PENERAPAN KRIPTOGRAFI MENGGUNAKAN TEKNIK EKSPANSI DAN PERMUTASI UNTUK PENGAMANAN DOKUMEN

Andi Setiawan[1], Alex wijaya[2]
Fakultas Teknik Ilmu Komputer, Universitas Bina Darma
Email: Setiawanandy708@gmail.com[1], alex_wj@binadarma.ac.id[2]

ABSTRACT

The development of computer technology and computer networks, especially the internet, is very fast and has become one of the needs of most humans. The convenience provided by technology causes the transfer of information to be no longer limited, either by distance or time. Data security requires a way that can maintain confidentiality and security refers to the protection of information from the disclosure of unauthorized parties. One mechanism to improve data security is using an advanced encryption standard algorithm with cryptographic techniques. This research will use expansion and permutation techniques to secure data in the form of Microsoft word, pdf, jpeg files. It is hoped that confidential documents will be safe and not leaked to irresponsible eavesdroppers using the desktop. The test was carried out with 10 rounds of 6 different files.

Keywords: *advanced encryption standard, cryptography, application*

ABSTRAK

Perkembangan teknologi komputer dan jaringan komputer khususnya internet, sangatlah cepat dan telah menjadi salah satu kebutuhan dari sebagian besar manusia. Kemudahan yang diberikan teknologi menyebabkan perpindahan informasi tidak lagi dibatasi, baik oleh jarak maupun waktu. Keamanan data dibutuhkan sebuah cara yang dapat menjaga kerahasiaan dan keamanan merujuk pada perlindungan informasi dari penyingkapan pihak yang tidak sah. Salah satu mekanisme untuk meningkatkan keamanan data menggunakan algoritma *advanced encryption standard* dengan teknik kriptografi penelitian ini akan menggunakan teknik ekspansi dan permutasi untuk pengamankan data yang berupa file *microsoft word*, pdf, jpeg. Diharapkan dokumen rahasia akan aman dan tidak bocor kepada penyadap orang yang tidak bertanggung jawab dengan menggunakan desktop. Pengujian dilakukan dengan 10 kali putaran yang berjumlah 6 file yang berbeda.

Kata kunci: *advanced encryption standard,* kriptografi, aplikasi

1. PENDAHULUAN

Perkembangan teknologi dan jaringan komputer khususnya internet, sangatlah cepat dan telah menjadi salah satu kebutuhan dari sebagian besar manusia. PT. Fillah Group merupakan perusahaan yang bergerak dibidang perdagangan barang dan jasa serta general kontraktor, penyimpanan data pada perusahaan belum menggunakan pengamanan sehingga mudah dicuri dan disalah gunakan oleh pihak luar perusahaan atau pun orang yang tidak bertanggung jawab.

Dalam keamanan data yaitu permasalah sangat penting untuk perkembangan teknologi, sehingga dibutuhkan dengan cara mendapatkan menjaga kerahasiaan dan keamanan merujuk pada perlindungan informasi dari penyingkapan pihak yang tidak sah. Salah satu mekanisme untuk meningkatkan keamanan data adalah dengan menggunakan teknik kriptografi [1].

Kriptografi adalah studi yang bertujuan untuk mengamankan dan merahasiakan dengan melakukan proses enkripsi dan dekripsi pada data yang akan diamankan [2]. Ada berbagai macam algoritma dalam kriptografi salah satunya adalah *Algoritme Advance Encryption Standard*, data-data yang disimpan diubah sedemikian rupa sehingga tidak mudah dibaca [3]. Enkripsi adalah proses

yang dilakukan untuk merubah suatu informasi sehingga tidak dapat dibaca oleh orang yang tidak bertanggung jawab [4]. Sebaliknya, proses dekripsi merupakan suatu proses yang mengembalikan informasi yang sudah dienkripsi menjadi bisa dibaca kembali [5]

