Plagiarism Checker X Originality Report

Similarity Found: 17%

Date: Thursday, December 13, 2018
Statistics: 481 words Plagiarized / 2905 Total words
Remarks: Low Plagiarism Detected - Your Document needs Optional Improvement.

Jurnal Ilmu Matematika dan Terapan | Desember 2018 | Volume 12 Nomor 2 | Hal. 107 – 116 : https://doi.org/10.30598/vol12iss2pp107-116ar623 | p-ISSN: 1978-7227 | e-ISSN : 2615-3017 107 https://ojs3.unpatti.ac.id/index.php/barekeng/ barekeng.math@yahoo.com | barekeng.jurmath@gmail.com MATRIKS SCORE DAN APLIKASINYA DALAM PENGAMANAN PESAN RAHASIA Berni P. Tomasouw1*, Glevi E. Mado2, E. R.

Persulessy3 1,2,3Jurusan Matematika, Fakultas MIPA, Universitas Pattimura Jln. Ir. M. Putuhena, Kampus Unpatti, Poka-Ambon, 97233, Indonesia email: bptomasouw@gmail.com1* ; madogleviejon@gmail.com2 ; richardelvinus@yahoo.com3 Corresponding Author * Abstrak Pertukaran informasi umum atau informasi rahasia antara dua orang melalui suatu media membuat pengirim informasi dan penerima informasi perlu waspada. Dalam hal ini, peran penyandian data sangat penting. Salah satu penyandian data yang sering digunakan dan dikenali banyak orang adalah kriptografi.

Kriptografi merupakan teknik untuk menyandikan data melalui proses enkripsi dan proses dekripsi dengan mengunakan kunci tertentu sehingga menghasilkan data baru yang rahasia. Salah satu pengamanan dengan kriptografi adalah pengamanan pesan rahasia menggunakan matriks score. Matriks score didefinisikan sebagai matriks simetris dengan unsur bilangan kompleks dan adalah matriks diagonal.

Kata Kunci: Bilangan kompleks, kriptografi, matriks, matriks score. SCORE MATRIX AND IT ' S APPLICATION IN SECURING SECRET MESSAGE Abstract The exchange of general information or confidential information between two persons through a medium does not guarantee its safety. This makes the sender of information and the recipient of

information needs to be vigilant.

In this case, the role of data encoding is very important. One of the most commonly used and recognized data encryption is cryptography. Cryptography is a technique for encrypting data through the process of encryption and decryption process by using certain keys so as generate new data that is secret. One of the cryptography is the security of secret messages using the Score matrix.

The score matrix is defined as a symmetric matrix with elements of complex number and is a diagonal matrix. Keywords: Complex number, Cryptography, Matrix, Score matrix. 108 Tomasouw, dkk. | Matriks Score dan Aplikasinya Dalam Pengamanan ..... 1. PENDAHULUAN Dalam aljabar, matriks adalah sekumpulan unsur, angka atau variabel yang disusun dalam bentuk persegi atau persegi panjang.

Selanjutnya dikenal beberapa jenis matriks diantaranya matriks baris dan matriks kolom. Suatu matriks baris dapat menjadi matriks kolom atau sebaliknya, apabila matriks tersebut ditransposkan. Transpose matriks didefinisikan sebagai sebuah matriks yang didapatkan dengan cara menukar unsur-unsur baris menjadi unsur-unsur kolom dan sebaliknya.

Dalam sistem bilangan kompleks sering dijumpai bilangan kompleks sekawan (konjugat kompleks). Dua bilangan kompleks disebut sekawan apabila nilai realnya sama dan tanda pada bagian imajinernya berbeda. Dengan mengunakan transpose matriks dan konjugat kompleks, matriks hermite didefinisikan sebagai suatu matriks kompleks dengan hasil transpose konjugatnya adalah dirinya sendiri. Untuk mengenali matriks hermite dapat dilihat dari diagonal utamanya yang merupakan bilangan real dan unsur lainnya adalah bilangan kompleks.

Dalam jaman modern seperti sekarang, sering terjadi pembajakan liar dan transaksi kriminal. Untuk mencegah kerahasiaan data dari seorang pembajak, harus ada pengamanan yang kuat dalam melindungi data tersebut. Salah satu pengamanan yang dapat digunakan adalah pengamanan pesan rahasia menggunakan matriks hermite.

