JURNAL INFORMATION SYSTEM
Volume 3, Nomor 1, Mei 2023, Page 001-009
Email : jis@unkris.ac.id
ISSN 2807-7849 (media online)
Available Online at https://jurnalteknik.unkris.ac.id/index.php/jis

Implementasi Algoritma Kriptografi RC4 Untuk Keamanan Database Aplikasi Voting Pemilihan Ketua Umum Berbasis WEB

Fadlilah Septyana Yanuba[1], Muhlis Tahir[2], M. Khamdi Fadli[3], Fathin Nisa Nafasa[4], Siti Aminatus Zahrah[5], Afifatur Rohmah[6]

[1,2,3,4,5,6] Ilmu Pendidikan, Pendidikan Informatika, Universitas Trunojoyo Madura, Bangkalan, Indonesia

Email: [1]190631100102@student.trunojoyo.ac.id, [2]muhlis.tahir@trunojoyo.ac.id, [3]190631100106@student.trunojoyo.ac.id , [4]190631100109@student.trunojoyo.ac.id , [5]190631100121@student.trunojoyo.ac.id , [6]190631100129@student.trunojoyo.ac.id

Abstrak− Rivest code 4 (RC4) adalah perhitungan kriptografi kunci simetris canggih yang memiliki mode kerja stream chipper, sehingga dalam menangani informasi dan data pada waktu tertentu menggunakan dua kotak pengganti (s-box) sebagai tampilan dengan panjang perubahan 256 dan selanjutnya s-box kedua yang merupakan elemen dari perhitungan public key. Rivest code 4 digunakan untuk menyandikan informasi, pesan atau data. Peneliti mencoba mengimplementasikan fitur login Sistem Pemilihan Ketua Umum yang menjadi pokok bahasan penelitian ini, dengan mengimplementasikan algoritma RC4 pada aplikasi yang sudah ada. Akibatnya, data terenkripsi yang tersimpan pada database akan sulit dicari tahu arti sebenarnya. Berdasarkan temuan penelitian ini, field yang berisi informasi pengguna yang mana dalam hal ini yaitu password dapat terenkripsi dengan baik, dan juga saat implementasi login juga dapat berjalan dengan baik dengan menggunakan algoritma RC4.
Kata Kunci: Keamanan; Algoritma *Rivest Code 4*; *Database*; *Voting*

Abstract− *Rivest code 4 (RC4) is a sophisticated symmetric key cryptographic calculation that has a stream chipper working mode, so that in handling information and data at a certain time it uses two replacement boxes (s-boxes) as displays with a change length of 256 and then the second s-box which is is an element of public key computation.rivest code 4 is used to encode information, messages or data. Researchers are trying to implement the Chairman Election System login feature which is the subject of this research, by implementing the RC4 algorithm in existing applications. as a result, encrypted data stored in databases will be difficult to find out its true meaning.based on the findings of this study, the field containing user information which in this case is the password can be encrypted properly, and also when the login implementation can also run well using the RC4 algorithm.*
Keywords: Safety; Algorithm *Rivest Code 4*; *Database*; *Voting*

1. PENDAHULUAN

Begitu banyak kehidupan modern yang bergantung pada teknologi informasi, teknologi memainkan peran penting dalam pertumbuhan sumber daya manusia. Alhasil, manusia kini dapat dengan mudah menjalin komunikasi maupun berbagi informasi, bertukar data dengan jarak jauh berkat teknologi yang semakin maju saat ini. setiap aspek kehidupan modern telah dipengaruhi oleh kemajuan teknologi informasi, yang memudahkan orang untuk bertukar data dalam berbagai format di komputer. Dampak negative dari teknologi yang semakin meningkat yakni kejahatan pencurian data ataupun penyelahgunaan data informasi[1]. Sebagai hasilnya, melindungi data yang disimpan dari akses, modifikasi, dan penghapusan yang tidak sah sangat penting jika ingin tetap aman dari berbagai ancaman.