Algoritma AES akan dimodifikasi dengan meningkatkan jumlah putaran bersamaan dengan panjang kunci menjadi 320bit dengan 16 putaran dengan tujuan meningkatkan keamanan dari algoritma AES [6]. Pengujian dilakukan dengan membandingkan waktu proses enkripsi dan dekripsi antara algoritma AES standar 10 putaran dengan algoritma AES modifikasi 16 putaran File dokumen yang dapat dienkripsi hanya berupa file dengan format *pdf*, *docx*, dan *txt*. Hasil pengujian menunjukkan bahwa semakin besar putaran dan panjang kunci, maka semakin lama waktu yang digunakan dalam proses enkripsi maupun dekrips [7]i. Hal ini dapat dibuktikan dengan algoritma AES modifikasi yang memiliki nilai waktu proses lebih besar dibanding algoritma AES standar sehingga dapat disimpulkan algoritma AES modifikasi memiliki tingkat keamanan yang lebih tinggi karena berpengaruh pada waktu yang dibutuhkan seorang kriptoanalis untuk memecahkan kode enkripsi [8].

Data pada komputer yang tidak memiliki pengamanan akan mudah diakses oleh pihak lain, Permasalahan dalam PT. Fillah di karenakan mereka masih menggunakan pengarsipan dokumen rahasia yang masih manual sehingga tidak efesien dalam pengamanan dokumen rahasia sehingga pada penelitian yang berkaitan dengan aplikasi pengamanan data dilakukan oleh Andi Setiawan pada tahun 2019 dengan judul Penerapan kriptografi menggunakan teknik ekspansi dan permutasi untuk pengamanan dokumen pada PT.Fillah Group, bertujuan untuk mengamankan data pada komputer PT.Fillah Group agar tidak mudah diakses dan dicuri oleh pihak luar perusahaan. Permasalahan pengamanan data ini hanya dibuat dengan dekstop sehingga tidak dapat dijalankan pada smartphone android.

2. METODOLOGI PENELITIAN

2.1 Waktu dan Tempat penelitian

Waktu untuk penelitian ini melakukan penelitian selama 3 bulan yang di mulai pada bulan maret 2020. Tempat penelitian PT. FILLAH GROUP beralamat di jalan basuki rahmat RT.24 RW.09 NO.37, kecamatan kemuning, keluruhan pahlawan, kota Palembang, sumatera Selatan.

2.2 Alat dan Bahan

Perangkat keras (*Hardware*) yang digunakan ialah laptop *Asus Tuf Gaming* AMD RYZEN 5. Perangkat lunak yang digunakan ialah sistem operasi *windows*, dan aplikasi penunjang seperti Visual Studio. Bahan yang digunakan ialah beberapa dokumen berformat acak.

2.3 Metode Pengumpulan Data

Penulis ini melakukan beberapa cara untuk memperoleh data yang di butuhkan oleh penelitian tersebut:

a. Studi Literature

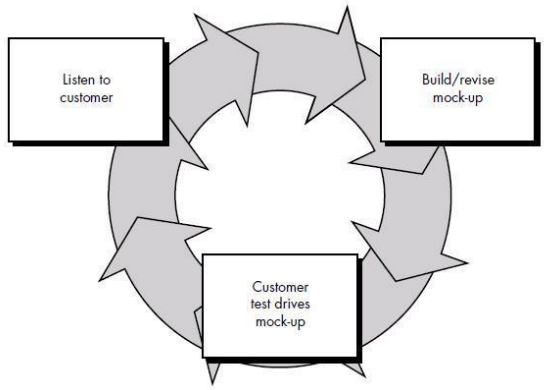
Pada penelitian untuk mencari sumber dan bahan, untuk mendukung dalam pendefinisian masalah konsep-konsep dasar yang landasi landasan teori penelitian untuk melakukan dalam penulisan penelitian ini melalui buku-buku, internet dan lain sebagainya yang erat kaitannya dengan objek permasalahan tersebut.

b. Pengumpulan dan data analisa

Berdasarkan penelitian ini melakukan pengumpulan dan analisa data yang berhubungan dengan penerapan kriptografi menggunakan teknik ekspansi dan permutasi untuk pengamanan dokumen menggunakan algoritma Aes.

2.4 Metode Pengembangan Aplikasi

Model *Prototyping* cocok digunakan untuk membantu pengembang dalam mengetahui kebutuhan pengguna secara detail tetapi memiliki resiko besar tehadap biaya pengembangan dan waktu pengerjaannya [9]. Dalam tahapan – tahapan metode *Prototyping* adalah sebagai berikut [10].



