Jurnal SAINTIKOM (Jurnal Sains Manajemen Informatika dan Komputer)
Volume 22 ; Nomor 2 ; Agustus 2023; Page 357-363
E-ISSN : 2615-3475; P-ISSN : 1978-6603
https://ojs.trigunadharma.ac.id/index.php/jis/index

Comparison AES and RC4 Algorithm for Secure Data Passed Through an URL

Bagus Ajie Iswara[1], Jeremia Tarigan[2], Sutarman[3], Ade Candra[4]

[1] Program Studi Magister Teknik Informatika, Universitas Sumatera Utara, Medan, Indonesia
[2] Program Studi Magister Teknik Informatika, Universitas Sumatera Utara, Medan, Indonesia
Email: [1] bagusajie@students.usu.ac.id, [2]jeremiatarigan@students.usu.ac.id, [3]sutarman@usu.ac.id , [4]ade_candra@usu.ac.id
Email Penulis Korespondensi: sutarman@usu.ac.id , ade_candra@usu.ac.id

Article History:
Received Jun 12th, 202x
Revised Aug 20th, 202x
Accepted Aug 26th, 202x

Abstrak

Keamanan pada aplikasi berbasis website merupakan hal yang harus diperhatikan, karena hal tersebut menjadi hal penting untuk menghindari terjadinya pencurian data oleh orang yang tidak bertanggung jawab. Salah satu serangan yang terjadi pada aplikasi website adalah serangan SQL Injection. Serangan SQL Injection menjadi ancaman yang terjadi diakibatkan perlindungan yang tidak diberikan pada halaman web. Serangan ini dapat terjadi ketika aplikasi web melakukan proses komunikasi data menggunakan parameter HTTP GET method dan HTTP POST method pada saat sisi klien melakukan proses transfer data dengan sisi server aplikasi web. Dalam paper ini akan membahas masalah keamanan pada aplikasi web tersebut dengan menerapkan solusi untuk membuat keamanan pada proses komunikasi data yaitu dengan menerapkan algoritma kriptografi. Salah satu algoritma kriptografi yang dapat diterapkan adalah Advance Encryption Standard (AES) dan Rivest cipher 4 (RC4).

Kata Kunci : AES, RC4, Kriptografi, HTTP

Abstract

Security in website-based applications is something that must be considered, because it is important to avoid data theft by irresponsible people. One of the attacks that occur on website applications is SQL Injection attacks. SQL Injection attacks are a threat that occurs due to protection that is not provided on web pages. This attack can occur when a web application processes data communication using the HTTP GET method and HTTP POST method parameters while the client side is transferring data to the web application server side. In this paper, we will discuss security issues in these web applications by implementing solutions to create security in the data communication process by implementing cryptographic algorithms. One of the cryptographic algorithms that can be applied is Advance Encryption Standard (AES) and Rivest cipher 4 (RC4).

Keyword : *AES, RC4, Kriptografi, HTTP*

1. PENDAHULUAN

Penggunaan website yang semakin luas, dapat menimbulkan berbagai macam tindak kejahatan seperti pencurian, manipulasi data atau informasi penting dari suatu website oleh orang yang tidak bertanggung jawab. Dalam pemrograman web terdapat dua metode untuk mengirimkan data dari client ke server. Kedua metode tersebut adalah parameter POST method dan parameter GET method. Kebutuhan sebuah website sendiri juga meningkat jumlah website dimana banyak website yang memiliki interface yang bagus namun terkadang banyak pembuat website yang melakukan komponen penting yaitu keamanan. Salah satu jenis serangan pada aplikasi web adalah serangan SQL Injection. Serangan SQL Injection menjadi ancaman yang terjadi diakibatkan perlindungan yang tidak diberikan pada halaman web. Hal tersebut dapat menyebabkan terjadinya pencurian data pada database yang akan membuat data kredensial pengguna dapat dicuri[1]. Serangan SQL Injection terjadi pada saat hacker melakukan penyisipan atau memasukkan kode berbahaya ke dalam aplikasi web melalui celah yang rentan kemudian kode berbahaya tersebut dapat berkomunikasi dengan kueri database[2].