Peneliti ingin membuat suatu pengamanan pesan rahasia dari matriks yang unsurnya merupakan kebalikan dari matriks hermite. Karena berkebalikan dengan matriks hermite maka untuk mengenali matriks tersebut dapat dilihat dari diagonal utamanya yang merupakan bilangan kompleks dan unsur lainnya adalah bilangan real, selanjutnya peneliti menyebut matriks tersebut dengan nama matriks score. Definisi 1.

[1] Bilangan kompleks dapat dituliskan sebagai { } dengan adalah bagian real

dinotasikan dengan dan merupakan bagian imajiner dinotasikan dengan . Jika dan maka dinamakan imajiner murni (pure imaginary). Jika dan maka dan dinamakan imajiner (imaginary unit). Jika maka menjadi bilangan real . Definisi 2. [1] Untuk sebarang bilangan kompleks , konjugat kompleks dari dinotasikan dengan ¯ dan didefinisikan sebagai: ¯ Defenisi 3.

[1] Apabila suatu bilangan kompleks dipandang sebagai suatu vektor, maka panjang vektor tersebut dinamakan modulus dari dan dinotasikan dengan | | . Jadi jika , maka: | | v Definisi 4. [2] Matriks adalah susunan segi empat siku-siku dari bilangan-bilangan. Bilangan-bilangan dalam susunan tersebut disebut entri dalam matriks. Definisi 5.

Matriks identitas adalah matriks persegi yang elemen-elemen di diagonal utamanya bernilai 1 dan elemen-elemen selain diagonal utama bernilai nol. Definisi 6. Diberikan matriks A berukuran maka transpose dari ditulis adalah matriks berukuran yang setiap kolom dari matriks menjadi baris pada matriks . Definisi 7. Diberikan matriks , matriks A dikatakan simetris jika dan hanya jika . Defenisi 8.

[3] Matriks disebut matriks diagonal jika semua unsur di luar diagonal utamanya adalah 0. Definisi 9. Diberikan matriks persegi [ ] dan matriks diagonal maka hasil pergandaan [ ] . Barekeng: Jurnal Ilmu Matematika dan Terapan | Desember 2018 | Volume 12 Nomor 2 | Hal. 49 – 59 109 Definisi 10.

Matriks kompleks adalah matriks yang entri-entrinya berisi bilangan kompleks. Definisi 11. Untuk sebarang matriks kompleks [ ] dimana , didefinisikan: 1. Real dari matriks Z: [ ] [ ] 2. Imajiner dari matriks Z: [ ] [ ] 3. Modulus dari matriks Z: | | [| |] [v] 4. Konjugat dari matriks Z: ¯ [¯ ¯ ¯ ¯] Definisi 12. [4] Diambil . Untuk , dikatakan kongruen dengan modulo jika | dan dituliskan .

Selanjutnya dinamakan sisa dari ketika dibagi oleh Selanjutnya dikatakan hasil dari ketika dibagi oleh jika dan ditulis . Kriptografi (cryptography) berasal dari Bahasa Yunani " cryptós " rty" secret " (rahasia), sdnkn gráphein "ariy writing "(ulsn ad kriptografi brrt secretwriting " lis rahasia) [5].

Ada 4 tujuan kriptografi sebagai berikut: 1) Kerahasiaan (confidentiality), adalah layanan yang ditujukan untuk menjaga agar pesan tidak dapat dibaca oleh pihak-pihak yang tidak berhak. 2) Integritas data (data integrity), adalah layanan yang menjamin bahwa pesan masih asli/utuh atau belum pernah dimanipulasi selama pengiriman. 3) Otentikasi (authentication), adalah layanan yang berhubungan dengan identifikasi, baik mengidentifikasi kebenaran pihak-pihak yang berkomunikasi (user authentication atau entity authentication) maupun mengidentifikasi kebenaran sumber pesan (data origin

authentication).

