

## PENERAPAN RC5 UNTUK PENGAMANAN NILAI MATAKULIAH MAHASISWA PADA KAMPUS XYZ

### *RC5 Application for Student Course Scores Safety at XYZ Campus*

Yohanes Setiawan Japriadi, [ysetiawanj@atmaluhur.ac.id](mailto:ysetiawanj@atmaluhur.ac.id)<sup>1)</sup>, Dian Novianto, [diannovianto@atmaluhur.ac.id](mailto:diannovianto@atmaluhur.ac.id)<sup>2)</sup>

<sup>1)2)</sup> Teknik Informatika, STMIK Atma Luhur

#### ABSTRACT

*Student course score datas are very important and confidential data at a campus. Due to the nature of the student's course score datas, it's need to securing the datas for their confidentiality. This is intended so that the data values are not easily read or manipulated by unauthorized parties. One of the data security solution is to use the RC5 cryptographic algorithm. Score datas (plain text) inputted by the lecturer need to pass an encryption process when it is stored in a database (cipher text) and need to pass a decryption process when the score that stored in the database can be seen by students. A good cryptographic algorithm is a cryptographic algorithm that can perform the encryption and decryption process without ruin or changing the original data. This study aims to determine whether the RC5 cryptographic algorithm can be applied as data security for student course scores with 100% encryption and decryption success rate. The score data used in this study was sourced from the score data of STMIK Atma Luhur Pangkalpinang students in the 2018/2019 school year even semester. From the results of testing the 2,060 records of Atma Luhur STMIK students' course scores, the results show that the RC5 cryptographic algorithm used has a 100% success rate in encrypting and decrypting the intended value data. Thus, RC5 is considered suitable to be used to secure data on student course score on a campus.*

**Keyword** : cryptography, encryption, decryption, RC5, students score safety

#### ABSTRAK

Data nilai matakuliah mahasiswa merupakan data yang sangat penting dan bersifat rahasia pada suatu kampus. Dikarenakan sifat dari data nilai matakuliah mahasiswa ini, tidak jarang perlu tindakan pengamanan untuk menjaga kerahasiannya. Hal ini dimaksudkan agar data nilai tidak gampang dibaca maupun dimanipulasi oleh pihak yang tidak berwenang. Salah satu solusi pengamanan data adalah menggunakan algoritma kriptografi RC5. Data nilai (*plain* teks) yang diinput dosen perlu mengalami proses enkripsi saat disimpan ke dalam basisdata (*cipher* teks) dan perlu mengalami proses dekripsi saat nilai yang tersimpan di dalam basisdata dapat dilihat oleh mahasiswa. Algoritma kriptografi yang baik adalah algoritma kriptografi yang dapat melakukan proses enkripsi dan proses dekripsi tanpa merusak atau mengubah data aslinya. Penelitian ini bertujuan untuk mengetahui apakah algoritma kriptografi RC5 dapat diterapkan sebagai pengaman data nilai matakuliah mahasiswa dengan tingkat keberhasilan enkripsi dan dekripsi 100%. Data nilai yang digunakan pada penelitian ini bersumber dari data nilai matakuliah mahasiswa STMIK Atma Luhur Pangkalpinang tahun ajaran 2018/2019 semester Genap. Dari hasil pengujian terhadap 2.060 record nilai matakuliah mahasiswa STMIK Atma Luhur, diperoleh hasil bahwa algoritma kriptografi RC5 yang digunakan memiliki tingkat keberhasilan 100% dalam mengenkripsi dan mendekripsi data nilai yang dimaksud. Sehingga, RC5 dianggap layak digunakan untuk mengamankan data nilai matakuliah mahasiswa pada suatu kampus..

**Kata Kunci**: kriptografi, enkripsi, dekripsi, RC5, pengamanan nilai mahasiswa.

#### PENDAHULUAN

Maraknya pemanfaatan teknologi web dalam menunjang kegiatan manusia

semakin tidak terlepas. Begitu juga pada kebanyakan kampus yang telah menggunakan web untuk mendukung

kegiatan pada kampusnya, terutama dalam bidang akademik. Sayangnya, di samping sifat dari web yang dapat diakses menggunakan internet secara luas, muncul kekhawatiran bahwa data yang disajikan dapat dibaca dan dimanipulasi oleh pihak yang tidak berwenang.