Terdapat banyak sekali pekerjaan yang dapat diselesaikan dengan cepat, akurat, dan efektif berkat kemajuan teknologi informasi. Keamanan basis data kemudian menjadi salah satu aspek terpenting dari teknologi informasi[2]. Integritas dan keamanan data merupakan pertimbangan penting. Pentingnya kerahasiaan dan keamanan data semakin meningkat. Keamanan data melibatkan banyak kasus yang sekarang menjadi pekerjaan dimana membutuhkan banyak keamanan dan uang untuk dikelola. Mekanisme keamanan yang baik diperlukan untuk mencegah informasi data diakses oleh pihak yang tidak berwenang[3].

Hacker yang suka mengubah, mengunci, menyadap, menghapus, dan memodifikasi isi data orang lain hanyalah salah satu contoh bagaimana teknologi modern dapat digunakan dalam sistem peradilan pidana. Kriptografi adalah disiplin terkenal di bidang keamanan data[4]. Steganografi dan kriptografi adalah dua dari banyak metode yang tersedia untuk melindungi data ini[5]. Kriptografi yang bertujuan untuk mengubah pesan (plaintext) menjadi pesan yang sulit dipahami (ciphertext), memiliki kelebihan dan kekurangan[6]. Namun, orang yang membaca data terenkripsi mungkin curiga terhadap kriptografi, yang dapat menyebabkan mereka merusak enkripsi.

Salah satu pemanfaatan teknologi yakni dengan dilakukannya pemilihaan dengan menggunakan media digital[7].

Submitted: **12/05/2023**; Accepted: **25/05/2023**; Published: **31/05/2023**

JURNAL INFORMATION SYSTEM
Volume 3, Nomor 1, Mei 2023, Page 001-009
Email : jis@unkris.ac.id
ISSN 2807-7849 (media online)
Available Online at https://jurnalteknik.unkris.ac.id/index.php/jis

Hal ini membantu dalam proses pemungutan suara yang penyelenggaraannya tidak dapat dilakukan secara langsung. Seperti yang kita ketahui, selama ini proses pemungutan suara untuk pemilihan ketua umum maupun pemilihan lainnya dilakukan dengan secara manual, dengan menggunakan media kertas dan dilakukan secara serentak disatu tempat yang telah ditentukan. Hal ini juga menjadi kendala pada seseorang yang tidak dapat datang dalam pemungutan suara ketempat yang telah ditentukan.

Oleh karena itu, diterapkanlah sistem pengamanan data pada proses pemilihan ketua umum yang dilakukan di Prodi Pendidikan Informatika guna mengamankan data dan informasi. Hal ini bertujuan untuk memberikan keamanan pada database yang berfungsi dalam penyimpanan hasil perolehan suara yang telah dilakukan[8]. Algoritma kriptografi yang digunakan yakni algoritma kriptografi RC4[9].

2. METODOLOGI PENELITIAN

2.1 Analisa Masalah

Kemajuan teknologi yang sangat pesat terus mengalami perubahan dan pembaruhan yang lebih baik. Salah satu contohnya yakni pada sistem pemilihan umum, baik dari sebuah organisasi kecil maupun besar, yang dimana sebelumnya dilakukan dengan cara pemilihan langsung yakni dengan melakukan pemungutan suara menggunakan kertas suara. Pemilihan ini mengalami perubahan yang dilakukan melalui media online. Maka dari itu diperlukan pengamanan yang sangat baik agar data hasil pemilihan bisa tersimpan dengan baik tanpa adanya kecurangan yang dapat merusak hasil pemungutan suara. Pada saat pemilih mau menggunakan hak suaranya kerap kali ditemukan kasus jika pemilih tersebut bahwasannya sudah memilih padahal yang sebenarnya belum melaksanakan hak suaranya.

Dengan adanya permasalahan tersebut, maka diperlukan suatu algoritma enkripsi untuk mengamankan akun dari pemilih yang mana nantinya algoritma ini akan dienkripsi pada hanya satu field saja yaitu password. sehingga pihak yang tidak bertanggung jawab atas keamanan database tidak dapat membaca ataupun mengetahui karena privasi data tersebut[10]. Algoritma yang digunakan yakni algoritma RC4.

