JURUSAN TEKNIK INFORMATIKA

FAKULTAS TEKNOLOGI INFORMASI

INSTITUT TEKNLOGI SEPULUH NOPEMBER

USULAN TUGAS AKHIR

1. IDENTITAS PENGUSUL

NAMA : **Muhammad Ilham Akbar Syamsuddin**
NRP : **05111640000114**
DOSEN WALI : **Ir. Muchammad Husni, M.Kom.**
DOSEN PEMBIMBING : **Rully Sulaiman**

2. JUDUL TUGAS AKHIR

Desain dan Implementasi Algoritma Enkripsi Simetris Berdasarkan Kubus Rubik

3. LATAR BELAKANG

Kemajuan teknologi informasi saat ini telah menyebabkan peningkatan jumlah data yang dihasilkan dan dikirimkan. Data ini mungkin berisi informasi penting yang tidak boleh diakses oleh orang yang tidak berwenang. Oleh karena itu, masalah perlindungan keamanan data tersebut menjadi masalah yang penting.

Untuk ini, ada banyak algoritma enkripsi yang dikembangkan, contohnya DES dan AES, Beberapa di antaranya, seperti DES, tidak lagi digunakan, dan Oleh karena itu perlu dikembangkan algoritma alternatif yang ringan dan aman[1].

Kubus rubik adalah alat permainan yang ditemukan oleh Erno Rubik pada tahun 1974. Kubus ini terdiri atas 26 bagian kecil yang berputar pada satu poros. Setiap pemukaan memiliki warna berbeda dan terbagi menjadi sembilan bagian.

Saat kubus Rubik dalam keadaan normal, semua permukaan pada sisi yang sama berwarna sama, dan akan berubah acak setelah beberapa kali putaran. Untuk mengembalikannya ke keadaan semula bisa dilakukan dengan membalik urutan putaran – putaran yang dilakukan. Urutan arah putaran ini bisa dijadikan kunci untuk mengenkripsi data[3]. Kubus rubik normal (ukuran 3 x 3 x 3) memiliki 43.252.003.274.489.856.000 kemungkinan posisi[1], Terlepas dari banyaknya posisi, kubus tersebut dapat dipecahkan dalam dua puluh gerakan atau kurang[2], Sehingga sangat menbantu dalam enkripsi.

Dalam proposal ini, diajukan sebuah algoritma enkripsi yang berdasar pada mekanisme kubus rubik.

4. RUMUSAN MASALAH

Rumusan masalah yang diangkat dalam tugas akhir ini dapat dipaparkan sebagai berikut:

1. Bagaimana cara merepresentasikan kubus rubik ke dalam struktur data?
2. Bagaimana cara merepresentasikan putaran kubus rubik pada struktur data tersebut?
3. Bagaimana cara mengaplikasikan struktur data tersebut pada mekanisme enkripsi simetris?
4. Bagaimana agar algoritma yang dihasilkan memenuhi semua kebutuhan keamanan, yaitu kerahasiaan(*confidentiality*), integritas data (*integrity*), otentikasi (*authentication*), dan anti-penyangkalan (*non-repudiation*)?

5. BATASAN MASALAH

Permasalahan yang dibahas dalam tugas akhir ini memiliki beberapa batasan antara lain:

1. Melakukan evaluasi performa menggunakan *performance metrics* antara lain waktu enkripsi, waktu dekripsi, *throughput of encryption*, *throughput of decryption*, *CPU process time*, *CPU clock cycle*, konsumsi baterai, dan penggunaan memori[4].
2. Implementasi menggunakan bahasa pemrograman C++.

6. TUJUAN PEMBUATAN TUGAS AKHIR

Tujuan dari pembuatan tugas akhir ini adalah merancang algoritma enkripsi yang cepat dan ringan dan memenuhi standar keamanan, serta mengetahui perbandingan performanya dengan algoritma enkripsi lain.

7. MANFAAT TUGAS AKHIR

Manfaat dari hasil pembuatan tugas akhir adalah mendapatkan algoritma enkripsi simetris baru yang cepat, ringan, dan memenuhi standar keamanan.

