**ENKRIPSI DAN DEKRIPSI DATA *QR CODE* MENGGUNAKAN METODE *RC4* PADA PEMBANGUNAN APLIKASI PRESENSI JURUSAN TI UHO**

**Muazharin Alfan\*1,** **Sutardi 2, Bambang Pramono 3**

1,2,3Jurusan Teknik Informatika, Fakultas Teknik, Universitas Halu Oleo, Kendari

e-mail: [**\*1alfanmuazharin@gmail.com**, 2](mailto:*1alfanmuazharin@gmail.com,%202)sutardi\_hapal@yahoo.com**,** 3bambangpramono09@gmail.com

**Abstrak**

Perkembangan teknologi saat ini sangat pesat, sistem keamanan semakin banyak diimplementasikan dalam berbagai sistem dan aplikasi. Dalam penyampaian pesan tersembunyi contohnya sudah terdapat banyak metode atau algoritma yang semakin marak digunakan. *Rivest Cipher 4 (RC4)* merupakan jenis aliran kode yang operasi enkripsinya dilakukan per karakter 1byte untuk sekali operasi. Algoritma ini merupakan salah satu algoritma pengamanan text yang menggunakan kunci simetris yang dibuat oleh *RSA DataSecurity Inc (RSADSI)* yang berbentuk *stream cipher*. Pada aplikasi ini metode tersebut digunakan dalam data *QR Code* agar dapat menyembunyikan karakter khusus yang ditanam dalam *QR Code* tersebut. Hasil yang didapatkan dari penelitian ini bahwa metode *RC4* berhasil diimplementasikan pada data *QR Code* dan kecepatan scanning tiap *QR Code* hanya berkisar 6 sampai 8 detik saja untuk setiap kelas. *QR Code* yang telah ditanamkan metode tersebut hanya dapat didekripsi menggunakan sistem ini. Sehingga meminimalisir kecurangan dalam proses absensi mahasiswa.

**Kata kunci** — *Kritografi, Rivest Cipher 4, QR Code*

***Abstract***

*The development of technology is currently very rapid, more and more security systems are implemented in various systems and applications. In delivering hidden messages for example there are already many methods or algorithms that are increasingly used. Rivest Cipher 4 (RC4) is a type of code stream which means that the encryption operation is performed per 1byte character for one operation. This algorithm is a text security algorithm that uses symmetric keys created by RSA DataSecurity Inc. (RSADSI) in the form of stream cipher. In this application the method is used in QR Code data in order to hide the special characters that are planted in the QR Code. The results obtained from this study that the RC4 method was successfully implemented on QR Code data and the scanning speed of each QR Code was only around 6 to 8 seconds for each class. QR Code that has been implanted with this method can only be decrypted using this system. Thus minimizing cheating in the student attendance process.*

**Keywords** - *Krytografi, Rivest Cipher 4, QR Code*

1. PENDAHULUAN

D

i era modern seperti sekarang ini, kemajuan teknologi berkembang semakin pesat. Berbagai sistem mulai diciptakan menggunakan teknologi dengan tujuan untuk mempermudah pekerjaan manusia. Mulai dari bidang pemerintahan, perusahaan, politik dan pendidikan seperti sekolah dan universitas. Adapun di universitas sendiri ada salah satu sistem pengelolaan yang masih di kerjakan secara manual yaitu daftar hadir. Sistem daftar hadir merupakan salah satu faktor yang sangat penting dalam dunia universitas. Selain digunakan sebagai alat kontrol mahasiswa, daftar hadir juga digunakan sebagai salah satu penunjang penilaian dosen dan syarat dokumentasi borang setiap 5 tahun sekali.

Universitas Halu Oleo merupakan salah satu universitas yang masih menggunakan sistem manual dalam penanganan daftar hadir di masing-masing jurusan. Tanpa terkecuali jurusan Teknik Informatika yang setiap semester harus mencetak lembaran daftar hadir dan merekap data tersebut di akhir semester. Dari 300 mahasiswa aktif dengan lebih dari 20 mata kuliah disetiap semester, tentu menjadi tugas yang tidak mudah bagi pegawai staff di jurusan untuk mengontrol data tersebut. Maka dengan kemajuan teknologi, tidak menutup kemungkinan untuk mengembangkan sebuah aplikasi agar dapat membantu dan memudahkan sistem daftar hadir tersebut.