2.2 Tahapan Penelitian

Dalam penelitian ini, metode waterfall digunakan. Dimulai dengan analisis, desain, pengkodean, pengujian, dan dukungan, model waterfall menawarkan pendekatan aliran hidup perangkat lunak berurutan atau sekuensial[11]. Berikut adalah tahapan-tahapan yang dilakukan pada penelitian ini dengan menggunakan waterfall:

a) Tahap analisis kebutuhan perangkat lunak
Pada tahap ini dimana semua masalah pengguna dipecah dan komponen sistem atau perangkat lunak, objek, hubungan antar objek, dan seterusnya diidentifikasi. Pada titik ini, penulis melakukan analisis kebutuhan yang diperlukan untuk menyusun program keamanan. Mulai dengan menganalisis kebutuhan program dengan menggunakan algoritma kriptografi RC4. Kemudian dilanjutkan ke tahap codingan, dan yan terakhir dilihat setelah pengujian apakah sudah berhasil atau tidak.

b) Perancangan
pada tahap ini merupakan proses multi langkah yang berfokus pada perancangan program perangkat lunak berdasarkan hasil data dari tahap analisis. Program perangkat lunak ini akan diimplementasikan dan mencakup diagram arsitektur perangkat lunak, kemajuan antar-representasi, dan desain basis data pembuatan kode program Pada tahap ini, penulis menerapkan desain sistem, dimana sistem menangani pemilihan perangkat keras dan aplikasi persiapan perangkat lunak (coding atau pengkodean). Program yang didasarkan pada logika yang dirancang dalam desain diberi kode.

c) Pengujian
Tahap pengujian menentukan apakah sistem atau perangkat lunak yang dikembangkan sesuai dengan kebutuhan pengguna dan menghilangkan atau meminimalkan cacat program (defect) sehingga sistem yang telah dikembangkan akan benar-benar membantu pengguna media dalam memperbaiki kesalahan pemrograman. Penulis menggunakan metode pengujian black box sebagai media pengujian.

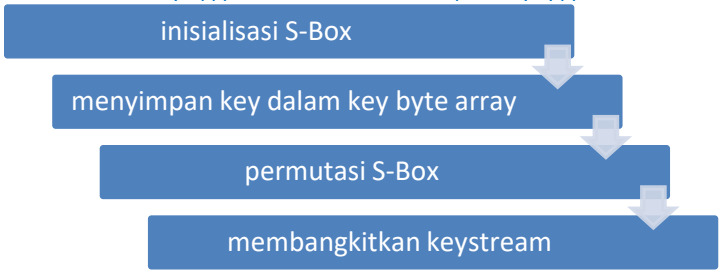
d) Pendukung (support) atau pemeliharaan (maintenance)
Pada tahapan ini dilakukam pemeliharaan pada produk dan membuat beberapa perubahan jika merasa ada sesuatu yang bener-benar perlu di kembangkan dalam produk tersebut.

2.3 Algoritma RC4

RC4 merupakan suatu algoritma yang dibuat pada tahun 1987 oleh Ron rivest di laboratorium RSA security[12]. Algoritma ini termasuk kedalam jenis stream chipper dan memiliki sifat kunci simetris. Algoritma ini melakukan proses enkripsi dengan cara byte per byte dengan operasi biner. Berikut ini rangkaian proses yang dimiliki RC 4 diantaranya :

Submitted: **12/05/2023**; Accepted: **25/05/2023**; Published: **31/05/2023**

JURNAL INFORMATION SYSTEM
Volume 3, Nomor 1, Mei 2023, Page 001-009
Email : jis@unkris.ac.id
ISSN 2807-7849 (media online)
Available Online at https://jurnalteknik.unkris.ac.id/index.php/jis



Gambar 1. Alur RC4

Pada waktu proses enkripsi RC 4 membangkitkan key stream yang nantinya dixor-kan dengan plaint text dan sebaliknya pada waktu deskripsi RC 4 keystream tersebut akan dixor-kan dengan chipper text. RC 4 memproses data yang mana dalam satu waktu hanya berukuran byte(1 byte = 8bit. RC 4 menggunakan 2 kotak subtitusi atau s box dengan array 256 byte[13]. Kotak subtitusi pertama berisi permutasi dari bilangan 0 sampai 255 dan kotak subtitusi kedua berisi permutasi fungsi dari kunci. Berikut ini penjelasan step by step dari algortima RC4[14] :