Gambar 1. Gambar *Prototyping*

a. Listen to customer (Mendengarkan Pelanggan)
"Pada tahap ini dilakukan pengumpulan kebutuhan dari sistem dengan cara mendengar keluhan dari pelanggan. Untuk membuat suatu sistem yang sesuai kebutuhan, maka harus diketahui terlebih dahulu bagaimana sistem yang sedang berjalan untuk kemudian mengetahui masalah yang terjadi."

b. Build/revise mock-up (Merancang dan Membuat Prototype)
"tahapan ini merupakan rancangan dalam membuat Prototyping *project*. Prototyping itu dibuat dengan kebutuhan *system* dalam didefinisikan sebelumnya dari keluhan pelanggan atau pengguna."

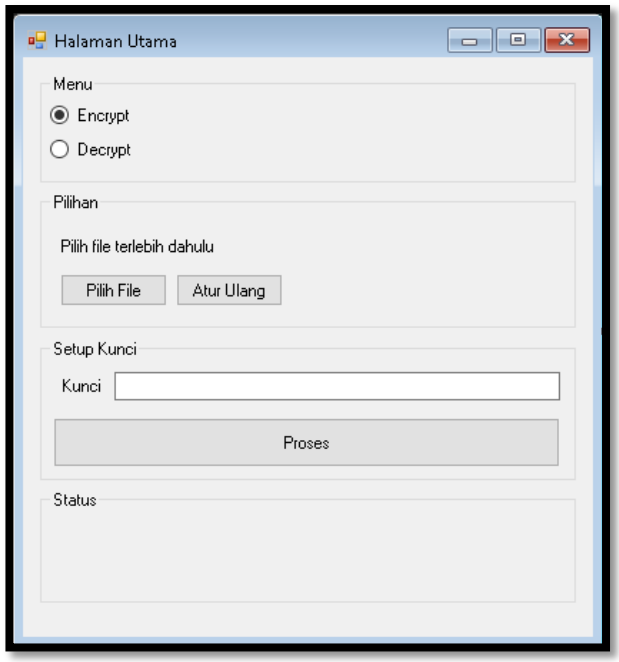
c. Customer test drives mock-up (Uji Coba)
"Pada tahap ini, Prototyping dari sistem di uji coba oleh pelanggan atau pengguna. Lalu dilakukan evaluasi kekurangan - kekurangan dari kebutuhan pelanggan. Pengembangan kemudian kembali mendengarkan keluhan dari pelanggan untuk memperbaiki Prototyping yang ada."

3. HASIL DAN PEMBAHASAN

Setelah melakukan pembahasan semua dalam tahapan pembuatan sistem pengamanan dokumen menggunakan metode *prototyping* yang diuraikan sebelumnya. Hasil berupa rancangan sistem ke sistem dalam nyata yang utuhnya sebenarnya dalam bentuk rekayasa sistem pengemanan data dokumen menggunakan teknik ekspansi dan permutasi menggunakan algoritma *Advanced Encryption Standard*. Dan sistem ini memasukan kata sandi jika user melaukan penginputan dokumen enkripsi dengan deskripsi kata sandi harus sama, apabila *user* lupa dengan kata sandi maka akses di sistem tidak dapat melakukan teknik permutasi. Untuk yang berbasis perangkat lunak dekstop untuk user melakukan permutasi atau pengamanan data dokumen. Dengan dibuatkan sistem aplikasi ini diharapkan dapat membantu perusahaan PT. Fillah Group untuk mempermudahkan pekerjaan mereka dalam melakukan pengamanan data penting di perusahaan mereka.

Hasil dari penelitian skripsi saya, penelitian ini sangat dituangkan dalam 1 bentuk, yaitu sistem pengamanan data dokumen teknik permutasi dan dekripsi yang berbasis perangkat lunak dekstop yang dapat diakses melalui komputer dalam bentuk untuk mempermudahkan karyawan dalam melakukan pengamanan data. Serta user dapat menginput dokumen yang ingin diamankan, serta pada aplikasi pengamanan dokumen user dapat melakukan input dokumen berupa pdf, doc,

image user melakukan penginputan kata sandi untuk dokumen supaya dokumen dengan aman. Dan untuk *source coding* menggunakan aplikasi *microsoft visual studio.*