Salah satu celah untuk terjadinya serangan ini ketika aplikasi web melakukan proses komunikasi data menggunakan parameter HTTP GET method dan HTTP POST method pada saat sisi klien melakukan proses transfer data dengan sisi server aplikasi web. Berdasarkan masalah keamanan pada aplikasi web tersebut terdapat solusi untuk membuat

keamanan pada proses komunikasi data yaitu dengan menerapkan algoritma kriptografi. Proses pengamanan proses komunikasi data dengan melakukan proses enkripsi nama dan nilai parameter pada metode GET dan metode POST. Salah satu algoritma kriptografi yang dapat diterapkan adalah Advance Encryption Standard (AES) dan Rivest cipher 4 (RC4)[2], [3].

Algoritma Advanced Encryption Standard (AES) merupakan jenis algoritma kriptografi dengan kunci simetris yang memiliki kunci yang sama untuk melakukan enkripsi dan dekripsi. Cipher yang dihasilkan algoritma AES memiliki ukuran blok 128 bit. AES memiliki panjang kunci berupa 128 bit, 192 bit, atau 256 bit[4].

Algoritma Rivest Cipher 4 (RC4) juga merupakan jenis algortima dengan kunci simetris yang melakukan enkripsi setiap karakter secara satu persatu. Algoritma RC4 memiliki panjang kunci yang bervariasi dari 40 bit – 2048 bit[3].

Sehingga pada paper ini melakukan akan mengimplentasikan kedua algoritma kriptografi ini untuk melakukan enkripsi pada url sebuah website terutama parameter yang dikirim menggunakan method GET atau id dari sebuah baris data ditampilkan begitu saja pada url address. Setelah diimplementasikan peneliti akan melakukan komparasi antara Advance Encryption Standard (AES) dan Rivest cipher 4 (RC4).

2. METODOLOGI PENELITIAN

2.1 Keamanan

Masalah keamanan merupakan salah satu aspek terpenting dari sebuah website. Keamanan jaringan adalah kumpulan peranti yang dirancang untuk melindungi data ketika transmisi terhadap pengaksessan, pengubahan dan penghalangan oleh pihak yang tidak berwenang[5].

2.2 Kriptografi

Kriptografi pada awalnya dijabarkan sebagai ilmu yang mempelajari bagaimana menyembunyikan pesan. Namun pada pengertian modern kriptografi adalah ilmu yang bersandarkan pada teknik matematika untuk berurusan dengan keamanan informasi seperti kerahasiaan, keutuhan, data dan otentikasi entitas. Jadi pengertian kriptografi modern adalah tidak saja berurusan hanya dengan penyembunyian pesan namun lebih pada sekumpulan teknik yang menyediakan keamanan informasi.

Kriptografi dikelompokan menjadi dua diantaranya berdasarkan kunci yang digunakan, yaitu algoritma simetri (mengunakan satu kunci untuk proses enkripsi dan dekripsi), sedangkan Algoritma asimetri (memiliki kunci yang berbeda saat proses enkripsi dan dekripsi serta fungsi. Sedangkan karakteristik kriptografi digolongkan menjadi dua bagian yaitu berdasarkan tipe operasi pada enkripsi dan dekripsi (teknik substitusi dan teknik permutasi) selain itu proses pengolahan pesan berupa block chipher dan stream chipher[5].

Proses enkripsi merupakan proses pengamanan suatu pesan penting dengan cara mengubah plaintext atau pesan asli menjadi ciphertext atau pesan tersembunyi. Sedangkan untuk proses lanjutanya dari proses enkripsi adalah proses dekripsi yang merupakan proses kebalikan dari enkripsi yang mengubah ciphertext menjadi plaintext[3].

2.3 *Uniform Resource Locator* (URL)

URL merupakan bagian dari Uniform Resource Identifiers (URI) yang digunakan untuk mengidentifikasi sebuah alamat sumber. Selain itu URL juga digunakan sebagai sarana untuk menemukan alamat sumber dengan cara mekanisme tertentu [4].