4) Nirpenyangkalan (non-repudiation), adalah layanan untuk mencegah entitas yang berkomunikasi melakukan penyangkalan, yaitu pengirim pesan menyangkal melakukan pengiriman atau penerima pesan menyangkal telah menerima pesan. Algoritma Kriptografi 1) Algoritma Simetris Algoritma simetris disebut juga algoritma kriptografi konvensional adalah algoritma yang menggunakan kunci untuk proses enkripsi sama dengan kunci untuk proses dekripsi. Gambar 1. Skema Algoritma simetris Plaintext Ciphertext Plaintext Enkripsi Dekripsi Kunci 110 Tomasouw, dkk.

| Matriks Score dan Aplikasinya Dalam Pengamanan ..... 2) Algoritma Asimetris Algoritma Asimetris disebut juga algoritma kunci publik, mengunakan dua jenis kunci, yaitu kunci publik (public key) dan kunci rahasia (secret key). Kunci publik merupakan kunci yang digunakan untuk mengenkripsi pesan. Sedangkan kunci rahasia digunakan untuk mendekripsi pesan. Gambar 2.

Skema Algoritma Asimetris 2. HASIL DAN PEMBAHASAN 2.1 Karakteristik Suatu Matriks Score Definisi 13. Diberikan suatu matriks simetris dengan unsur bilangan kompleks, matriks disebut score jika adalah matriks diagonal. Teorema matriks Score: Suatu matriks kompleks bujur sangkar dikatakan Score jika pernyataan-pernyataan berikut ekuivalen i. ii. [ ] Dengan dan matriks diagonal.

2.2 Pengamanan Pesan Rahasia Mengunakan Matriks Score Dalam pengamanan pesan rahasia mengunakan matriks score peneliti menggunakan 71 karakter yang terdiri dari a-z, A-Z, angka-angka dari 0 - 9 dan 9, karakter tambahan yang terdiri dari spasi . , % ? : + - #.

Secara rinci proses pengamanan pesan rahasia menggunakan matriks score terdiri dari 2 yaitu proses enkripsi dan proses dekripsi. Proses Enkripsi Langkah 1: Konversikan karakter-karakter teks dalam bilangan-bilangan pada 71. a b c d e f g H I j k l m 1 2 3 4 5 6 7 8 9 10 11 12 13 n o p q r s t u v W x y z 14 15 16 17 18 19 20 21 22 23 24 25 26 A B C D E F G H I J K L M 27 28 29 30 31 32 33 34 35 36 37 38 39 N O P Q R S T U V W X Y Z 40 41 42 43 44 45 46 47 48 49 50 51 52 Kunci Publik penerima Kunci Privat penerima Plaintext Ciphertext Plaintext Enkripsi Dekripsi Barekeng: Jurnal Ilmu Matematika dan Terapan | Desember 2018 | Volume 12 Nomor 2 | Hal. 49 – 59 111 1 2 3 4 5 6 7 8 9 0 .

, 53 54 55 56 57 58 59 60 61 62 63 64 65 % ? : + - # 66 67 68 69 70 0 Langkah 2. Pilih matriks score , sebagai matriks penyandi. Langkah 3. Transformasikan matriks score [ ] ke dalam matriks real | ¯ | dimana . Langkah 4. Jika teks dari pesan mempunyai jumlah karakter yang tidak habis dibagi maka tambahkan sejumlah karakter terakhir ( ) agar

jumlah teks habis dibagi , atau jika teks dari pesan mempunyai jumlah karakter maka tambahkan sejumlah karakter terakhir ( ). Selanjutnya jika jumlah karakter habis di bagi maka jumlah karakter adalah n.

Konversikan masing-masing huruf teks tersebut dengan nilai numeriknya. Langkah 5. Kelompokkan semua karakter menjadi sebuah matriks yang berukuran . Susunlah karakter-karakter tersebut secara berurutan dimulai dari kolom pertama. Langkah 6. Bentuk perkalian kemudian hitung dan . Selanjutnya hitung dan . Langkah 7. Susun elemen-elemen pada matriks , dan secara selang seling atau .

Selanjutnya konversikan masing-masing nilai numerik menjadi karakternya yang setara selain . Proses Dekripsi: Langkah 1. Transformasikan matriks Score [ ] ke dalam matriks real | ¯ | dengan , selanjutnya hitung . Langkah 2. Berikan nomor pada karakter pesan dari Selanjutnya nomor karakter dimodulo dengan 3. Langkah 3. Bentuk teks yang terdiri dari hasil satu secara berurutan.

