RESOLUSI : Rekayasa Teknik Informatika dan Informasi
ISSN 2745-7966 (Media Online)
Vol 1, No 2, November 2020
Hal 142-151
https://djournals.com/resolusi

Implementasi Kriptografi Untuk Keamanan Pesan Chatting Menggunakan Algoritma Pontifex

Ricki Rezandi Batubara

[1] Fakultas Ilmu Komputer dan Teknologi Informasi, Prodi Teknik Informatika, Universitas Budi Darma, Medan, Indonesia
Email: rickirez@gmail.com

Abstrak−Data merupakan kumpulan unsur-unsur penting yang berguna, seperti gambar, suara, teks. Data merupakan komponen yang rentan terhadap pencurian ataupun penyadapan, terlebih apabila data tersebut berisi hal yang penting dan rahasia. Banyak orang yang memiliki kepentingan ingin mendapatkan data secara illegal tanpa melalui prosedur resmi. Pin, Pasword, Nomor Rekening, atau Nomor Kartu Kredit merupakan sebagian kecil data yang sering disalahgunakan oleh oknum-oknum tidak bertanggung jawab. Hal tersebut tentu perlu dicegah agar kejadian-kejadian tindak pencurian data tidak berulang-ulang terjadi. Untuk memudahkan proses pengamanan teks agar tidak mudah dibaca oleh orang lain sehingga terjaga keaslian data tersebut. Untuk menjaga informasi dari yang tidak berhak mengakses maka digunakan suatu algoritma yaitu algoritma Pontifex dalam menjaga kerahasian pesan teks tersebut. Teknik pengamanan data sudah banyak dikembangkan pada saat ini, hal tersebut tentu semakin memudahkan semua pihak dalam melakukan pengamanan data. Salah satu yang banyak dipergunakan saat ini adalah sistem pengamanan berbasis komputerisasi yang dapat dipergunakan kapan saja dan dimana saja. Peelitian ini menggunakan alat bantu Visual Basic 2008 dalam proses penjagaan informasi dari pihak lain yang tidak berhak mengaksesnya.

Kata Kunci: Kriptografi, Pesan, Chatting, Algoritma Pontifex

Abstract−Data is a collection of important elements that are useful, such as images, sounds, text. Data is a component that is vulnerable to theft or wiretapping, especially if the data contains important and confidential matters. Many people who have an interest want to get data illegally without going through official procedures. Pin, Password, Account Number, or Credit Card Number are small pieces of data that are often misused by irresponsible individuals. This of course needs to be prevented so that incidents of data theft do not occur repeatedly. To facilitate the process of securing text so that it is not easily read by others so that the authenticity of the data is maintained. To protect information from those who are not entitled to access, an algorithm is used, namely the Pontifex algorithm in maintaining the confidentiality of the text message. Many data security techniques have been developed at this time, this certainly makes it easier for all parties to secure data. One that is widely used today is a computerized security system that can be used anytime and anywhere. This research uses Visual Basic 2008 tools in the process of safeguarding information from other parties who are not entitled to access it.

Keywords: Cryptography, Message, Chat, Pontifex Algorithm

1. PENDAHULUAN

Dimasa ini penggunaan teknologi internet di dunia sudah berkembang pesat. Semua kalangan telah menikmati internet. Bahkan, perkembangan teknologi internet tersebut semakin memudahkan penggunanya dalam berkomunikasi melalui bermacam-macam media maupun aplikasi. Sistem keamanan pengiriman data (komunikasi data yang aman) dipasang untuk mencegah pencurian, kerusakan, dan penyalahgunaan data yang terkirim melalui jaringan komputer. Dalam praktek, pencurian data berwujud pembacaan oleh pihak yang tidak berwenang biasanya dengan menyadap saluran publik. Teknologi jaringan komputer telah dapat mengurangi bahkan membuang kemungkinan adanya kerusakan data akibat buruknya konektivitas fisik, namun gangguan tetap bisa terjadi karena ada unsur kesengajaan yang mengarah kepenyalah gunaan sistem dari pihak-pihak tertentu.

Kriptografi adalah ilmu yang mempelajarin menyembunyikan pesan, pesan yang akan dirahasiakan disebut plaintext. Pesan yang sudah diacak disebut ciphertext. Proses untuk mengkonversi plaintext menjadi ciphertext disebut enkripsi. Proses untuk mengembalikan plaintext dari ciphertext disebut deskripsi. Algoritma kriptografi (ciphers) adalah fungsi-fungsi matematika yang digunakan untuk melakukan enkripsi dan deskripsi. Dalam kriptografi diperlukan kunci yaitu kode untuk melakukan enkripsi dan deskripsi.

Banyak orang yang memiliki kepentingan ingin mendapatkan data secara ilegal tanpa melalui prosedur resmi. Pin, Password, Nomor Rekening, atau Nomor Kartu Kredit merupakan sebagian kecil data yang sering disalah gunakan oleh oknum-oknum tidak bertanggung jawab. Hal tersebut tentu perlu dicegah agar kejadian-kejadian tindak pencurian data tidak berulang-ulang terjadi. Apabila semua data aman akan menjadikan individu ataupun institusi mendapat kepercayaan dari masyarakat sehingga menjamin keberlangsungan proses bisnis pada individu ataupun institusi tersebut.

Teknik pengamanan data sudah banyak dikembangkan pada saat ini, hal tersebut tentu semakin memudahkan semua pihak dalam melakukan pengamanan data. Salah satu yang banyak dipergunakan saat ini adalah sistem pengamanan berbasis komputerisasi yang dapat dipergunakan kapan saja dan dimana saja. Pada kriptografi, terdapat proses enkripsi yang mengubah teks polos menjadi ciphertext, dan proses deskripsi yang mengubah ciphertext menjadi teks polos kembali algoritma ini juga dapat memanfaatkan kunci yang dimasukkan dari luar.

