METODE ASSYMETRIC CRYPTOGRAPHY UNTUK MENJAMIN OTENTIKASI DOKUMEN ELEKTRONIK PADA DINAS KOMUNIKASI DAN INFORMATIKA KOTA SERANG

Apud Ismail, Muhammad Sohari
Sistem Informasi, Universitas Muhammadiyah Banten, Serang
Email: apud88@live.com, sohari88@gmail.com

ABSTRAK
Penggunaan dokumen elektronik dan tanda tangan digital kini semakin krusial di era digital. Dokumen elektronik memudahkan pertukaran informasi secara cepat, efisien, dan hemat biaya. Sementara itu, tanda tangan digital berbasis enkripsi menjamin keamanan serta integritas dokumen, sehingga meminimalkan potensi pemalsuan. Penelitian ini bertujuan untuk merancang sistem informasi berbasis web yang dapat menghasilkan dokumen elektronik sekaligus menyematkan tanda tangan digital menggunakan metode *Asymmetric Cryptography*. Sistem dikembangkan menggunakan model *Waterfall* dengan tahapan analisis kebutuhan, perancangan sistem, implementasi, dan pengujian menggunakan *black box testing*. Hasil penelitian menunjukkan bahwa aplikasi ini mampu menjamin keaslian dan keamanan dokumen elektronik secara efisien dan dapat mendukung penerapan *e-government* di lingkungan Pemerintah Kota Serang.

Kata kunci: Dokumen Elektronik, Tanda Tangan Digital, *Asymmetric Cryptography*

ABSTRACT
The use of electronic documents and digital signatures has become increasingly crucial in today's digital era. Electronic documents enable fast, efficient, and cost-effective information exchange. Meanwhile, digital signatures based on encryption ensure document security and integrity, minimizing the risk of forgery. This study aims to design a web-based information system capable of generating electronic documents while embedding digital signatures using the principles of Asymmetric Cryptography. The system was developed using the Waterfall model through stages of requirements analysis, system design, implementation, and testing using black box testing. The results indicate that the application ensures authenticity and security of electronic documents efficiently and supports the implementation of e-government in Serang City.
Keywords: Electronic Document, Digital Signature, Asymmetric Cryptography

PENDAHULUAN

Transformasi digital dalam tata kelola pemerintahan mendorong perubahan signifikan pada sistem administrasi publik, terutama dalam pengelolaan dokumen dan pelayanan berbasis elektronik. Salah satu tantangan utama adalah memastikan keaslian dan integritas dokumen elektronik yang beredar antar instansi. Walaupun sudah diatur dalam Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (ITE) serta Peraturan Pemerintah Nomor 82 Tahun 2012 tentang Penyelenggaraan Sistem dan Transaksi Elektronik,

implementasi tanda tangan digital di daerah masih belum optimal. Dinas Komunikasi dan Informatika (Diskominfo) Kota Serang membutuhkan sistem yang mampu menghasilkan dan memverifikasi dokumen elektronik dengan aman. Oleh karena itu, penelitian ini merancang aplikasi dokumen elektronik berbasis *Asymmetric Cryptography* untuk menjamin otentikasi dan keamanan dokumen secara digital.

METODE

Metode *Asymmetric Cryptography* atau kriptografi asimetris merupakan pendekatan fundamental dalam penerapan tanda tangan digital *(digital signature)* yang berfungsi untuk menjamin keaslian (autentikasi), keutuhan (integritas), serta penyangkalan *(non-repudiation)* dokumen elektronik. Sistem ini menggunakan dua kunci yang berbeda namun saling berpasangan, yaitu kunci privat *(private key)* dan kunci publik *(public key)*. Kunci privat hanya diketahui oleh pemilik tanda tangan, sedangkan kunci publik dapat diakses secara terbuka oleh pihak yang berkepentingan dalam proses verifikasi.

Dalam konteks penerapan tanda tangan digital, proses otentikasi dokumen elektronik melalui kriptografi asimetris dilakukan melalui dua tahapan utama, yaitu pembuatan tanda tangan digital dan verifikasi tanda tangan digital.

Pada tahap pertama, dokumen elektronik yang akan ditandatangani diolah menggunakan algoritma fungsi *hash* untuk menghasilkan nilai *hash* unik yang merepresentasikan isi dokumen secara menyeluruh. Nilai *hash* ini kemudian dienkripsi menggunakan kunci privat milik penandatangan, menghasilkan tanda tangan digital yang disertakan bersama dokumen elektronik tersebut.

