *Software Development Life Cycle* (SDLC). Model ini dipilih kerana ia menyediakan struktur fasa pembangunan yang teratur dan berperingkat, melibatkan lima fasa utama iaitu fasa perancangan, analisis, reka bentuk, pelaksanaan dan pengujian. Pemilihan model ini juga memudahkan pengurusan projek kerana setiap fasa perlu disiapkan terlebih dahulu sebelum fasa berikutnya bermula.



Rajah 1 Model Air Terjun

Fasa Analisis

Dalam fasa ini, keperluan fungsian dan bukan fungsian sistem ditentukan melalui perbincangan bersama penyelia serta rujukan daripada penyelidikan berkaitan. Keperluan fungsian termasuklah kemampuan sistem untuk menjana pasangan kunci, menandatangani fail, mengesahkan tandatangan, dan memaparkan hasil penanda aras prestasi bagi algoritma RSA, ECDSA, CRYSTALS-Dilithium dan SPHINCS+. Keperluan bukan fungsian pula merangkumi aspek seperti keselamatan penyimpanan kunci, paparan antara muka mesra pengguna serta kecekapan sistem dalam memproses operasi tandatangan digital. Analisis turut melibatkan kajian literatur berkaitan teknologi tandatangan digital sedia ada, algoritma kriptografi pasca-kuantum serta pustaka kriptografi sumber terbuka seperti Bouncy Castle yang digunakan untuk integrasi algoritma dalam pembangunan sistem ini. Hasil daripada analisis ini menjadi asas kepada reka bentuk sistem yang terperinci.

Fasa Reka Bentuk

Pada fasa ini, reka bentuk sistem dijalankan, termasuk reka bentuk arkitektur sistem, dan aliran keselamatan dalam sistem. Keputusan tentang bagaimana aliran sistem, struktur sijil, dan integrasi algoritma PQC dalam proses tandatangan dan pengesahan digital.

Fasa Implementasi

Pembangunan sebenar sistem bermula. Pembangunan sistem web dilaksanakan menggunakan Java Spring Boot untuk bahagian belakang dan Bootstrap bagi bahagian depan. Algoritma RSA, ECDSA, CRYSTALS-Dilithium (Dilithium3), serta SPHINCS+ diintegrasikan menggunakan pustaka Bouncy Castle. Antara muka pengguna membolehkan pemilihan algoritma secara dinamik, serta penyimpanan hasil tandatangan dan kunci secara tempatan. Fungsi pengujian tanda aras juga disediakan untuk memaparkan prestasi setiap algoritma.

Fasa pengujian

Fasa pengujian adalah fasa penting untuk memastikan semua fungsi sistem beroperasi seperti yang ditetapkan dalam spesifikasi. Ujian fungsian dijalankan untuk mengesahkan proses penjanaan kunci, tandatangan dan pengesahan berjalan dengan tepat serta integriti data asal

kekal terpelihara. Pengujian prestasi turut dilaksanakan untuk mendapatkan maklumat seperti masa penjanaan kunci, masa tandatangan, masa pengesahan, dan saiz tandatangan yang dihasilkan oleh ketiga-tiga algoritma. Data yang diperoleh dipaparkan dalam bentuk carta prestasi menggunakan Chart.js untuk analisis lanjut. Proses pengujian ini memastikan sistem yang dibangunkan stabil, memenuhi semua keperluan, serta bersedia untuk diaplikasikan atau ditambah baik pada masa hadapan.

KAJIAN KESUSASTERAAN

Algoritma kriptografi tradisional seperti RSA dan Elliptic Curve Digital Signature Algorithm (ECDSA) telah lama digunakan secara meluas dalam infrastruktur kunci awam (PKI) untuk tujuan penyulitan dan tandatangan digital.

Algoritma RSA

RSA bergantung kepada kesukaran matematik memfaktorkan integer besar yang terhasil daripada dua nombor perdana. Keselamatan RSA bergantung kepada masa yang diambil untuk memecahkan masalah pemfaktoran tersebut menggunakan komputer klasik. Walau bagaimanapun, dengan kemunculan komputer kuantum, algoritma RSA menjadi terdedah kepada algoritma kuantum seperti algoritma Shor yang dapat memecahkan pemfaktoran integer dalam masa polinomial, sekali gus menggugat keselamatan RSA.

Algoritma ECDSA

ECDSA merupakan variasi tandatangan digital yang dibina berdasarkan Elliptic Curve Cryptography (ECC). ECC bergantung pada kesukaran masalah logaritma diskret eliptik, (*Elliptic Curve Discrete Logarithm Problem,* ECDLP) yang memberikan tahap keselamatan tinggi dengan saiz kunci yang lebih kecil berbanding RSA. Namun, ECDSA juga tidak kebal terhadap ancaman kuantum kerana algoritma Shor mampu menyelesaikan ECDLP dengan berkesan jika komputer kuantum berskala besar wujud. Selain itu, algortima Grover memberikan ancaman terhadap algoritma simetri dengan mengurangkan kerumitan carian daripada $O(N)$ kepada $O(\sqrt{N})$, yang secara tidak langsung memaksa saiz kunci simetri ditingkatkan untuk mengekalkan tahap keselamatan.