Algoritma Pontifex adalah suatu cara atau proses untuk melakukan pengamanan pengolahan data. Pontifex adalah jaringan permutasi substitusi 32-putaran (SPN) yang beroperasi pada empat kata 32-bit, sehingga memiliki ukuran blok 128 bit. Pontifex mengenkripsi plaintext 128-bit ke 128-bit ciphertext dalam 32 putaran dengan 33 subkunci. Pengguna Pontifex adalah jaringan permutasi substitusi 32-putaran (SPN) yang beroperasi pada empat kata 32-bit, sehingga memiliki ukuran blok 128 bit. Pontifex mengenkripsi plaintext 128-bit ke 128-bit ciphertext dalam 32 putaran dengan 33

ISSN 2745-7966 (Media Online)
Vol 1, No 2, November 2020
Hal 142-151
https://djournals.com/resolusi

sub kunci. Panjang kunci pengguna diasumsikan variabel tetapi dalam proposal, itu tetap menjadi 128, 192 atau 256 bit. [1]

2. METODOLOGI PENELITIAN

2.1 Kriptografi

Kriptografi (Cryptography) merupakan cabang ilmu pengetahuan yang menggunakan persamaan matematis untuk melakukan proses enkripsi maupun deskripsi data. Teknik ini digunakan untuk mengkonversi atau mengubah data ke dalam bentuk kode-kode tertentu, dengan tujuan informasi yang disimpan maupun ditransmisikan melalui jaringan yang tidak aman seperti internet, tidak dapat dibaca oleh siapapun kecuali oleh orang yang berwenang. Kriptografi adalah suatu ilmu yang menciptakan suatu komunikasi secara aman yang tidak dapat dimengerti atau diterjemahkan oleh setiap orang kecuali orang tertentu yang dimaksud.

Pada kriptografi modern proses enkripsi dan deskripsi biasanya dilakukan dengan kunci yang dipilih oleh pelaku komunikasi ataupun dapat dibangkitkan secara acak. Algoritma kriptografi modern seperti DES, AES, dan IDEA merupakan algoritma kriptografi modern yang sangat rumit dan kompleks. Algoritma kriptografi modern secara umum memiliki daya tahan yang cukup tinggi terhadap serangan, namun memiliki alur proses yang rumit serta membutuhkan sumber daya yang relative besar. Suatu pesan yang tidak disandikan disebut sebagai plaintext ataupun dapat disebut juga sebagai cleartext. Proses yang dilakukan untuk mengubah plaintext ke dalam ciphertext disebut encryption atau encipherment. Sedangkan proses untuk mengubah ciphertext kembali ke plaintext disebut decryption atau decipherment. [2].

2.2 Pesan

Pesan merupakan bagian dari unsur-unsur komunikasi, Hafied Cangara dalam bukunya Pengantar Ilmu Komunikasi menyatakan bahwa “Dalam proses komunikasi, pengertian pesan adalah sesuatu yang disampaikan pengirim kepada penerima. Pesan dapat disampaikan dengan cara tatap muka atau melalui media komunikasi. Isinya bisa berupa ilmu pengetahuan, hiburan, informasi, nasihat atau propaganda”. Pengertian pesan itu sendiri menurut Onong Uchjana Effendy adalah merupakan terjemahan dari bahasa asing “message” yang artinya adalah lambang bermakna (meaningful symbols), yakni lambang yang membawakan pikiran atau perasaan komunikator. Menurut kedua pendapat di atas dapat disimpulkan bahwa pesan adalah suatu gagasan (ide) yang dituangkan dalam lambang-lambang untuk disebarkan dan kemudian diteruskan oleh komunikator. [6]

2.3 Algoritma Pontifex

Pontifex adalah jaringan permutasi substitusi 32-putaran (SPN) yang beroperasi pada empat kata 32-bit, sehingga memiliki ukuran blok 128 bit [3,11]. Pontifex mengenkripsi plaintext 128-bit ke 128-bit ciphertext dalam 32 putaran dengan 33 subkunci. Pengguna Panjang kunci diasumsikan variabel tetapi dalam proposal, itu tetap menjadi 128, 192 atau 256 bit. Harus disebutkan bahwa kunci pendek dengan kurang dari 256 bit dipetakan ke kunci 256 bit dengan menambahkan satu '1' bit ke akhir MSB diikuti oleh sebanyak '0' bit yang diperlukan untuk menghasilkan 256 bit. Cipher terdiri dari IP permutasi awal, 32 putaran, dan FP permutasi final. Setiap putaran melibatkan operasi pencampuran kunci, melewati S-kotak, dan transformasi linear. Di babak terakhir, transformasi linear digantikan oleh operasi pencampuran tombol tambahan [1].

Algoritma untuk menghasilkan kunci untuk proses enkripsi dan deskripsi terdiri dari enam langkah. Enam tahap ini akan menghasilkan sebuah angka yang merupakan salah satu bagian aliran kunci. Enam tahap ini kemudian dilakukan kembali untuk mendapatkan kunci kedua dan terus diulang sampai panjang kunci yang diinginkan atau disepakati. Adapun langkah-langkah dalam Keenam langkah tersebut adalah sebagai berikut:

1. Urutkan tumpukan kartu berdasarkan kunci tertentu.
2. Temukan joker A (yang bernilai 27).
3. Temukan joker B (yang bernilai 28).
4. Lakukan triple cut.
5. Susunan kartu sebelum triple cut dilakukan
6. Lakukan count cut.
7. Temukan kartu keluaran.

Langkah-langkah dalam melakukan enkripsi dan deskripsi dengan menggunakan algoritma pontifex antara lain :

1. Ambil sebuah karakter dari kata kunci
2. Lakukan enam langkah untuk mendapatkan huruf aliran kunci
3. Lakukan triple cut, sejumlah cut_size kartu awal diganti dengan kartu terakhir.
4. Lakukan pemindahan kartu berikutnya, dengan meletakan kartu pertama sebagai kartu paling bawah.
5. Dengan demikian proses untuk mendapatkan susunan kartu menurut karakter pertama dari kunci telah dilakukan. Langkah-langkah diatas diulangi untuk semua karakter lain dari kata kunci.