Tahap kedua adalah verifikasi, yang dilakukan oleh penerima dokumen. Penerima menggunakan kunci publik milik pengirim untuk mendekripsi tanda tangan digital dan memperoleh kembali nilai *hash* asli yang dihasilkan pada saat penandatanganan. Selanjutnya, penerima melakukan proses hashing terhadap dokumen yang diterima untuk memperoleh nilai *hash* pembanding. Apabila kedua nilai *hash* tersebut identik, maka dapat dipastikan bahwa dokumen tidak mengalami perubahan (integritas terjamin) dan tanda tangan benar berasal dari pemegang kunci privat yang sah (otentikasi terjamin). Sebaliknya, apabila nilai hash berbeda, maka dokumen dianggap tidak valid karena telah dimodifikasi atau tanda tangan tidak sah.

Dengan demikian, penerapan metode *Asymmetric Cryptography* dalam sistem tanda tangan digital mampu memberikan jaminan keamanan terhadap dokumen elektronik melalui tiga aspek utama, yaitu:

- Autentikasi, memastikan bahwa dokumen benar berasal dari pihak yang berwenang;
- Integritas, menjamin isi dokumen tidak mengalami perubahan setelah penandatanganan;
- *Non-repudiation,* mencegah penandatangan menyangkal keterlibatannya dalam proses autentikasi dokumen.

Sebagai contoh, implementasi tanda tangan digital di lingkungan Pemerintah Kota Serang yang terintegrasi dengan layanan Balai Sertifikasi Elektronik (BSrE) Badan Siber dan Sandi Negara (BSSN), menggunakan mekanisme kriptografi asimetris untuk memastikan keaslian dokumen resmi pemerintah. Dengan metode ini, setiap dokumen yang telah ditandatangani secara digital dapat diverifikasi secara elektronik oleh penerima tanpa mengurangi keabsahan hukum dokumen tersebut, sebagaimana diatur dalam Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik serta peraturan turunannya.

1. Lokasi dan Waktu Penelitian
   Penelitian dilakukan di Dinas Komunikasi dan Informatika Kota Serang, Jl. Jenderal Sudirman No. 25, Sumur Pecung, Serang – Banten. Waktu pelaksanaan dimulai pada 26 Juni 2023 hingga 3 Agustus 2023.
2. Metode Pengembangan Sistem
   Metode pengembangan perangkat lunak yang digunakan adalah model *Waterfall* yang terdiri dari lima tahap:
   a. Analisis kebutuhan sistem
   b. Perancangan sistem *(System Design)*
   c. Implementasi *(Coding)*
   d. Pengujian *(Testing)*
   e. Pemeliharaan *(Maintenance)*

   Gambar 1. Model Pengembangan Waterfall

   ```
   Analisis → Desain → Implementasi → Uji Coba → Pemeliharaan
   ```
3. Teknik Pengumpulan Data
   a. Observasi: Melihat langsung proses persuratan di Diskominfo Kota Serang.
   b. Wawancara: Dengan staf pengelola dokumen dan pejabat terkait.
   c. Studi pustaka: Mengkaji teori kriptografi dan regulasi *e-government*
4. Rumus Kriptografi.
   Penelitian ini menggunakan algoritma *Asymmetric Cryptography* yang terdiri dari dua kunci berbeda:

$$h = H(M)$$

$$S = E_{PrivK}(h)$$

$$h' = D_{PubK}(S)$$

   Jika h = h′, maka dokumen dianggap autentik dan tidak dimodifikasi.

   Proses pengujian dilakukan menggunakan metode *black box* untuk memastikan bahwa setiap fungsi berjalan sesuai spesifikasi.

HASIL DAN PEMBAHASAN

1. Analisis Kebutuhan Sistem

   Berdasarkan hasil observasi, dibutuhkan sistem yang dapat melakukan proses pembuatan, penandatanganan, dan verifikasi dokumen elektronik secara otomatis.

Tabel 1. Kebutuhan Sistem dan Aktor Utama

No	Aktor	Fungsi	Deskripsi
1	Admin	Manajemen user	Membuat, menghapus, dan mengatur pengguna
2	Pegawai	Membuat dokumen elektronik	Menginput data dokumen ke sistem
3	Pejabat	Menandatangani digital	Membubuhkan tanda tangan digital
4	Sistem	Verifikasi dokumen	Memverifikasi keaslian dan hash dokumen

2. Desain Sistem

   Aplikasi dokumen elektronik dirancang berbasis web menggunakan bahasa pemrograman PHP dan basis data MySQL. Sistem memiliki fitur utama berupa pembuatan dokumen, tanda tangan digital, verifikasi dokumen, dan arsip elektronik.