Kriptografi Pasca-Kuantum

Kriptografi Pasca-Kuantum (Post-Quantum Cryptography, PQC) ialah cabang keselamatan digital yang membangunkan algoritma mampu menahan serangan komputer kuantum, berbeza daripada algoritma tradisional seperti RSA dan ECDSA yang bergantung pada pemfaktoran integer atau logaritma diskret. PQC menggunakan struktur matematik seperti kekisi, fungsi hash, kon ralat dan polinomial multivariat, dan sedang melalui proses piawaian standard oleh NIST. Dalam pengumuman pusingan ketiga pada Julai 2022, NIST mengesahkan CRYSTALS-Dilithium dan SPHINCS+ sebagai algoritma tandatangan digital utama. Walaupun begitu, cabaran utama PQC ialah saiz kunci yang lebih besar, yang memerlukan penyesuaian protokol seperti TLS dan IKE, dan organisasi digesa mula mengadaptasi teknologi ini bagi menghadapi ancaman komputer kuantum pada masa hadapan.

Algoritma CRYSTALS-Dilithium

CRYSTALS-Dilithium ialah algoritma tandatangan digital berasaskan kekisi yang direka untuk menahan serangan komputer kuantum dan telah dipilih sebagai piawaian NIST. Ia menggunakan masalah matematik seperti *Module Learning With Errors,* MLWE, *Short Integer Solution,* SIS dan *Ring Learning With Errors,* RLWE untuk memastikan keselamatan tandatangan. Merujuk Jadual 2 di bawah, terdapat tiga varian utama algoritma ini iaitu Dilithium-2, Dilithium-3 dan Dilithium-5 yang berbeza dari segi saiz kunci, saiz tandatangan dan tahap keselamatan, membolehkan pemilihan mengikut keperluan sistem.

Jadual 2: Jenis Algoritma Dilithium

Jenis	Saiz Kunci Awam	Saiz Kunci Rahsia	Saiz Tandatangan	Tahap Keselamatan
Dilithium 2	1312	2528	2420	AES-128
Dilithium 3	1952	4000	3293	AES-192
Dilithium 5	2592	4864	4595	AES-256

Sumber: Sutherland 2025

Algoritma SPHINCS+

SPHINCS+ ialah algoritma tandatangan digital berasaskan fungsi hash yang juga dipilih oleh NIST sebagai piawaian PQC. Ia menggunakan struktur pokok seperti *Hypertree*, *Forest of Random Subsets*, FORS dan *Winternitz One-Time Signature*, WOTS+ untuk menghasilkan tandatangan digital yang selamat tanpa bergantung pada andaian matematik baharu. SPHINCS+ mempunyai beberapa varian dengan tahap keselamatan 128, 192 dan 256 bit, namun menghasilkan tandatangan yang lebih besar dan masa tandatangan lebih lama berbanding Dilithium. Jadual 3 di bawah menunjukkan varians algoritma SPHINCS+:

Jadual 3: Jenis dan Saiz Algoritma SPHINCS+

Jenis	Saiz Kunci Awam	Saiz Kunci Rahsia	Saiz Tandatangan
SPHINCS+-128s	32	64	7856
SPHINCS+-128f	32	64	17088
SPHINCS+-192s	48	96	16224
SPHINCS+-192f	48	96	35664
SPHINCS+-256s	64	128	29792
SPHINCS+-256f	64	128	49856

Sumber: Hülsing et al. 2022.

METODOLOGI

Bab ini menerangkan metodologi pembangunan dan pengujian sistem pengesahan tandatangan digital berasaskan web yang menggabungkan algoritma tradisional RSA dan ECDSA serta algoritma pasca-kuantum CRYSTALS-Dilithium dan SPHINCS+. Sistem dibangunkan sebagai platform bukti konsep (PoC) bagi membolehkan pengguna menjana kunci, menandatangani dan mengesahkan fail digital secara interaktif melalui antara muka web mesra pengguna. Metodologi memberi tumpuan kepada fungsi kriptografi seperti penjanaan kunci, tandatangan dan pengesahan, serta penilaian prestasi meliputi masa pemprosesan dan saiz kunci atau tandatangan. Pembangunan menggunakan Java Spring Boot, pustaka Bouncy Castle, dan antaramuka HTML, JavaScript serta Bootstrap, direka bentuk sebagai sistem kendiri untuk simulasi dan kajian keberkesanan algoritma PQC.