ISSN 2745-7966 (Media Online)
Vol 1, No 2, November 2020
Hal 142-151
https://djournals.com/resolusi

3. HASIL DAN PEMBAHASAN

3.1 Analisa Masalah

Bedasarkan analisa yang dilakukan oleh penulis terhadap data yang tidak diamankan menggunakan teknik *enkripsi* dan *deskripsi* maka data hanya disimpan dalam bentuk data yang tidak amankan sehingga siapapun masih bisa membaca dan mengerti isinya. Hal ini sangat rentan dengan terjadinya kecurangan yang dapat dilakukan oleh pihak–pihak yang tidak bertanggung jawab. Karena data tersebut dapat dengan mudah dimanipulasi karena tidak ada sistem yang dapat mengamankan data tersebut.

Pada proses pengamanan pesan *chatting* memastikan bahwa *user* (pengguna) dan orang yang berkomunikasi dengan *user* (pengguna) saja yang dapat membaca apa yang dikirimkan. Pesan-pesan yang akan diamankan *(enkripsi)* dengan kunci dan hanya penerima dan *user* (pengguna) saja yang memiliki kunci special yang diperlukan untuk membuka dan membaca pesan yang dikirimkan. Untuk membuka pesan yang telah dikirim si penerima pesan harus melakukan proses *dekripsi* dan penggunaan kunci yang telah ditentukan oleh *user* (pengguna) sehingga pesan tersebut dapat dibaca oleh si penerima pesan.

3.2 Penerapan Algoritma Pontifex

Algoritma untuk menghasilkan kunci untuk proses *enkripsi* dan *deskripsi* terdiri dari enam langkah. Enam tahap ini akan menghasilkan sebuah angka yang merupakan salah satu bagian aliran kunci. Enam tahap ini kemudian dilakukan kembali untuk mendapatkan kunci kedua dan terus diulang sampai panjang kunci yang diinginkan atau disepakati. Keenam langkah tersebut adalah sebagai berikut:

1. Urutkan tumpukan kartu berdasarkan kunci tertentu.
   Bagian ini adalah bagian paling penting, karena pihak yang mengetahui sebuah nilai awal dari deck dapat dengan mudah mendapatkannilai yang sama darinya. Bagaimana sebuah tumpukan diinisialisasi terserah oleh penerima. Mengocok kartu dengan benar-benar acak akan lebih baik, walaupun masih ada beberapa metode lain.
   Urutan awal seperti ini:
   1 47 10 13 16 19 22 25 **28** 3 6 9 12 1518 21 24 **27** 2 5 8 11 14 17 20 23 26
2. Temukan joker A (yang bernilai 27).
   Pindahkan satu kartu ke bawah (dengan kata lain, menukar dengan satu kartu dibawahnya). Jika joker tersebut berada di tumpukan paling bawah, pindahkan ke tepat di bawah tumpukan teratas.
   Urutan kartu tersebut akan menjadi seperti ini:
   1 47 10 13 16 19 22 25 **28** 3 6 9 12 1518 21 24 2 **27** 5 8 11 14 17 20 23 26
3. Temukan joker B (yang bernilai 28).
   Pindahkan dua kartu ke bawah. Jika joker tersebut berada pada tumpukan terbawah, pindahkan ke bawah kartu kedua dari atas (jadi kartu ketiga). Jika joker tersebut berada pada posisi kedua dari bawah, pindahkan ke bawah kartu teratas (menjadi kartu kedua).
   Setelah langkah ketiga ini, urutan kartu akan menjadi:
   1 47 10 13 16 19 22 25 3 6 **28** 9 12 15 18 21 24 2 **27** 5 8 11 14 17 20 23 26
4. Lakukan *triple cut*.
   Yaitu ganti kartu-kartu yang berada di bagian kiri kartu joker pertama dengan kartu-kartu di bagian kanan dari kartu joker kedua. Perlu diperhatikan bahwa joker pertama adalah joker yang berada di posisi lebih tinggi dari kartu joker lain, tidak penting apakah itu joker A atau B.
   Susunan kartu sebelum *triple cut* dilakukan:
   1 4 7 10 13 16 19 22 25 3 6 **28** 9 12 15 18 21 24 2 **27** 5 8 11 14 17 20 23 26
   Susunankartu setelah *triple cut* dilakukan:
   5 8 11 14 17 2023 26 **28** 9 12 15 18 21 24 2 **27** 1 4 7 10 13 16 19 22 25 3 6
5 Lakukan *count cut*.
   Lihat nilai kartu terbawah, anggap nilai tersebut adalah n. Ambil n kartu pertama dan pindahkan ke posisi kedua dari bawah.
   Susunan kartu sebelum *count cut* dilakukan:
   5 8 11 14 17 20 23 26 **28** 9 12 15 18 21 24 2 **27** 1 4 7 10 13 16 19 22 25 3 6
   Susunankartu setelah *count cut* dilakukan:
   23 26 **28** 9 12 15 18 21 24 2 **27** 1 4 7 10 13 16 19 22 25 3 5 8 11 14 17 206
6. Temukan kartu keluaran.
   Untuk melakukan ini, lihat kartu paling atas. Hitung sebanyak nilai kartu tersebut mulai dari kartu setelah kartu paling atas. Nilai kartu pada urutan tersebut adalah nilai berikutnya dalam kunci aliran.
   Pada contoh yang digunakan, nilai kartu paling atas adalah 23. Nilai kartu ke 23 dari kartu setelah kartu paling atas adalah 11. Nilai 11 inilah yang dimasukkan ke dalam kunci aliran. Setelah itu ulangi lagi dari langkah kedua sampai ke enam. Lakukan terus sampai sebanyak panjang kunci yang digunakan. Sebelum mengulang langkah-langkah tersebut, urutan kartu dari proses sebelumnya tidak perlu
   Untuk contoh Implementasi ini, pesan dan kunci yang digunakan harus ditentukan terlebih dahulu.
   Pesan : ILHAMMUDDIN

ISSN 2745-7966 (Media Online)
Vol 1, No 2, November 2020
Hal 142-151
https://djournals.com/resolusi

Kunci : BUDIDARMA

Sesuai dengan langkah-langkah *enkripsi* yang diberikan pada bagian sebelumnya, maka hal yang pertama harus dilakukan adalah pengurutan sesuai dengan kunci yang diberikan.