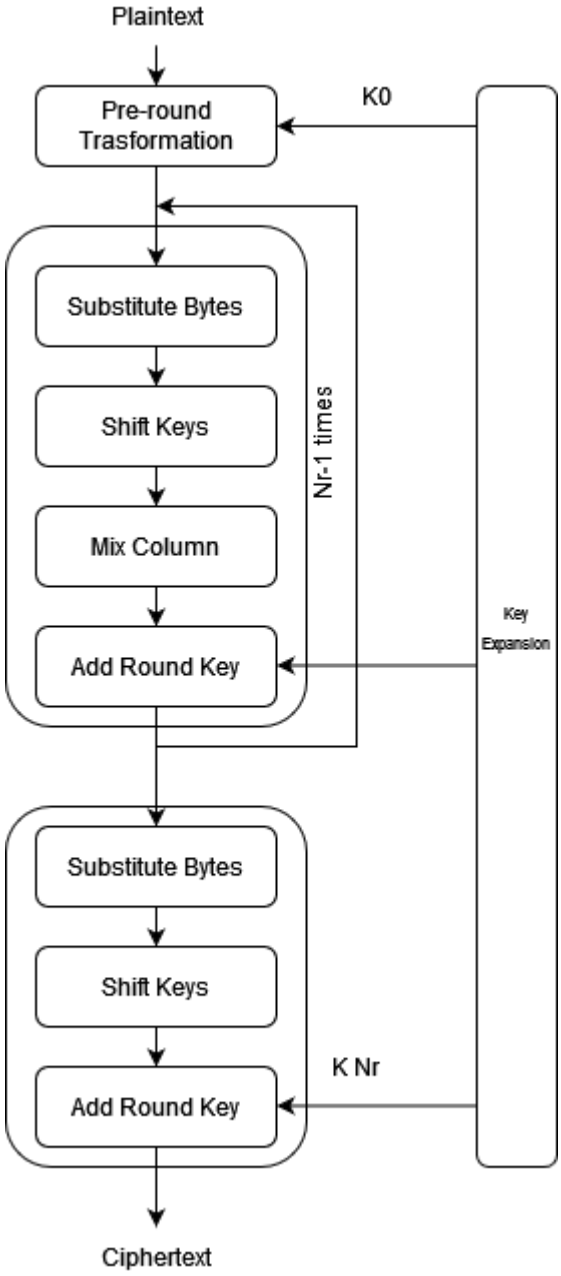
URI = scheme ":" main-domain ["?" query_parameter] ["#" fragment]

Pada sintaks URI umum diatas terdapat beberapa komponen, yang digunakan sebagai indetifikasi sebuah alamat sumber. Pada komponen pertama yaitu schema biasanya dideklarasikan dengan http, https dan ftp. Dan dilanjutkan dengan main-domain yang deklarasikan untuk domain utama pada URL. Komponen query_parameter digunakan untuk mendeklarasikan data yang dikirim dari front-end ke backend. Sedangkan fragmen hanya digunakan secara optional untuk memberikan posisi ke suatu titik pada halaman yang sama.

2.4 *Advance Encryption Standard (AES)*

Algoritma Advance Encryption Standard (AES) ditemukan oleh Rijndael. Algoritma AES merupakan algoritma cipher blok simetris yang prosesnya menggunakan satu kunci yang sama pada saat proses enkripsi dan dekripsinya. AES memiliki ukuran blok 128 bit dan panjang kunci pada AES diantaranya 128 bit, 192 bit dan 256 bit[4]. Dengan panjang ukuran kunci tersebut, Algoritma AES dapat melakukan 10, 12, 14 putaran kunci. Operasi yang dilakukan algoritma ini diantaranya substitute bytes, shift keys, mix column dan add round key. Algoritma AES dikatakan memberikan tingkat keamanan yang baik[3]. Proses enkripsi AES ditunjukkan pada Gambar 1[3].

Jurnal SAINTIKOM (Jurnal Sains Manajemen Informatika dan Komputer)
Volume 22 ; Nomor 2 ; Agustus 2023; Page 357-363
E-ISSN : 2615-3475; P-ISSN : 1978-6603
https://ojs.trigunadharma.ac.id/index.php/jis/index