Analisis Keperluan

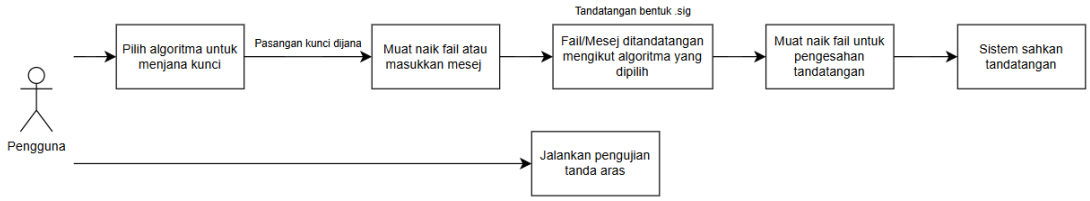
Analisis keperluan dilakukan untuk memastikan sistem pengesahan tandatangan digital yang dibangunkan memenuhi objektif projek serta beroperasi dengan stabil dalam persekitaran sebenar. Proses ini melibatkan penentuan keperluan fungsian, keperluan bukan fungsian serta spesifikasi perkakasan dan perisian yang diperlukan.

Dari segi keperluan fungsian, sistem perlu menyediakan ciri utama seperti pemilihan algoritma (RSA, ECDSA CRYSTALS-Dilithium dan SPHINCS+), penjanaan pasangan kunci awam dan peribadi, penandatanganan fail atau mesej digital menggunakan algoritma yang dipilih, serta pengesahan tandatangan dengan membandingkan nilai ringkasan dokumen asal dan tandatangan digital menggunakan kunci awam. Selain itu, sistem juga perlu memaparkan keputusan pengujian tanda aras bagi membolehkan perbandingan prestasi antara algoritma dilakukan.

Manakala bagi keperluan bukan fungsian, analisis memberi tumpuan kepada aspek prestasi seperti kelajuan penjanaan kunci, masa tandatangan dan masa pengesahan. Aspek keselamatan seperti integriti data dan perlindungan kunci. Aspek kebolehgunaan seperti antara muka mesra pengguna serta ketahanan sistem untuk digunakan dalam tempoh operasi yang lama tanpa ralat.

Model Sistem

Bahagian ini menerangkan kaedah cadangan untuk model pembangunan sistem yang terbahagi kepada lima langkah-langkah utama iaitu, pemilihan algoritma, penjanaan kunci, menjana tandatangan fail, pengesahan tandatangan fail, dan paparan pengujian tanda aras. Model sistem memastikan pembangunan sistem lebih sistematik dan teratur sejajar dengan objektif projek.



Rajah 2 Cadangan Model Sistem Pengesahan Tandatangan Digital

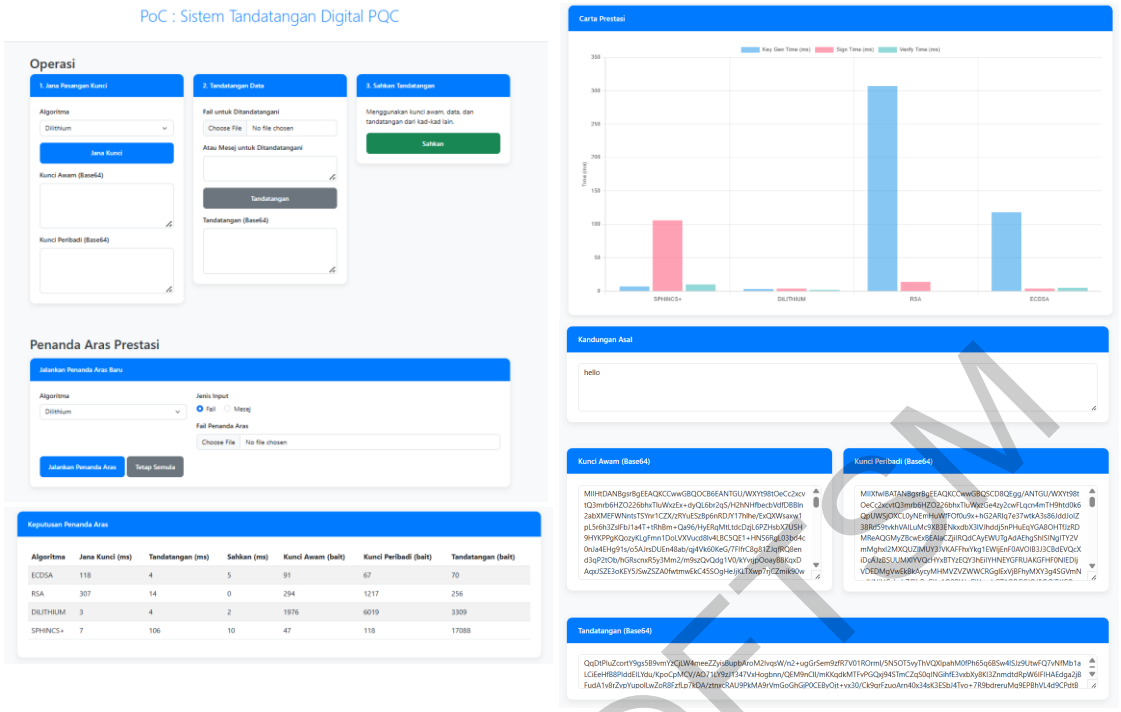
Sistem yang dibangunkan menggunakan pendekatan berasaskan modul, di mana keseluruhan fungsi dipecahkan kepada lima modul utama iaitu pemilihan algoritma, penjanaan kunci, penjanaan tandatangan, pengesahan tandatangan dan paparan pengujian tanda aras. Modul-modul ini digabungkan untuk membentuk satu aliran kerja yang lengkap dalam proses tandatangan digital.