Konversikan masing-masing huruf teks tersebut dengan nilai numeriknya. Selanjutnya bentuk matriks yang berukuran . Susunlah karakter-karakter tersebut secara berurutan dimulai dari kolom pertama. Langkah 4. Bentuk teks yang terdiri dari hasil dua secara berurutan. Konversikan masing-masing huruf teks tersebut dengan nilai numeriknya. Selanjutnya bentuk matriks yang berukuran .

Susunlah karakter-karakter tersebut secara berurutan dimulai dari kolom pertama. Langkah 5. Bentuk teks yang terdiri dari hasil nol secara berurutan. Selanjutnya bentuk matriks yang berukuran . Susunlah karakter-karakter tersebut secara berurutan dimulai dari kolom pertama. Langkah 6. Hitung dan . Langkah 7. Hitung . Selanjutnya konversikan angka ke karakternya yang sesuai.

Selanjutnya, contoh berikut ini memperlihatkan bahwa proses pengamanan pesan menggunakan matriks Score dapat mengenkripsi dan mendekripsi pesan rahasia dengan baik. 112 Tomasouw, dkk. | Matriks Score dan Aplikasinya Dalam Pengamanan ..... Contoh kasus: Saat terjadi perang dunia ke-2, setiap negara yang mengambil bagian dalam perang menyusun strategi perang mereka masing-masing agar dapat menang dalam pertempuran tersebut. Salah satunya Inggris. Negara tersebut memasang bom pada daerah perbatasan yang adalah daerah pertempuran Inggris dengan lawannya.

Namun para prajurit tidak mengetahui besar daya ledak dari bom tersebut agar mereka dapat menghindar, sehingga panglima mereka mengirimkan pesan besar daya ledak dari bom tersebut yai: , M ari p usat o” . Pesan ini tidak boleh diketahui oleh lawan

perang mereka sehingga panglima membuat pesan rahasia dari pesan tersebut. Penyelesaian: Untuk membuat pesan yang dikirim tidak diketahui oleh musuh maka panglima melakukan proses enkripsi. Proses Enkripsi Langkah 1.

Konversikan karakter-karakter teks dalam bilangan-bilangan pada 71. 7 , 5 K M d a R i p u s a t b o m 59 65 57 63 39 37 63 4 1 18 9 63 16 21 19 1 20 63 2 15 13 Langkah 2. Pilih matriks score , sebagai matriks penyandi. Pilih matriks Score [ ] Langkah 3.

Transformasikan matriks score [ ] ke dalam matriks real | ¯ | Karena [ ] maka ¯ [ ] | ¯ | | [ ] [ ] | | [ ] | | [ ] | [v v v v v v v v v] [ ] Langkah 4. Karena jumlah karakter adalah 21 dan =3 dan 21 habis dibagi 3 maka n=21 7 , 5 K M d a r i p u s a t b O m 59 65 57 63 37 39 63 4 1 18 9 63 16 21 19 1 20 63 2 15 13 Langkah 5. Bentuk matriks Barekeng: Jurnal Ilmu Matematika dan Terapan | Desember 2018 | Volume 12 Nomor 2 | Hal. 49 – 59 113 [ ] Langkah 6.

Bentuk perkalian kemudian hitung dan . Selanjutnya hitung dan . [ ] [ ] [ ] [ ] [ ] [ ] [ ] [ ] [ ] [ ] [ ] [ ] Langkah 7. Susun elemen-elemen pada matriks , dan dan konversikan masing-masing nilai numerik menjadi karakternya yang setara. 50 4 0 12 2 0 65 7 0 64 10 0 33 15 0 28 6 0 69 7 0 114 Tomasouw, dkk. | Matriks Score dan Aplikasinya Dalam Pengamanan ..... X d 0 L b 0 , g 0 .

j 0 G o 0 B f 0 + g 0 50 14 0 56 14 0 35 15 0 36 18 0 55 13 0 70 10 0 50 16 0 X n 0 4 n 0 I o 0 J r 0 3 m 0 - j 0 X p 0 39 9 0 37 7 0 18 10 0 34 16 0 0 8 0 29 7 0 8 10 0 M i 0 K g 0 R j 0 H p 0 # h 0 C g 0 h j 0 Jadi pesan yang dikirim panglima adalah Xd0Ib0,g0.j0Go0Bf0+g0Xn04n0Io0Jr03m0 -j0Xp0Mi0Kg0rj0Hp0#h0Cg0hj0 Untuk mengetahui pesan tersebut maka para prajurit harus melakukan proses d ekripsi. Proses Dekripsi Langkah 1.

