



Plagiarism Checker X Originality Report

Similarity Found: 26%

Date: Monday, May 27, 2019

Statistics: 629 words Plagiarized / 2105 Total words

Remarks: Medium Plagiarism Detected - Your Document needs Selective Improvement.

Implementasi Algoritma Modular Multiplication Based Block Cipher dalam mengamankan Data Teks Feri Anita STMIK Budi Darma Medan, Jl. SM.Raja No.338 Sp.Limun Medan, Sumut, Indonesia E-Mail : ferianita@gmail.com ABSTRACT Securing text data is very necessary to secure a data so that it is not stolen by irresponsible parties. Cryptography is one technique that can be used to secure data, namely by encoding the original data that is understood to be incomprehensible data.

Cryptography is one way that is used to secure a data. Cryptography has several algorithms, one of which is a modular multiplication based block cipher algorithm which is one of the classic cryptographic algorithms that uses substitution in encoding data.

Modular multiplication based block ciphers use 128-bit keys and an iterative algorithm consisting of linear steps (such as XOR and key applications) and parallel applications of four non-linear substitutions that can be reversed. Keywords: Cryptography, Implementation, Modular Multiplication based block cipher

PENDAHULUAN Pengiriman dan penyimpanan data atau pesan melalui media elektronik sudah banyak dilakukan. Terkadang perlakuan terhadap data digital tersebut perlu dirahasiakan untuk menjamin keamanan dan keutuhan data atau pesan yang dikirimkan.

Dengan demikian setiap orang yang bermaksud menyimpan sesuatu secara pribadi dan rahasia akan melakukan segala cara untuk menyimpan data atau pesan tersebut agar orang lain tidak tahu. Modular multiplication based block cipher merupakan salah satu algoritma kriptografi klasik, yang menggunakan substitusi dalam proses enkripsinya. Substitusi ditentukan oleh sebuah operasi perkalian modulo $2^{32}-1$ dengan faktor konstan.

Berdasarkan cara memproses teks (plaintext), MMB (Modular Multiplication based Blok cipher) bekerja dengan menggunakan plaintext 128 bit dan algoritma iteratif yang terdiri dari langkah-langkah linier (seperti XOR dan aplikasi kunci) serta aplikasi paralel dari empat substitusi non linier yang bisa dibalik [1]. Berdasarkan uraian latar belakang di atas, maka penulis merumuskan masalah sebagai berikut :1).

Bagaimana menerapkan proses enkripsi dan dekripsi menggunakan algoritma modular multiplication based block cipher pada data teks?, 2) Bagaimana menguji proses algoritma modular multiplication-based blok cipher dalam pengamanan data teks menggunakan program aplikasi Matlab? Perumusan masalah di atas agar dapat lebih jelas, terdapat batasan-batasan masalah yang akan dibahas lebih khusus yang hanya difokuskan pada: 1). Panjang kunci yang digunakan adalah 128 bit., 2).

Pengujian proses enkripsi dan dekripsi menggunakan program aplikasi Matlab. Adapun manfaat dari penelitian ini adalah: Memahami proses enkripsi dan dekripsi dalam pengamanan data teks dan Mempersulit para hacker untuk mencuri atau mengetahui data rahasia. LANDASAN TEORI 2.1

Implementasi Implementasi adalah kegiatan akhir dari proses penerapan sistem baru dimana sistem yang baru akan dioperasikan secara menyeluruh. Implementasi bertujuan untuk melakukan proses penerapan sistem yang baru. Berdasarkan pengertian tersebut dapat disimpulkan bahwa implementasi merupakan tindakan yang dilakukan untuk melaksanakan atau merealisasikan program-program yang telah disusun demi tercapainya tujuan dari kebijakan atau program-program yang telah direncanakan [2].
2.2

Algoritma Algoritma adalah urutan langkah yang logis untuk menyelesaikan masalah tertentu [2]. Yang ditekankan adalah urutan langkah logis, yang berarti algoritma harus mengikuti suatu urutan tertentu, tidak boleh melompat-lompat. Secara definisi,

algoritma adalah alur pemikiran logis yang dapat dituangkan ke dalam bentuk tulisan.

