Jurnal CyberTech

Vol.4. No.2, Februari 2021, pp. xx~xx
P-ISSN : 9800-3456
E-ISSN : 2675-9802

Aplikasi Smart School Dengan Pengamanan Data Menggunakan Metode RSA (Rivest Shamir Adleman) Pada PKBM Hanuba Medan

Yosua Tarigan *, Ahmad Fitri Boy **, Ita Mariami **

* Sistem Informasi, STMIK Triguna Dharma
** Sistem Informasi, STMIK Triguna Dharma

Article Info

Article history:
Received Feb 12th, 2021
Revised Feb 20th, 2021
Accepted Feb 26th, 2021

Keyword:
Aplikasi Smart School
Kriptografi,
RSA *(Rivest Shamir Adleman)*

ABSTRACT

Aplikasi Smart School mampu mempermudah sekolah dalam mengelola data. Akan tetapi, disisi lain akan terjadi masalah lain jika data dapat dimodifikasi oleh pihak yang tidak berhak. Permasalahan keamanan data adalah hal yang harus diselesaikan demi menjaga keabsahan suatu data. Salah satu cara untuk mengamankan data ialah dengan algoritma RSA. Dengan algoritma RSA, setiap data dapat diubah menjadi bentuk text yang berbeda dengan bentuk aslinya, sehingga tidak dapat dipahami oleh pihak yang tidak memiliki kunci untuk membaca pesannya. Proses enkripsi akan membentuk kode yang diubah menjadi QR Code yang disisipkan pada rapor, kemudian proses dekripsi dilakukan dengan cara men-scan kode QR code tersebut untuk membuktikan keabsahannya. Algoritma RSA mampu menjaga keabsahan data aplikasi smart school. Sehingga dengan demikian, aplikasi tersebut dapat dipakai dan tetap menjaga keaslian dari nilainya.

Corresponding Author: *First Author
Yosua Tarigan
Sistem Informasi
STMIK Triguna Dharma
Email: yosuatarigan7@gmail.com

1. PENDAHULUAN

Database merupakan hal yang sangat penting bagi kehidupan masyarakat dalam hal informasi dan pengetahuan. Database berperan penting dalam perkembangan teknologi informasi dan suatu bagian utama dalam sebuah sistem informasi [1]. Database dan sistem informasi merupakan hal yang tidak dapat dipisahkan, bahkan kehadiran sistem informasi juga menandakan adanya sebuah database.

Suatu sistem informasi dibangun mengikuti database yang ada di dalamnya. Salah satu bentuk sistem informasi ialah aplikasi android. Aplikasi android banyak digunakan oleh organisasi seperti perusahaan, lembaga, pemerintahan, perguruan tinggi maupun individual. Aplikasi yang menggunakan database akan terlihat lebih dinamis dan interaktif, sehingga akan lebih membantu para user yang menggunakannya. Dengan mengakses aplikasi tersebut, user akan mendapatkan data-data yang telah disediakan oleh database yang ada di dalamnya. Aplikasi android juga bisa berhubungan dengan user melalui *form* yang telah disediakan dan para user juga bisa mengubah data yang ada di dalam aplikasi tersebut. Sehingga dengan demikian , proses

pengelolaan data benar-benar dipermudah oleh aplikasi tersebut. Akan tetapi, terdapat aplikasi yang berisikan informasi yang bersifat rahasia yang hanya boleh diakses oleh orang tertentu saja.

Oleh sebab itu sekolah PKBM Hanuba Medan membutuhkan pengamanan data untuk melindungi Aplikasi Smart School PKBM Hanuba Medan dari serangan ataupun akes dari pihak luar yang tidak memiliki izin. Salah satu cara untuk melindungi data tersebut adalah dengan kriptografi. Kriptografi adalah ilmu yang mempelajari teknik-teknik matematika untuk mengamankan suatu data rahasia, baik berupa dokumen rahasia serta otentikasi. Dalam kriptografi terdapat dua prinsip dasar yaitu Enkripsi dan Dekripsi. Enkripsi adalah suatu proses yang mengubah pesan asli (*plainteks*) menjadi sebuah pesan terkode (*chiperteks*), sedangkan Dekripsi merupakan kebalikan dari Enkripsi, yaitu mengubah suatu pesan terkode (*chiperteks*) menjadi sebuah pesan asli (*plainteks*) [2]. Salah satu algoritma kriptografi yang baik cukup aman adalah REVEST SHAMIR ADLEMAN (RSA). RSA merupakan metode kriptografi dengan jenis asimetris, yaitu metode dengan menggunakan dua kunci yang berbeda untuk enkripsi dan dekripsi. Dengan penerapan RSA pada aplikasi, diharapkan dapat mengamankan data-data pada aplikasi tersebut.