8. TINJAUAN PUSTAKA

1. Kubus Rubik

Kubus rubik adalah alat permainan yang ditemukan oleh Erno Rubik pada tahun 1974. Kubus ini terdiri atas 26 kepingan kecil yang berputar pada satu poros, yang terdiri dari delapan kepingan sudut, dua belas kepingan rusuk, dan 6 kepingan pusat. Setiap pemukaan memiliki warna berbeda dan terbagi menjadi sembilan bagian[3].

Kubus Rubik normal (3x3x3) memiliki delapan sudut dan dua belas rusuk. Ada 8! cara untuk mengatur sudut kubus. Setiap sudut memiliki tiga warna, dengan tujuh bisa berorientasi mandiri, dan orientasi sudut kedelapan tergantung pada tujuh sudut sebelumnya, sehiungga 3^7 kemungkinan. Ada 12! Cara untuk mengatur rusuk kubus. Setiap rusuk memiliki dua warna, dengan sebelas rusuk bisa berorientasi mandiri dan orientasi rusuk keduabelas tergantung pada sebelas rusuk sebelumnya, sehingga ada 2^{11} kemungkinan.

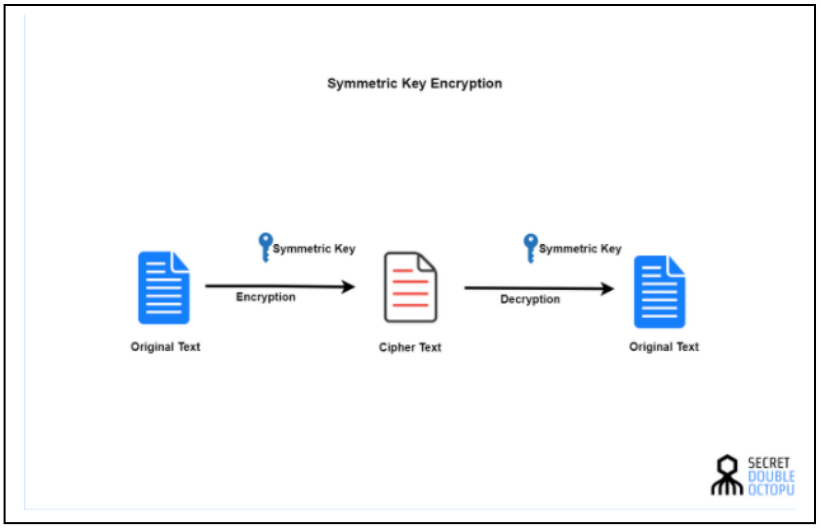
Kemudian, Kubus rubik tidak dapat dipecahkan jika hanya kepingan sudut atau kepingan rusuknya saja yang ditukar, sehingga banyak kemungkinan harus dikurang setengahnya, sehingga total banyak kemungkinan posisi kubus rubik ada

$$\frac{1}{2} \times 8! \times 3^7 \times 12! \times 2^{11} = 43.252.003.274.489.856.000 \text{ kemungkinan.}$$

2. Enkripsi Kunci Simetris.

Enkripsi kunci simetris adalah enkripsi yang hanya melibatkan satu kunci rahasia untuk menyandikan dan menguraikan informasi.

Metode ini umumnya relatif lebih cepat dibandingkan enkripsi kunci asimetris, karena itu lebih ideal untuk data berukuran besar. Contoh enkripsi kunci simetris adalah Blowfish, AES, RC4, DES.



Sumber gambar:https://doubleoctopus.com/security-wiki/encryption-and-cryptography/symmetric-key-cryptography/

9. RINGKASAN ISI TUGAS AKHIR

Kemajuan teknologi informasi membuat isu keamanan data semakin penting. Sehingga perlu dikembangkan algoritma enkripsi yang cepat, ringan dan aman.

Kubus rubik memiliki 43.252.003.274.489.856.000 kemungkinan posisi, dan hanya membutuhkan 20 gerakan atau kurang untuk memecahkannya. Data dapat diisikan ke kubus rubik kemudian dilakukan pergerakan untuk mengacak data. Urutan gerakan kubus rubik dapat digunakan sebagai kunci untuk melakukan enkripsi. Banyaknya variasi kunci serta kesederhanaan pemecahannya menjadikan kubus rubik cocok sebagai alat enkripsi.