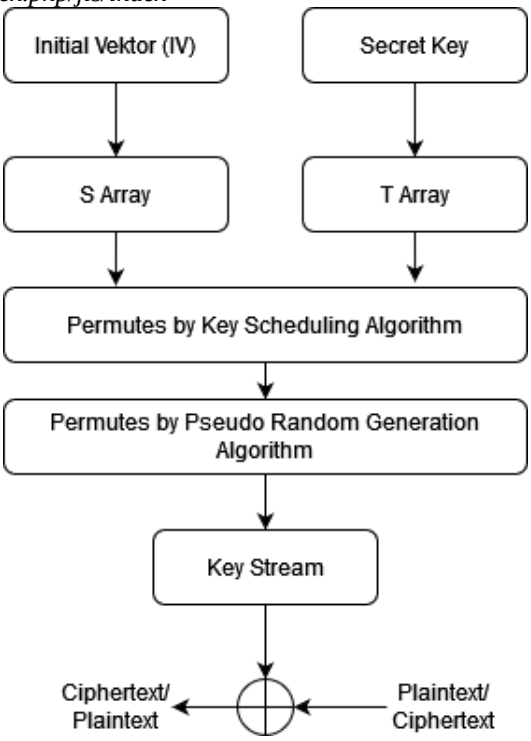


Gambar 1. Proses Enkripsi AES

2.5 *Rivest Cipher 4 (RC4)*

Algoritma Rivest Cipher 4 merupakan bagian dari algoritma cipher enkripsi RC. RC4 didefenisikan sebagai algoritma yang melakukan proses cipher dengan menggunakan satu kunci yang sama atau dapat dikatakan bagian dari stream cipher dengan kunci simetris. Algoritma ini memiliki panjang kunci yang bervariasi dari 40 bit – 2048 bit[3]. RC4 akan membangkitkan keystream dengan pseudorandom generator dan hasil dari keystream akan dilakukan operasi dengan XOR dan operasi logika yang akan mengenkripsi plaintext pada setiap bitnya[6]. Untuk proses dekripsi dilakukan proses yang sama karena RC4 adalah stream cipher dengan kunci simetris. Proses enkripsi pada algoritma RC4 ditunjukkan pada Gambar 2[3].

Jurnal SAINTIKOM (Jurnal Sains Manajemen Informatika dan Komputer)
Volume 22 ; Nomor 2 ; Agustus 2023; Page 357-363
E-ISSN : 2615-3475; P-ISSN : 1978-6603
https://ojs.trigunadharma.ac.id/index.php/jis/index



Gambar 2. Proses Enkripsi RC4

2.6 Workflow Method

Pada bagian ini akan menjelaskan alur kerja yang akan diterapkan pada proses mengamankan komunikasi data dengan menggunakan parameter GET dan POST pada URL.

http[s]://path[?value][=ciphertext]

Pada struktur URI diatas akan dilakukan proses enkripsi pada value yang akan menyamarkan data yang ada pada URI tersebut. Proses pengiriman URI dilakukan pada sisi klien yang nanti akan diterima pada sisi server untuk proses pengiriman kueri data yang diingikan. Proses ini komunikasi ini akan diamankan dengan menggunakan algoritma kriptografi mulai dari proses enkripsi pada sisi klien lalu akan didekripsi pada sisi server. Algoritma yang akan diterapkan pada kasus ini ialah algoritma AES dan RC4.

2.7 Implementasi

Untuk melalukan percobaan, kami melakukan implementasi dengan membangun halaman web sederhana dengan membuat tampilan dengan menggunakan elemen HTML dan CSS. Tampilan web ini dapat dilihat pada Gambar 3 yang menunjukan antarmuka pada halaman browser. Untuk mengakses halaman ini diperlukan browser yang mendukung.

Gambar 3. Antarmuka Aplikasi

Jurnal SAINTIKOM (Jurnal Sains Manajemen Informatika dan Komputer)
Volume 22 ; Nomor 2 ; Agustus 2023; Page 357-363
E-ISSN : 2615-3475; P-ISSN : 1978-6603
https://ojs.trigunadharma.ac.id/index.php/jis/index

Tabel 1. Limit URL Web Browser

Name	Max.Bytes
Firefox	>64000
Chrome	32779 (windows), 1000(mac)
Android Browser	8192
Edge	2083

Pada Tabel 1 diperlihatkan URL yang dapat diakses pada setiap Web Browser memiliki limit yang berbeda-beda. Panjang URL yang akan dihasilkan dengan masing-masing algoritma nantinya akan mempengaruhi penggunaan URL pada setiap browser.