Telpon seluler (*Smartphone*) merupakan tools yang tepat dalam membangun sistem tersebut. Dengan kemampuan kamera di setiap *Smartphone* yang dapat mengambil, menyimpan dan menampilkan gambar dengan format JPEG. Memunculkan ide untuk memanfaatkan *QR Code* dan *Smartphone* Android dalam mengembangkan sistem daftar hadir tersebut. Dimana dalam *QR Code* ini nantinya akan menyimpan data setiap mahasiswa dan dapat dicetak.

Informasi yang dikodekan dalam *QR Code* dapat berupa URL, nomor telepon, pesan SMS, V-Card atau teks apa pun. Disebut *QR Code* karena teknologi memungkinkan sistem untuk memecahkan kode konten dengan kecepatan tinggi. Ditambah lagi dengan sistem operasi Android pada *Smartphone* yang sangat populer dan banyak digunakan, membuat sistem ini akan menjadi lebih cepat,

dan praktis. Namun, karena *QR Code* ini dapat dibaca dengan aplikasi QR Scanner apapun, maka penting menambahkan algoritma pada aplikasi ini yang berguna untuk mengamankan data pada *QR Code* tersebut [2].

Salah satu metode yang banyak digunakan dalam sistem pengamanan data adalah Algoritma *RC4* (Rivers Code 4). Algoritma ini bekerja dengan kunci enkripsi yang didapat dari 256 bit state array yang diinisialisasi dengan sebuah key tersendiri dengan panjang 1-256 bit. Setelah itu, state array yang didapatkan diacak kembali dan diproses untuk menghasilkan sebuah kunci enkripsi yang akan di-XOR dengan plaintext ataupun ciphertext sehingga didapatkan hasil dari enkripsi ataupun dekripsi (Sholeh, 2019).

Dengan modifikasi yang digabungkan dengan algoritma ini akan membuat data dalam *QR Code* ini sulit untuk dipecahkan. Adapun pesan yang keluar tidak akan mudah dimengerti karena telah dienkripsi sehingga *QR Code* tersebut hanya dapat digunakan pada aplikasi tertentu. Selain itu, proses algoritma ini menggunakan kunci simetris yang dapat membuat proses enkripsi dan dekripsi *QR Code* menjadi lebih cepat [5].

2. METODE PENELITIAN

## 2.1 Kriptografi

Kriptografi adalah ilmu mengenai teknik enkripsi dimana “naskah asli” (plaintext) diacak menggunakan suatu kunci enkripsi menjadi “naskah acak yang sulit dibaca” (ciphertext) oleh seseorang yang tidak memiliki kunci dekripsi. Dekripsi menggunakan kunci dekripsi bisa mendapatkan kembali data asli. Probabilitas mendapat kembali naskah asli oleh seseorang yang tidak mempunyai kunci dekripsi dalam waktu yang tidak terlalu lama adalah sangat kecil.

Teknik enkripsi yang digunakan dalam kriptografi klasik adalah enkripsi simetris dimana kunci dekripsi sama dengan kunci enkripsi. Untuk public key cryptography, diperlukan teknik enkripsi asimetris dimana kunci dekripsi tidak sama dengan kunci enkripsi. Enkripsi, dekripsi dan pembuatan kunci untuk teknik enkripsi asimetris memerlukan komputasi yang lebih intensif dibandingkan enkripsi simetris, karena enkripsi asimetris menggunakan bilangan – bilangan yang sangat besar[6].

2.2 *Rivest Cipher 4 (RC4)*

*RC4* merupakan jenis aliran kode yang berarti operasi enkripsinya dilakukan per karakter 1byte untuk sekali operasi. Algoritma kriptografi Rivest Code 4 (*RC4*) merupakan salah satu algoritma kunci simetris dibuat oleh RSA DataSecurity Inc (RSADSI) yang berbentuk stream cipher. Algoritma ini ditemukan pada tahun 1987 oleh Ronald Rivest dan menjadi simbol keamanan RSA (merupakan singkatan dari tiga nama penemu yaitu Rivest, Shamir, dan Adleman).

Secara garis besar algoritma dari metode *RC4* StreamCipherini terbagi menjadi dua bagian, yaitu Key Setup atau Key Schedulling Algorithm (KSA) dan Stream Generation atau Pseudo Random Generation Algorithm (PRGA) dan proses XOR dengan stream data.