Oleh karena hal tersebut, maka penilitian ini diberi judul "**APLIKASI SMART SCHOOL DENGAN PENGAMANAN DATA MENGGUNAKAN METODE RSA (REVEST SHAMIR ADLEMAN) PADA PKBM HANUBA MEDAN**" agar dapat mengamankan data aplikasi sekolah tersebut.

2. METODE PENELITIAN

Model pengembangan sistem merupakan salah satu unsur yang penting dalam penilitian. Dalam perancangan sistem khususnya software atau perangkat lunak dapat menggunakan beberapa model pengembangan. Model pengembangan akan digunakan ialah model sekuensi linier (waterfall).

Berikut ini adalah tahapan dalam model waterfall, yaitu:

1. Analisa Kebutuhan
   Proses penganalisa kebutuhan dilakukan agar mengetahui kebutuhan apa yang harus dipenuhi oleh perangkat lunak yang akan dibuat nantinya.
2. Desain
   Proses desain sistem yang dibagi beberapa elemen yaitu pemodelan menggunakan flowchart sistem, pemodelan menggunakan UML (Unified Modelling Language), struktur data, dan tampilan sistem.
3. Pengkodean
   Setelah desain sistem sudah dibuat, maka tahap selanjutnya ialah mengkodekan program sesuai dengan desain sistem dan kebutuhan sistem yang diperlukan
4. Pengujian
   Setelah perangkat lunak selesai dibuat, dilakukan pengujian untuk mengetahui apakah semua fitur sesuai dengan yang diinginkan. Pengujian ini dilakukan untuk meminimalisir kesalahan dan memastikan bahwa hasilnya sesuai dengan kebutuhan
5. Pendukung (support) atau pemeliharaan (maintenance)
   Pemeliharaan dilakukan jika suatu saat perangkat lunak yang sudah dibuat mengalami error atau kerusakan, maka dari itu diperlukan pemeliharaan sistem guna menjaga agar perangkat lunak tetap bekerja seperti yang diinginkan [3].

3. ANALISA DAN HASIL

Adapun dalam analisa ini menggunakan metode RSA. Pemanfaatan algoritma RSA akan melindungi data dengan mengenkripsi data menjadi QR *code* yang menjaga keabsahan data.

3.1. RSA (Rivest Shamir Adleman)

Algoritma RSA merupakan algoritma enkripsi yang memiliki kunci yang sangat dimana hingga saat ini masih belum ditemukan cara untuk memecahkannya. Kekuatan algoritma RSA terletak pada tingkat kesulitan dalam memfaktorkan bilangan menjadi faktor-faktor prima pada saat membangkitkan kuncinya. Semakin banyak digit bilangan yang digunakan untuk menghasilkan kunci maka semakin sulit untuk mencari faktor bilangan prima yang membangkitkan kunci tersebut [4].

Algortima RSA dijabarkan pada tahun 1977 oleh tiga orang : Ron Rivest, Adi Shamir dan Len Adleman dari Massachusetts Institute of Technology. Huruf RSA itu sendiri berasal dari inisial nama mereka (Rivest—Shamir—Adleman). Algoritma tersebut dipatenkan oleh Massachusetts Institute of Technology (MIT) pada tahun 1983 di Amerika Serikat sebagai U.S. Algoritma RSA menjadi salah satu algoritma asimetris yang popular dan bahkan masih banyak digunakan hingga saat ini. Dalam algoritma RSA ada tiga proses yaitu proses pembangkitan kunci, proses enkripsi, dan proses dekripsi. Pada proses pembangkitan kunci akan menghasilkan dua buah kunci yaitu kunci privat yang digunakan untuk proses dekripsi dan kunci publik yang digunakan untuk proses enkripsi [5].

3.2 Penerapan Dengan Metode

Berikut ini adalah data yang digunakan sebagai sampel dalam penelitian yaitu [6]:

Tabel 1. Data Awal

No. Induk	Kelas
0044599325	7

1. Data awal yang diperoleh selanjutnya akan dilakukan proses encoding ke ASCII, yaitu :

Tabel 2. Hasil Perubahan Plaintext ke dalam bentuk Desimal (ASCII)

Plainttext (P)	**Desimal (ASCII)**
0	48
0	48
4	52
4	52
5	53
9	57
9	57
3	51
2	50
5	53
7	55