Yang ditekankan pertama adalah alur pikiran, sehingga algoritma seseorang dapat berbeda dengan algoritma orang lain. Sedangkan penekanan kedua adalah tertulis, yang berarti dapat berupa kalimat, gambar atau tabel tertentu [3]. Algoritma adalah deretan instruksi yang jelas untuk memecahkan masalah, yaitu untuk memperoleh keluaran yang diinginkan dari suatu masukan dalam jumlah waktu yang terbatas [4].

2.3 Kriptografi

Kriptografi berasal dari bahasa Yunani, *crypto* dan *graphia*. *Crypto* berarti *secret* (rahasia) dan *graphia* berarti *writing* (tulisan).

Menurut terminologinya, kriptografi adalah ilmu dan seni untuk menjaga keamanan pesan ketika pesan dikirim dari suatu tempat ke tempat lain [4]. Adapun tujuan kriptografi adalah untuk memberi layanan keamanan (aspek-aspek keamanan) sebagai berikut:

1. Authentication Penerima informasi dapat memastikan keaslian pesan, bahwa pesan itu datang dari orang yang dimintai informasi.

2. Integrity Dengan kata lain, informasi itu benar-benar datang dari orang yang dikehendaki. Keaslian pesan yang dikirim melalui jaringan dan dapat dipastikan bahwa informasi yang dikirim tidak dimodifikasi oleh orang yang tidak berhak.

3. Non-repudation Merupakan hal yang berhubungan dengan si pengirim. Pengirim tidak dapat mengelak bahwa dialah yang mengirim informasi tersebut.

4. Confidentiality Merupakan usaha untuk menjaga informasi dari orang yang tidak berhak mengakses. Kerahasiaan ini biasanya berhubungan dengan informasi yang diberikan ke pihak lain.

2.4. Algoritma Modular Multiplication Based Blok Cipher

Kelemahan metode IDEA yang menggunakan plaintext 64 bit dan operasi perkalian modulo $2^{16} + 1$, diperbaiki oleh Joan Daemen dalam sebuah algoritma yang dinamakan MMB (Modular Multiplication-based Block cipher).

Dengan menggunakan plaintext 64 bit (4 buah 16 bit subblock text), metode IDEA hanya dapat diimplementasikan pada prosesor 16 bit, sehingga dinilai tidak dapat mengikuti perkembangan teknologi pada saat ini yang kebanyakan telah menggunakan prosesor 32 bit. Kriptografi metode MMB menggunakan plaintext 128 bit dan algoritma iteratif yang terdiri dari langkah-langkah linier (seperti XOR dan aplikasi kunci) serta aplikasi paralel dari empat substitusi non linier besar yang dapat dibalik [7].

Substitusi ini ditentukan oleh sebuah operasi perkalian modulo $2^{32} - 1$ dengan faktor konstan, yang memiliki tingkat sekuritas lebih tinggi bila dibandingkan dengan metode IDEA 16 yang hanya menggunakan operasi perkalian modulo $2^{16} + 1$. MMB menggunakan 32 bit subblock text (x_0, x_1, x_2, x_3) dan 32 bit subblock kunci (k_0, k_1, k_2, k_3).

Hal ini membuat algoritma tersebut sangat cocok diimplementasikan pada prosesor 32 bit. Sebuah fungsi non linier, f , diterapkan enam kali bersama dengan fungsi XOR. PEMBAHASAN 3.1 Analisa Kriptografi algoritma Modular Multiplication Based Block Cipher menggunakan algoritma iterative yang terdiri dari langkah-langkah linier (seperti XOR dan aplikasi kunci) serta aplikasi paralel dari empat substitusi non linier besar yang ditentukan oleh sebuah modulo $2^{32} - 1$ yaitu nilai sisa hasil bagi dengan hasil perpangkatan 232 dikurang 1. Hal ini menyebabkan tingkat keamanan dari algoritma MMB menjadi lebih tinggi dan sulit untuk dipecahkan.

Sama seperti algoritma kriptografi simetris lainnya, proses penyelesaian metode MMB ini dapat dibagi menjadi 3 tahapan, yaitu: Proses pembentukan kunci Proses enkripsi Proses dekripsi 3.1.1 Proses Pembentukan Kunci Metode MMB ini memiliki input 128 bit kunci (key) yang identik dengan 32 digit heksadesimal ataupun 16 karakter yang akan dipecah menjadi 4 buah sub kunci (subkey) dengan panjang masing-masing sub kunci adalah sebesar 32 bit.