*RC4* menghasilkan pseudorandom stream bit. Seperti halnya stream cipher lainnya, algoritma *RC4* ini dapat digunakan untuk mengenkripsi dengan mengombinasikannya dengan plainteks dengan menggunakan bit-wise XOR (Exclusive-or). Proses dekripsinya dilakukan dengan cara yang sama (karena XOR merupakan fungsi simetrik). Untuk menghasilkan key-stream, cipher menggunakan state internal yang meliputi dua bagian :

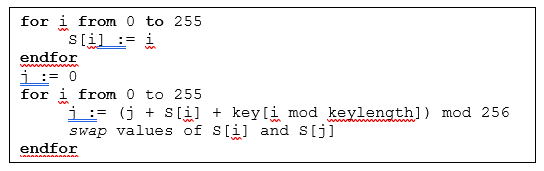
1. Sebuah permutasi dari 256 kemungkinan byte.

2. 2 Indeks-pointer 8-bit.

Permutasi diinisialisasi dengan sebuah variabel panjang kunci, biasanya antara 40 sampai 256 bit dengan menggunakan algoritma key-scheduling (KSA). Setelah proses ini selesai, stream yang terdiri dari sekumpulan bit tersebut terbentuk dengan menggunakan Pseudo-Random Generation Algorithm (PRGA). Berikut ini akan dijelaskan tentang kedua algoritma tersebut.

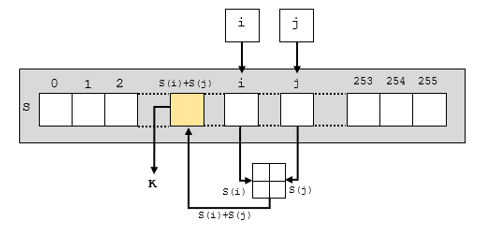
1. *Key-Scheduling Algorithm (KSA)*

Algoritma key scheduling digunakan untuk menginisialisasi permutasi di array “S”. panjang kunci didefinisikan sebagai jumlah byte di kunci dan mempunyai rentang panjang kunci dari 1 sampai 256, khususnya antara 5-16 tergantung dari panjang kunci 40-128 bit. Pertama-tama array “S” diinisialisasi untuk identitas permutasi. S kemudian diproses ke 256 iterasi dengan cara yang sama dengan PRGA utama, tapi juga dikombinasikan dalam byte dari kunci dalam waktu yang bersamaan. Berikut adalah algoritma KSA :

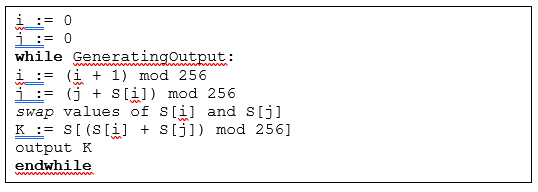


1. *Pseudo-Random Generation Algorithm (PRGA)*

PRGA (Pseudo-Random Generation Algortihm) memodifikasi state dan output sebuah byte dari key-stream. Hal ini penting karena banyaknya dibutuhkan iterasi. Dalam setiap iterasi, PRGA menginkremen i, menambahkan nilai S yang ditunjuk oleh i sampai j, kemudian menukar nilai S[i] dan S[j], lalu mengembalikan elemen dari S di lokasi S[i] + S[j] (modulo 256). Setiap elemen S ditukar dengan elemen lainnya paling tidak satu kali setiap 256 iterasi.



Realisasi dari algoritma PRGA yaitu:



3. HASIL DAN PEMBAHASAN

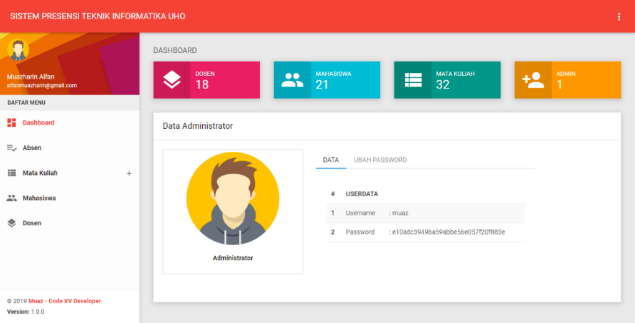
3.1 Implementasi

Implementasi merupakan tahap di mana sistem telah siap untuk digunakan. Hasil analisis dan perancangan sistem yang telah dilakukan sebelumnya diimplementasikan dalam bentuk aplikasi berupa aplikasi web services dan aplikasi berbasis android serta *QR Code* yang data di dalamnya telah dienkripsi menggunakan algoritma RC 4 (*Rivest Cipher 4*). Kedua aplikasi ini dibangun dengan bahasa pemrograman PHP pada server side dan Dart pada aplikasi androidnya.