Modul pemilihan algoritma membolehkan pengguna memilih antara RSA, ECDSA, CRYSTALS-Dilithium (Dilithium3) atau SPHINCS+ untuk proses penjanaan kunci. Modul penjanaan kunci menghasilkan pasangan kunci awam dan peribadi berdasarkan algoritma yang dipilih; RSA bergantung kepada pemfaktoran integer, Dilithium3 kepada persamaan kekisi (MLWE), manakala SPHINCS+ menggunakan struktur pokok hash. Modul penjanaan tandatangan memastikan mesej atau fail yang dihantar ditandatangani dengan selamat menggunakan kunci peribadi mengikut algoritma, manakala modul pengesahan tandatangan menggunakan kunci awam untuk memastikan tandatangan adalah sah dan data tidak diubah.

Akhir sekali, modul paparan pengujian tanda aras merekod dan memaparkan prestasi setiap algoritma dalam bentuk carta dan jadual, termasuk masa penjanaan kunci, masa tandatangan, masa pengesahan, serta saiz kunci dan tandatangan. Melalui gabungan modul-modul ini, sistem dapat berfungsi sebagai bukti konsep yang interaktif untuk menguji dan membandingkan keberkesanan algoritma tradisional dan pasca-kuantum dalam persekitaran yang mesra pengguna.

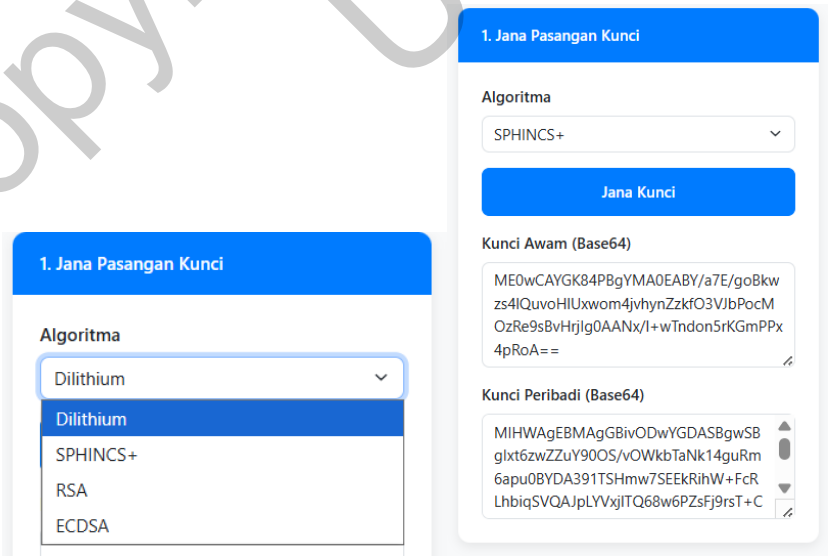
Reka Bentuk Antara Muka

Reka bentuk antara muka adalah proses mencipta prototaip antaramuka yang memenuhi aspek yang memudahkan pengguna. Antara muka yang direka dengan baik perlu memenuhi ciri-ciri seperti mesra pengguna, mudah difahami, tersusun, dan seragam untuk memastikan ia mudah digunakan serta memenuhi keperluan pengguna dengan efektif. Rajah 3 menunjukkan cadangan antara muka sistem.



Rajah 3 Antara muka Sistem Tandatangan Digital

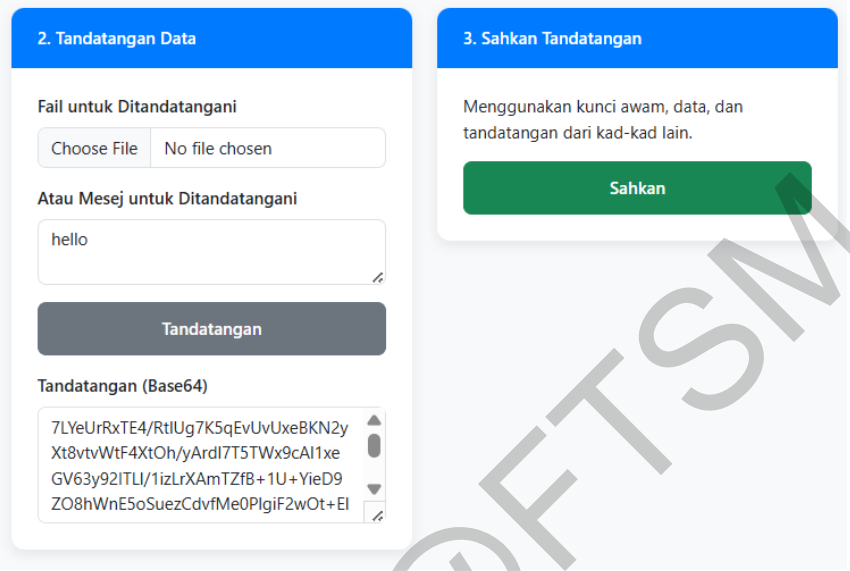
Paparan utama sistem PoC ini memaparkan modul untuk operasi tandatangan digital PQC. Ia dibahagikan kepada bahagian *Jana Pasangan Kunci*, *Tandatangan Data*, *Sahkan Tandatangan*, serta modul *Penanda Aras Prestasi*. Setiap modul diatur dengan jelas untuk memudahkan pengguna.