Kampus STMIK Atma Luhur Pangkalpinang merupakan salah satu kampus yang memanfaatkan teknologi web untuk mendukung sistem akademik terkait nilai matakuliah mahasiswa. Dosen akan menginput nilai mahasiswa menggunakan web dosen, sedangkan mahasiswa akan melihat nilai yang telah diinput oleh dosen pada web mahasiswa. Akan tetapi, data nilai yang ada pada basisdata belum mengalami proses enkripsi, atau dengan kata lain masih dalam bentuk *plain* teks. Hal ini tentunya akan mempermudah pihak yang tidak berwenang untuk membaca dan memanipulasi data nilai matakuliah mahasiswa jika data nilai tersebut masih dalam keadaan *plain* teks.

Kriptografi menggunakan algoritma RC5 dapat dimanfaatkan untuk beberapa keperluan, misalnya saja penyandian file<sup>[1]</sup>, pengamanan pesan instan<sup>[2]</sup>, pengamanan file teks<sup>[3]</sup>, pengamanan nilai<sup>[4]</sup>, sampai dengan steganografi pada audio<sup>[5]</sup>.

Tujuan dari penelitian ini dimaksudkan untuk mengetahui apakah algoritma RC5 dapat digunakan untuk mengamankan *plain* teks berupa nilai tugas, nilai UTS, dan nilai UAS ke dalam bentuk terenkripsi (*cipher* teks), dan mencoba untuk mendekripsi *cipher* teks kembali ke dalam bentuk asli dengan tingkat keberhasilan 100%.

Sedangkan, penelitian ini diharapkan dapat memberikan manfaat kepada kampus untuk mengamankan data nilai yang diinput dosennya sehingga meminimalkan kemungkinan untuk dibaca maupun dimanipulasi oleh pihak yang tidak berwenang.

## METODE PENELITIAN

### Studi Pustaka/Literatur

Penelitian terdahulu terkait RC5 dikumpulkan dan dipelajari sehingga peneliti menemukan bagaimana cara kerja algoritma RC5 dalam mengenkripsi maupun bagaimana algoritma RC5 dimanfaatkan.

### Pengkodean Algoritma RC5

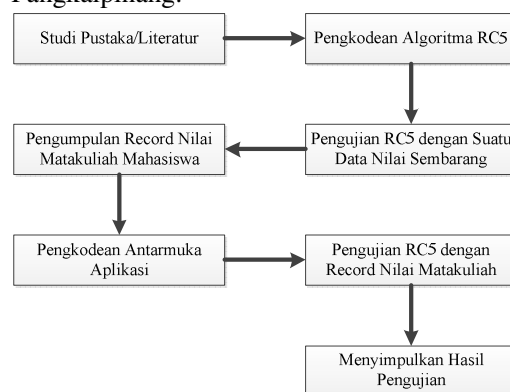
Setelah memahami cara kerja algoritma RC5, selanjutnya peneliti akan mengkodekan algoritma RC5 ke dalam bahasa pemrograman PHP. Pengkodean pada tahap ini meliputi pemberian kunci, enkripsi, dan dekripsi.

### Pengujian RC5 dengan Suatu Data Nilai Sembarang

Menggunakan kode yang telah dibuat, peneliti menguji data nilai dari rentang 0-100 untuk mengetahui apakah berhasil dilakukan enkripsi dan dekripsi.

### Pengumpulan Record Nilai Matakuliah Mahasiswa

Setelah pengujian dengan data sembarang berhasil dilakukan, selanjutnya peneliti mengumpulkan record nilai matakuliah mahasiswa yang diperoleh dari basisdata Oracle nilai sistem akademik yang ada di kampus STMIK Atma Luhur Pangkalpinang.



Gambar 1. Skema Penelitian

Data yang digunakan berupa record nilai matakuliah mahasiswa pada tahun ajaran 2018/2019 semester genap, mengingat data record nilai matakuliah pada semester ini sudah lengkap. Data yang digunakan sebanyak 6.020 record nilai matakuliah mahasiswa.

Data yang dikumpulkan ini selanjutnya disiapkan ke dalam bentuk basisdata MySQL.