1. *Interface* Aplikasi

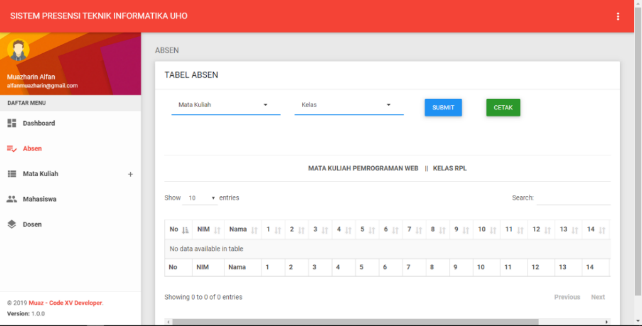
Pada *interface* Aplikasi diantaranya :

1. Menu Dashboard

Menu Dashboard menampilkan data aplikasi secara umum. Mulai dari jumlah dosen, mahasiswa, mata kuliah dan user. Selain itu pada halaman ini, sistem juga menampilkan data admin serta form untuk mengubah password admin. 

Gambar 3 Menu Dashboard.

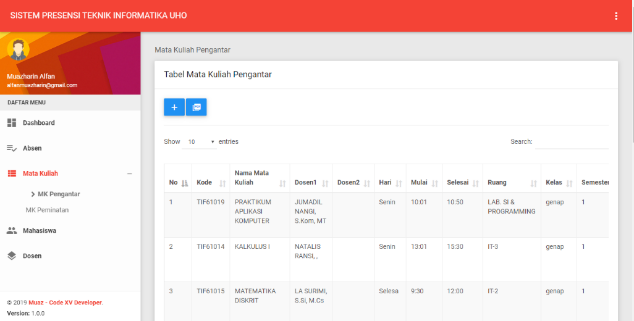
1. Menu Absen

Menu absen menampilkan data absensi berdasarkan nama mata kuliah dan kelas. Terdapat tabel yang berisikan nama dan nim masing-masing mahasiswa serta daftar kehadirannya dari pertemuan 1 sampai pertemuan ke 16. Serta informasi persentase kehadiran mahasiswa tersebut. Selain itu, juga terdapat tombol cetak untuk melakukan print out data absensi tersebut. 

Gambar 4 Menu Absen

1. Menu Mata Kuliah

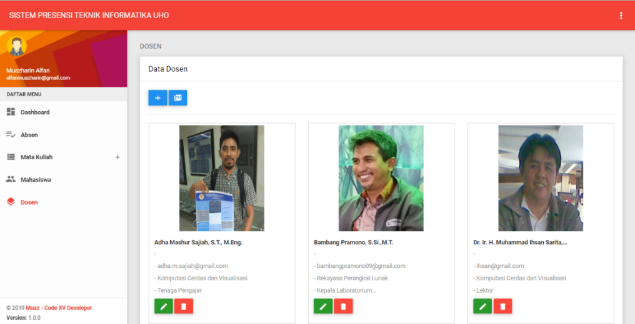
Menu mata kuliah berisi daftar mata kuliah yang terdapat pada jurusan Teknik Informatika UHO mulai dari semester 1 sampai semester 8.



Gambar 5 Menu Mata Kuliah

1. Menu Dosen

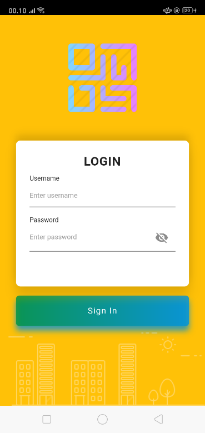
Menu dosen berisi data setiap dosen yang ada pada jurusan Teknik Informatika UHO. Terdapat pula foto dari masing data dosen agar lebih memudahkan dalam mencari data atau informasi tentang dosen.



Gambar 6 Menu Dosen

1. Login Mobile

Halaman login pada aplikasi *mobile* menampilkan *form login* yang terdiri dari *username* dan *password*. Setiap *field* harus diisi agar dapat melakukan *login.* Selain itu, *form* ini juga telah ditambahkan fungsi validasi agar dapat menyaring data *user* yang benar.