Kunci : BUDIDARMA

Untuk pengurutan kartu awal ini, langkah yang harus dilakukan adalah

1. Ambil sebuah karakter dari kata kunci untuk contoh implementasi pertama (huruf B) maka *Cut size* = 2
2. Lakukan enam langkah untuk mendapatkan huruf aliran kunci yang telah dijelaskan dari contoh sebelumnya, maka pengurutan kartu dimulai. Urutan kartu awal dari huruf terkecil ke nilai terbesar. Perlu di ingat kembali bahwa nilai 1-13 diberikan untuk kartu As-kartu king keriting (*clubs*) secara berurutan. Nilai 14-26 untuk kartu berjenis wajik (*diamonds*), nilai 27-39 untuk kartu hati (*heart*) dan nilai 40-52 untuk kartu pohon (*spades*).

   1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18
   19 20 21 22 23 24 25 26 27 28 29 30 31 32 33 34 35 36
   37 38 39 40 41 42 43 44 45 46 47 48 49 50 51 52 A B

   Langkah pertama adalah pemindahan joker A maka susunan kartu akan menjadi

   1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18
   19 20 21 22 23 24 25 26 27 28 29 30 31 32 33 34 35 36
   37 38 39 40 41 42 43 44 45 46 47 48 49 50 51 52 B A

   Langkah kedua adalah Pemindahan joker B. Susunan kartu akan berubah menjadi

1 B 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17
   18 19 20 21 22 23 24 25 26 27 28 29 30 31 32 33 34 35
   36 37 38 39 40 41 42 43 44 45 46 47 48 49 50 51 52 A

   Langkah selanjutnya adalah *triple cut* yang akan menjadi susunan kartu seperti berikut

   B 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18
   19 20 21 22 23 24 25 26 27 28 29 30 31 32 33 34 35 36
   37 38 39 40 41 42 43 44 45 46 47 48 49 50 51 52 A 1

   Langkah keempat adalah *count cut* yang akan memindahkan 1 kartu

   Pertama . posisi kartu selanjutnya.

   2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19
   20 21 22 23 24 25 26 27 28 29 30 31 32 33 34 35 36 37
   38 39 40 41 42 43 44 45 46 47 48 49 50 51 52 A B 1

   Setelah *count cut* ini, proses pembangkitan aliran kunci untuk penyusunan kartu sesuai kunci telah selesai.
3. Lakukan *triple cut*. Sejumlah *cut_size* kartu awal diganti dengan kartu terakhir. Dari hasil di nomor dua, maka posisi urutan kartu berikutnya didapatkan dengan mengganti 2 kartu pertama dengan kartu terakhir.

   1 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20
   21 22 23 24 25 26 27 28 29 30 31 32 33 34 35 36 37 38
   39 40 41 42 43 44 45 46 47 48 49 50 51 52 A B 2 3
4. Lakukan pemindahan kartu berikutnya, dengan meletakan kartu pertama sebagai kartu paling bawah. Posisi kartu lain tidak diubah.

   4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21
   22 23 24 25 26 27 28 29 30 31 32 33 34 35 36 37 38 39
   40 41 42 43 44 45 46 47 48 49 50 51 52 A B 2 3 1

Dengan demikian proses untuk mendapatkan susunan kartu menurut karakter pertama dari kunci telah dilakukan. Langkah-langkah diatas diulangi untuk semua karakter lain dari kata kunci. Selanjutnya akan dicontohkan pengaturan kunci untuk karakter kedua, yaitu U. susunan kartu awal untuk karakter U ini diambil dari susunan yang dihasilkan untuk pengaturan kartu berdasarkan karakter B. maka sususnan awal pengaturan kunci untuk karakter U ini adalah

4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21
22 23 24 25 26 27 28 29 30 31 32 33 34 35 36 37 38 39
40 41 42 43 44 45 46 47 48 49 50 51 52 A B 2 3 1

Langkah-langkahnya adalah :

1. Penentuan *cut_size*

Cut_size = 21

2. Enam langkah mendapatkan aliran kunci, hasil dari perggesran joker A

   4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21
   22 23 24 25 26 27 28 29 30 31 32 33 34 35 36 37 38 39
   40 41 42 43 44 45 46 47 48 49 50 51 52 B A 2 3 1

   Hasil dari penggeseran joker B :

   4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21
   22 23 24 25 26 27 28 29 30 31 32 33 34 35 36 37 38 39
   40 41 42 43 44 45 46 47 48 49 50 51 52 A 2 B 3 1

   Hasil dari *triple cut :*

   3 1 A 2 B 4 5 6 7 8 9 10 11 12 13 14 15 16
   17 18 19 20 21 22 23 24 25 26 27 28 29 30 31 32 33 34

ISSN 2745-7966 (Media Online)
Vol 1, No 2, November 2020
Hal 142-151
https://djournals.com/resolusi

35 36 37 38 39 30 41 42 43 44 45 46 47 48 49 50 51 52
Hasil dari *count cat* :
51 3 1 A 2 B 4 5 6 7 8 9 10 11 12 13 14 15
16 17 18 19 20 21 22 23 24 25 26 27 28 29 30 31 32 33
34 35 36 37 38 39 30 41 42 43 44 45 46 47 48 49 50 52

3. *Triple cut*
Hasil dari *triple cut* :
52 3 1 A 2 B 4 5 6 7 8 9 10 11 12 13 14 15
16 17 18 19 20 21 22 23 24 25 26 27 28 29 30 31 32 33
34 35 36 37 38 39 30 41 42 43 44 45 46 47 48 49 50 51

4. Pemindahan kartu pertama
Hasilnya ;
3 1 A 2 B 4 5 6 7 8 9 10 11 12 13 14 15 16
17 18 19 20 21 22 23 24 25 26 27 28 29 30 31 32 33 34
35 36 37 38 39 40 41 42 43 44 45 46 47 48 49 50 51 52
Penyusunan kartu untuk karakter (D) :
Susunan kartu awal
3 1 A 2 B 4 5 6 7 8 9 10 11 12 13 14 15 16
17 18 19 20 21 22 23 24 25 26 27 28 29 30 31 32 33 34
35 36 37 38 39 40 41 42 43 44 45 46 47 48 49 50 51 52
Langkah yang dilakukan :