Transformasikan matriks Score [ ] ke dalam matriks real | ¯ | dan hitung . Karena [ ] maka ¯ [ ] | ¯ | | [ ] [ ] | | [ ] | | [ ] | [v v v v v v v v v] [ ] [ ] [ ] Langkah 2. No 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 Karakter X d 0 I b 0 , g 0 .

j 0 G o 0 B f 0 Mod 3 1 2 0 1 2 0 1 2 0 1 2 0 1 2 0 1 2 0 No 19 20 21 22 23 24 25 26 27 28 29 30 31 32 33 34 35 36 Karakter + g 0 X n 0 4 n 0 I o 0 J r 0 3 m 0 Mod 3 1 2 0 1 2 0 1 2 0 1 2 0 1 2 0 1 2 0 No 37 38 39 40 41 42 43 44 45 46 47 48 49 50 51 52 53 54 Karakter - j 0 X p 0 M i 0 K g 0 r j 0 H p 0 Mod 3 1 2 0 1 2 0 1 2 0 1 2 0 1 2 0 1 2 0 Barekeng: Jurnal Ilmu Matematika dan Terapan | Desember 2018 | Volume 12 Nomor 2 | Hal.

49 – 59 115 No 55 56 57 58 59 60 61 62 63 Karakter # h 0 C g 0 h j 0 Mod 3 1 2 0 1 2 0 1 2 0 Jadi . Langkah 3. Bentuk matriks yang berukuran . Susunlah karakter-karakter

tersebut secara berurutan dimulai dari kolom pertama. Tedgan sil atu I,G+XIJ - X#h" . X I , . G B + X 4 I J 3 - X M K r H # C h 50 12 65 64 33 28 69 50 56 35 36 55 70 50 39 37 18 34 0 29 8 [ ] Langkah 4. Bentuk matriks yang berukuran .

Susunlah karakter-karakter tersebut secara berurutan dimulai dari kolom pertama. Tedgan sil ua bfnojph . d b g j o f g n n o r m j p i g j p h g j 4 2 7 10 15 6 7 14 14 15 18 13 10 16 9 7 10 16 8 7 10 [ ] Langkah 5. Bentuk matriks yang berukuran . Susunlah karakter-karakter tersebut secara berurutan dimulai dari kolom pertama. Tedan il I 0000000000" .

0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 [ ] Langkah 6. Hitung dan . [ ] [ ] [ ] 116 Tomasouw, dkk. | Matriks Score dan Aplikasinya Dalam Pengamanan .... [ ] [ ] [ ] [ ] [ ] Langkah 7. Hitung . Selanjutnya konversikan angka ke karakternya yang sesuai. [ ] [ ] [ ] 7 , 5 K M d a r i p u s a t b o m 59 65 57 63 37 39 63 4 1 18 9 63 16 21 19 1 20 63 2 15 13 Ji esan ng i rimopa rajadh 75Kari usat o" . 3.

KESIMPULAN Karakteristik suatu matriks score adalah suatu matriks kompleks dengan hasil transposnya adalah dirinya sendiri, dan jika bagian real dari matriks tersebut digandakan dengan bagian imajinernya maka menghasilkan matriks real yang berbentuk [( ) ( )] dengan syarat bagian imajinernya adalah matriks diagonal. Dalam penelitian ini, telah dibuat langkah-langkah pengamanan pesan menggunakan matriks Score.