Gambar 2. Diagram *Use Case* Sistem Dokumen Elektronik

```
Pegawai → [Membuat Dokumen]
Pejabat → [Tanda Tangan Digital]
Sistem → [Verifikasi & Arsip Dokumen]
```

3. Implementasi Sistem

   Implementasi sistem meliputi pembuatan antarmuka pengguna, modul tanda tangan digital, serta modul arsip dokumen.

Tabel 2. Skenario Pengujian Black Box

No	Fungsi Diuji	Skenario	Hasil
1	*Login*	Kredensial valid	Sukses
2	Pembuatan dokumen	Dokumen disimpan	Sukses
3	Tanda tangan digital	Enkripsi dan hash diverifikasi	Sukses
4	Verifikasi dokumen	Cocokkan kunci publik/privat	Sukses
5	Unduh dokumen	Dokumen terarsip dengan benar	Sukses

4. Analisis Hasil Uji Validasi *Pre-Test* dan *Post-Test*
   Uji validasi *pre-test* dan *post-test* dilakukan untuk mengukur tingkat pemahaman serta efektivitas penggunaan Aplikasi Dokumen Elektronik dengan Metode *Asymmetric Cryptography* pada Dinas Komunikasi dan Informatika Kota Serang. Pengujian ini bertujuan untuk mengetahui sejauh mana penerapan sistem mampu meningkatkan efisiensi dan pemahaman pengguna terhadap proses bisnis tanda tangan digital.
   a. Tahapan Pengujian
      Tahapan validasi dilakukan melalui dua fase utama, yaitu:
      - *Pre-Test*, yaitu pengisian kuesioner sebelum implementasi sistem, yang bertujuan untuk mengukur tingkat pengetahuan dan kesiapan pengguna terhadap penerapan tanda tangan digital.
      - *Post-Test*, yaitu pengisian kuesioner setelah sistem diterapkan, dengan menggunakan instrumen pertanyaan yang sama, untuk melihat perubahan signifikan terhadap pemahaman dan penerimaan pengguna.

      Kuesioner disusun berdasarkan 10 butir pertanyaan yang mencakup aspek pemahaman proses bisnis, kendala waktu dan tempat, kemudahan penggunaan alat, serta kesiapan mengadopsi sistem tanda tangan digital. Penilaian menggunakan skala Likert 1–5, di mana skor 1 menunjukkan ketidaksepakatan dan skor 5 menunjukkan tingkat persetujuan tertinggi.
   b. Tahapan Pengujian
      Hasil pengisian kuesioner *pre-test* oleh 10 responden menunjukkan total skor sebesar 269, dengan rata-rata nilai 26,90 dan standar deviasi 6,184. Nilai ini menggambarkan bahwa sebelum implementasi sistem, sebagian besar pegawai masih memiliki pemahaman yang terbatas terhadap konsep tanda tangan digital dan penerapannya pada dokumen elektronik.
      Kendala utama yang diidentifikasi pada tahap ini adalah:
      - Proses tanda tangan dokumen masih dilakukan secara manual;
      - Terjadi keterlambatan akibat ketergantungan pada keberadaan fisik pejabat penandatangan;
      - Minimnya sosialisasi dan pemahaman terhadap aplikasi *e-sign* dari BSSN.
   c. Hasil *Post-Test*
      Setelah implementasi aplikasi dokumen elektronik berbasis *Asymmetric Cryptography*, dilakukan pengisian kuesioner *post-test* oleh responden yang sama. Total skor keseluruhan meningkat menjadi 467, dengan rata-rata 46,70 dan standar deviasi 3,090. Hasil ini menunjukkan adanya peningkatan signifikan dalam pemahaman dan kemudahan penggunaan sistem.
      Peningkatan skor tersebut menunjukkan bahwa pengguna merasakan manfaat nyata dari sistem, di antaranya:

- Kemudahan proses tanda tangan dokumen secara elektronik tanpa batas waktu dan tempat;
- Terjaminnya aspek keaslian *(authenticity)* dan integritas *(integrity)* dokumen;
- Adanya kepercayaan lebih tinggi terhadap keabsahan tanda tangan digital yang dikeluarkan melalui mekanisme kriptografi asimetris.

d. Analisis Statistik

Untuk mengetahui signifikansi perbedaan hasil sebelum dan sesudah implementasi sistem, dilakukan analisis menggunakan *Paired Sample T-Test* melalui perangkat lunak *SPSS* versi 27.