2. Proses Pembangkitan Kunci

Berikut ini adalah tahapan dalam membangkitkan kunci pada algoritma RSA, yaitu:

a. Kriptografi RSA membutuhkan dua buah bilangan prima untuk membangkitkan kunci publik dan kunci privat, maka pertama akan dilakukan inisialisasi variabel p dengan nilai 11 dan variabel q dengan nilai 13.

b. Kemudian mencari nilai variabel n yang dibutuhkan untuk membangkitkan kunci. Untuk mendapatkan nilai n dilakukan proses perkalian variabel p dan q. Nilai n = p * q maka n = 11 * 13 = 143
c. Mencari nilai variabel m dengan rumus m= (p-1)(q-1), maka m = (11-1)(13-1) = 120.
d. Lalu pilih nilai e dengan syarat e > 1 dan greatest comman divisior (e,1872) = 1. Nilai e yang diambil adalah 17, maka nilai kunci publik adalah 17.
e. Untuk mendapatkan kunci privat atau variabel d, menggunakan rumus (dxe) mod m =1. (dx17) mod 120 = 1 , maka kunci privat = 113. Bukti , (113x17) mod 120 = 1.

3. Proses Enkripsi

Setelah kunci public dan privat didapatkan, maka dilakukan proses enkripsi terhadap data yang sudah diubah ke Desimal (ASCII) dengan rumus Ci = Pie mod n. Data yang dienkripsi adalah 00445993257.

$C1 = 48^{17} \bmod 143 = 16$

$C2 = 48^{17} \bmod 143 = 16$

$C3 = 52^{17} \bmod 143 = 13$

$C4 = 52^{17} \bmod 143 = 13$

$C5 = 53^{17} \bmod 143 = 92$

$C6 = 57^{17} \bmod 143 = 18$

$C7 = 57^{17} \bmod 143 = 18$

$C8 = 51^{17} \bmod 143 = 116$

$C9 = 50^{17} \bmod 143 = 85$

$C10 = 53^{17} \bmod 143 = 92$

$C11 = 55^{17} \bmod 143 = 22$

4. Proses Dekripsi

Melakukan proses dekripsi untuk memvalidasi kebabsahan suatu data dengan rumus Pi = Cid mod n. Sebelum ciphertext di dekripsi , ciphertext di encoding ke desimal, lalu di dekripsi. Setelah didekripsi, data tersebut kemudian di decoding.

$P1 = 16^{113} \bmod 143 = 48$

$P1 = 16^{113} \bmod 143 = 48$

$P1 = 13^{113} \bmod 143 = 52$

$P1 = 13^{113} \bmod 143 = 52$

$P1 = 92^{113} \bmod 143 = 53$

$P1 = 18^{113} \bmod 143 = 57$

$P1 = 18^{113} \bmod 143 = 57$

$P1 = 116^{113} \bmod 143 = 51$

$P1 = 85^{113} \bmod 143 = 50$

P1 = 92^{113} mod 143 = 53

P1 = 22^{113} mod 143 = 55

3.4 Pengujian

Dengan selesainya pembuatan aplikasi smart school, maka langkah selanjutnya akan dilakukan pengujian terhadap sistem. Pengujian ini menunjukan apakah sistem bekerja sesuai keinginan yakni memvalidasi akses pengguna dihalaman login, membentuk QR Code yang berisikan data yang sudah dienkripsi pada halaman rapor online, dan dapat memvalidasi (dekrip) data yang terdapat pada QR Code rapor online.

Pada tahap awal implementasi, admin dan siswa harus melakukan login pada sistem, jika valid maka akan masuk ke menu utama, jika tidak akan kembali ke halaman login. Adapun tahap ini dapat dilihat dibawah ini :

Gambar 1. Akses Pengguna

Jika akses berhasil maka akan menampilkan halaman menu utama. Pada tahap pengguna berhasil login, maka akan dilakukan pengecekan role untuk admin dan siswa. Admin dan siswa memiliki fungsi halaman yang berbeda pada halaman akun. Siswa dapat mengakses rapor melalui halaman akun siswa. Berikut tampilan halaman rapor online yang sudah memiliki kode QR Code :

Gambar 2. Rapor online dengan QR Code

Selanjutnya untuk proses validasi admin cukup memilih menu validasi dan scan pada QR Code pada rapor tersebut. Jika data tidak valid maka sistem akan menunjukkan halaman tidak valid, jika valid maka sistem akan menampilkan rapor sesuai QR code tersebut. Admin akan memeriksa apakah rapor tersebut sama dengan hasil rapor yang tampil setelah melakukan validasi.