**

Gambar 8 Login Mobile

1. *Home Mobile*

Halaman home mobile menampilkan daftar semester 1 sampai 8.

**

Gambar 9 Home Mobile

1. Mata Kuliah Mobile

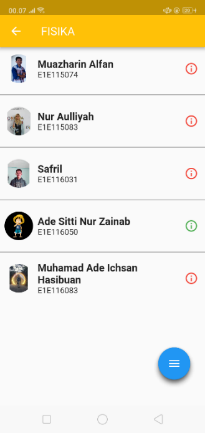
Halaman mata kuliah *mobile* menampilkan daftar mata kuliah pada semester dan kelas tertentu. Keterangan mata kuliah juga dicantumkan seperti jadwal dan nama ruangan perkuliahan.

**

Gambar 10 Tampilan *Menu* Pilihan Sumber Citra

1. Mahasiswa Mobile

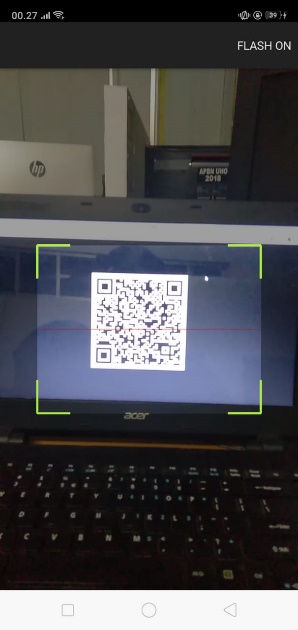
Berdasarkan gambar di atas, terlihat daftar mahasiswa yang mengambil mata kuliah FISIKA. Tercantum nama dan NIM mahasiswa tersebut dengan simbol informasi pada sisi kanan berwarna merah/hijau. Simbol ini menandakan tingkat persentase kehadiran mahasiswa. Jika berwarna merah, maka persentase kehadiran mahasiswa tersebut tidak mencapai 80% dan sebaliknya jika berwarna hijau maka persentase kehadiran mahasiswa tersebut mencapai 80% atau lebih.

**

Gambar 11 Mahasiswa Mobile

1. Scanner

Halaman *scanner* menampilkan alat *scanner* berupa kamera yang siap melakukan *scanning* terhadap *QR Code* yang ditemukan.



Gambar 12 Scanner

3.2 Pengujian Sistem

Pengujian merupakan tahap yang utama dalam pembuatan suatu aplikasi. Hasil dari pengujian yang didapat akan dijadikan sebagai tolak ukur dalam proses pengembangan selanjutnya.

1. Pengujian Black Box

Pengujian *black box* dilakukan dengan menguji perangkat lunak dari segi fungsionalitas perangkat lunak. Fungsionalitas perangkat lunak yang diuji sesuai dengan skenario pada tahap desain

Tabel 1. Pengujian Black Box

|  |  |  |
| --- | --- | --- |
| Input/Event | Output | Hasil Uji |
| Memilih menu dashboard | Menampilkan menu dashboard | Berhasil |
| Memilih menu absen | Menampilkan menu absen | Berhasil |
| Memilih menu mata kuliah | Menampilkan menu mata kuliah | Berhasil |
| Memilih menu dosen | Menampilkan menu dosen | Berhasil |
| Masuk ke halaman *home mobile* | Menampilkan halaman *home mobile* | Berhasil |
| Masuk ke halaman mata kuliah *mobile* | Menampilkan halaman mata kuliah *mobile* | Berhasil |
| Masuk ke halaman mahasiswa *mobile* | Menampilkan halaman mahasiswa *mobile* | Berhasil |
| Mengaktifkan scanner | Mengaktifkan kamera dan menampilkan alat scanner | Berhasil |