Hasil uji menunjukkan :

- Rata-rata *(Mean Difference)* antara *pre-test* dan *post-test* sebesar -19,800,
- Nilai t = -10,490, dengan derajat kebebasan (df) = 9,
- Signifikansi (Sig. 2-tailed) = 0,001.

Karena nilai signifikansi lebih kecil dari 0,05 (0,001 < 0,05), maka hipotesis nol (H_0) ditolak dan hipotesis alternatif (H_a) diterima. Dengan demikian, dapat disimpulkan bahwa terdapat perbedaan yang signifikan antara hasil pre-test dan post-test, yang berarti penerapan aplikasi dokumen elektronik dengan metode kriptografi asimetris berdampak positif secara signifikan terhadap peningkatan efektivitas dan pemahaman pengguna.

Selain itu, hasil korelasi antara *pre-test* dan *post-test* sebesar 0,595 menunjukkan hubungan positif yang cukup kuat, yang mengindikasikan bahwa responden yang sebelumnya memiliki tingkat pemahaman rendah mengalami peningkatan setelah sistem diterapkan.

Hasil uji validasi ini membuktikan bahwa penerapan tanda tangan digital dengan prinsip *Asymmetric Cryptography* tidak hanya memberikan jaminan keamanan dan keaslian dokumen, tetapi juga mendorong perubahan perilaku kerja pegawai menuju digitalisasi administrasi yang lebih efisien. Implementasi sistem terbukti dapat meminimalisasi kendala birokrasi manual, mempercepat proses penandatanganan dokumen, serta meningkatkan kesadaran terhadap pentingnya tanda tangan digital dalam mendukung program *e-government*.

Dengan demikian, hasil penelitian ini sejalan dengan teori kriptografi asimetris yang dikemukakan oleh Rinaldi Munir (2019), di mana penggunaan pasangan kunci publik dan privat dapat menjamin *authenticity, integrity*, dan *non-repudiation* pada dokumen elektronik.

Tabel 3. Efisiensi Proses Dokumen

Aspek	Sebelum	Sesudah	Peningkatan (%)
Waktu pembuatan dokumen	15 menit	5 menit	66,7%
Waktu tanda tangan	10 menit	2 menit	80%
Akurasi dokumen	85%	98%	+13%
Kepuasan pengguna	70%	95%	+25%

SIMPULAN

Penelitian ini berhasil merancang aplikasi dokumen elektronik berbasis *Asymmetric Cryptography* yang menjamin otentikasi dokumen elektronik pada Dinas Komunikasi dan Informatika Kota Serang. Aplikasi ini meningkatkan efisiensi waktu, mengurangi penggunaan kertas, dan mendukung implementasi *e-government* di lingkungan pemerintah daerah. Pengembangan selanjutnya dapat diarahkan pada integrasi antar-Organisasi Perangkat Daerah (OPD) serta penerapan teknologi *blockchain* untuk meningkatkan keamanan dan transparansi sistem.

UCAPAN TERIMAKASIH

Penulis mengucapkan terima kasih kepada Dinas Komunikasi dan Informatika Kota Serang atas dukungan dan izin penelitian, serta kepada Universitas Muhammadiyah Banten yang telah memberikan bimbingan dan fasilitas selama proses penelitian ini.

DAFTAR PUSTAKA

Agung, H., & Ferry. (2016). *Kriptografi Menggunakan Hybrid Cryptosystem dan Digital Signature*. Jurnal Jatisi, 3(1).

Izzah, A. N. E., & Sugandha, W. (2021). *Penggunaan Tanda Tangan Elektronik Dalam Penyelenggaraan E-Government Guna Mewujudkan Pelayanan Publik yang Efisien*. JOLSIC.

Margianto, R., Patonah, Lisnawati, & Santoso. (2022). *Tanda Tangan Elektronik untuk Efisiensi dan Efektivitas Birokrasi*. Lex Specialis.

Munir, R. (2019). *Kriptografi.* Bandung: Informatika.

Prabowo, E. C., & Afrianto, I. (2017). *Penerapan Digital Signature dan Kriptografi pada Otentikasi Sertifikat Tanah Digital*. KOMPUTA.

Pressman, R. S. (2015). *Software Engineering: A Practitioner's Approach*. New York: McGraw-Hill.

Walikota Serang. (2022). *Peraturan Walikota Serang Nomor 14 Tahun 2022 Tentang Penerapan Sertifikat Elektronik Pada SPBE di Pemerintah Kota Serang.*