INDOTECH
Indonesian Journal of Education And Computer Science
Vol. 1, No. 3, Desember 2023
Hal 89-97
E-ISSN : 2987-2650
P-ISSN : 2987-7644
Site : https://jurnal.intekom.id/index.php/indotech

Hybrid Sistem Algoritma *Rivest Shamir Adleman (RSA)* dan Algoritma Blum Blum Shub (BBS) dalam Mengamankan File Database *E-Absensi*

Tania Br Surbakti[1], Achmad Fauzi[2], Husnul Khair[3]
[1,2,3] Fakultas Teknik Informatika, STMIK Kaputama, Binjai, Indonesia

Article Info

Article history:

Received June 12, 2023
Revised July 28, 2023
Accepted August 31, 2023

Kata Kunci:

Hybrid Sistem,
Algoritma RSA,
Algoritma BBS,
E-Absensi,
Keamanan Data.

Keywords:

Hybrid System,
RSA Algorithm,
BBS Algorithm,
E-Attendance,
Data Security.

ABSTRAK

Sistem E-Absensi telah menjadi solusi efisien dalam memantau kehadiran individu di berbagai institusi. Namun, tantangan baru muncul terkait keamanan dan privasi data dalam pengelolaan file database E-Absensi. Menghadapi risiko potensial seperti peretasan dan kebocoran data, pengamanan data menjadi hal yang sangat penting. Oleh karena itu, dalam penelitian ini, kami mengusulkan penerapan hybrid sistem yang menggabungkan kekuatan Algoritma Rivest Shamir Adleman (RSA) dan Algoritma Blum Blum Shub (BBS) untuk meningkatkan keamanan file database E-Absensi. RSA adalah algoritma kriptografi yang banyak digunakan untuk enkripsi dan tanda tangan digital. Di sisi lain, BBS adalah algoritma pembangkitan bilangan acak yang memiliki tingkat keamanan yang kuat. Kombinasi dari keduanya dalam bentuk hybrid sistem diharapkan dapat memberikan tingkat keamanan yang lebih tinggi dalam pengamanan data E-Absensi. Tujuan dari penelitian ini adalah untuk mengembangkan hybrid sistem RSA dan BBS dalam konteks mengamankan file database E-Absensi. Penelitian ini menguraikan konsep dasar dari kedua algoritma tersebut dan bagaimana mereka dapat diintegrasikan. Hasil dari penelitian ini adalah Kombinasi algoritma Rivers, Shamir, Adleman (RSA) dan algoritma Blum Blum Shub (BBS) dalam hybrid sistem meningkatkan keamanan dalam proses penyandian pesan.

ABSTRACT

The E-Attendance System has become an efficient solution in monitoring individual attendance at various institutions. However, new challenges arise regarding data security and privacy in managing E-Attendance database files. Facing potential risks such as hacking and data leaks, data security becomes very important. Therefore, in this study, we propose the implementation of a hybrid system that combines the strengths of the Rivest Shamir Adleman (RSA) Algorithm and the Blum Blum Shub (BBS) Algorithm to improve the security of the E-Absence database file. RSA is a cryptographic algorithm that is widely used for encryption and digital signatures. On the other hand, BBS is a random number generation algorithm that has a strong level of security. The combination of the two in the form of a hybrid system is expected to provide a higher level of security in securing E-Absence data. The aim of this research is to develop a hybrid RSA and BBS system in the context of securing E-Attendance database files. This research outlines the basic concepts of the two algorithms and how they can be integrated. The results of this study are the combination of the Rivers, Shamir, Adleman (RSA) algorithm and the Blum Blum Shub (BBS) algorithm in a hybrid system to increase security in the process of encoding messages.

This is an open access article under the CC BY license.

