PRAKTIKUM SISTEM KEAMANAN DATA

**REVIEW JURNAL**

**“AES”**

****

**DISUSUN OLEH :**

Ahitsa Dawang Ransifa (V3922002)

Alia Dewanto (V3922004)

Ariel Fajar Herdanto (V3922007)

**DOSEN :**

Yusuf Fadlila Rachman S.Kom,. M.Kom

**PS D-III TEKNIK INFORMATIKA**

**SEKOLAH VOKASI**

**UNIVERSITAS SEBELAS MARET**

**2023**

1. **JURNAL 1**

| Judul | Model Keamanan Informasi Berbasis Digital Signature dengan Algoritma RSA |
| --- | --- |
| Nama Jurnal | Journal Of Computer Engineering System And Science |
| Volume & Halaman | Vol. 9 halaman belum |
| Tahun | 2016 |
| Penulis | Muhammad Arif Zainuddin, Dadang Iskandar Mulyana |
| Reviewer | Ahitsa Dawang Ransifa |
| Tanggal | 11-11-2023 |

| Latar Belakang Masalah | Dalam era digital saat ini, keamanan informasi menjadi sangat penting untuk menjaga kerahasiaan dan integritas data perusahaan. Salah satu teknik yang digunakan untuk menjaga keamanan informasi adalah kriptografi. Namun, kriptografi saja tidak cukup untuk membuktikan keaslian identitas pengirim atau penandatangan dari suatu pesan atau dokumen digital. Oleh karena itu, diperlukan teknik lain yang dapat membuktikan keaslian identitas pengirim atau penandatangan dari suatu pesan atau dokumen digital, yaitu Digital Signature Algorithm (DSA). Dalam penelitian ini, akan dibahas tentang bagaimana DSA dapat digunakan untuk membuktikan keaslian identitas pengirim atau penandatangan dari suatu pesan atau dokumen digital dengan menggunakan algoritma RSA. |
| --- | --- |
| Tujuan Penelitian | Penelitian ini bertujuan untuk mengembangkan teknik keamanan informasi berbasis digital signature dengan menggunakan algoritma RSA. Teknik ini diharapkan dapat membuktikan keaslian identitas pengirim atau penandatangan dari suatu pesan atau dokumen digital dengan lebih efektif dan efisien. Selain itu, penelitian ini juga bertujuan untuk menguji keamanan teknik ini dan membandingkannya dengan teknik keamanan informasi lainnya. Dengan demikian, diharapkan penelitian ini dapat memberikan kontribusi dalam meningkatkan keamanan informasi perusahaan dan masyarakat secara umum. |
| Algoritma dan Alur Penelitian | Algoritma yang dipakai dalam penelitian ini adalah Digital Signature Algorithm (DSA) yang dikombinasikan dengan algoritma RSA. Berikut adalah alur penelitiannya:  1. Studi literatur tentang kriptografi, DSA, dan RSA.  2. Perancangan model keamanan informasi berbasis digital signature dengan algoritma RSA.  3. Implementasi model keamanan informasi berbasis digital signature dengan algoritma RSA menggunakan bahasa pemrograman PHP.  4. Uji coba model keamanan informasi berbasis digital signature dengan algoritma RSA pada sistem operasi Windows 10.  5. Analisis hasil uji coba dan perbandingan dengan teknik keamanan informasi lainnya.  6. Evaluasi keamanan model keamanan informasi berbasis digital signature dengan algoritma RSA.  7. Penulisan laporan hasil penelitian.  