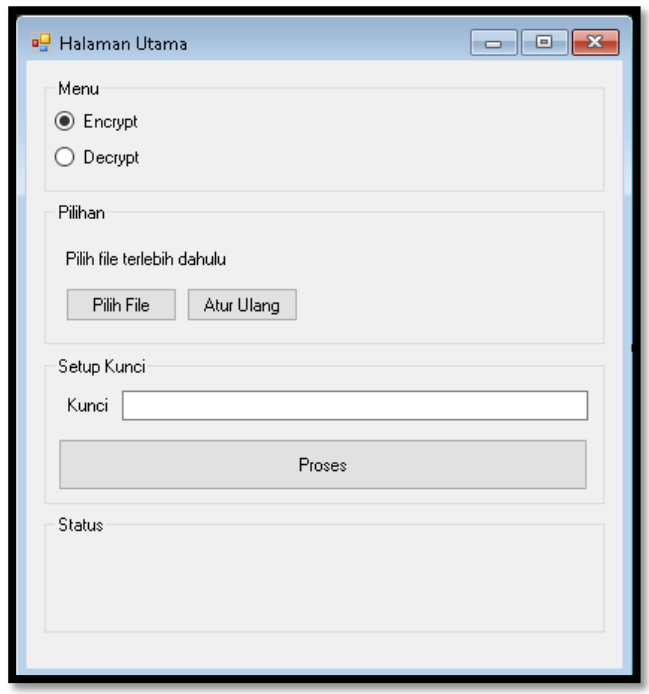


Gambar 2. Tampilan hasil aplikasi

Pada pembahasan ini akan membahas tentang sistem yang telah dibuat merupakan aplikasi yang terdiri dari perangkat desktop. Pada sistem ini user diminta untuk membuka aplikasi terlebih dahulu sebelum melakukan penginputan dokumen yang ingin diamankan. Pada sistem pengamanan data dokumen teknik ekspansi dan permutasi menggunakan algoritma *Advanced Encryption Standard* berbasis desktop.

3.1 Halaman menu utama

Pada menu utama ini, user dapat menggunakan 2 pilihan menu utama pada sistem perangkat lunak yaitu menu enkripsi dan menu dekripsi. Pada menu 2 itu digunakan untuk melakukan dalam pemilihan dokumen yang akan di inputkan untuk enkripsi dan dekripsi. Dimana pada menu pilihan file ada 2 buttom yaitu: pilih file dan atur ulang. setelah itu pada menu berikutnya ada menu setup kunci, dimana pengguna memasukan kata kunci. dan upload semua, pengguna melakukan proses, jika sudah melakukan proses akan muncul status di kolom seperti gambar 4.1 menu halaman utama.



Gambar 3. Menu halaman utama

3.2 Alur proses enkripsi

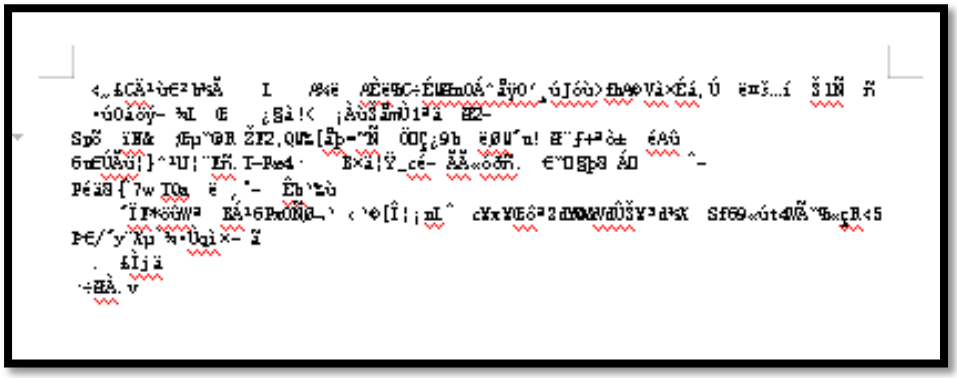
Pada *source coding* pemilihan file docx, pdf, dan jpeg, penulis melakukan alur dari proses jalananya file yang akan di enkripsi. jika sudah upload file nanti sistem akan memproses file dan akan muncul di bagian status jika file yang akan dienkripsi. Berikut adalah potongan *source coding* proses enkripsi.

```
if (rb_encrypt.Checked)
            {
                fileDialog.Title = "Pilih file yang ingin diencrypt";

                if (fileDialog.ShowDialog() == DialogResult.OK)
                {
                    lbl_output.Text = "File yang akan diencrypt " + fileDialog.FileName;
                    source_path = fileDialog.FileName;
                    file_extension = Path.GetExtension(fileDialog.FileName);
                    file_name= Path.GetFileNameWithoutExtension(fileDialog.FileName);
                    file_label.Text = source_path;
                }
```