1. Penentuan *cut_size*
cut_size = 3
2. Enam langkah mendapatkan aliran kunci.
Hasil dari penggeseran joker A :
3 1 2 A B 4 5 6 7 8 9 10 11 12 13 14 15 16
17 18 19 20 21 22 23 24 25 26 27 28 29 30 31 32 33 34
35 36 37 38 39 40 41 42 43 44 45 46 47 48 49 50 51 52
Hasil dari penggeseran joker B :
3 1 2 A 4 5 B 6 7 8 9 10 11 12 13 14 15 16
17 18 19 20 21 22 23 24 25 26 27 28 29 30 31 32 33 34
35 36 37 38 39 40 41 42 43 44 45 46 47 48 49 50 51 52
Hasil dari *triple cut* :
6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23
24 25 26 27 28 29 30 31 32 33 34 35 36 37 38 39 40 41
42 43 44 45 46 47 48 49 50 51 52 A 4 5 B 3 1 2
Hasil *count cat*
8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25
26 27 28 29 30 31 32 33 34 35 36 37 38 39 40 41 42 43
44 45 46 47 48 49 50 51 52 A 4 5 B 3 1 6 7 2

3. *Triple cut*
Hasil dari *triple cut* :
2 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26 27
28 29 30 31 32 33 34 35 36 37 38 39 40 41 42 43 44 45
46 47 48 49 50 51 A 4 5 B 3 1 6 7 52 8 9 10

4. Pemindahan kartu pertama, hasil nya :
11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26 27 28
29 30 31 32 33 34 35 36 37 38 39 40 41 42 43 44 45 46
47 48 49 50 51 A 4 5 B 3 1 6 7 52 8 9 1 0 2
Penyusunan berikutnya adalah penyusunan karakter keempat. Yaitu I. susunan kartu awal untuk karakter I :
11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26 27 28
29 30 31 32 33 34 35 36 37 38 39 40 41 42 43 44 45 46
47 48 49 50 51 A 4 5 B 3 1 6 7 52 8 9 1 0 2
Langkah untuk menyusun kartu :

1. Penentuan *cut _size* = 9
2. Enam langkah mendapatkan aliran kunci.
Hasil dari penggeseran joker A :
11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26 27 28
29 30 31 32 33 34 35 36 37 38 39 40 41 42 43 44 45 46
47 48 49 50 51 4 A 5 B 3 1 6 7 52 8 9 1 0 2
Hasil dari penggeseran joker B :
11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26 27 28

ISSN 2745-7966 (Media Online)
Vol 1, No 2, November 2020
Hal 142-151
https://djournals.com/resolusi

29 30 31 32 33 34 35 36 37 38 39 40 41 42 43 44 45 46
47 48 49 50 51 4 A 5 3 1 B 6 7 52 8 9 1 0 2
Hasil dari *triple cut* :
6 7 52 8 9 1 0 2 A 5 3 1 B 11 12 13 14 15 16
17 18 19 20 21 22 23 24 25 26 27 28 29 30 31 32 33 34
35 36 37 38 39 40 41 42 43 44 45 46 47 48 49 50 51 4
Hasil dari *count cut* :
A 5 3 1 B 11 12 13 14 15 16 17 18 19 20 21 22 23
24 25 26 27 28 29 30 31 32 33 34 35 36 37 38 39 40
41 42 43 44 45 46 47 48 49 50 51 4 6 7 52 8 9 1 0 2

3. *Triple cut* :
2 4 6 7 52 8 9 10 A 5 3 1 B 11 12 13 14 15
16 17 18 19 20 21 22 23 24 25 26 27 28 29 30 31 32 33
34 35 35 36 37 38 39 40 41 42 43 44 45 46 47 48 49 50 51 4
4. Pemindahan kartu pertama
Hasilnya :
4 6 7 52 8 9 10 A 5 3 1 B 11 12 13 14 15 16 17
18 19 20 21 22 23 24 25 26 27 28 29 30 31 32 33 34 35 35
36 37 38 39 40 41 42 43 44 45 46 47 48 49 50 51 4 2
Penyusunan kartu untuk karakter kelima (D)
Dimulai dengan sususnan kartu :
4 6 7 52 8 9 10 A 5 3 1 B 11 12 13 14 15 16 17
18 19 20 21 22 23 24 25 26 27 28 29 30 31 32 33 34 35 35
36 37 38 39 40 41 42 43 44 45 46 47 48 49 50 51 4 2
Langkah untuk penyusunan kartu :

1. Penentuan *cut_size* = 4
2. Enam langkah mendapatkan aliran kunci.

Hasil dari penggeseran joker A :
4 6 7 52 8 9 10 5 3 A 1 B 11 12 13 14 15 16 17
18 19 20 21 22 23 24 25 26 27 28 29 30 31 32 33 34 35 35
36 37 38 39 40 41 42 43 44 45 46 47 48 49 50 51 4 2
Hasil dari penggeseran joker B :
4 6 7 52 8 9 10 5 3 A 1 11 12 B 13 14 15 16 17
18 19 20 21 22 23 24 25 26 27 28 29 30 31 32 33 34 35 35
36 37 38 39 40 41 42 43 44 45 46 47 48 49 50 51 2
Hasil dari *triple cut* :
13 14 15 16 17 18 19 20 21 22 23 24 25 26 27 28 29 30
31 32 33 34 35 35 36 37 38 39 40 41 42 43 44 45 46 47
48 49 50 51 4 2 A 1 11 12 B 4 6 7 52 8 9 10 5 3
Hasil dari *count cut* ;
B 4 6 7 52 8 9 10 5 3 13 14 15 16 17 18 19 20 21 22
23 23 24 25 26 27 28 29 30 31 32 33 34 35 35 36 37 38
38 39 40 41 42 43 44 45 46 47 48 49 50 51 4 2 A 1 11 12

