INFOKOM : Jurnal Informasi dan Komputer
p-ISSN: 1978-6433
e-ISSN: xxxx-xxxx
Vol.16, No.1, Juli 2023, pp. 58 – 64

ALGORITMA AES128-CBC UNTUK ENKRIPSI DAN DESKRIPSI BERKAS DOKUMEN PT. XYZ

Yalson Cahaya Pratama*[1], Faisal Akbar[2], Wahyu Ariandi[3]
[1,2,3] *Program Studi Teknologi Informatika, Sekolah Tinggi Ilmu Komputer Poltek Cirebon, Indonesia*
*e-mail: *[1] yalsonnoor@outlook.co.id , [2] faisal.akbar@stikompoltek.ac.id , [3] wahyuariandi@mail.ugm.ac.id*

Abstrak

Keamanan pengiriman informasi dan data merupakan hal yang penting untuk mencegah kebocoran informasi dan jatuh ke tangan orang yang tidak bertanggung jawab. Metode untuk pengaman informasi dan data tersebut berupa *watermarking*, steganografi, kriptografi, dan tanda tangan digital. Sebagai perusahaan, PT. XYZ mempunyai data yang sangat penting untuk diamankan, dikarenakan perusahaan tersebut pernah kebobolan data berupa berkas (*file*) dokumen berupa *spreadsheet* yang di mana data tersebut diubah-ubah oleh orang yang iseng sehingga *file* tersebut tidak sesuai dengan laporan per periode oleh staf IT di sana.Sistem pengamanan berkas dokumen (*file*) yang dipakai adalah AES128-CBC, artinya algoritma AES *Advanced Encryption Standard* (AES) kunci sepanjang 128 *bit* dengan mode blok *Cipher Block Chaining* (CBC). AES128-CBC adalah salah satu mode blok *cipher* untuk AES di samping mode lainnya seperti ECB, OFB, CFB, CTR, dan XTS. Proses enkripsi dalam pengamanan AES-CBC dimulai dari proses CBC terlebih dahulu untuk mengacak masukan (*plaintext*) yang kemudian diproses dalam algoritma AES, dan proses dekripsinya merupakan kebalikan dari proses enkripsi yang di mana proses AES dilakukan terlebih dahulu dan kemudian hasil dekripsi AES tersebut diacak dalam proses CBC, yang proses tersebut merupakan hasil akhirnya. Diharapkan implementasi pengamanan *file* dokumen tersebut dapat memproteksi data dokumen yang dimiliki oleh PT. XYZ dari kebobolan dan perubahan isi oleh orang yang tidak bertanggung jawab.

Kata kunci : Kriptografi, AES, CBC, Berkas Dokumen Digital

1. PENDAHULUAN

Perkembangan teknologi komputer dan telekomunikasi dewasa ini telah mengalami kemajuan yang sangat pesat dan sudah menjadi suatu kebutuhan, dikarenakan banyaknya pekerjaan yang dapat diselesaikan dengan cepat, akurat, dan efisien. Sejalan dengan perkembangan teknologi yang sedang berkembang saat ini, semakin mengubah cara masyarakat dalam berkomunikasi. Dahulu komunikasi jarak jauh masih menggunakan cara yang konvensional dengan cara saling mengirim surat, tetapi sekarang komunikasi jarak jauh dapat dilakukan dengan mudah dan cepat dengan adanya teknologi seperti email, *Short Messaging Service* (SMS), dan internet yang merupakan salah satu teknologi telekomunikasi yang paling banyak digunakan saat ini. Internet telah membuat komunikasi semakin terbuka dan pertukaran informasi juga semakin cepat yang melewati batas-batas negara dan budaya. Namun tidak semua perkembangan teknologi komunikasi memberikan dampak yang positif dan menguntungkan. Salah satu dampak negatif dalam perkembangan teknologi adalah adanya penyadapan data, yang menjadikan salah satu masalah yang paling ditakuti oleh para pengguna jaringan komunikasi. Dengan adanya penyadapan data, maka aspek keamanan dalam pertukaran informasi dapat dianggap begitu penting, dikarenakan suatu komunikasi data jarak jauh belum tentu memiliki jalur transmisi yang aman dari penyadapan, sehingga keamanan informasi menjadi bagian penting dalam dunia informasi itu sendiri. Di dalam dunia informasi terdapat data-data yang tidak terlalu penting jadi jika publik mengetahui data tersebut pemilik data tidak terlalu dirugikan. Tetapi apabila pemilik data adalah pihak militer atau pihak pemerintah,

History of article:
Received: 27 Januari, 2023 : Accepted: 28 Januari, 2023

keamanan dalam pertukaran informasi menjadi sangatlah penting karena data yang mereka kirim adalah data-data rahasia yang tidak boleh diketahui oleh publik.

Sejarah yang panjang dari kriptografi. Penulisan rahasia 3000 tahun SM pada saat itu digunakan oleh bangsa Mesir. Mereka menggunakan hieroglyphcs untuk sembunyikan tulisan agar terhindar dari apapun yang tidak diharapkan. Hieroglyphcs diturunkan dari bahasa Yunani Hieroglyphica yang berarti ukiran rahasia. Hieroglyphs berevolusi menjadi hieratic, yaitu stylized script yang lebih mudah digunakan. Sekitar 400 SM, kriptografi militer digunakan oleh bangsa Spartan dalam bentuk sepotong papyrus atau perkamen dibungkus dengan sebuah batang kayu. Sistem ini disebut juga dengan Scytale [1], [2].