Corresponding Author:

Tania Br Surbakti
Fakultas Teknik Informatika, STMIK Kaputama
Binjai, Indonesia
Email: brsurbaktitania@gmail.com

1. PENDAHULUAN

Tidak dapat dipungkiri, kemajuan teknologi saat ini membawa kebaikan dan kemudahan dalam pertukaran informasi bagi setiap pihak yang membutuhkan. Namun, hal ini juga diiringi dengan resiko yang cukup tinggi, yaitu pencurian informasi oleh pihak yang tidak berwenang untuk kepentingan pribadi. Salah satu pencurian informasi yang dilakukan oleh pihak yang tidak berwenang adalah pencurian identitas. Berdasarkan objeknya, pencurian identitas dibagi atas 2 bagian yaitu: 1) Pencurian identitas pada korporasi atau perusahaan, dan 2) Pencurian identitas pada perseorangan [1]. Agar hal ini tidak terjadi dan dapat teratasi, banyak pihak berupaya untuk menyandikan informasi yang mereka miliki sehingga informasi tersebut tidak memiliki arti dan sulit dipecahkan. Metode yang dapat diterapkan dalam menyandikan pesan atau informasi ini adalah metode kriptografi. Absensi elektronik memiliki himpunan data-data penting yang mencatat aktifitas kehadiran dan kepulangan dan pegawai. File basis data yang menyimpan data pegawai, kehadiran maupun kepulangan, ijin dan cuti dari pegawai perlu di enkripsi sehingga tidak di salahgunakan.

Algoritma *Rivers Shamir Adleman* (RSA) adalah algoritma asimetri kriptografi yang memanfaatkan kunci publik dan kunci privat yang didapatkan melalui perhitungan matematis memanfaatkan bilangan prima acak. Berdasarkan hasil penelitian, dibutuhkan waktu yang cukup lama untuk membobol algoritma RSA yang menggunakan bilangan prima acak yang besar. Kelemahan algoritma *Rivers Shamir Adleman* (RSA) adalah butuh waktu yang lama untuk menghasilkan bilangan prima acak yang sesuai. Berdasarkan penelitian lain penggunaan algoritma *Rivers Shamir Adleman* (RSA) pada e-complaint mampu diterapkan dengan baik. Proses enkrpsi dan dekripsi pesan keluhan menghasilkan ciphertext dan plaintext yang tepat dan sesuai [2]. Kemudian pada penelitian lainnya juga mendapatkan hasil bahwa penggunaan hybrid algoritma enigma dan algoritma RSA dapat meningkatkan keamanan penyandian pesan karena kekuatan dalam proses penyandian pesan telah meningkat [3].

Algoritma *Blum Blum Shub* adalah algoritma pembangkit bilangan kunci acak yang telah teruji dan memenuhi syarat dalam kriptografi. Untuk membangkitkan bilangan kunci acak pada algoritma *Blum Blum Shub* (BBS), bilangan prima yang dipilih harus mengikuti ketentuan yaitu bilangan prima yang kongruen 3 modulo 4. Sehingga tidak sembarang bilangan prima yang dapat digunakan. Penggunaan kedua algoritma ini diharapkan dapat menghasilkan sistem yang lebih kuat dan akurat sehingga sulit untuk di pecahkan. Namun algoritma *Blum Blum Shub* (BBS) hanya dapat digunakan untuk membangkitkan bilangan kunci acak, bukan untuk menyandikan pesan. Badan Kepegawaian Daerah Kota Binjai merupakan salah satu organisasi perangkat daerah yang ada di Pemerintahan Kota Binjai yang bertugas untuk menyusun dan