Gambar 4. *Source coding* enkripsi

Pengujian ini penulis melakukan percobaan di microsoft word 2016 dengan ukuran 1.61 Mb. Pada tahapan enkripsi isi dokumen akan berubah menjadi tulisan yang sangat tidak bisa dibaca.



Gambar 5. Pengujian *microsoft word*

3.3 Alur proses dekripsi

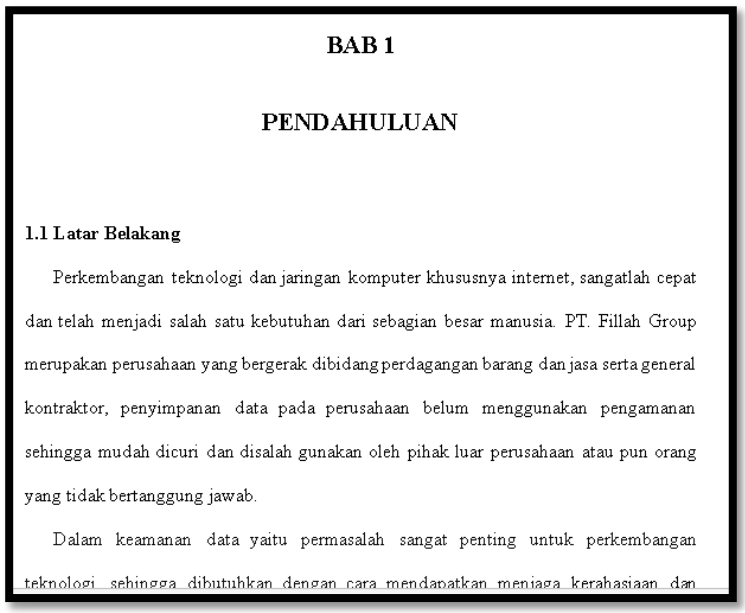
Pada halaman coding di Microsoft visual studio, untuk pemilihan file docx, pdf, jpeg penulis melakukan alur dari proses jalananya file yang di dekripsi. Aplikasi untuk membuat program menggunakan *microsoft visual studio*. jika sudah import file yang sudah di enkripsi nanti sistem akan memproses file akan muncul di bagian status jika file yang akan didekripsi. Berikut ini adalah potongan *source coding* proses dekripsi.

```
fileDialog.Title = "Pilih file yang ingin di decrypt";

                if (fileDialog.ShowDialog() == DialogResult.OK)
                {
                    lbl_output.Text = "File yang akan didecrypt " +
fileDialog.FileName;
                    source_path = fileDialog.FileName;
                    file_extension = Path.GetExtension
(fileDialog.FileName);
                    file_name = Path.GetFileNameWithoutExtension
(fileDialog.FileName);
                    file_label.Text = source_path;
                }
```

Gambar 6. Alur *source coding* dekripsi

Pengujian juga melakukan pengujian dekripsi di microsoft word 2016 dengan ukuran 1.61 MB, dan setelah dilakukan dekripsi pada dokumen tersebut, maka isi dokumen akan berubah menjadi tulisan seperti awal.



BAB 1

PENDAHULUAN

1.1 Latar Belakang

Perkembangan teknologi dan jaringan komputer khususnya internet, sangatlah cepat dan telah menjadi salah satu kebutuhan dari sebagian besar manusia. PT. Fillah Group merupakan perusahaan yang bergerak dibidang perdagangan barang dan jasa serta general kontraktor, penyimpanan data pada perusahaan belum menggunakan pengamanan sehingga mudah dicuri dan disalah gunakan oleh pihak luar perusahaan atau pun orang yang tidak bertanggung jawab.