1. Pengujian Metode *RC4*

|  |  |  |  |
| --- | --- | --- | --- |
| No. | Sebelum Enkripsi | Kunci | Sesudah Enkripsi |
| 1. | E1E11996-11-0715074Raha | 15074 | F�6�� �ƥ�5��̶�҆m�� |
| 2. | E1E11997-10-2815001Kendari | 15001 | �}����:~P��n�������g�c |
| 3. | E1E11998-05-1815022Dili | 15022 | m�;\*��c�Ɍ�%,�޾�0�� |
| 4. | E1E11997-11-0715026Kendari | 15026 | \*J��>�~����v�>�J^���4a? |
| 5. | E1E11997-09-1815030Boloimbu | 15030 | ��q�d�e�����D�W�l"u� c�ݜTe |
| 6. | E1E11997-02-2815035Kendari | 15035 | �����Z��u�(DU��-��! ���� |
| 7. | E1E11997-04-0516010Tampo | 16010 | �n���U����RB� �v�c� |
| 8. | E1E11998-10-2816024Pondidaha | 16024 | ����|�-3l���XJ8�z‑����θ�� |
| 9. | E1E11997-05-0516026Lambubalano | 16026 | b�0]j��g�VT�G�P�q�Y�[j |
| 10. | E1E12000-06-1917027kendari | 17027 | v�XF�/S�{���� �w ��6�� |

1. Pengujian Aplikasi Pada Kelas

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| No. | Jumlah Kelas | Jumlah Mahasiswa | | Waktu | Rata-rata Kecepatan Scanning | | |
| 1. | 1 K | 20 | | 2 m 5 d | 6.25 d | | |
| 2. | 2 K | K1 | K2 | K1 | K2 | K1 | K2 |
| 20 | 23 | 2 m 13 d | 3 m 5 d | 6.65 d | 8.04 d |
| Rata-rata Kecepatan Scanning Setiap Mahasiswa | | | | | (6.25 d+ 6.65 d+ 8.04 d) / 3 = (20.94 d) / 3 = 6.93 d | | |

4. KESIMPULAN

Berdasarkan penelitian dan hasil pengujian yang dilakukan pada metode *Rivest Cipher 4,* maka disimpulkan sebagai berikut :

1. Algoritma *RC4* dapat diimplementasikan dalam mengamankan data *QR Code*.
2. Rata-rata proses scanning setiap mahasiswa berkisar antara 6-8 detik.
3. Proses scanning dan hasilyang dikeluarkan tergolong mudah untuk dipahami karena dapat digunakan pada *Smartphone*, serta membantu dalam mengamankan data pada aplikasi ini.
4. Saran

Saran yang dapat diberikan dalam pengembangan selanjutnya adalah sebagai berikut :

1. Menggunakan *RC4* termasuk ke dalam kriptografi simetris dan tergolong mudah untuk diimplementasikan dalam berbagai aplikasi.
2. Sistem ini dapat dikembangkan lagi dengan system keamanan yang lebih baik lagi.

DAFTAR PUSTAKA

[1] ADC, D. (2011). *QR Code ® Essentials*. 1–12.

[2] Ashford, R. (2016). *QR Codes and academic libraries: Reaching mobile users*. Retrieved from College and Research Libraries News: <https://crln.acrl.org/index.php/crlnews/article/view/8454/8696>

[3] ASWIN WIBISURYA, S. M. (2018). *Pengenalan QR Code*. Retrieved from School of Computer Science: <http://socs.binus.ac.id/2018/12/15/pengenalan-qr-code/>

[4] Jakfar. (2018). *Pengertian Autentikasi*. Retrieved from SCRIBD: <https://www.scribd.com/document/389239727/Pengertian-Autentikasi>

[5] Jumrin, Sutardi, & Subardin. (2016). Aplikasi sistem keamanan basis data dengan teknik kriptografi *RC4*. *SemanTIK*, *2*(1), 59–64.

[6] Kromodimoeljo, S. (2010). *Teori & aplikasi kriptografi*.

[7] Parmaza, B. (2015). *Mengenal Ilmu Kriptografi*. Retrieved from KomTIK Jambi: <http://itjambi.com/mengenal-ilmu-kriptografi/>

[8] qrcode.com. (n.d.). *What is a QR Code*. Retrieved from QRCode.com: <https://www.qrcode.com/en/>

[10] Saragih, U. S. (2017). *Implementasi enkripsi dan deskripsi dengan metode RC4 untuk pengaman data sistem informasi*.

[11] Sholeh, M. L., & Muharom, L. A. (2016). *SMART PRESENSI MENGGUNAKAN QR-*. *13*(2), 31–44.

[12] Zakaria, M. (2018). *Pengertian Data Beserta Fungsi Data dan Jenis-jenis Data yang Wajib Anda Ketahui*. Retrieved from Nesabamedia: <https://www.nesabamedia.com/pengertian-data/>