3. Triple cut

Hasil dari *triple cut* sususnan kartu :
12 52 8 9 10 5 3 13 14 15 16 17 18 19 20 21 22 23 23
24 25 26 27 28 29 30 31 32 33 34 35 35 36 37 38 39
40 41 42 43 44 45 46 47 48 49 50 51 4 2 A 1 B 11

4. Pemindahan kartu pertama, hasilnya :
52 8 9 10 5 3 13 14 15 16 17 18 19 20 21 22 23 2 24
25 26 27 28 29 30 31 32 33 34 35 35 36 37 38 39 40
41 42 43 44 45 46 47 48 49 50 51 4 2 A 1 B 11 12
Selanjutnya adalah penyusunan kartu berdasarkan karakter A susunan awal kartunya:
52 8 9 10 5 3 13 14 15 16 17 18 19 20 21 22 23 2 24
25 26 27 28 29 30 31 32 33 34 35 35 36 37 38 39 40
41 42 43 44 45 46 47 48 49 50 51 4 2 A 1 B 11 12

1. Penentuan *cut_size*

Cut_size = 1

2. Penggerakan joker A. hasilnya :
52 8 9 10 5 3 13 14 15 16 17 18 19 20 21 22 23 2 24
25 26 27 28 29 30 31 32 33 34 35 35 36 37 38 39 40
41 42 43 44 45 46 47 48 49 50 51 4 2 1 A B 11 12

ISSN 2745-7966 (Media Online)
Vol 1, No 2, November 2020
Hal 142-151
https://djournals.com/resolusi

Penggeseran joker B. hasilnya :
52 8 9 10 5 3 13 14 15 16 17 18 19 20 21 22 23 2 24
25 26 27 28 29 30 31 32 33 34 35 36 37 38 39 40
41 42 43 44 45 46 47 48 49 50 51 4 2 1 A 11 12 B
Triple cut :
52 A 11 12 B 9 10 5 3 13 14 15 16 17 18 19 20 21
22 23 2 24 25 26 27 28 29 30 31 32 33 34 35 36 37 38
39 40 41 42 43 44 45 46 47 48 49 50 51 4 2 1
Count cut ;
B 9 10 5 3 13 14 15 16 17 18 19 20 21 22 23 24 4 2
25 26 27 28 29 30 31 32 33 34 35 36 37 38 39 40 41
42 43 44 45 46 47 48 49 50 51 52 A 11 12 1

3. *Triple cut* :
1 A 11 12 B 9 10 5 3 13 14 15 16 17 18 19 20 21
22 23 24 4 2 25 26 27 28 29 30 31 32 33 34 35 36
36 37 38 39 40 41 42 43 44 45 46 47 48 49 50 51 52
4. Hasil dari pemindahan kartu pertama
A 11 12 B 9 10 5 3 13 14 15 16 17 18 19 20 21 22
23 24 4 2 25 26 27 28 29 30 31 32 33 34 35 36 37
38 39 40 41 42 43 44 45 46 47 48 49 50 51 52 1
Penyusunan berikutnya dimulai dengan susunan :
A 11 12 B 9 10 5 3 13 14 15 16 17 18 19 20 21 22
23 24 4 2 25 26 27 28 29 30 31 32 33 34 35 36 37
38 39 40 41 42 43 44 45 46 47 48 49 50 51 52 1

1. Penentuan *cut size* = 18
2. Hasil dari penggeseran joker A ;
11 A 12 B 9 10 5 3 13 14 15 16 17 18 19 20 21 22
23 24 4 2 25 26 27 28 29 30 31 32 33 34 35 36 37
38 39 40 41 42 43 44 45 46 47 48 49 50 51 52 1
Penggeseran joker B ;
11 A 12 9 10 B 5 3 13 14 15 16 17 18 19 20 21 22
23 24 4 2 25 26 27 28 29 30 31 32 33 34 35 36 37
38 39 40 41 42 43 44 45 46 47 48 49 50 51 52 1
Triple cut :
B 5 3 13 14 15 16 17 18 19 20 21 22 23 24 4 2 25 26
27 A 12 9 10 28 29 30 31 32 33 34 35 36 37 38
39 40 41 42 43 44 45 46 47 48 49 50 51 52 1 11
Count cut :
5 3 13 14 15 16 17 18 19 20 21 22 23 24 4 2 25 26 27
A 12 9 10 28 29 30 31 32 33 34 35 36 37 38 39 40
41 42 43 44 45 46 47 48 49 50 51 52 1 B 11

3. Triple cut
11 12 A 9 10 28 29 30 31 32 33 34 35 36 37 38 39 40
5 3 13 14 15 16 17 18 19 20 21 22 23 24 4 2 25 26 27
41 42 43 44 45 46 47 48 49 50 51 52 1 B

4. Pemindahan kartu pertama
12 9 A 10 28 29 30 31 32 33 34 35 36 37 38 39 40 5
3 13 14 15 16 17 18 19 20 21 22 23 24 4 2 25 26 27
41 42 43 44 45 46 47 48 49 50 51 52 1 B 11
Selanjutnya penyusunan kartu berdasarkan karakter R. susunan awal kartunya :
12 9 A 10 28 29 30 31 32 33 34 35 36 37 38 39 40 5
3 13 14 15 16 17 18 19 20 21 22 23 24 4 2 25 26 27
41 42 43 44 45 46 47 48 49 50 51 52 1 B 11
Langkah-langkah penyusunan kartu ;

1. Penentuan nilai *cut_size*
Cut_size = 9
2. Empat langkah pembangkitan aliran kunci.
Pertama, penggesran joker A :
12 9 10 A 28 29 30 31 32 33 34 35 36 37 38 39 40 5
3 13 14 15 16 17 18 19 20 21 22 23 24 4 2 25 26 27
41 42 43 44 45 46 47 48 49 50 51 52 1 B 11
Kedua, penggeseran joker B :

ISSN 2745-7966 (Media Online)
Vol 1, No 2, November 2020
Hal 142-151
https://djournals.com/resolusi