1) S-box di inisialisasi dengan persamaan seperti dibawah ini :
   for m = 0 to 255
   S[m] = m
2) Kemudian alur inisialisasi S-box (Larik/array K) dengan persamaan dibawah ini:
   Panjang kunci “length” for m = 0 to 255
   K[m] = Kunci [m mod length]

3) Setelah itu S-box diacak dengan menggunakan persamaan dibawah ini :
   M = 0 ; n = 0
   for m = 0 to 255
   n = (n + S[m] + K[n]) mod 256
   swap S[m] dan S[n]
4) Terakhir buatlah pseudocode random dengan rumus persamaan dibawah ini :
   m = (m + 1) mod 256
   n = (n + S[m]) mod 256
   swap S[m] dan S[n]
   t = (S[m] + S[n]) mod 256
   K = S[t]

3. HASIL DAN PEMBAHASAN

3.1 Analisa Sistem

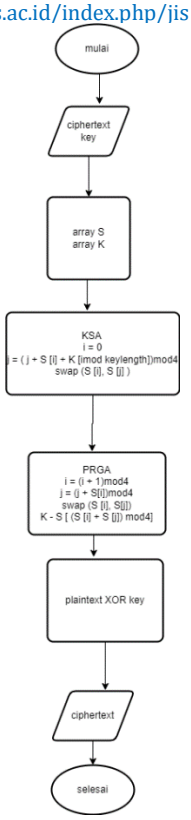
Analisa sistem merupakan sebuah proses dimana kita akan menyusun susunan dalam pembuatan projek yang diusulkan. Dibawah ini merupakan flowchart dari proses enkripsi dan dekripsi

Flowchart Sistem

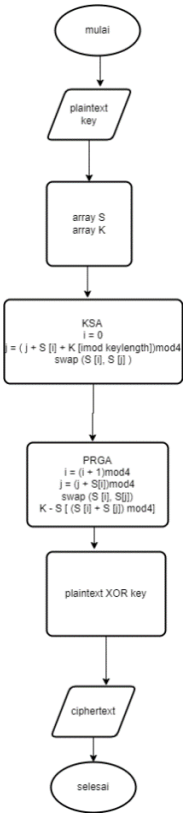
Alur proses enkripsi dan dekripsi pada dabatase merupakan definisi dari fungsi sebuah flowchart yang dimana pada penelitian ini menggunma RC4.

Submitted: **12/05/2023**; Accepted: **25/05/2023**; Published: **31/05/2023**

JURNAL INFORMATION SYSTEM
Volume 3, Nomor 1, Mei 2023, Page 001-009
Email : jis@unkris.ac.id
ISSN 2807-7849 (media online)
Available Online at https://jurnalteknik.unkris.ac.id/index.php/jis



Gambar 2. *Flowchart* proses dekripsi RC4 pada *database*



Gambar 3. *Flowchart* proses enkripsi RC4 pada database

Submitted: **12/05/2023**; Accepted: **25/05/2023**; Published: **31/05/2023**

JURNAL INFORMATION SYSTEM
Volume 3, Nomor 1, Mei 2023, Page 001-009
Email : jis@unkris.ac.id
ISSN 2807-7849 (media online)
Available Online at https://jurnalteknik.unkris.ac.id/index.php/jis

3.2 Implementasi dan Pengujian Aplikasi

Berikut ini kode program yang digunakan dalam keamanan data algoritma RC4 pada database aplikasi voting, antara lain:

a. Kode program inisialisasi S-Box

```
// inisialisasi sbox
  public static function sbox()
  {
    self::$state = array();
    for ($i=0; $i < 256; $i++) {
      self::$state[$i] = $i;
    }
    return self::$state;
  }
```

b. Proses inisialisasi S-Box (Array K)

```
//menyimpan kunci ke bentuk array
  public static function menk($key)
  {
    $keybyte[] = strlen($key);
    $n  = strlen($key);
    $keyar = [];
    for ($a=0; $a < 256; $a++) {
      $keyar[$a]=ord($key[$a % $n]);
    }
    return $keyar;
  }
```

c. Proses pengacakan S-Box (permutasi S-Box)

```
//permutasi nilai s box
  public static function mtsnsbox($keyq)
  {
    $kunci = self::menk($keyq);
    $j = 0;
    for ($i=0; $i < 256 ; $i++) {
      $j = ($j+self::$state[$i]+$kunci[$i]) % 256;
      $temp = self::$state[$i];
      self::$state[$i] = self::$state[$j];
      self::$state[$j] = $temp;
    }
    return self::$state;
  }
```

d. Proses pseudorandom code (keystream)

```
//membangkitkan pseudorandom (keystream)
  public static function
psdrndm($keyqq,$kalimat)
```