Untuk lebih memahami proses pembentukan kunci pada metode MMB, diberikan sebuah contoh berikut ini: Kunci = FERI_ANITA_ABCDE Maka proses pembentukan kuncinya adalah sebagai berikut: Ubah terlebih dahulu kunci ke dalam bentuk biner = 0100011001000101010100100100000101011111010000010100111001001001010101000100000101011111010000010100010010000101010001000001010111110100000101000010010000110100010001000101 Dipecah menjadi 4 buah sub kunci: $K_0 = 01000110010001010101001001000001$ $K_1 = 01011111010000010100111001001001$ $K_2 = 01010100010000010101111101000001$ $K_3 = 01000010010000110100010001000101$ 3.1.2 Proses Enkripsi Proses enkripsi dari algoritma MMB ini memiliki input data plainteks 128 bit yang identik dengan 12 digit heksadesimal atau 16 karakter.

Proses enkripsi metode MMB memiliki langkah-langkah sebagai berikut: Plainteks dibagi menjadi 4 buah plainteks masing-masing berukuran 32 bit. Melakukan operasi XOR antara plainteks dengan sub kunci yang pertama (K_0).. Kemudian gunakan fungsi f terhadap hasil operasi XOR. Melakukan operasi XOR antara plainteks dengan sub kunci yang kedua (K_1), kemudian gunakan fungsi f terhadap hasil operasi XOR.

Melakukan operasi XOR antara plainteks dengan sub kunci yang ketiga (K_2), kemudian gunakan fungsi f terhadap hasil operasi XOR. Melakukan operasi XOR antara plainteks dengan sub kunci yang keempat (K_3), kemudian gunakan fungsi f terhadap hasil operasi XOR. Lakukan kembali langkah 2 sampai 5 sebanyak satu kali. Gabungkan keempat plainteks sehingga mendapatkan cipherteks.

Fungsi f yang digunakan adalah sebagai berikut: Mengalikan hasil XOR plainteks dan kunci dengan konstanta yang sudah ditentukan kemudian di-Mod-kan dengan $2^{32} - 1$. Konstanta yang sudah ditentukan adalah sebagai berikut: $C = (2AAAAAAA)_{16}$ $C_0 = (025F1CDB)_{16}$ $C_1 = 2 * c_0$ $C_2 = 23 * c_0$ $C_3 = 27 * c_0$ Setelah mendapatkan hasil perkalian, kemudian dicari **least significant bit (LSB)** dari x_0 , jika LSB dari $x_0 = 1$, maka x_0 di XOR kan dengan C jika tidak maka dilihat LSB x_3 , jika LSB $x_3 = 0$ maka x_3 di XOR kan dengan C , jika tidak maka $x_i = x_{i-1} XOR x_i XOR x_{i+1}$. 3.1.3

Proses Dekripsi Algoritma **yang digunakan pada proses** dekripsi agak sedikit berbeda dengan proses enkripsi. Inti proses dekripsi dari metode MMB dapat dijabarkan seperti berikut : Cipherteks dibagi menjadi 4 subblock yang sama besar (P_0, \dots, P_3). **Melakukan operasi XOR antara cipherteks dengan kunci yang** keempat (K_3), kemudian gunakan fungsi f .

Melakukan operasi XOR antara **cipherteks dengan kunci yang** ketiga (K_2), kemudian gunakan fungsi f . **Melakukan operasi XOR antara cipherteks dengan kunci yang** kedua (K_1), kemudian gunakan fungsi f . **Melakukan operasi XOR antara cipherteks dengan kunci yang** pertama (K_1), kemudian gunakan fungsi f . Ulangi langkah 2 sampai 5 sebanyak satu kali.

Gabungkan 4 subblock sehingga didapatkan plainteks. Fungsi f yang digunakan dalam dekripsi berbeda dengan yang digunakan dalam dekripsi, yaitu sebagai berikut: Melakukan operasi XOR dengan ketentuan sebagai berikut: $X_i = X_{i-1} XOR X_i XOR X_{i+1}$.