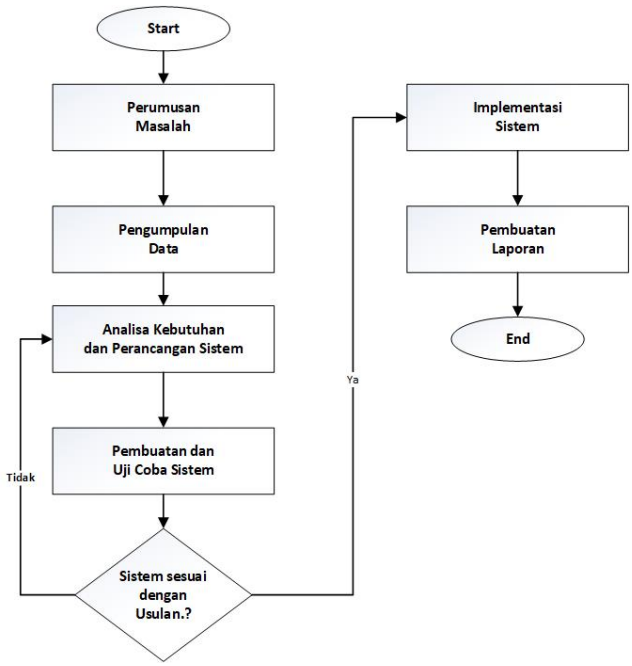
melaksanakan kebijakan pemerintahan di bidang kepegawaian. Salah satu tugas utama Badan Kepegawaian Daerah adalah melaksanakan penegakan disiplin pada Aparatur Sipil Negara atau ASN di lingkungan Pemerintahan Kota Binjai. Dalam penegakan displin Aparatur Sipil negara, salah satu hal yang bisa diterapkan adalah menggunakan absensi elektronik. Perlunya penyandian pada file basis data e-absensi elektronik yang digunakan dikarenakan dalam file basis data absensi elektronik tersebut terdapat data-data penting dari seorang pegawai antara lain data pribadi seperti Nomor Induk Pegawai (NIP), data kehadiran dan kepulangan, ijin, cuti maupun besaran potongan disiplin maupun tunjangan yang didapatkan oleh pegawai setiap bulannya. Penyandian pesan dalam aplikasi absensi elektronik masih menggunakan metode *hash* lama yaitu MD5, sehingga rentan untuk dibobol menggunakan metode yang telah banyak tersedia di internet.

Kriptografi merupakan ilmu yang mempelajari bagaimana dapat menyembunyikan pesan atau tulisan dengan teknik tertentu sehingga hanya dapat diakses oleh pihak yang memiliki kewenangan [4]. Algoritma kriptografi kunci publik yang jamak digunakan adalah algoritma RSA (*Rivest, Shamir, Adleman*). Keamanan algoritma RSA pada penggunaan pemfaktoran bilangan yang besar menjadi faktor prima. Tujuan pemfaktoran bertujuan untuk menemukan kunci privat [5]. Algoritma *Blum Blum Shub* atau yang sering dikenal dengan algoritma BBS digunakan untuk membangkitkan bilangan kunci acak yang tidak dapat di tebak polanya dengan mudah [6]. Dalam prakteknya, penggunaan kriptografi dibagi akan 3 bagian, yaitu kriptografi klasik atau kriptografi simeteri, kriptografi modern atau kriptografi asimetri dan kriptografi hybrid, yaitu kriptografi yang menggabungkan beberapa metode kriptografi untuk proses pengamanan datanya [7].

2. METODE

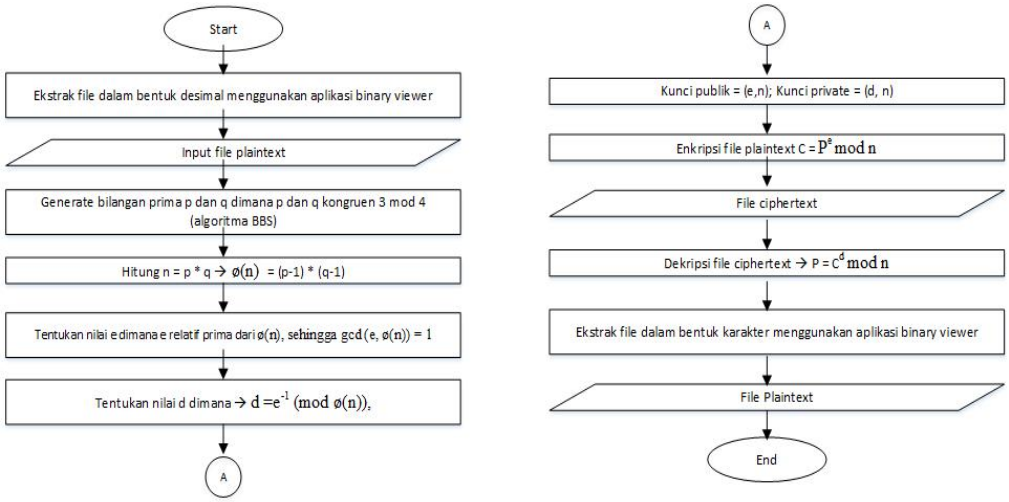
Pada penelitian ini, penulis mengambil studi kasus pada Badan Kepegawaian Daerah Kota Binjai. Badan Kepegawaian Daerah Kota Binjai adalah organisasi perangkat daerah yang ada pada Pemerintahan Kota Binjai yang melaksanakan fungsi untuk pengelolaan, penegakan disiplin serta pelatihan Aparatur Sipil Negara (ASN). Untuk melaksanakan fungsi penegakan dan peningkatan disiplin Aparatur Sipil Negara (ASN). Badan Kepegawaian Daerah Kota Binjai menggunakan absensi elektronik dengan model swafoto dengan waktu kehadiran serta kepulangan yang telah ditetapkan sebelumnya. Perlunya sebuah peningkatan keamanan pada aplikasi absensi elektronik yang dikelola oleh Badan Kepegawaian Daerah Kota Binjai sehingga aplikasi absensi elektronik tersebut, hanya dapat diakses oleh pihak yang berwenang.