Dalam penelitian ini, algoritma RSA digunakan untuk melakukan proses enkripsi pada hashing MD5 sehingga message digest terjaga dan terenkripsi. Sedangkan DSA digunakan untuk membuktikan keaslian identitas pengirim atau penandatangan dari suatu pesan atau dokumen digital. Proses enkripsi dilakukan dengan membagi plainteks menjadi 2 bagian, yaitu bagian plainteks asli dan bagian plainteks yang diubah menjadi message digest dengan menggunakan hashing MD5. Kemudian, proses enkripsi message digest dilakukan dengan menggunakan RSA. Proses dekripsi dilakukan dengan mendekripsi cipherteks RSA sehingga menghasilkan message digest yang diperoleh dari hasil hashing MD5. Plainteks asli akan dijadikan message digest dengan MD5 dan akan dicocokkan dengan hasil message digest dari dekripsi RSA. |
| Hasil Penelitian dan Kesimpulan | Hasil penelitian yang dilaporkan pada jurnal tersebut adalah berhasilnya pengembangan teknik keamanan informasi berbasis digital signature dengan algoritma RSA. Teknik ini dapat membuktikan keaslian identitas pengirim atau penandatangan dari suatu pesan atau dokumen digital dengan lebih efektif dan efisien. Selain itu, teknik ini juga memiliki keamanan yang lebih baik dibandingkan dengan teknik keamanan informasi lainnya.  Dalam uji coba yang dilakukan, teknik keamanan informasi berbasis digital signature dengan algoritma RSA berhasil menghasilkan tanda tangan digital yang valid dan dapat membuktikan keaslian identitas pengirim atau penandatangan dari suatu pesan atau dokumen digital. Selain itu, teknik ini juga berhasil mengatasi kelemahan dari sisi plainteks yang dimiliki oleh algoritma DSA dengan fungsi hash.  Berdasarkan hasil penelitian, dapat disimpulkan bahwa teknik keamanan informasi berbasis digital signature dengan algoritma RSA dapat menjadi alternatif yang baik dalam menjaga keamanan informasi perusahaan dan masyarakat secara umum. Teknik ini dapat digunakan untuk membuktikan keaslian identitas pengirim atau penandatangan dari suatu pesan atau dokumen digital dengan lebih efektif dan efisien. Namun, penelitian lebih lanjut masih diperlukan untuk menguji keamanan teknik ini pada skala yang lebih besar dan lebih kompleks. |
| Kelebihan dan Kekurangan | Kelebihan dari teknik keamanan informasi berbasis digital signature dengan algoritma RSA adalah sebagai berikut:  1. Dapat membuktikan keaslian identitas pengirim atau penandatangan dari suatu pesan atau dokumen digital dengan lebih efektif dan efisien.  2. Lebih aman dibandingkan dengan teknik keamanan informasi lainnya karena menggunakan kombinasi dari algoritma RSA dan DSA.  3. Dapat mengatasi kelemahan dari sisi plainteks yang dimiliki oleh algoritma DSA dengan fungsi hash.  Namun, teknik keamanan informasi berbasis digital signature dengan algoritma RSA juga memiliki beberapa kekurangan, yaitu:  1. Memerlukan waktu yang lebih lama untuk melakukan proses enkripsi dan dekripsi dibandingkan dengan teknik keamanan informasi lainnya.  2. Memerlukan sumber daya komputasi yang lebih besar untuk melakukan proses enkripsi dan dekripsi.  3. Memerlukan kunci yang lebih panjang untuk menghasilkan tingkat keamanan yang lebih tinggi, sehingga memerlukan pengelolaan kunci yang lebih rumit. |