Rajah 4 *Dropdown Menu* untuk pengguna memilih algoritma dan penjanaan pasangan kunci

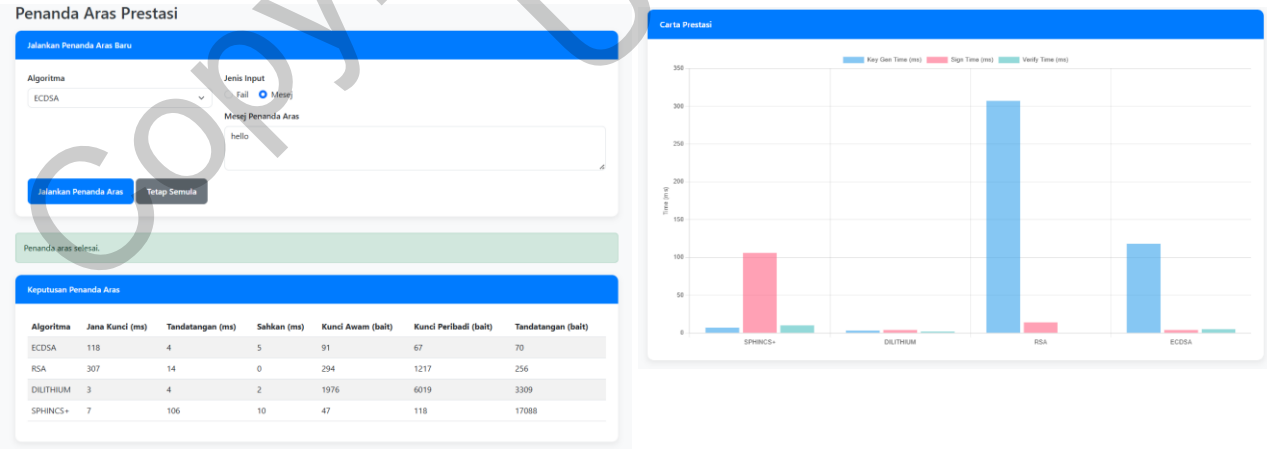
Dalam bahagian Jana Pasangan Kunci, terdapat menu lungsur (dropdown menu) yang membolehkan pengguna memilih algoritma kriptografi yang diingini seperti Dilithium,

SPHINCS+, RSA, atau ECDSA sebelum menekan butang Jana Kunci. Pasangan kunci yang telah dijana akan dipaparkan dalam format Base64 sebagai rujukan pengguna atau penyelidik untuk membuat kajian.



Rajah 5 Paparan pengguna sahkan tandatangan

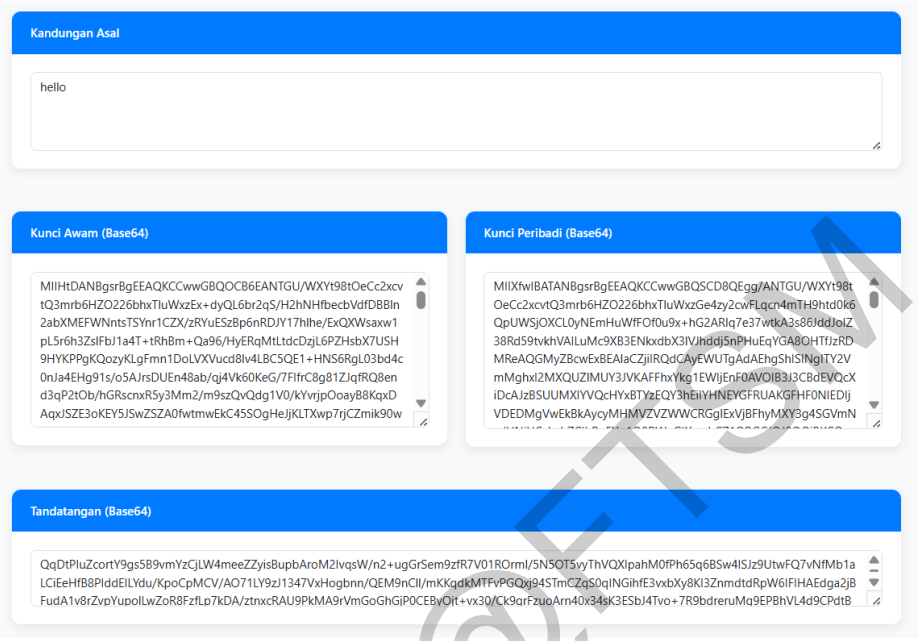
Paparan boleh menandatangani data atau mesej dan tandatangan dalam bentuk Base64 dipaparkan di kotak teks. Pengguna boleh menggunakan kunci awam, data asal, dan tandatangan ini dalam modul *Sahkan Tandatangan* untuk mengesahkan kesahihan tandatangan.