Setelah mendapatkan hasil operasi XOR, kemudian dicari **least significant bit (LSB)** dari x_0 , jika LSB dari $x_0 = 1$, maka x_0 di XOR kan dengan C jika tidak maka dilihat LSB x_3 , jika LSB $x_3 = 0$ maka x_3 di XOR kan dengan C , jika tidak maka $X_i = C_i * X_i$. Setelah menganalisa bagaimana **proses enkripsi dan dekripsi** dengan menggunakan algoritma Modular Multiplication Based Cipher Block, maka pembahasannya dapat dilihat dalam contoh berikut ini: Plaintext = AYO_KITA_NGAMPUS Kunci = FERI_ANITA_ABCDE
Pembentukan kunci Ubah kunci ke dalam bentuk biner:
010001100100010101010010010010010101111101000001010011100100100101010100
0100000101011111010000010100001001000011010001000100 0101 Bagi kunci menjadi 4 buah subkey: $K_0 = 01000110010001010101001001001001$ $K_1 = 01011111010000010100111001001001$ $K_2 = 01010100010000010101111101000001$ $K_3 = 01000010010000110100010001000101$ Proses enkripsi Ubah plainteks ke dalam bentuk biner Bagi menjadi 4 subblock: $P_0 = 01000001010010010100111101011111$ $P_1 = 01001011010010010100010001000001$ $P_2 = 01001111010011100100011101000001$ $P_3 = 01001101010000000101010101010011$ Meng-xor-kan plainteks dengan K_0 $X_0 = P_0 _ K_0 = 01000001010010010100111101011111$

01000110010001010101001001001001 _ 00000111000011000001110100011110 X1 =
 P1 _ K0 = 01001011010010010100010001000001
 01000110010001010101001001001001 _ 00001101000011000001011000000000 X2 =
 P2 _ K0 = 01001111010011100100011101000001
 01000110010001010101001001001001 _ 00001001000010110001010100000000 X3 =
 P3 _ K0 = 01001101010000000101010101010011
 01000110010001010101001001001001 _ 00001011000001010000011100010010
 Gabungkan X0, X1, X2, X3 dan konversi ke dalam bentuk karakter dan menghasilkan cipherteks.

Hasil:

010010110101000110110100110011000111011111111000101110100001010010100111
 01111111110111001101100001010010101001101011000011110100 Dalam bentuk
 karakter: KQ'lwø'süØR!°ô ALGORITMA DAN IMPLEMENTASI 4.1. Algoritma
 Pembentukan Kunci Proses pembentukan kunci pada metode MMB sangat sederhana.
 Prosedur kerja dari algoritma ini dapat dijabarkan seperti berikut : Input : K (Kunci
 Output : K0, K1, K2, K3 (Kunci setelah diekspansi Proses : K/4 K0 = K [0] K1 = K [1] K2 =
 K [2] K3 = K [3] 4.2.

Algoritma Enkripsi Modular Multiplication Based Block Cipher Prosedur kerja dari proses
 enkripsi ini dapat dijabarkan menjadi dua bagian besar yaitu : Input : K (Kunci P (Plainteks
 Output : C (Cipherteks Proses : Mulai P/4 = P0, P1, P2, P3 For j = 1 to 2 For i =
 0 to 3 Pi = Pi XOR Ki F(P0, P1, P2, P3) Next i For i = 0 to 3 Pi = Pi XOR Ki+1 F(P0, P1, P2,
 P3) Next i For i = 0 to 3 Pi = Pi XOR Ki+2 F(P0, P1, P2, P3) Next i Next j Selesai 4.3.

Algoritma Enkripsi Modular Multiplication Based Block Cipher Prosedur kerja dari proses
 dekripsi ini dapat dijabarkan menjadi dua bagian besar yaitu : Input : K (Kunci C (Cipherteks
 Output : P (Plainteks Proses : Mulai C/4 = C0, C1, C2, C3 For j = 1 to 2 For i =
 0 to 3 Xi = Ci XOR Ki+2 F(C0, C1, C2, C3) Next i For i = 0 to 3 Ci = Ci XOR Ki+1 F(C0, C1,
 C2, C3) Next i For i = 0 to 3 Ci = Ci XOR Ki F(C0, C1, C2, C3) Next i Next j Selesai 4.2.

Implementasi Pengujian terhadap algoritma modular multiplication based block cipher
 dengan menggunakan aplikasi program Matlab 6.1 dilakukan untuk mengetahui apakah
 algoritma dapat mengenkripsi atau mengamankan suatu data teks [6][8]. Berikut adalah
 hasil dari pengujian yang dilakukan. Pada gambar berikut dilakukan pengujian dengan
 masukan plainteks AYO_KITA_NGAMPUS dan kunci FERI_ANITA_ABCDE, kemudian
 didapatkan hasil enkripsi atau cipherteks KQ'lwø'süØR!°ô. _ Gambar 1 Hasil pengujian
 pertama KESIMPULAN Berdasarkan pembahasan sebelumnya, maka dapat diambil
 kesimpulan-kesimpulan.