12 B 9 10 A 28 29 30 31 32 33 34 35 36 37 38 39
40 5 3 13 14 15 16 17 18 19 20 21 22 23 24 4 2 25
26 27 41 42 43 44 45 46 47 48 49 50 51 52 1 11
Ketiga, *triple cut* :
9 10 A 28 29 30 31 32 33 34 35 36 37 38 39 40 5 3
13 14 15 16 17 18 19 20 21 22 23 24 4 2 25 26 27 41
42 43 44 45 46 47 48 49 50 51 52 1 11 12 B
Keempat, *count cut* :
38 39 40 5 3 13 14 15 16 17 18 19 20 21 22 23 24 4
2 A 28 29 30 31 32 33 34 35 36 37 25 26 27 41 42
43 44 45 46 47 48 49 50 51 9 10 52 1 11 12 B

3. *Triple cut*
B 29 30 31 32 33 34 35 36 37 25 26 27 41 42 43 44
45 46 47 48 49 50 51 9 10 52 1 11 12 38 39 40 5
3 13 14 15 16 17 18 19 20 21 22 23 24 4 2 A 28
4. Pemindahan kartu pertama
29 30 31 32 33 34 35 36 37 25 26 27 41 42 43 44
45 46 47 48 49 50 51 9 10 52 1 11 12 38 39 40 5
3 13 14 15 16 17 18 19 20 21 22 23 24 4 2 A 28 B

Selanjutnya adalah proses penyusunan kartu terakhir dengan dengan karakter M. susunan kartu awlnya sama dengan susunan terakhir yang dihasilkan oleh penyusunan kartu dengan karakter A yaitu ;

29 30 31 32 33 34 35 36 37 25 26 27 41 42 43 44
45 46 47 48 49 50 51 9 10 52 1 11 12 38 39 40 5
3 13 14 15 16 17 18 19 20 21 22 23 24 4 2 A 28 B

Langkah-langkah penyusunan kartu :

1. Penentuan nilai *cut size*
Cut_size = 1
2. Empat langkah pembangkitan aliran kunci.
Pertama, penggeseran joker A :
29 30 31 32 33 34 35 36 37 25 26 27 41 42 43 44
45 46 47 48 49 50 51 9 10 52 1 11 12 38 39 40 5
3 13 14 15 16 17 18 19 20 21 22 23 24 4 2 28 A B
Kedua, penggeseran joker B:
30 B 31 32 33 34 35 36 37 25 26 27 41 42 43 44
45 46 47 48 49 50 51 9 10 52 1 11 12 38 39 40 5
3 13 14 15 16 17 18 19 20 21 22 23 24 4 2 28 A 29
Ketiga , *triple cut* :
B 31 32 33 34 35 36 37 25 26 27 41 42 43 44 45 46
47 48 49 50 51 9 10 52 1 11 12 38 39 40 5 3 13
14 15 16 17 18 19 20 21 22 23 24 4 2 28 A 29 30
Keempat, *count cut* :
37 25 26 27 41 42 43 44 45 46 47 48 49 50 51 9
10 52 B 31 32 33 34 35 36 1 11 12 38 39 40 5 3 13
14 15 16 17 18 19 20 21 22 23 24 4 2 28 A 29 30
3. *Triple cut*
30 49 50 51 9 10 52 B 31 32 33 34 35 36 37 25 26
27 41 42 43 44 45 46 47 48 49 50 51 1 11 12 38 39
40 5 3 13 14 15 16 17 18 19 20 21 22 23 24 4 2 28 A 29
Pemindahan kartu pertama
49 0 51 9 10 52 B 31 32 33 34 35 36 37 25 26 27
41 2 43 44 45 46 47 48 49 50 51 1 11 12 38 39 40
3 13 14 15 16 17 18 19 20 21 22 23 24 4 2 28 A 30
Dengan demikian proses pengurutana
Kartu awal telah selesai.susunan kartu yang terakhir dihasilkan sudah bisa digunakan untuk melakukan *enkripsi* pesan

Adapun untuk penjumlahan *keystream* dengan *planteks* antara lain :

1. Penentuan nilai dari kartu keluaran untuk kunci **B**
Nilai keluaran = nilai kartu pada posisi (nilai kartu pertama +1).dengan demikian posisi kartu keluaran adalah pada (4+1)=5.
Maka kartu keluaran adalah pada posisi 5. Nilai kartu pada posisi 5 tersebut adalah 9. Kartu dengan nilai 9 adalah Sembilan As. Sehingga hasilnya adalah
Nilai keluaran = 9
Kartu keluaran = Sembilan As.

ISSN 2745-7966 (Media Online)
Vol 1, No 2, November 2020
Hal 142-151
https://djournals.com/resolusi