Rajah 6 Antara muka penanda aras dan carta prestasi algoritma

Bahagian *Penanda Aras Prestasi* membolehkan pengguna memilih algoritma, memilih jenis input (fail atau mesej), dan memuat naik input untuk menjalankan ujian prestasi. Selepas ujian, keputusan dipaparkan dalam bentuk jadual. Hasil penanda aras juga divisualkan dalam carta bar. Carta ini memaparkan masa yang diambil untuk menjana kunci, masa tandatangan, dan

masa pengesahan bagi setiap algoritma, membolehkan perbandingan prestasi dibuat dengan mudah.



Rajah 7 Antara muka kandungan pasangan kunci, tandatangan dan mesej

KEPUTUSAN DAN PERBINCANGAN

Bahagian ini membincangkan keputusan ujian yang diperoleh daripada pelaksanaan sistem tandatangan digital yang dibangunkan, diikuti dengan perbincangan terhadap keputusan tersebut. Ujian dilaksanakan untuk mengesahkan fungsi sistem dan menilai prestasi setiap algoritma yang digunakan, iaitu RSA, ECDSA, CRYSTALS-Dilithium dan SPHINCS+.

Keputusan Pengujian Prestasi Algoritma

Pengujian bukan fungsian telah dilaksanakan untuk menilai prestasi algoritma tandatangan digital yang digunakan dalam sistem ini, iaitu RSA, ECDSA, CRYSTALS-Dilithium, dan SPHINCS+. Ujian ini melibatkan penilaian terhadap beberapa metrik penting iaitu masa penjanaan kunci, masa tandatangan, masa pengesahan, serta saiz kunci dan tandatangan yang dihasilkan. Keputusan pengujian purata yang diperoleh daripada 10 ulangan ditunjukkan dalam Jadual 4.

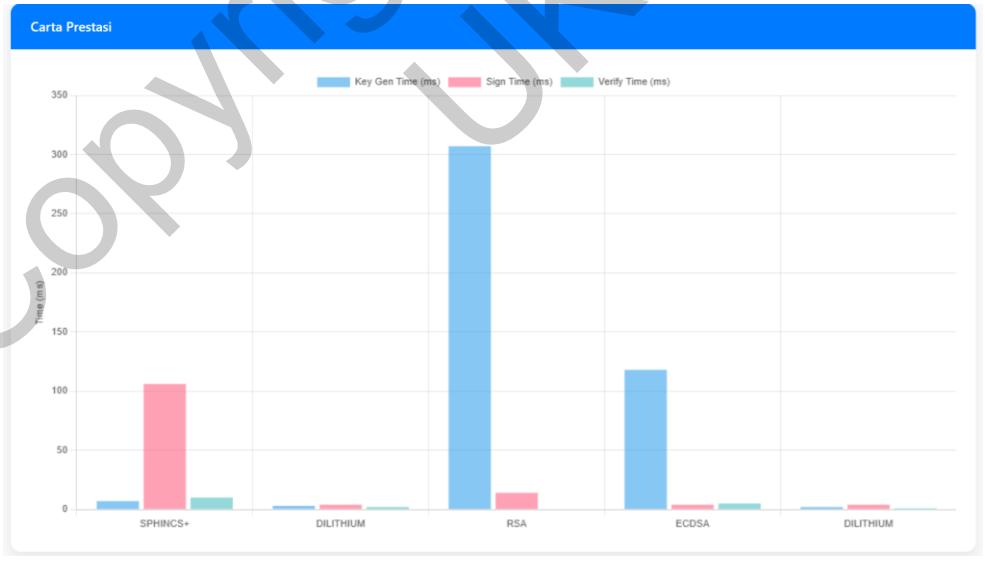
Jadual 4: Keputusan pengujian tanda aras bagi algoritma yang diuji

Keputusan Penanda Aras

Algoritma	Jana Kunci (ms)	Tandatangan (ms)	Sahkan (ms)	Kunci Awam (bait)	Kunci Peribadi (bait)	Tandatangan (bait)
DILITHIUM	2	4	1	1976	6019	3309
ECDSA	118	4	5	91	67	70
RSA	307	14	0	294	1217	256
DILITHIUM	3	4	2	1976	6019	3309
SPHINCS+	7	106	10	47	118	17088

Berdasarkan Jadual 4, keputusan pengujian prestasi algoritma menunjukkan variasi masa penjanaan kunci, masa tandatangan, masa pengesahan, serta saiz kunci dan tandatangan bagi setiap algoritma yang diuji iaitu RSA, ECDSA, CRYSTALS-Dilithium dan SPHINCS+. Hasil ujian menunjukkan bahawa algoritma pasca-kuantum seperti CRYSTALS-Dilithium mampu menjana kunci dan mengesahkan tandatangan dengan masa yang jauh lebih singkat berbanding RSA dan ECDSA. Walaupun SPHINCS+ mempunyai tahap keselamatan yang kukuh, algoritma ini menunjukkan masa tandatangan yang lebih lama dan menghasilkan saiz tandatangan yang lebih besar, sekali gus menuntut penggunaan storan yang lebih tinggi.