Adapun kesimpulan-kesimpulan tersebut adalah sebagai berikut: Algoritma modular multiplication based block cipher mengenkripsi data menggunakan algoritma iteratif yang terdiri dari langkah-langkah linier (seperti XOR dan aplikasi kunci) serta aplikasi parallel dari empat substitusi non linier. Pengujian algoritma modular multiplication based block cipher dilakukan dengan menggunakan program aplikasi Matlab 6.1

dengan memasukkan data teks serta kunci kemudian akan diproses dengan sebuah tombol enkripsi yang telah disisipi algoritma tersebut. DAFTAR PUSTAKA Mukhlisulfatih Latief. (2010). Studi perbandingan Enkripsi Menggunakan Algoritma IDEA dan MMB Suarga. (2006). Algoritma dan Pemrograman. Yogyakarta: Penerbit Andi. Ariyus, Dony. (2008). Pengantar Ilmu Kriptografi Teori Analisis dan Implementasi. Yogyakarta: Penerbit Andi. Munir, Rinaldi. (2006). Kriptografi.

Bandung: Informatika Bandung. Munir, Rinaldi. (2011). Algoritma dan Pemrograman. Bandung: Informatika Bandung. Nugroho, Adi. (2010). Rekayasa Perangkat Lunak Berorientasi Objek dengan Metode USDP. Yogyakarta: Penerbit Andi. Rachmat C, Antonius. (2010). Algoritma dan Pemrograman dengan Bahasa C-Konsep, Teori & Implementasi. Yogyakarta: Penerbit Andi. Sadikin, Rifki. (2010).

Kriptografi untuk Keamanan Jaringan dan Implementasinya dalam Bahasa Java. Yogyakarta: Penerbit Andi.

INTERNET SOURCES:

<1% - http://ejournal.ust.ac.id/index.php/Jurnal_Means/article/view/277

<1% -

https://www.researchgate.net/publication/283042210_A_New_Modified_Caesar_Cipher_Cryptography_Method_with_LegibleCiphertext_From_a_Message_to_Be_Encrypted

<1% -

https://www.academia.edu/29971557/Cryptography_Technique_with_Modular_Multiplication_Block_Cipher_and_Playfair_Cipher

<1% -

<https://contohmakalah4.blogspot.com/2013/02/pretty-good-privacy-untuk-keamanan-e.html>

<1% -

<https://security-komputer.blogspot.com/2009/12/teknik-keamanan-komputerenkripsi.html>

3% - <http://core.ac.uk/display/35377608>

1% -

<http://repository.usu.ac.id/bitstream/handle/123456789/55583/Chapter%20II.pdf;sequen>

ce=4

1% - <http://scholar.unand.ac.id/24647/2/BAB%20I%20%28PENDAHULUAN%29.pdf>

<1% -

<http://repository.usu.ac.id/bitstream/handle/123456789/55583/Chapter%20I.pdf;sequence=5>

ce=5

<1% -

<https://saepudinonline.wordpress.com/2010/11/30/hukum-digital-signature-tanda-tangan-elektronik/>

<1% -

https://www.academia.edu/6952425/PENGUJIAN_SISTEM_ENKRIPSI-DEKRIPSI_DENGAN_METODE_RSA_UNTUK_PENGAMANAN_DOKUMEN

<1% -

https://www.researchgate.net/publication/228538128_Keamanan_Sistem_Informasi_Berbasis_Internet

1% -

<https://id.123dok.com/document/zglll58q-bab-ii-tinjauan-pustaka-2-1-landasan-teori-2-1-1-laporan-keuangan-bab-ii-ari-waryati-akuntansi-13.html>

1% - <https://dittadiean.blogspot.com/2015/01/laporan-kerja-praktek-pkl.html>

2% -

<https://percobaanfahmi.blogspot.com/2016/02/implementasi-algoritmaknuth-morris.html>

<1% - <https://slideplayer.info/slide/2378387/>

1% - <https://hanifsaeful.wordpress.com/2011/11/12/algoritma-pemrograman-dasar/>

1% -

https://www.researchgate.net/profile/Antonius_Rachmat/publication/263820517_Algoritma_dan_Pemrograman_dengan_Bahasa_C_Konsep_Teori_dan_Implementasi/links/5829b0d908ae825cda7efc07/Algoritma-dan-Pemrograman-dengan-Bahasa-C-Konsep-Teori-dan-Implementasi.pdf