Dalam keamanan data yaitu permasalah sangat penting untuk perkembangan teknologi sehingga dibutuhkan dengan cara mendapatkan menjaga kerahasiaan dan

Gambar 7. Pengujian dokumen dekripsi

3.4 Tampilan Notifikasi status proses enkripsi dan dekripsi berhasil

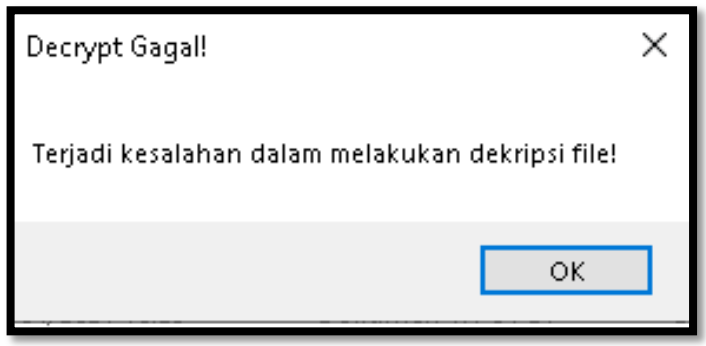
Berikut ini adalah tampilan dari menu notifikasi yang akan muncul pada saat sistem penginputan dokumen yang telah berhasil dalam melakukan proses. Dan akan tampil text seperti gambar 4.11 dan gambar 4.12.

Gambar 8. status enkripsi telah selesai

Gambar 9. status dekripsi telah selesai

3.5 Tampilan Notifikasi status yang gagal

Pada menu ini, notifikasi yang gagal dikarenakan user lupa dengan kata sandi jadi sistem tidak akan melanjutkan dalam melakukan proses dokumen yang ingin di enkripsi dan dekripsi.



Gambar 10. Notifikasi Error

3.6 Alur Proses Algoritma Aes

Alur dari algoritma aes ini merupakan algoritma untuk enkripsi, dekripsi dan di source coding dialgortima pada gambar 4.14 ada alur teknik ekspansi dan permuntasi, dimana algoritma ini untuk ekspansi untuk menambahkan kata dan untuk permuntasi merupakan posisinya di putar balik. Algoritma aes juga untuk mengamankan data dan memcahkan kata kunci. Pada tahap enkripsi adalah untuk mengubah plain text menjadi cipher text yang bertujuan untuk mengamankan data atau isi pesan yang bersifat rahasia agar tidak disadap oleh orang lain. Sedangkan untuk proses dekripsi merupakan kebalikannya dari proses enkripsi, untuk mengubah cipher text menjadi plain text. Dalam melakukan proses dekripsi, isi file yang berupa cipher text harus diubah kembali menjadi pesan atau file yang asli.berikut ini adalah potongan source coding alur proses algoritma.

```
SymmetricAlgorithm crypt = Aes.Create();
                        HashAlgorithm hash = MD5.Create();
                        crypt.BlockSize = BlockSize;

                        crypt.Key = hash.ComputeHash(Encoding.Unicode.GetBytes(tb_key.Text));
                        crypt.IV = IV;

                        try
                        {
                            using (MemoryStream memoryStream = new MemoryStream(source_file_bytes))
                            {
                                using (CryptoStream cryptoStream =
                                   new CryptoStream(memoryStream, crypt.CreateDecryptor(), CryptoStreamMode.Read))
                                {
                                    byte[] decryptedBytes = new byte[source_file_bytes.Length];
                                    cryptoStream.Read(decryptedBytes, 0, decryptedBytes.Length);
                                    File.WriteAllBytes(sf.FileName, decryptedBytes);
                                }
                            }

                            lbl_output.Text = "Dekripsi selesai ! File disimpan di " + sf.FileName;

                        } catch (Exception ex)
                        {
                            string title = "Decrypt Gagal!";
                            string message = "Terjadi kesalahan dalam melakukan dekripsi file!";
                            MessageBox.Show(message, title);

                            lbl_output.Text = "Dekripsi gagal karena kesalahan.";
                        }
                    }
                    stopwatch.Stop();
                    lblExecutionTime.Text = "Waktu proses : " + stopwatch.ElapsedMilliseconds + " ms";
                }
            } else
            {
                lbl_output.Text = "Permintaan tidak dapat diproses, Harap periksa kembali data yang harus diisi!";

                string title = "Peringatan!";
                string message = "Harap isi beberapa kolom yang kosong";
                MessageBox.Show(message, title);
            }
        }
```