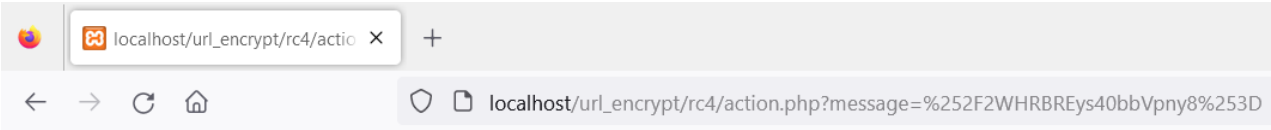
Untuk code dari algoritma yang dimplementasikan menggunakan Javascript dan PHP. Proses pengiriman URL berawal dari sisi klien yang akan dilakukan proses enkripsi yang diimplementasikan dengan menggunakan Javascript, dan selanjutnya proses pengiriman dari melalui URL terjadi dan informasi tersebut diterima oleh sisi server. Pada sisi server data yang telah dienkripsi tadi dilakukan proses dekripsi pada sisi server yang diimplementasikan dengan menggunakan PHP.

3. HASIL DAN PEMBAHASAN

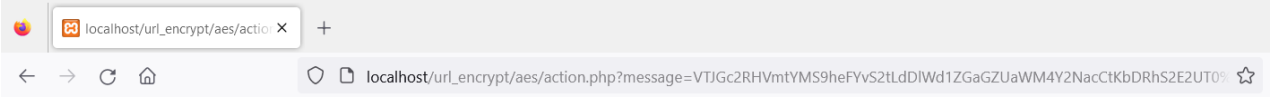
Kami membuat sejumlah URL yang berisikan parameter data pecobaan yang akan dikirimkan dengan ukuran panjang yang berbeda-beda. Kemudian akan dilakukan pengujian dengan parameter waktu berdasarkan ukuran panjang data yang dikirimkan. Beberapa URL percobaan dapat dilihat dibawah ini.

a. http://localhost/url_encrypt/rc4/action.php?message=sangat rahasia
b. http://localhost/url_encrypt/rc4/action.php?message=sangat rahasia sekali
c. http://localhost/url_encrypt/rc4/action.php?message=harus sangat rahasia sekali
d. http://localhost/url_encrypt/aes/action.php?message=sangat rahasia
e. http://localhost/url_encrypt/aes/action.php?message=sangat rahasia sekali
f. http://localhost/url_encrypt/aes/action.php?message=harus sangat rahasia sekali

Pengiriman data dilakukan dengan menginputkan informasi pada form dan data akan dikirimkan dengan menggunakan parameter GET pada URL. Setelah dilakukan enkripsi pada form, maka URL dengan data yang telah dienkripsi akan terlihat seperti Gambar 4 dan Gambar 5.



Gambar 4. URL Setelah Dienkripsi Dengan RC4



Gambar 5. URL Setelah Dienkripsi Dengan AES

Percobaan dilakukan dengan menjalankan program yang telah dibangun dengan menggunakan URL percobaan untuk dijalankan pada masing masing algoritma. Sejumlah hasil percobaan telah didapatkan dengan ukuran panjang yang berbeda-beda dirancang dan selanjutnya dilakukan percobaan dengan algoritma RC4. Hasil enkripsi algoritma RC4 ditunjukkan pada Tabel 2.

Tabel 2. Hasil Enkripsi RC4

Kasus	Plaintext	Hasil Enkripsi pada URL	Time
Kasus 1	sangat rahasia	%252F2WHRBREys40bbVpny8%253D	0,1 ms
Kasus 2	sangat rahasia sekali	%252F2WHRBREys40bbVpny%252BD BzI7yFMp	0,2 ms
Kasus 3	Harus sangat rahasia sekali	5GWbVgYQmd07YrVu1jzCHDYjwF5g XgvAOQnb	0,2 ms

Selanjutnya dilakukan percobaan dengan algoritma AES. Hasil enkripsi algoritma AES ditunjukkan pada Tabel 3.

Tabel 3. Hasil Enkripsi AES

Kasus	Plaintext	Hasil Enkripsi pada URL	Time
Kasus 1	sangat rahasia	VTJGc2RHVmtYMSsxQkFhS WlHWnBqVTZQS2pPbmZS QVhLcWUxMVJlWldhRT0%253D	1,1 ms
Kasus 2	sangat rahasia sekali	VTJGc2RHVmtYMTgxQlFoV0 ZMVVliVnhGZEo1Q2ppdjE4cl FEeE9rN0hyaklFVnFTSUo4W TJYbUdxRFRReFBzZA%253D%253D	1,2 ms
Kasus 3	Harus sangat rahasia sekali	VTJGc2RHVmtYMStwem5ZSjZt SEpxcmh4TkhNVURxMnNMRz FsR1Nad2h3WUFmTDJlZnZBe it1cDNlVTJUTTdHWA%253D%253D	1,79 ms