Berdasarkan penjelasan yang telah disampaikan diatas, maka dibuat sebuah alur yang dapat menggambarkan rencana kerja dalam penelitian ini. Alur rencana kerja penelitian ini dapat dilihat pada gambar berikut.



Gambar 1. Rencana Kerja Penelitian

Pada penelitian ini, akan dikembangkan sebuah *hybrid* sistem yang menggunakan algoritma *Rivers Shamir Adleman* (RSA) dan algoritma *Blum Blum Shub* dalam peningkatan data keamanan file basis data pada aplikasi absensi elektronik di Badan Kepegawaian Daerah Kota Binjai. File basis data e-absensi, akan dienkripsi menggunakan *hybrid* sistem algoritma *Rivers Shamir Adleman* (RSA) dan algoritma *Blum Blum Shub* (BBS). Penggunaan *hybrid* sistem pada aplikasi absensi elektronik di Badan Kepegawaian Daerah Kota Binjai diharapkan akan meningkatan keamanan data pada aplikasi tersebut sehingga hanya pihak yang memiliki wewenang yang diijinkan untuk mengakses file tersebut. Penerapan *hybrid* sistem algoritma *Rivers Shamir Adleman* (RSA) dan algoritma *Blum Blum Shub* dapat dilihat pada gambar 2. Berdasarkan *flowchart* pada gambar 1, cara kerja *hybrid* sistem algoritma RSA dan algoritma BBS dapat diuraikan sebagai berikut:



Gambar 3. Rencana Kerja Penelitian

3. HASIL DAN PEMBAHASAN

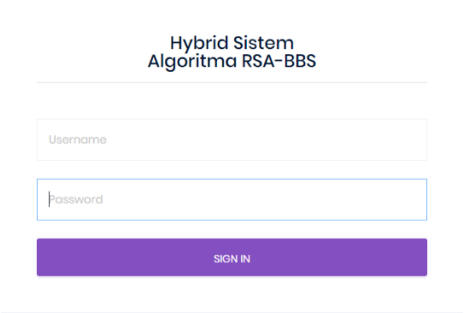
Dalam pengamanan data, dibutuhkan metode yang dapat menyandikan pesan tersebut sehingga pesan tersebut hanya dapat di ketahui oleh pihak yang memiliki kewenangan atas pesan tersebut. Pada tahapan ini, akan di jelaskan mengenai bagaimana hasil dari implementasi penerapan hybrid sistem algoritma *Rivers Shamir Adleman (RSA)* dan Algoritma *Blum Blum Shub* (BBS) dalam pengamanan file basis data di Badan Kepegawaian Daerah Kota Binjai. Dalam penelitian ini menghasilkan sebuah sistem yang mampu melakukan pengacakan isi dari sebuah file teks dan hanya dapat dikembalikan ke dalam file teks bermakna oleh pihak yang memiliki kewenangan berdasarkan kunci *privat* yang dimiliki.

Sebelum hybrid sistem yang dibangun, diimplementasikan, maka perlu dilakukan pengujian terlebih dahulu. Pengujian terhadap hybrid sistem menggunakan algoritma *Rivers Shamir Adleman (RSA)* dan Algoritma *Blum Blum Shub* (BBS) bertujuan untuk memastikan bahwa aplikasi yang digunakan telah mencapai tujuan yang telah ditetapkan dan terhindar dari kesalahan dalam proses implementasinya. Hasil dari pengujian pada hybrid sistem akan dijadikan sebagai bahan untuk melakukan perbaikan terhadap program tersebut.