1. **JURNAL 2**

| Judul | APLIKASI PENGAMANAN DATA DAN DISISIPKAN PADA GAMBAR DENGAN ALGORITMA RSA DAN MODIFIED LSB BERBASIS ANDROID |
| --- | --- |
| Nama Jurnal | Journal Of Computer Engineering System And Science |
| Volume & Halaman |  |
| Tahun | 2019 |
| Penulis | Muhammad Ridwan Rambe, Edy Victor Haryanto, Adil Setiawan |
| Reviewer | Alia Dewanto |
| Tanggal | 11 November 2023 |

| Latar Belakang Masalah | Keamanan data pada smartphone, terutama dalam hal penyimpanan username dan password akun yang dapat disalahgunakan oleh pihak yang tidak bertanggung jawab. Dokumen ini membahas tentang metode kriptografi dan steganografi yang dapat digunakan untuk mengamankan data pada smartphone, serta merancang aplikasi pengamanan data berbasis Android dengan menggunakan algoritma RSA dan Modified LSB. |
| --- | --- |
| Tujuan Penelitian | Merancang dan mengembangkan aplikasi pengamanan data berbasis Android dengan menggunakan metode kriptografi dan steganografi. Aplikasi ini dirancang untuk mengamankan data sensitif pada smartphone, terutama dalam hal penyimpanan username dan password akun. Selain itu, penelitian ini juga bertujuan untuk menguji keamanan aplikasi yang dikembangkan dengan melakukan serangkaian pengujian dan analisis. |
| Algoritma dan Alur Penelitian | Dalam dokumen ini, terdapat dua algoritma yang digunakan, yaitu algoritma RSA dan Modified LSB. Algoritma RSA digunakan untuk mengamankan data dengan cara melakukan enkripsi dan dekripsi data menggunakan pasangan kunci publik dan kunci privat. Alur penelitian untuk algoritma RSA meliputi: 1. Menganalisis dan memahami konsep dasar algoritma RSA 2. Merancang dan mengimplementasikan algoritma RSA pada aplikasi pengamanan data berbasis Android 3. Melakukan pengujian dan analisis keamanan pada aplikasi yang dikembangkan dengan menggunakan algoritma RSA Sedangkan algoritma Modified LSB digunakan untuk menyembunyikan data dalam media gambar dengan cara memodifikasi bit pada piksel gambar. Alur penelitian untuk algoritma Modified LSB meliputi: 1. Menganalisis dan memahami konsep dasar algoritma Modified LSB 2. Merancang dan mengimplementasikan algoritma Modified LSB pada aplikasi pengamanan data berbasis Android 3. Melakukan pengujian dan analisis keamanan pada aplikasi yang dikembangkan dengan menggunakan algoritma Modified LSB Kedua algoritma tersebut kemudian digabungkan untuk menciptakan aplikasi pengamanan data berbasis Android yang lebih aman dan terjamin keamanannya. |
| Hasil Penelitian dan Kesimpulan | Berhasilnya pengembangan aplikasi pengamanan data berbasis Android dengan menggunakan algoritma RSA dan Modified LSB. Aplikasi ini mampu mengamankan data sensitif pada smartphone, terutama dalam hal penyimpanan username dan password akun. Selain itu, aplikasi ini juga mampu menyembunyikan data dalam media gambar dengan menggunakan algoritma Modified LSB.  Berdasarkan hasil penelitian, dapat diambil beberapa kesimpulan sebagai berikut: - Aplikasi pengamanan data berbasis Android dengan menggunakan algoritma RSA dan Modified LSB dapat dikembangkan dengan baik dan mampu mengamankan data sensitif pada smartphone. - Algoritma RSA dan Modified LSB yang digunakan pada aplikasi ini mampu meningkatkan keamanan data pada smartphone. - Pengujian dan analisis keamanan pada aplikasi ini menunjukkan bahwa aplikasi ini cukup aman dan terjamin keamanannya. Dengan demikian, aplikasi pengamanan data berbasis Android dengan menggunakan algoritma RSA dan Modified LSB dapat menjadi solusi yang efektif untuk mengamankan data sensitif pada smartphone. |
| Kelebihan dan Kekurangan | Kelebihan dari aplikasi pengamanan data berbasis Android dengan menggunakan algoritma RSA dan Modified LSB adalah: - Mampu mengamankan data sensitif pada smartphone dengan baik. - Algoritma RSA dan Modified LSB yang digunakan pada aplikasi ini mampu meningkatkan keamanan data pada smartphone. - Aplikasi ini juga mampu menyembunyikan data dalam media gambar dengan menggunakan algoritma Modified LSB. Kekurangan dari aplikasi pengamanan data berbasis Android dengan menggunakan algoritma RSA dan Modified LSB adalah: - Pembangkitan bilangan prima p dan q sebaiknya menghasilkan nilai n yang besar, sehingga menghasilkan nilai n yang sulit untuk difaktorkan agar keamanan kunci private pada algoritma RSA tetap dapat terjaga. - Pengembangan metode modified LSB juga dapat dilakukan dengan menambah byte warna biru dan hijau, atau menyisipkan bit – bit cipherteks secara diagonal kedalam byte – byte cover object. Namun, secara keseluruhan, aplikasi pengamanan data berbasis Android dengan menggunakan algoritma RSA dan Modified LSB dapat menjadi solusi yang efektif untuk mengamankan data sensitif pada smartphone. |