Submitted: **12/05/2023**; Accepted: **25/05/2023**; Published: **31/05/2023**

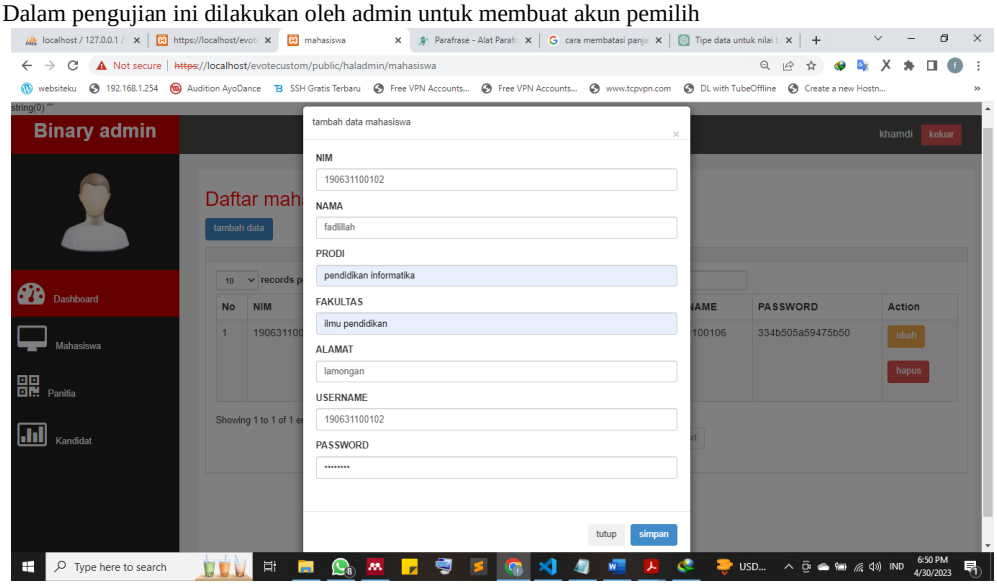
JURNAL INFORMATION SYSTEM
Volume 3, Nomor 1, Mei 2023, Page 001-009
Email : jis@unkris.ac.id
ISSN 2807-7849 (media online)
Available Online at https://jurnalteknik.unkris.ac.id/index.php/jis

```
{
    self::mtsnsbox($keyqq);
    $kstrm[] = strlen($keyqq);
    $strkstrm = '';
    $binkstrm[] = strlen($keyqq);

    $i = $j = 0;
    for ($c=0; $c < strlen($kalimat); $c++) {
        $i = ($i+1)%256;
        $j = ($j+self::$state[$i])%256;
        $temp = self::$state[$i];
        self::$state[$i] = self::$state[$j];
        self::$state[$j] = $temp;
        $t = (self::$state[$i]+self::$state[$j])%256;
        $strkstrm = $strkstrm . self::$state[$t];
        $kstrm[] = self::$state[$t]; //keystream
    }
    return $strkstrm;
}
```

Berikut ini merupakan hasil pengujian dari aplikasi voting yang telah dibuat. Pengujian dilakukan melalui web browser dengan menjalankan alamat yang tersimpan di htdocs.