1% - <https://kadry-teknoblogspot.com/2011/05/algoritma-adalah.html>

1% - <https://kuliahmsi.blogspot.com/2010/07/dasar-dasar-algoritma.html>

1% -

<https://belajarplog.blogspot.com/2011/12/apakah-algoritma-dan-pemrograman-itu.html>

1% -

<https://docplayer.info/33569953-Implementasi-kriptografi-dan-steganografi-menggunakan-algoritma-rsa-dan-metode-lsb.html>

1% - <https://gerbangteknologi.blogspot.com/2011/03/pengertian-md5-dan-sha.html>

<1% -

<http://repository.usu.ac.id/bitstream/handle/123456789/40881/Chapter%20II.pdf?sequence=4&isAllowed=y>

1% -
https://www.academia.edu/11926458/Sniffing_dan_Spoofing_Pada_Aspek_Keamanan_Komputer

1% - <https://azdythahawi.blogspot.com/2011/12/kisah-inspirasi-hikayat-abu-nawas.html>

1% -
<https://indrahardiansyahiss.blogspot.com/2013/10/jenis-jenis-keamanan-sistem-informasi.html>

1% -
<https://boediedoeloeonenine.blogspot.com/2012/09/v-behaviorurldefaultvmlo.html>

1% -
<https://safniagustina.blogspot.com/2017/01/skema-keamanan-jaringan-network.html>

5% - <https://core.ac.uk/download/pdf/11511010.pdf>

1% - http://eprints.dinus.ac.id/11801/1/abstrak_11496.pdf

1% -
<https://docplayer.info/402105-Sistem-pengamanan-pesan-sms-menggunakan-internasional-data-encryption-algorithm.html>

1% - <https://zonaskripsi.blogspot.com/2012/03/skripsi-komputer-2.html>

<1% - <https://desintyapermatasari.blogspot.com/2011/>

<1% -
<https://id.123dok.com/document/9ynd41zv-perancangan-perangkat-lunak-kriptografi-metoda-idea-international-data-encryption-algorithm.html>

<1% - <http://publikasi.dinus.ac.id/index.php/joins/article/download/2190/1391>

2% - <https://vaskoedo.wordpress.com/2010/03/page/2/>

<1% - <https://id.scribd.com/doc/239620105/Naskah-Jurnal-Jitika-Vol7no1-Stmik-Asia>

<1% -
https://www.academia.edu/29722693/IMPLEMENTASI_ALGORITMA_TWOFISH_DENGAN_KEY_128-BIT_UNTUK_ENKRIPSI_DAN_DEKRIPSI_DATA_TEKST_LAPORAN_TUGAS_AKHIR

<1% - <https://benni05530.wordpress.com/2011/01/04/enkripsi-dan-deskripsi/>

1% - <https://vaskoedo.wordpress.com/2010/03/23/pengenalan-kriptografi/>

<1% - <https://vaskoedo.wordpress.com/category/uncategorized/page/21/>

<1% - <https://vaskoedo.wordpress.com/page/27/>

<1% -
https://www.researchgate.net/publication/319881962_A_Novel_Network_Coding_Approach_Packets_Conflict_Based_for_Matrix_Optimization

1% - <https://contohproposaltesis.com/tag/teknik-elektro/page/4/>

<1% -
<http://ana.staff.gunadarma.ac.id/Publications/files/3112/IMPLEMENTASI+ALGORITMA+ADVANCED+ENCRYPTION+STANDARD.pdf>

<1% -
<https://docplayer.info/52322926-Implementasi-algoritma-kriptografi-vigenere-chiper-u>

ntuk-mengamankan-file-text-menggunakan-java-netbean-8-0.html

<1% -

<http://etd.repository.ugm.ac.id/downloadfile/70677/potongan/S2-2014-338768-bibliography.pdf>

<1% - <https://repository.bsi.ac.id/index.php/repo/viewitem/1191>

<1% -

<https://libraryuniku.blogspot.com/2012/02/buku-yang-ada-di-perpustakaan-uniku.html#!>

1% - <https://iopscience.iop.org/article/10.1088/1757-899X/453/1/012018/meta>