Dalam pengujian terhadap hybrid sistem menggunakan algoritma *Rivers Shamir Adleman (RSA)* dan Algoritma *Blum Blum Shub* (BBS), dapat diketahui bahwa hybrid sistem tersebut berjalan dengan baik. Kesalahan dalam penginputan data, dapat diminimalisir dengan melakukan validasi terhadap data yang akan diinput. Dengan tampilan hybrid sistem yang sederhana namun interaktif, memudahkan pengguna untuk menggunakan sistem tersebut dalam mengamankan file basis data di Badan Kepegawaian Daerah Kota Binjai.

3.1 Tampilan Website

Pada saat aplikasi hybrid sistem algoritma kriptogra RSA dan Algoritma BBS dijalankan, maka pengguna diminta untuk login terlebih dahulu dengan menginputkan username dan password. Tampilan form login dapat dilihat pada gambar berikut.

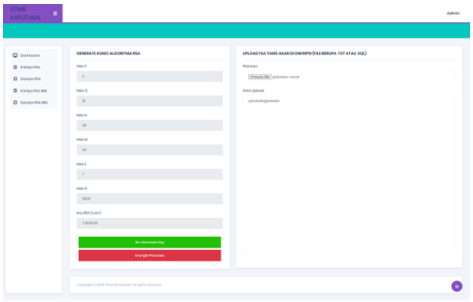


Gambar 1. Tampilan Form Login

Tampilan home merupakan tampilan yang muncul setelah pengguna menginputkan username dan password dengan benar. Tampilan home dapat dilihat pada gambar berikut.

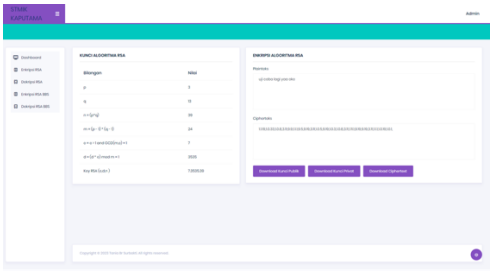
Gambar 2. Tampilan Home

Berikutnya tampilan enkripsi algoritma RSA merupakan tampilan yang digunakan oleh pengguna untuk melakukan enkripsi pada file plainteks yang diupload. Tampilan enkripsi algoritma RSA dapat dilihat pada gambar berikut.



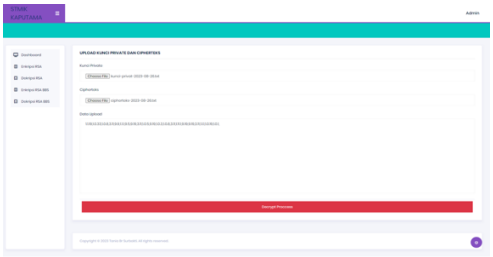
Gambar 4. Tampilan proses enkripsi algoritma RSA.

Berikutnya yaitu tampilan enkripsi algoritma RSA. Pada bagian ini merupakan hasil proses enkripsi menggunakan algoritma RSA. Pada tampilan ini, pengguna dapat mendownload hasil proses enkripsi berupa kunci privat maupun cipherteks hasil enkripsi. Tampilan proses enkripsi algoritma RSA dapat dilihat pada tampilan berikut.



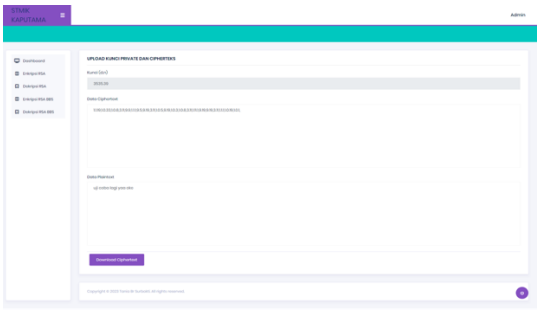
Gambar 5. Tampilan proses enkripsi algoritma RSA.