a. Dalam pengujian ini dilakukan oleh admin untuk membuat akun pemilih

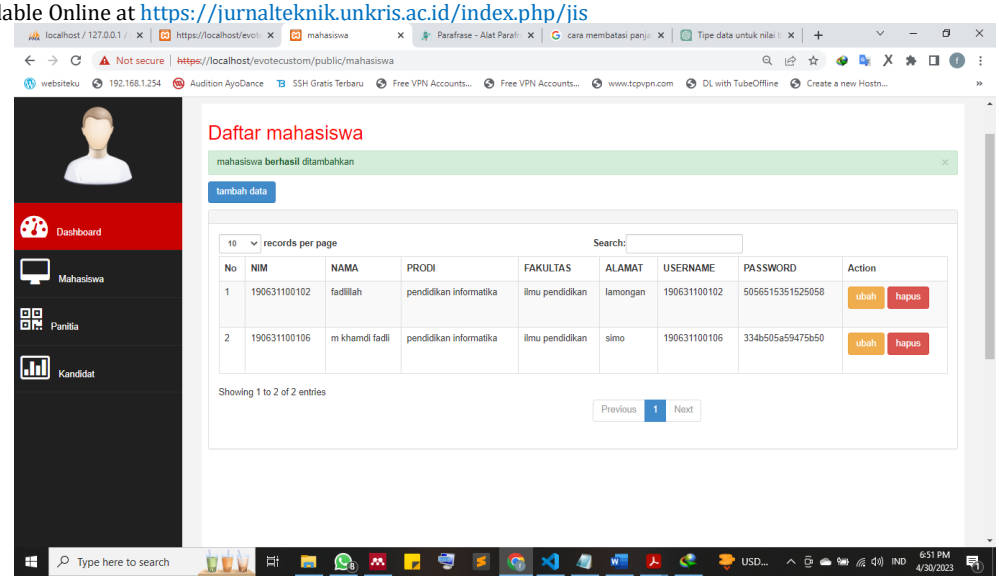


Gambar 4. Tampilan admin untuk membuat akun pemilih

Dan hasilnya adalah

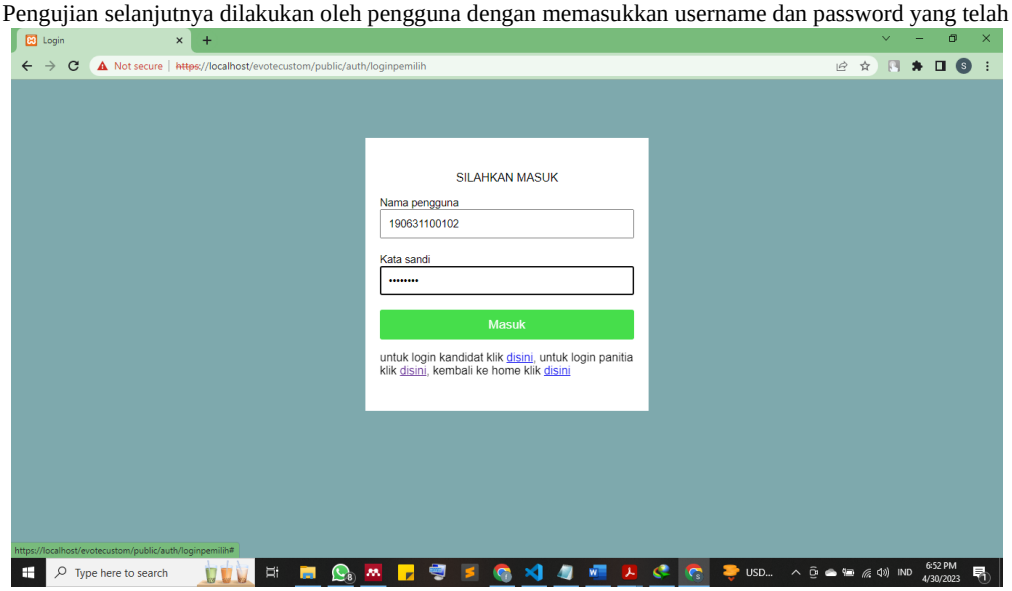
Submitted: **12/05/2023**; Accepted: **25/05/2023**; Published: **31/05/2023**

JURNAL INFORMATION SYSTEM
Volume 3, Nomor 1, Mei 2023, Page 001-009
Email : jis@unkris.ac.id
ISSN 2807-7849 (media online)
Available Online at https://jurnalteknik.unkris.ac.id/index.php/jis



Gambar 5. Tampilan dashboard admin

b. Pengujian selanjutnya dilakukan oleh pengguna dengan memasukkan username dan password yang telah dibuat.