Bagi memperkukuh pemahaman terhadap data ujian, sistem telah mengintegrasikan *Chart.js* sebagai komponen visualisasi. *Chart.js* merupakan pustaka JavaScript sumber terbuka yang membolehkan data untuk dipaparkan dalam bentuk carta interaktif dan responsif. Dalam konteks sistem ini, *Chart.js* digunakan untuk memaparkan data prestasi dalam bentuk carta bar seperti yang ditunjukkan dalam Rajah 8 dibawah:



Rajah 8 Keputusan pengujian tanda aras bagi algoritma yang diuji

Carta prestasi memaparkan tiga metrik utama iaitu masa penjanaan kunci, masa tandatangan dan masa pengesahan, dengan setiap algoritma diwakili oleh bar berbeza warna untuk memudahkan perbandingan. RSA menunjukkan masa penjanaan kunci tertinggi melebihi 300

ms, CRYSTALS-Dilithium mencatatkan masa terendah bagi semua metrik, manakala SPHINCS+ mempunyai masa tandatangan paling tinggi walaupun metrik lain rendah. Visualisasi melalui *Chart.js* memudahkan pemahaman prestasi setiap algoritma, membolehkan keputusan dibuat dengan lebih tepat serta menyokong objektif projek dalam menilai keberkesanan algoritma PQC.

Cadangan Penambahbaikan

Beberapa cadangan boleh dipertimbangkan bagi menambahbaik dan memperluas sistem ini di masa hadapan:

1. Menambah sokongan terhadap sijil digital seperti X.509 dan format penyimpanan seperti PKCS#12 supaya sistem dapat diintegrasikan dengan infrastruktur kunci awam (PKI) sebenar. Dengan ciri ini, sistem akan lebih bersedia digunakan dalam persekitaran organisasi atau komersial yang memerlukan pengurusan sijil yang patuh piawaian.

2. Menyediakan mekanisme untuk menyimpan kunci awam, kunci peribadi yang disulitkan, sijil digital, dan log aktiviti pengguna dalam pangkalan data berskala besar. Ciri ini membolehkan sistem mengurus ratusan atau ribuan entiti dengan lebih sistematik, menyokong capaian pantas, kawalan akses terperinci, serta meningkatkan tahap keselamatan dan kebolehkesanan.

3. Menyediakan fungsi untuk membatalkan sijil atau kunci yang telah disalah guna, hilang atau tidak lagi sah. Ciri ini penting bagi memastikan keselamatan jangka panjang, kerana pengguna lain boleh merujuk kepada CRL untuk mengenal pasti sijil yang telah dibatalkan sebelum mempercayai sesuatu tandatangan digital.

KESIMPULAN

Secara keseluruhannya, sistem tandatangan digital ini telah berjaya dibangunkan sebagai sebuah platform bukti konsep (PoC) yang memenuhi objektif kajian dan keperluan yang telah ditetapkan. Sistem ini berupaya menjana kunci, menandatangani serta mengesahkan tandatangan digital dengan menyokong algoritma tradisional seperti RSA dan ECDSA serta algoritma pasca-kuantum CRYSTALS-Dilithium dan SPHINCS+. Sepanjang pembangunan, beberapa cabaran teknikal berjaya diatasi, sekali gus memastikan sistem ini dapat berfungsi dengan stabil dan memenuhi fungsi yang telah dirancang. Diharapkan sistem ini menjadi asas rujukan dan titik permulaan bagi kajian dan pembangunan lanjut dalam bidang tandatangan digital berasaskan algoritma pasca-kuantum.

Kekuatan Sistem

Sistem ini menyokong pelbagai algoritma tandatangan digital termasuk RSA, ECDSA, CRYSTALS-Dilithium dan SPHINCS+, menjadikannya bersedia menghadapi ancaman keselamatan kuantum pada masa hadapan. Keupayaan untuk menjana, menandatangani dan mengesahkan tandatangan secara automatik bagi semua algoritma menunjukkan fleksibiliti dan keberkesanan sistem. Antara muka pengguna yang dibangunkan dengan Bootstrap juga

mesra pengguna, ringkas dan responsif, memudahkan proses penggunaan. Selain itu, fungsi tanda aras prestasi yang disediakan dapat mengukur dan membandingkan masa serta saiz kunci dan tandatangan, sekali gus membantu pemilihan algoritma yang sesuai mengikut keperluan.