Berikutnya tampilan deskripsi algoritma RSA. Tampilan pada bagian ini merupakan tampilan yang digunakan untuk melakukan dekripsi pada file cipherteks. Pengguna wajib menginputkan kunci privat dan cipherteks dengan benar. Tampilan dekripsi algoritma RSA dapat dilihat pada gambar berikut.



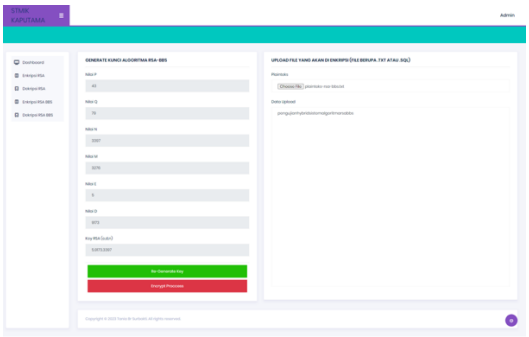
Gambar 6. Tampilan dekripsi algoritma RSA

Berikutnya tampilan Proses Dekripsi Algoritma RSA. Tampilan pada bagian ini merupakan hasil proses dekripsi algoritma RSA. Pengguna dapat mendownload hasil dekripsi berupa file plainteks. Tampilan proses dekripsi algoritma RSA dapat dilihat pada gambar berikut.



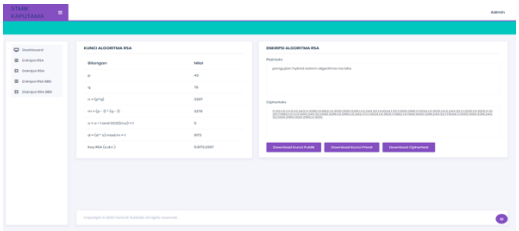
Gambar 7. Tampilan proses dekripsi algoritma RSA.

Berikutnya tampilan enkripsi algoritma RSA dan BBS Pada tampilan ini, dilakukan proses enkripsi menggunakan hybrid sistem algoritma RSA dan Algoritma BBS. Bilangan p dan bilangan q yang digunakan harus memenuhi standard pada algoritma BBS yaitu bilangan prima yang kongruen 3 apabila di modulo kan 4. Tampilan proses enkripsi algoritma RSA dan algoritma BBS dapat dilihat pada gambar berikut.



Gambar 8. Tampilan enkripsi algoritma RSA dan BBS

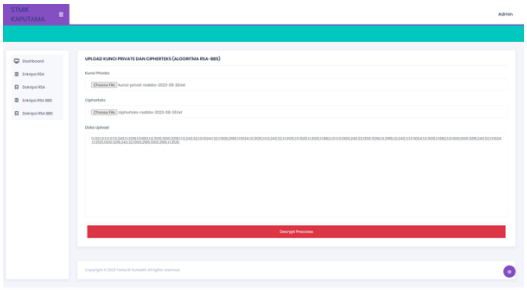
Berikutnya yaitu tampilan Proses Enkripsi Algoritma RSA dan Algoritma BBS. Tampilan pada bagian ini merupakan hasil proses enkripsi menggunakan algoritma RSA dan algoritma BBS. Pada tampilan ini, pengguna dapat mendownload hasil proses enkripsi berupa kunci privat maupun cipherteks hasil enkripsi. Tampilan proses enkripsi algoritma RSA dan algoritma BBS dapat dilihat pada tampilan berikut.



Gambar 9. Tampilan proses enkripsi algoritma RSA dan Algoritma BBS

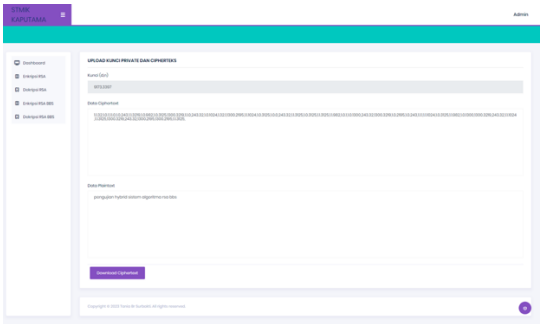
Selanjutnya tampilan Dekripsi Algoritma RSA dan Algoritma BBS. Tampilan pada bagian ini merupakan tampilan yang digunakan untuk melakukan dekripsi pada file cipherteks.