#	Name	Type
1	CTHAJAR	char(8)
2	CSMT	char(1)
3	CNOTAB	varchar(6)
4	CNIM	char(10)
5	CKELOMPOK	varchar(6)
6	CKDDOS	char(5)
7	NNILTGS	tinyint(4)
8	NNILMID	tinyint(4)
9	NNILFIN	tinyint(4)

Gambar 2. Struktur Tabel Nilai

Showing rows 0 - 24 (6020 total. Query took 0.0040 seconds.)

```
SELECT * FROM `nilai1819`
```

Options	CTHAJAR	CSMT	CNOTAB	CNIM	CKELOMPOK	CKDDOS	NNILTGS	NNILMID	NNILFIN
20182019	E	IT801	1311500029	TIZA	00004	100	80	50	
20182019	E	IT801	1411500053	TIZA	00004	100	100	100	
20182019	E	IT801	1511500133	TIZA	00004	0	0	0	
20182019	E	IT801	1811500001	TIZA	00004	100	100	100	
20182019	E	IT801	1811500002	TIZA	00004	100	100	100	
20182019	E	IT801	1811500005	TIZA	00004	100	100	100	
20182019	E	IT801	1811500006	TIZA	00004	100	80	100	

Gambar 3. Record Tabel Nilai

### Pengkodean Antarmuka Aplikasi

Peneliti mengkodekan antarmuka aplikasi, termasuk koneksi dari PHP ke MySQL untuk menampilkan data nilai tugas, UTS, dan UAS dalam bentuk sebelum dienkripsi, setelah dienkripsi, maupun setelah didekripsi.

### Pengujian RC5 dengan Record Nilai Matakuliah

Setelah melakukan pengkodean antarmuka aplikasi, peneliti menguji algoritma RC5 dengan data yang berasal dari record nilai matakuliah.

### Menyimpulkan Hasil Pengujian

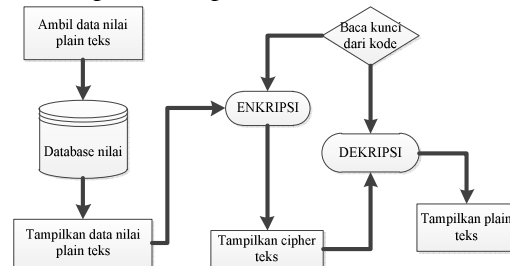
Berdasarkan pengujian yang telah dilakukan, hasil pengujian disampaikan

apakah tercapai tingkat keberhasilan enkripsi dan dekripsi sebesar 100%.

## HASIL DAN PEMBAHASAN

### Proses Enkripsi dan Proses Dekripsi

Proses enkripsi dan proses dekripsi pada penelitian ini berfokus pada record atau data nilai matakuliah mahasiswa yang terdiri dari nilai tugas, nilai UTS, dan nilai UAS pada basisdata MySQL. Adapun skema kerja proses enkripsi dan dekripsi nilai dapat dilihat pada Gambar 4.



Gambar 4. Skema Proses Enkripsi dan Dekripsi

### Implementasi

Pada saat implementasi algoritma RC5 ke dalam data nilai yang digunakan, digunakan kunci "1511500150" yang diberikan disimpan ke dalam konstanta \$this->magic = "1511500150". Berikut ini beberapa potongan kode RC5 yang digunakan.

```

class RC5 {
    private $magic;
    function __construct() {
        $this->magic = "1511500150";
    }
}
  
```

Gambar 5. Potongan Kode Kunci pada Class RC5

Selain itu, pada proses enkripsi dan dekripsi masing-masing untuk nilai tugas, nilai UTS, dan nilai UAS, peneliti menggunakan potongan kode seperti yang ditunjukkan pada Gambar 6.

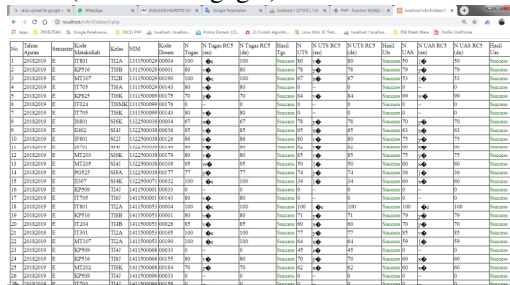
```

33 while($data = $query->fetch_object()) {
34     $detgs=$enc->encrypt($data->NNILTGS);
35     $detgs=$enc->decrypt($detgs);
36     $hasilrts = "";
37     if ($data->NNILTGS<>$detgs) $hasilrts = "<font
color:red>Failed</font>";
38     elseif ($data->NNILTGS==$detgs) $hasilrts = "<font
color:green>Success</font>";
    
```