Dari contoh yang diberikan juga terlihat bahwa proses pengamanan pesan menggunakan matriks Score dapat mengenkripsi dan mendekripsi pesan rahasia dengan baik. Daftar Pustaka [1] A. Lubab, Fungsi Kompleks, Surabaya: IAIN Press, 2015. [2] A. Howard, Aljabar Linier, Jakarta: Erlangga, 1992. [3] D. W. Gere, Aljabar Matriks Untuk Para Insinyur, Jakarta: Erlangga, 1987. [4] D. B. Nugroho, Diktat Kuliah Teori Bilangan, Salatiga, 2009. [5] R.

Munir, Kriptografi, Bandung: Informatika, 2006.

INTERNET SOURCES:

0% - Empty
0% - http://repository.unpas.ac.id/28111/5/BA
0% - https://ardin2016.wordpress.com/category
0% - http://helmishare.blogspot.com/2007/12/s
1% - http://lib.unnes.ac.id/3094/1/6576.pdf
0% - http://digilib.unila.ac.id/30620/2/SKRIP

0% - http://www.engpaper.net/steganography-pa
0% - http://home.snu.edu/~jsmith/library/body
0% - https://www.owasp.org/index.php/Guide_to
0% - https://patents.google.com/patent/US7278
0% - https://www.scribd.com/document/16794790
0% - https://stattrek.com/statistics/dictiona
0% - https://sites.google.com/site/statistiku
0% - http://ppg.spada.ristekdikti.go.id/cours
0% - https://www.slideshare.net/AryaDNingrat1
0% - http://elisa.ugm.ac.id/user/archive/down
1% - https://thebookee.net/pe/pembuktian-sifa
0% - https://www.scribd.com/document/26223637
0% - http://ngadiyonopendmtk.blogspot.com/201
0% - http://rumus-matematika.com/berkenalan-d
0% - http://download.portalgaruda.org/article
1% - https://www.scribd.com/doc/303795217/3-B
0% - http://www.academia.edu/32349462/ALJABAR
1% - http://repository.usu.ac.id/bitstream/ha
0% - http://kaamingsun.blogspot.com/2016/10/m
0% - http://rahadiandimas.staff.uns.ac.id/fil
0% - https://www.scribd.com/document/39386665
0% - http://wikimatematika.blogspot.com/2016/
0% - http://www.pustaka.ut.ac.id/lib/wp-conte
0% - http://download.portalgaruda.org/article
1% - http://repository.usu.ac.id/bitstream/ha
1% - http://repository.usu.ac.id/bitstream/ha
1% - http://informatika.stei.itb.ac.id/~rinal
1% - http://fakhri010595.blogspot.com/
2% - http://download.portalgaruda.org/article
2% - http://download.portalgaruda.org/article
0% - https://bukittinggimedia.wordpress.com/2
0% - https://www.scribd.com/document/37898608
0% - http://jasa-pembuatan-tesis-informatika.
1% - http://repository.usu.ac.id/bitstream/ha
1% - http://informatika.stei.itb.ac.id/~rinal
0% - https://docplayer.info/47678369-Simposiu
0% - http://www.academia.edu/30454309/Aljabar
0% - https://ellanatriah.wordpress.com/
0% - http://contoh-contohskripsi.blogspot.com
0% - http://timurbelambangan.blogspot.com/201

0% - https://www.slideshare.net/msyani/implem
0% - http://www.academia.edu/5626010/Kriptogr
0% - https://www.bing.com/aclick?ld=d3t21b5sS
0% - http://ekladata.com/pmev.eklablog.com/pe
0% - http://analgokenkinanti.blogspot.com/
0% - https://kardorajagukguk.wordpress.com/ev
0% - http://williamcolter.blogspot.com/2010/0
0% - http://repository.gunadarma.ac.id/309/1/
0% - http://www.academia.edu/13450305/modul_a
0% - https://es.scribd.com/doc/269779194/Kela
0% - https://www.animenoem.com/2018/01/anime-
0% - https://www.scribd.com/doc/182587215/kri
0% - http://www.mhhe.com/math/devmath/streete
0% - http://nuremberg.law.harvard.edu/documen
0% - https://www.scribd.com/document/35799157
0% - https://www.scribd.com/document/37394981
0% - https://pt.scribd.com/document/188809785
0% - http://contoh-contohskripsi.blogspot.com
0% - http://ojs.amikom.ac.id/index.php/semnas