Pengguna wajib menginputkan kunci privat dan cipherteks dengan benar. Tampilan dekripsi algoritma RSA dan algoritma BBS dapat dilihat pada gambar berikut.



Gambar 10. Tampilan dekripsi algoritma RSA dan Algoritma BBS

Yang terakhir adalah tampilan Proses Dekripsi Algoritma RSA dan Algoritma BBS. Tampilan pada bagian ini merupakan hasil proses dekripsi algoritma RSA dan algoritma BBS. Pengguna dapat mendownload hasil dekripsi berupa file plainteks. Tampilan proses dekripsi algoritma RSA dan Algoritma BBS dapat dilihat pada gambar berikut.



Gambar 11. Proses dekripsi algoritma RSA dan Algoritma BBS

4. KESIMPULAN

Penyandian pesan merupakan salah satu hal penting yang perlu dilakukan dalam kegiatan teknologi informasi sehingga pesan tersebut hanya dapat diketahui oleh pihak yang memiliki kewenangan. Salah satu algoritma dalam metode kriptografi adalah algoritma *Rivers, Shamir, Adleman* (RSA). Algoritma RSA adalah algoritma kriptografi asimetris yang menggunakan dua kunci berbeda dalam proses enkripsi maupun dekripsi pesan. Kombinasi algoritma *Rivers, Shamir, Adleman* (RSA) dan algoritma *Blum Blum Shub* (BBS) dalam hybrid sistem meningkatkan keamanan dalam proses penyandian pesan.

REFERENSI

[1] Sudama, W., Imanto, M. A., Wijayanti, S. W., Agustini, Y., Fatoni, Z., Kartini, J. R., Barat, C., & Selatan, J. (2020). *Pengaruh Risiko Pencurian Identitas dan Persepsi atas Risiko terhadap Niat Belanja Online* (Vol. 3, Issue 2).

[2] Yuny, S. D., Juniawan, F. P., Laurentinus, & Hengki. (2022). Pengamanan Pesan E-Complaint Fasilitas dan Kinerja Civitas Akademika Menggunakan Algoritma RSA. *Jurnal Teknologi Informasi Dan Ilmu Komputer (JTIK)*, *9*(6), 1203–1210. https://doi.org/10.25126/jtiik.202295388

[3] Prasetio, Y., Triandi, B., & Hardianto. (2018). Perancangan Aplikasi Pengamanan File Teks dengan Skema Hybrid Menggunakan Algoritma Enigma dan Algoritma RSA. In *46. IT Journal* (Vol. 6, Issue 1).
[4] Saragi, D. R., Gultom, J. M., Tampubolon, J. A., & Gunawan, I. (2020). Pengamanan Data File Teks (Word) Menggunakan Algoritma RC4. *Jurnal Sistem Komputer Dan Informatika (JSON)*, *1*(2), 114. https://doi.org/10.30865/json.v1i2.1745
[5] Rizki, M., & Ariyani, F. (2021). Penerapan Kriptografi dengan Menggunakan Algoritma RSA untuk Pengamanan Data Berbasis Desktop pada PT. Trias Mitra Jaya Manunggal. *SKANIKA*, *4*(2), 1–6.
[6] Saputra, R. A., Windiarti, A., Sarita, I., & Sasilo, A. A. (2021). Konferensi Nasional Ilmu Komputer (KONIK) 2021 Implementasi Metode Blum Blum Shub (BBS) Untuk Pengacakan Soal Kuis Pada Aplikasi Media Pembelajaran Ipa Tingkat Sekolah Dasar Kelas 6 Berbasis Mobile. *Konferensi Nasional Ilmu Komputer (KONIK)*, 428–433.
[7] Suhandinata, S., Rizal, R. A., Wijaya, D. O., Warren, P., & Srinjiwi, S. (2019). Analisis Performa Kriptografi Hybrid ALgoritma Blowfish dan Algoritma RSA. *JURTEKSI (Jurnal Teknologi Dan Sistem Informasi)*, *6*(1), 1–10. https://doi.org/10.33330/jurteksi.v6i1.395