Gambar 3. Halaman untuk data tidak valid

4. KESIMPULAN

Adapun kesimpulan dari penelitian ini yaitu sebagai berikut :

1. Berdasarkan hasil pengujian pembentukan sepasang kunci dilakukan dengan menetapkan 2 buah bilangan prima pada nilai p dan q, kemudian menghitung n dan m, lalu menentukan nilai e sebagai kunci publik dan d sebagai kunci privat.
2. Berdasarkan hasil pengujian proses pembentukan enkripsi data dapat dilakukan dengan mengambil kode dokumen siswa yang akan dienkripsi lalu diproses menggunakan kunci publik (e).
3. Berdasarkan hasil pengujian validasi data dapat dilakukan dengan mengambil kode dengan scan QR code, kemudian didekrip menggunakan kunci privat (d).
4. Berdasarkan hasil penelitian pengamanan data dapat dilakukan menggunakan algoritma RSA. Pemanfaatan algoritma RSA mampu menjaga keabsahan suatu data agar tidak mudah untuk dipalsukan. Pengimplementasian RSA pada sistem juga dapat dengan mudah dilakukan karena proses algoritma RSA cukup sederhana, namun memiliki kekuatan yang kuat dalam pengamanan data. Merubah data hasil enkripsi menjadi sebuah QR code merupakan langkah yang baik karena akan mempermudah admin dalam memvalidasi data.

UCAPAN TERIMA KASIH

Penulis mengucapkan terimakasih kepada program studi S1 Sistem Informasi STMIK Triguna Dharma yang telah memberikan dukungan dalam penyelesaian tulisan ini.

REFERENSI

[1] K. Surbakti, "Kajian Mengenai Pentingnya Basis Data Bagi Sekolah Saat Ini," J. Curere, vol. 02, no. 02, pp. 2597–9515, Jan. 2018, Accessed: Mar. 02, 2021. [Online]. Available: http://portaluniversitasquality.ac.id:5388/ojssystem /index.php/CURERE/article/view/156.R. Munir, Kriptografi, 2nd Ed. Yogyakarta: Informatika Bandung, 2019.
[2] Y. Yusfrizal, "Rancang Bangun Aplikasi Kriptografi Pada Teks Menggunakan Metode Reverse Chiper," J. Tek. Inform. Kaputama, vol. 3, no. 2, pp. 29–37, 2019.
[3] H. Larasati and S. Masripah, "Analisa Dan Perancangan Sistem Informasi Pembelian GRC Dengan Metode Waterfall," J. Pilar Nusa Mandiri, vol. 13, no. 2, pp. 193–198, 2017.
[4] E. H. A. Mendrofa, M. Zarlis, and E. Y. Purba, "Implementasi Algoritma RSA dengan Kunci EM2B dalam Mengenkripsi Pesan," Semant. (Seminar Nas. Tek. Inform., vol. 1, no. 1, pp. 155–162, 2017.
[5] N. Wiyono and M. Hardjianto, "Pengamanan Email Menggunakan Algoritma RSA dan Digital Signature SHA-1 Berbasis Mobile," Ipsikom, vol. 4, no. 2, pp. 1–11, 2016.
[6] PKBM Hanuba Medan, Raport.

BIBLIOGRAFI PENULIS

	**Yosua Tarigan** lahir pada tahun 1997, Desa Deli tua. Saat ini sedang menempuh studi Sistem Informasi di STMIK Triguna Dharma. Bekerja sebagai freelancer programmer disalah satu situs freelance di indonesia. Mengikuti rangkaian kegiatan kursus pemograman di udemy dan membangun usaha jasa pemograman.
	**Ahmad Fitri Boy, S.Kom, M.Kom** pria kelahiran Aceh 04 Mei 1980 ini merupakan Dosen Tetap STMIK Triguna Dharma yang aktif mengampu mata kuliah Pemrograman Visual, Web dan Open Source. Tamat S1 di STMIK Multimedia Prima Bidang Sistem Informasi dan Tamat S2 di Universitas Putra Indonesia YPTK Padang Bidang Sistem Informasi.
	**Ita Mariami, SE, M.Si** merupakan Dosen Tetap STMIK Triguna Dharma yang telah lama aktif dalam melaksanakan kegiatan penelitian dan pengabdian kepada masyarakat. Saat ini beliau telah tersertifikasi sebagai dosen dengan mengampu mata kuliah PMB, Teknik Pemasaran, Teknik Preneurship, E Buissnes, Etika Profesi dan Teknik Periklanan. Tamat S1 STIK Sukma Medan bidang Manajemen Pemasaran dan Tamat S2 Univeristas Sumatera Utara Bidang Ilmu Manajemen.