**Gambar 6. Potongan Kode Enkripsi dan Dekripsi RC5**

**Antarmuka Aplikasi**

Antarmuka aplikasi yang dibuat terdiri dari kolom No, Tahun Ajaran, Semester, Kode Matakuliah, Kelas, NIM, Kode Dosen, Nilai Tugas (dalam bentuk *plain* teks), Nilai Tugas (dalam bentuk terenkrip), Nilai Tugas (dalam bentuk didekrip), Hasil dekrip nilai Tugas (sukses atau gagal), Nilai UTS (dalam bentuk *plain* teks), Nilai UTS (dalam bentuk terenkrip), Nilai UTS (dalam bentuk didekrip), Hasil dekrip nilai UTS (sukses atau gagal), Nilai UAS (dalam bentuk *plain* teks), Nilai UAS (dalam bentuk terenkrip), Nilai UAS (dalam bentuk didekrip), dan Hasil dekrip nilai UAS (sukses atau gagal).



**Gambar 7. Antarmuka Aplikasi**

**Pengujian Aplikasi**

Pengujian aplikasi dilakukan dengan membuat kode yang menampilkan record dari basisdata MySQL secara 6.020 record sekaligus ke dalam sebuah halaman. Kolom Hasil digunakan untuk mengetahui hasil pembalikan *cipher* teks menjadi *plain* teks apakah berhasil atau gagal. Setelah melakukan pengujian pada aplikasi, diperoleh hasil bahwa seluruh record nilai matakuliah mahasiswa yang terdiri dari nilai tugas, nilai UTS, dan nilai UAS dapat didekripsi dengan tingkat keberhasilan 100%.

**Tabel 1. Sampel Pengujian Nilai Matakuliah**

NIM	Plain	Cipher	Decrypt	Hasil
1311500029	100	◆c	100	Sukses
1322500038	77	y◆	77	Sukses
1422500098	20	l◆	20	Sukses
1411500053	59	{◆	59	Sukses
1422500146	45	z◆	45	Sukses
1422500031	35	} ◆	35	Sukses
1422500183	80	v◆	80	Sukses
1511500133	0	~	0	Sukses
1522500082	60	x◆	60	Sukses

6019	20182019	E	IF901	SI2A	1822500191		
6020	20182019	E	II302	SI2A	1822500191		
00005	100	◆c	100	Success			
00035	98	w◆	98	Success			
85	◆	85	Success	60	◆	60	Success
55	◆	55	Success	65	◆	65	Success

**Gambar 8. Record Terakhir Data Nilai**

**SIMPULAN**

Setelah menganalisa, membahas, dan melakukan pengujian, dapat ditarik kesimpulan bahwa algoritma kriptografi RC5 layak digunakan untuk mengamankan data nilai pada kampus XYZ karena memiliki tingkat keberhasilan 100% dalam proses enkripsi dan dekripsi. Dengan tingkat keberhasilan 100% ini, artinya tidak terjadi kesalahan sedikitpun dalam pengungkapan *cipher* teks ke dalam bentuk *plain* teks pada data nilai tugas, nilai UTS, maupun nilai UAS.

**DAFTAR PUSTAKA**

[1] Prabowo, W., Harahap, A., & Ismadiyah, R. (2018). Penyandian File Word Berdasarkan Algoritma Rivest Code 5 (RC5). *J-SAKTI (Jurnal Sains Komputer dan Informatika)*, 2(1), 47-56.

[2] Rifky, Ilham (2018). Kombinasi Algoritma RC5 Block Cipher dan Rebalanced RSA dalam Pengamanan Pesan Instan. Universitas Sumatera Utara.

- [3] Nilawati (2017). Perancangan Aplikasi Keamanan File Teks Menggunakan Algoritma RC5 Dengan Algoritma RC6. *Pelita Informatika Budi Darma*, Volume : XVI, Nomor: 2, April 2017, 147-151.
- [4] Amalia, Zia (2019). Model Implementasi Algoritma Rc5 Pada Halaman Entri Nilai Dan Khs Mahasiswa (Studi Kasus: Website Dosen Dan Mahasiswa STMIK Atma Luhur Pangkalpinang). *STMIK Atma Luhur Pangkalpinang*.
- [5] Atis, Ahmed (2017). Steganography in Audio Using RC5 and Rijndael Algorithms. *Journal of The Iraqi University*, Year: 2017 Issue: 39-1 Pages: 765-774.