Gambar 11. Algoritma aes proses

4. KESIMPULAN DAN SARAN

Aplikasi pengamanan data pesan teks yang berisi file dokumen docx, pdf, dan jpeg, dapat mengenkripsi dan mendekripsi dokumen. Aplikasi pengamanan dokumen berbasis desktop didukung menggunakan algoritma *advanced encryption standard* dan pendukung rancangan prototyping, sehingga dapat mempermudah perusahaan mengamankan dokumen yang bersifat rahasia. adapun saran yang berguna dalam melakukan pengembangan aplikasi ini sebagai berikut:

1) Diharapkan untuk pengembang selanjutnya, agar menambahkan fungsi enkripsi dan deskripsi yang berisi audio.
2) Untuk pengembang selanjutnya diharapkan menambahkan fitur di button desktop agar tidak terlihat sederhana
3) Dalam Memaksimalkan aplikasi ini, penelitian berikutnya diharapkan tidak hanya mengenkripsi dokumen Microsoft Office 2019 saja, tetapi dapat digunakan juga untuk Microsoft Office 2007 – 2020

DAFTAR PUSTAKA

[1] A. A. Permana, "Penerapan Kriptografi Pada Teks Pesan dengan Menggunakan Metode Vigenere Cipher Berbasis Android," *Jurnal AL-AZHAR INDONESIA SERI SAINS DAN TEKNOLOGI*, vol. 4, no. 3, pp. 110-115, 2018.

[2] Y. Yusfrizal, " Rancang Bangun Aplikasi Kriptografi Pada Teks Menggunakan Metode Reverse Chiper," *Jurnal Teknik Informatika Kaputama (JTIK)*, vol. 3, no. 2, p. 29–37, 2019.

[3] D. Q. P. A. Paramarta and et al, "Implementasi Algoritme Advance Encryption Standard (AES) pada Enkripsi dan Dekripsi QR-Code," *Jurnal Pengembangan Teknologi Informasi dan Ilmu Komputer*, vol. 2, no. 12, pp. 6729-6736, 2018.

[4] Ahyuna and et al, "Perancangan Aplikasi Enkripsi Menggunakan Algoritma AES Berbasis Android," in *Prosiding Seminar Nasional Komunikasi dan Informatika #3* , Makassar, 2019.

[5] R. V. H. Chandra and et al, "Analisis Performa Proses Enkripsi dan Dekripsi Menggunakan Algoritme AES-128 Pada Berbagai Format File," *Jurnal Pengembangan Teknologi Informasi dan Ilmu Komputer*, vol. 3, no. 1, pp. 481-486, 2019.

[6] E. B. H. Sibarani and et al, "ANALISIS KRIPTO SISTEM ALGORITMA AES DAN ELLIPTIC CURVE CRYPTOGRAPHY (ECC) UNTUK KEAMANAN DATA," *Jurnal Nasional Informatika dan Teknologi Informatika*, vol. 1, no. 2, pp. 106-112, 2017.

[7] D. Nurnaningsih and et al, "Rancangan Aplikasi Pengamanan Data Dengan Algoritma Advanced Encyption Standard (Aes)," *Jurnal Teknik Informatika*, vol. 11, no. 2, p. 177–186, 2018.

[8] A. Hermawan and et al, "Implementasi Enkripsi Data Menggunakan Kombinasi AES dan RSA," *InfoTekJar : Jurnal Nasional Informatika dan Teknologi Jaringan*, vol. 5, no. 2, pp. 325-330, 2021.

[9] S. Mulyani, Metode Analisis dan perancangan sistem, Bandung: Abdi Sistematika, Bandung: Abdi Sistematika, 2017.

[10] T. A. Kurniawan and et al, "PENERAPAN METODE PROTOTYPE DALAM PENGEMBANGAN SISTEM UNTUK PERANCANGAN APLIKASI WEB JASA RESTORASI PADA PT. QUANTUM NUSATAMA," *Jurnal Ilmiah Fakultas Teknik LIMIT'S,* vol. 13, no. 1, pp. 1-10, 2017.