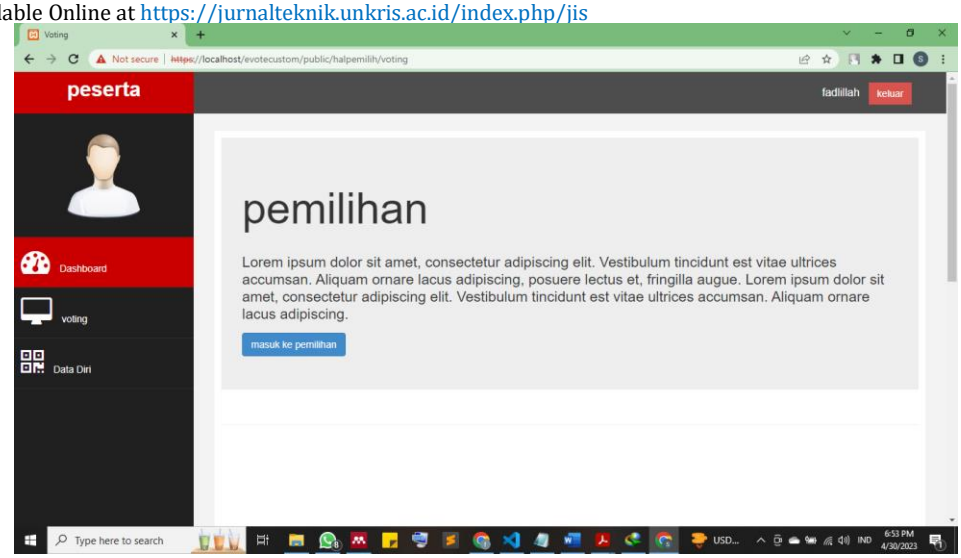


Gambar 6. Tampilan halaman login pemilih

Dan hasilnya

Submitted: **12/05/2023**; Accepted: **25/05/2023**; Published: **31/05/2023**

JURNAL INFORMATION SYSTEM
Volume 3, Nomor 1, Mei 2023, Page 001-009
Email : jis@unkris.ac.id
ISSN 2807-7849 (media online)
Available Online at https://jurnalteknik.unkris.ac.id/index.php/jis



Gambar 7. Tampilan dashboard pemilih

4. KESIMPULAN

Berdasarkan hasil pengujian yang telah dilakukan, kesimpulan yang dapat ditarik berdasarkan penelitian dan analisis diatas adalah sebagai berikut :

1. Pada penelitian ini menghasilkan sebuah aplikasi *e-voting* dengan menggunakan keamanan database kriptografi RC4 yang dilakukan pada pemilihan ketua umum HIMAPIF.
2. Perancangan sistem menggunakan metode *waterfall*.
3. Akun yang dibuat oleh admin dapat dienkripsi dengan baik sehingga terjamin kerahasiaan dan keamanannya.
4. Ketika user akan masuk kedalam halaman pemilu user dapat memasukkan username dan password yang mana password tersebut sudah terenkripsi dan dapat masuk kedalam halaman pemilu.
5. Sistem sebelumnya hanya menyimpan data dalam database sesuai dengan apa yang dimasukkan ke dalam sistem informasi. Ini berarti siapa pun yang melihat isi database dapat membaca artinya, dan keamanannya tidak terjamin. Namun pada penelitian ini sudah tidak bisa lagi dilakukan hal yang sama dikarenakan keamanan database sudah ditingkatkan dengan menggunakan kriptografi RC4.

REFERENCES

[1] W. P. Abdul Kodir, "IMPLEMENTASI KRIPTOGRAFI DENGAN MENGGUNAKAN METODE RC4 DAN BASE64 UNTUK MENGAMANKAN DATABASE SEKOLAH PADA SDN GROGOL UTARA 10," *Skanika*, vol. 4, no. 1, pp. 7–14, 2021, doi: 10.21856/j-pep.2021.4.08.

[2] I. Afrianto and N. Taliasih, "Sistem Keamanan Basis Data Klien P.T. Infokes Menggunakan Kriptografi Kombinasi RC4 Dan Base64," *J. Nas. Teknol. dan Sist. Inf.*, vol. 6, no. 1, pp. 9–18, 2020, doi: 10.25077/teknosi.v6i1.2020.9-18.