Tugas akhir ini bertujuan untuk mendesain dan mengimplementasi algoritma, serta melakukan perbandingan performanya dengan algoritma-algoritma lain yang sudah ada.

10. METODOLOGI

a. Penyusunan proposal tugas akhir

Proposal tugas akhir ini berisi tentang deskripsi pendahuluan dari tugas akhir yang akan dibuat. Pendahuluan ini terdiri atas hal yang menjadi latar belakang diajukannya usulan tugas akhir, rumusan masalah yang diangkat, batasan masalah untuk tugas akhir, tujuan dari pembuatan tugas akhir, dan manfaat dari

hasil pembuatan tugas akhir. Selain itu dijabarkan pula tinjauan pustaka yang digunakan sebagai referensi pendukung pembuatan tugas akhir. bagian metodologi berisi penjelasan mengenai tahapan penyusunan tugas akhir mulai dari penyusunan proposal hingga penyusunan buku tugas akhir. Terdapat pula sub bab jadwal kegiatan yang menjelaskan jadwal pengerjaan tugas akhir.

b. Studi literatur

Pada tahap ini, akan dipelajari sejumlah referensi yang diperlukan untuk merancang dan mengimplementasikan algoritma enkripsi, terkait untuk menyelesaikan studi kasus, diantara lain adalah buku, situs web, serta jurnal - jurnal terkait.

c. Desain dan Implementasi Algoritma

Pada tahap ini dilakukan perancangan algoritma dan implementasinya menggunakan C++.

d. Pengujian dan evaluasi

Pengujian dilakukan dengan membandingkan performa algoritma dengan beberapa algoritma-algoritma menggunakan *performance metrics*, antara lain :

1. Waktu enkripsi
2. Waktu dekripsi.
3. Throughput of encryption
4. Throughput of decryption
5. CPU process time
6. CPU clock cycle
7. Konsumsi baterai.
8. Penggunaan memori.

e. Penyusunan Buku Tugas Akhir

Pada tahap ini dilakukan penyusunan laporan yang menjelaskan dasar teori dan metode yang digunakan dalam tugas akhir ini serta hasil dari implementasi aplikasi perangkat lunak yang telah dibuat. Sistematika penulisan buku tugas akhir secara garis besar antara lain:

1. Pendahuluan
    a. Latar Belakang
    b. Rumusan Masalah
    c. Batasan Tugas Akhir
    d. Tujuan
    e. Metodologi
    f. Sistematika Penulisan
2. Tinjauan Pustaka
3. Desain dan Implementasi
4. Pengujian dan Evaluasi
5. Kesimpulan dan Saran
6. Daftar Pustaka

11. JADWAL KEGIATAN

Jadwal pengerjaan tugas akhir ditunjukkan pada Tabel 1.

Tabel 1. Jadwal Pengerjaan Tugas Akhir

Tahapan	2020												2021											
	Oktober				November				Desember				Januari				Februari				Maret			
Penyusunan Proposal																								
Studi Literatur																								
Perancangan Sistem																								
Implementasi																								
Pengujian dan Evaluasi																								
Penyusunan Buku																								

12. DAFTAR PUSTAKA

[1] P Elayaraja, M Sivakumar, 'New Approach and Additional Security to Existing Cryptography Using Cubical Combinatorics', Master of Computer Applications; Dhanalakshmi College of Engineering, Chen-nai.

[2] God's Number is 20[online]. Available: http://www.cube20.org. [diakses 10 Oktober 2020]

[3] Zeng, D., Li, M., Wang, J. *et al.* Overview of Rubik's Cube and Reflections on Its Application in Mechanism. *Chin. J. Mech. Eng.* **31,** 77 (2018). https://doi.org/10.1186/s10033-018-0269-7

[4] Kumar, Dr. M. Anand & Balasubramanian, Bharathi & G.Manivasagam,. (2017). METRICS FOR PERFORMANCE EVALUATION OF ENCRYPTION ALGORITHMS. International Journal of Advance Research in Science and Engineering. 6. 62-72.