Kelemahan Sistem

Walau bagaimanapun, terdapat beberapa kekangan yang dikenal pasti. Algoritma SPHINCS+ menghasilkan tandatangan bersaiz sangat besar (sekitar 17 KB), yang kurang praktikal untuk aplikasi dengan keperluan pemindahan data yang kecil atau pantas. Sistem ini juga hanya menyimpan pasangan kunci dan tandatangan dalam format Base64 asas tanpa sokongan pengurusan sijil digital standard seperti X.509 atau PKCS#12, menyebabkan ia kurang sesuai untuk persekitaran PKI sebenar. Di samping itu, sistem ini hanya memfokuskan kepada fungsi tandatangan digital tanpa melibatkan penyulitan data atau pengurusan identiti yang lebih komprehensif. Walaupun begitu, kekangan ini membuka ruang untuk penambahbaikan masa hadapan bagi meningkatkan kebolehlaksanaan sistem dalam kegunaan sebenar.

PENGHARGAAN

Syukur ke hadrat Ilahi atas kekuatan dan kesihatan yang mengizinkan saya menyiapkan projek ini. Setinggi-tinggi penghargaan ditujukan kepada penyelia saya, Dr. Azana Hafizah binti Mohd Aman, penasihat industri Encik Hazhar Ismail serta seluruh pasukan teknikal MSC Trustgate atas bimbingan dan sokongan yang tidak ternilai sepanjang pembangunan projek. Projek ini juga mendapat sokongan dana daripada MSC Trustgate yang banyak membantu dalam merealisasikan kajian ini. Ucapan terima kasih turut ditujukan kepada semua pensyarah dan staf Fakulti Teknologi dan Sains Maklumat atas tunjuk ajar serta dorongan berterusan, serta kepada semua yang memberi sokongan moral sepanjang perjalanan projek ini.

RUJUKAN

Ankita. (2024). *SPHINCS+: A Comprehensive Guide to Post-Quantum Signatures in Blockchain* https://medium.com/@ankitacode11/sphincs-a-comprehensive-guide-to-post-quantum-signatures-in-blockchain-7c6e0bbfd4aa [24 Jun 2025]

Bos, J. W., Ducas, L., Kiltz, E., Lepoint, T., Lyubashevsky, V., Schwabe, P., Seiler, G., & Stehlé, D. (2018). *CRYSTALS – Kyber and Dilithium in Practice.* In Advances in Cryptology – EUROCRYPT 2018. Springer, Cham.

Bouncy Castle. (2025). *The Legion of the Bouncy Castle.* https://www.bouncycastle.org/.

Chen, L., Chen, L.-K., Jordan, S., Liu, Y.-K., Moody, D., Peralta, R., Perlner, R., & Smith-Tone, D. (2016). *Report on Post-Quantum Cryptography.* U.S. Department of Commerce, NIST.

Dorota, D. (2023). *An Overview of Cryptography and Network Security.* International Journal of Advanced Trends in Computer Science and Engineering, 12(1), 1–9.

Hülsing, A., Rijneveld, J., Künnemann, R., Kampanakis, P., & Wiggers, T. (2022). *SPHINCS+ Specification v3.1.* https://sphincs.org/data/sphincs+-r3.1-specification.pdf

Moody, D., Perlner, R., Regenscheid, A., Robinson, A., & Cooper, D. (2024). Transition to post-quantum cryptography standards (No. NIST Internal or Interagency Report (NISTIR) 8547 (Draft)). National Institute of Standards and Technology.

NIST. (2022, 2024). *NIST Announces First Post-Quantum Cryptography Standards.* https://www.nist.gov/news-events/news/2024/08/nist-announces-pqc-standards

Post-Quantum. (2025). *NIST's PQC Technical Standardization: What You Need to Know.* https://postquantum.com/post-quantum/nists-pqc-technical

Rdogan, Y. (2021). *The Elliptic Curve Digital Signature Algorithm (ECDSA).* https://dev.to/yusuferdogan/the-elliptic-curve-digital-signature-algorithm-ecdsa-jng

Sutherland, B. (2025). *Kyber and Dilithium: Post-Quantum Cryptography Demonstration.* https://asecuritysite.com/encryption/kyber3

Wang, M., & Long, G. L. (2024). Lattice-based access authentication scheme for quantum communication networks. Science China Information Sciences, 67(12), 222501.

Zachary, M. Z., Sylviani, S., & Kurniadi, E. (2024). Implementasi Algoritma RSA (Rivest-Shamir-Adleman) pada Kriptografi Klasik. Mathematical Sciences and Applications Journal, 4(2), 54–59. https://doi.org/10.22437/msa.v4i2.28863

Nurul Syafiqah Binti Norihsan (A194682)
Dr. Azana Hafizah Binti Mohd Aman
Fakulti Teknologi & Sains Maklumat
Universiti Kebangsaan Malaysia