[3] A. Setiawan and T. Fatimah, "Implementasi Algoritma Kriptografi Rc4 Untuk Keamanan Database Aplikasi Penggajian Karyawan Berbasis Web Pada Pt. Trans Intra Asia," *Skanika*, vol. 4, no. 1, pp. 66–71, 2021, doi: 10.36080/skanika.v4i1.2044.

[4] M. D. Wulandari *et al.*, "Aplikasi Pengamanan Database Berbasis Desktop dengan Algoritma AES-128 dan Rivest Code (RC4)," *Skanika*, vol. 1, no. 1, pp. 373–379, 2018.

[5] Z. Basim, "Steganografi Dengan Algoritma Eof Untuk Keamanan Data Berbasis Desktop Pada Smk As- Su ' Udiyyah," *Skanika*, vol. 3, no. 4, pp. 54–60, 2020.

[6] R. Maulana and R. M. Simanjorang, "Implementasi Kriptografi Pengamanan Data Pribadi Siswa SMA Swasta Jaya Krama Beringin Dengan Algoritma RC4," *J. Nas. Komputasi dan Teknol. Inf.*, vol. 4, no. 6, pp. 377–383, 2021, doi: 10.32672/jnkti.v4i6.3533.

[7] S. Jaleha and E. Suriyani, "Implementasi Sistem E-Voting Dilihat Aspek Komunikasi Dalam Rangka Pemilihan Kepala Desa Di Desa Kambitin Raya Kecamatan Tanjung Kabupaten Tabalong," *J. Adm. Publik dan Bisnis*, vol. 3, no. 2, pp. 1253–1264, 2020.

Submitted: **12/05/2023**; Accepted: **25/05/2023**; Published: **31/05/2023**

[8] I. Anas, G. L. Ginting, E. Ndruru, A. S. Sembiring, and T. Zebua, "Perancangan Aplikasi Keamanan Data Dengan Kombinasi Algoritma Kriptografi RC4 dan One Time Pad," *J. Ris. Komput.*, vol. 8, no. 1, pp. 20–27, 2021, doi: 10.30865/jurikom.v7i5.2541.

[9] J. S. Surbakti and S. Subandi, "Aplikasi Pengamanan Database Keuangan Berbasis Desktop Menggunakan Algoritma Rc4 Dan Vigenere Cipher," *Skanika*, vol. 1, no. 1, pp. 237–242, 2018, [Online]. Available: https://jom.fti.budiluhur.ac.id/index.php/SKANIKA/article/view/187

[10] S. Susanto, "Implementasi Keamanan Data Menggunakan Algoritma Rivest Code 4 (RC4) Pada Sistem Informasi Inventory Stock Barang Pada Distributor PT.Wings Food," *Lontar Komput. J. Ilm. Teknol. Inf.*, vol. 8, no. 2, pp. 77–88, 2017, doi: 10.24843/lkjiti.2017.v08.i02.p02.

[11] S. Murni, L. Latifah, R. Sabaruddin, and Y. L, "Penerapanan Metode Waterfall Dalam Pembangunan Aplikasi Akuntansi Kontraktor Dengan Pemrograman Php," *J. Teknol. Inf. MURA*, vol. 11, no. 1, pp. 55–67, 2019, doi: 10.32767/jti.v11i1.452.

[12] G. Grehasen and S. Mulyati, "Pengamanan Database Pada Aplikasi Test Masuk Karyawan Baru Berbasis Web Menggunakan Algoritma Kriptografi AES-128 Dan RC4," *Budi Luhur Inf. Technol.*, vol. 14, no. 1, pp. 52–60, 2017, [Online]. Available: https://journal.budiluhur.ac.id/index.php/bit/article/view/464%0A

[13] K. Fahmi, "Pengamanan Data Arsip Pada Balai Desa Sidodadi Menggunakan Kriptografi Modern RC4," *Resolusi Rekayasa Tek. Inform. dan Inf.*, vol. 2, no. 2, pp. 58–66, 2021, [Online]. Available: http://www.djournals.com/resolusi/article/view/241

[14] Taronisokhi zebua, "Pengamanan citra digital berdasarkan Modifikasi algoritma rc4," *J. Teknol. Inf. dan Ilmu Komput. (JTIIK*, vol. 4, no. 4, pp. 275–282, 2017, doi: 10.25126/jtiik.201744474.