2. Penentuan nilai dari kartu keluaran untuk kunci **U**
   Nilai keluaran = nilai kartu pada posisi (nilai kartu pertama +1).dengan demikian posisi kartu keluaran adalah pada (3+1)=4.
   Maka kartu keluaran adalah pada posisi 4. Nilai kartu pada posisi 4 tersebut adalah joker B atau sama dengan nilai 54. Kartu dengan nilai 54 adalah joker B. Sehingga hasilnya adalah
   Nilai keluaran = 54
   Kartu keluaran = joker B
3. Penentuan nilai dari kartu keluaran untuk kunci **D**
   Nilai keluaran = nilai kartu pada posisi (nilai kartu pertama +1).dengan demikian posisi kartu keluaran adalah pada (11+1)=12.
   Maka kartu keluaran adalah pada posisi 12. Nilai kartu pada posisi 12 tersebut adalah 23. Kartu dengan nilai 23 adalah Sepuluh Wajik. Sehingga hasilnya adalah
   Nilai keluaran = 10
   Kartu keluaran = Sepuluh wajik
4. Penentuan nilai dari kartu keluaran untuk kunci **I**
   Nilai keluaran = nilai kartu pada posisi (nilai kartu pertama +1).dengan demikian posisi kartu keluaran adalah pada (4+1)=5.
   Maka kartu keluaran adalah pada posisi 5. Nilai kartu pada posisi 5 tersebut adalah 9. Kartu dengan nilai 9 adalah Sembilan As. Sehingga hasilnya adalah
   Nilai keluaran = 9
   Kartu keluaran = Sembilan As
5. Penentuan nilai dari kartu keluaran untuk kunci **D**
   Nilai keluaran = nilai kartu pada posisi (nilai kartu pertama +1).dengan demikian posisi kartu keluaran adalah pada (52+1)=53.
   Maka kartu keluaran adalah pada posisi 53. Nilai kartu pada posisi 53 tersebut adalah 12. Kartu dengan nilai 12 adalah pro As. Sehingga hasilnya adalah
   Nilai keluaran = 12
   Kartu keluaran = pro As
6. Penentuan nilai dari kartu keluaran untuk kunci **A**
   Nilai keluaran = nilai kartu pada posisi (nilai kartu pertama +1).dengan demikian posisi kartu keluaran adalah pada (joker A atau 53 +1)=54.
   Maka kartu keluaran adalah pada posisi 54. Nilai kartu pada posisi 54 tersebut adalah joker B atau bernilai 54. Kartu dengan nilai 54 adalah pro As.karena melebihi 26, maka nilainya dikurangi 26 menjadi 28.Sehingga hasilnya adalah
   Nilai keluaran = 28
   Kartu keluaran = dua hati
7. Penentuan nilai dari kartu keluaran untuk kunci **R**
   Nilai keluaran = nilai kartu pada posisi (nilai kartu pertama +1).dengan demikian posisi kartu keluaran adalah pada (12 +1)=13.
   Maka kartu keluaran adalah pada posisi 13. Nilai kartu pada posisi 13 tersebut adalah 37. Kartu dengan nilai 37 adalah jack hati. .karena melebihi 26, maka nilainya dikurangi 26 menjadi 11. Sehingga hasilnya adalah
   Nilai keluaran = 11
   Kartu keluaran = jack As
8. Penentuan nilai dari kartu keluaran untuk kunci **M**
   Nilai keluaran = nilai kartu pada posisi (nilai kartu pertama +1).dengan demikian posisi kartu keluaran adalah pada (29 +1)=30.
   Maka kartu keluaran adalah pada posisi 30. Nilai kartu pada posisi 30 tersebut adalah 39. Kartu dengan nilai 39 adalah king hati. .karena melebihi 26, maka nilainya dikurangi 26 menjadi 13. Sehingga hasilnya adalah
   Nilai keluaran = 13
   Kartu keluaran = king As
9. Penentuan nilai dari kartu keluaran untuk kunci **A**
   Nilai keluaran = nilai kartu pada posisi (nilai kartu pertama +1).dengan demikian posisi kartu keluaran adalah pada (49 +1)=50.
   Maka kartu keluaran adalah pada posisi 50. Nilai kartu pada posisi 50 tersebut adalah 28. Kartu dengan nilai 28 adalah dua hati. karena melebihi 26, maka nilainya dikurangi 26 menjadi 2. Sehingga hasilnya adalah
   Nilai keluaran = 2
   Kartu keluaran = dua As

Setelah Sembilan kali pembangkitan *keystream* yang dilakukan di atas, maka *keystream* yang didapatkan adalah :

B U D I D A R M A
9 54 10 9 12 28 11 13 2

Dengan *plainteks*

I L H A M M U D D I N,
9 12 8 1 13 13 21 4 4 9 14

ISSN 2745-7966 (Media Online)
Vol 1, No 2, November 2020
Hal 142-151
https://djournals.com/resolusi

Maka penjumlahannya adalah
9 54 10 9 12 28 11 13 2
9 12 8 1 13 13 21 4 4 9 14 + (mod 26)
18 16 18 10 25 15 6 17 6 9 14
Maka *plainteksnya* adalah
R P R J Y O F Q F I N

Untuk proses *deskripsi*, dua langkah yang harus dilakukan sama dengan dua langkah pertama *enkripsi*. Jika pada *enkripsi keystream* dijumlahkan dengan *plainteks*, maka pada *deskripsi chiperteks* dikurangi dengan *keystream*. Untuk contoh di atas, setelah mendapatkan *keystream*.

B U D I D A R M A
9 54 10 9 12 28 11 13 2
Maka *chiperte*knya adalah
R P R J Y O F Q F I N
18 16 18 10 25 15 6 17 6 9 14
Dikurangi dengan *keystream* tersebut. Hasilnya
R P R J Y O F Q F I N
9 54 10 9 12 28 11 13 2 – (mod 26)
9 12 8 1 13 13 21 4 4 9 14
Adalah :
9 12 8 1 13 13 21 4 4 9 14
I L H A M M U D D I N

Dari hasil *deskripsi*, penerima bisa menebak apakah karakter terakhir adalah karakter *padding* atau tidak

4. KESIMPULAN

Berdasarkan hasil penelitian maka dapat disimpulkan bahwa algoritma *pontifex* dapat mengamankan pesan dengan aman sampai pada tujuan saat pengiriman pesan. Informasi yang dikirimkan tidak dapat disadap atau dibaca oleh pihak lain tanpa memiliki kunci khusus.

REFERENCES

[1] M.A.Amri, dkk, 2009, "Pontifex Implementation In Quantum Cellular Automata", Journal IEEE Trans. On Computer, Vol. 58, No. 6, pp.721-727.
[2] Ariyus, Dony, 2005, "Kriptografi Keamanan Data Dan Komunikasi". Edisi Pertama. Yogyakarta. Graha Ilmu.
[3] Sadikin, Rifki, 2012, "Kriptografi Untuk Keamanan Jaringan", Penerbit Andi, Yogyakarta.
[4] Ariyus, Dony, 2008, "Computer Security, Andi, Yogyakarta.
[5] https://www.maxmanroe.com/vid/teknologi/pengertian-chatting.html,diakses tanggal 24 April 2018.
[6] https://nisaahaniblog.wordpress.com/2016/07/15/teori-ascii-american-standard-code-for-information-interchange/, diakses tanggal 26 Juni 2018
[7] A.S. Rosa dan Shalahuddin. M, 2013, "Rekayasa Perangkat Lunak Terstruktur", Andi, Yogyakarta.
[8] Aditya, Arif Primananda, 2013, "Dasar-Dasar Pemrograman Database Dekstop Dengan Visual Basic. Net 2008, PT. Elex Media Komputindo, Jakarta.