Dengan melakukan implementasi dengan masing-masing algoritma, kemudian kami akan melakukan analisis terhadap kedua algoritma. Sesuai dengan hasil enkripsi yang dihasilkan yang terlihat pada Tabel 2 dan Tabel 3, dapat dilihat bahwa hasil enkripsi dengan menggunakan algorima AES menghasilkan string yang lebih panjang dibandingkan algoritma RC4. Hasil tersebut membuat URL yang dihasilkan dengan algoritma AES juga lebih panjang dibandingkan algoritma RC4. Dan dari sisi waktu ekseskusi proses enkripsi dari tiap algoritma menghasilkan bahwa algoritma RC4 memiliki waktu eksekusi enkripsi lebih cepat dibandingkan dengan algorima AES.

4. KESIMPULAN

Algoritma kriptografi digunakan untuk melindungi dan menyamarkan data dari serangan. Penerapan yang dilakukan pada paper ini algoritma kriptografi ini dapat melakukan pengamanan data yang dikirimkan. Proses yang dilakukan dengan melakukan enkripsi pada URL dengan menggunakan parameter method GET atau sebuah id dari sebuah baris data ditampilkan pada URL address. Dalam paper ini dilakukan proses percobaan dengan sejumlah URL yang berisikan parameter data yang akan dikirimkan dengan ukuran panjang yang berbeda-beda.

Dapat disimpulkan bahwa proses penerapan algoritma kriptografi pada proses komunikasi data pada URL dapat diterapkan, sehingga data yang dikirimkan melalui URL dapat disamarkan. Hasil enkripsi pada algoritma AES mendapatkan panjang string yang lebih panjang dibandingkan algoritma RC4, sehingga hal tersebut membuat URL yang dihasilkan dengan algoritma AES juga lebih panjang dibandingkan algoritma RC4. Waktu eksekusi pada setiap algoritma memiliki hasil yang berbeda-beda, tetapi dari hasil percobaan dapat dilihat bahwa algoritma RC4 menghasilkan rata-rata waktu eksekusi yang lebih cepat dibandingkan dengan algoritma AES.

UCAPAN TERIMA KASIH

Terima kasih disampaikan kepada pihak-pihak yang telah mendukung terlaksananya penelitian ini.

DAFTAR PUSTAKA

[1] A. K. Mishra and A. Kumar, “Performance-based Comparative Analysis of Open Source Vulnerability Testing Tools for Web Database Applications,” *2020 11th International Conference on Computing, Communication and Networking Technologies, ICCCNT 2020*, Jul. 2020, doi: 10.1109/ICCCNT49239.2020.9225324.

[2] M. F. Muttaqin, “Implementation of AES-128 and Token-Base64 to Prevent SQL Injection Attacks via HTTP,” *International Journal of Advanced Trends in Computer Science and Engineering*, vol. 9, no. 3, pp. 2876–2882, Jun. 2020, doi: 10.30534/ijatcse/2020/60932020.

[3] M. N. Alenezi, H. K. Alabdulrazzaq, and N. Q. Mohammad, "Symmetric Encryption Algorithms: Review and Evaluation Study," *International Journal of Communication Networks and Information Security (IJCNIS)*, vol. 12, no. 2, 2020, doi: 10.17762/IJCNIS.V12I2.4698.

[4] G. Prasetyadi, U. T. Hantoro, A. B. Mutiara, A. Muslim, and R. Refianti, "Heresy: A Serverless Web Application to Store Compressed and Encrypted Document in the Form of URL," *Proceedings of 2019 4th International Conference on Informatics and Computing, ICIC 2019*, Oct. 2019, doi: 10.1109/ICIC47613.2019.8985735.

[5] R. Sadikin, *Kriptografi untuk keamanan jaringan*. Penerbit ANDI, 2012.

[6] H. K. Ronaldo Cahyono, C. Atika Sari, D. R. Ignatius Moses Setiadi, and E. Hari Rachmawanto, "Dual Protection on Message Transmission based on Chinese Remainder Theorem and Rivest Cipher 4," in *2019 International Conference on Information and Communications Technology (ICOIACT)*, IEEE, Jul. 2019, pp. 74–78. doi: 10.1109/ICOIACT46704.2019.8938568.