Kriptografi merupakan salah satu solusi atau metode pengamanan data yang tepat untuk menjaga kerahasiaan dan keaslian data, serta dapat meningkatkan aspek keamanan suatu data atau informasi. Metode ini bertujuan agar informasi yang bersifat rahasia dan dikirim melalui suatu jaringan, seperti LAN atau Internet, tidak dapat diketahui atau dimanfaatkan oleh orang atau pihak yang tidak berkepentingan. Kriptografi mendukung kebutuhan dua aspek keamanan informasi, yaitu perlindungan terhadap kerahasiaan data informasi dan perlindungan terhadap pemalsuan dan pengubahan informasi yang tidak diinginkan [3].

Kriptografi adalah ilmu ataupun seni yang mempelajari bagaimana membuat suatu pesan yang dikirim oleh pengirim dapat disampaikan kepada penerima dengan aman. Kriptografi merupakan bagian dari suatu cabang ilmu matematika yang disebut kriptologi (cryptologi). Kriptografi bertujuan menjaga kerahasiaan informasi yang terkadung dalam data sehingga informasi tersebut tidak dapat diketahui oleh pihak yang tidak sah. Perancang algoritma kriptografi disebut kriptografer [4], [5].

Kriptografi Simetris Kunci untuk enkripsi dan dekripsi yang sama merupakan konsep dasar dari kriptografi simetris. Istilah lainnya adalah private-key cryptography, secretkey cryptography, atau conventional cryptography. Dalam kriptografi kunci simetris, karena penerima dan pengirim pesan telah terlebih dahulu berbagi kunci sebelum pesan dikirim. Keamanan dari sistem ini terletak pada kerahasiaan kuncinya [6]. Perkembangan teknologi sangatlah berpengaruh terhadap keamanan data pada sebuah perusahaan untuk mencegah orang-orang yang tidak berwenang melihat dokumen tersebut.

PT. XYZ merupakan perusahaan Perseroan Terbatas (PT) yang salah satu produk yang dijual adalah pembuatan minuman kemasan. Permasalahan mengamankan sebuah data pada sebuah aplikasi merupakan tanggung jawab penyedia *software*. Oleh karena itu, perusahaan ini terus mengembangkan diri untuk menjaga kerahasiaan dan keamanan data dari setiap kliennya. Penelitian ini bertujuan melakukan pengujian untuk proses pengaman data yang dilakukan dengan menggunakan Algoritma Kriptografi yang mengadopsi sistem enkripsi dekripsi serta menggunakan metode *Advanced Encryption Standard* (AES-128).

Algoritma ini sangat aman untuk mengamankan dokumen yang akan dimasukan kedalam aplikasi, sehingga aplikasi ini dapat menjaga dan mengamankan data data tersebut. Metode *Advanced Encryption Standard* (AES-128) dipilih karena algoritma ini sangat aman dalam melindungi data karena memiliki Teknik enkripsi dekripsi panjang kunci 128-bit, sehingga kecil kemungkinan untuk seseorang membobol dokumen ini walaupun sudah menggunakan kompuer yang cepat.

Penelitian ini dilakukan untuk mengamankan berkas dokumen PT. XYZ dengan mengenkripsi-dekripsi isi berkas dokumen tersebut. Pengamanan data di perusahaan tersebut masih belum memadai, dan terjadi kebobolan data yang isinya dapat dirubah oleh orang yang tidak bertanggung jawab.

2. METODE PENELITIAN

Rational Unified Process (*RUP*) merupakan suatu metode pengembangan perangkat lunak yang *iterative* dan *incremental*, serta berfokus pada arsitektur. *RUP* dapat menangani risiko yang berhubungan dengan pengembangan kebutuhan sistem yang berdasarkan perubahan yang

diinginkan oleh klien. Untuk mengurangi risiko tersebut dilakukan dengan pengujian pada setiap akhir tahapan RUP, sehingga akan mudah melakukan perubahan sebelum mencapai tahap akhir [7].

UML merupakan salah satu *tool*/model untuk merancang pengembangan *software* yang berbasis *object-oriented*. *UML* sendiri juga memberikan standar penulisan sebuah sistem *blueprint*, yang meliputi konsep proses bisnis, penulisan kelas-kelas dalam bahasa program yang spesifik, skema *database*, dan komponen yang diperlukan dalam sistem *software* [8].

Diagram *use case* merupakan pemodelan untuk kelakuan sistem informasi yang akan dibangun. *Use case* mendeskripsikan sebuah interaksi antara satu atau lebih aktor dengan sistem informasi yang akan dibangun. *Use case* digunakan untuk mengetahui fungsi apa saja yang ada pada sebuah sistem informasi dan siapa saja yang berhak menggunakan fungsi-fungsi tersebut.

Diagram aktivitas atau *activity diagram* menggambarkan *workflow* (aliran kerja) atau aktivitas dari sebuah sistem atau proses bisnis atau menu yang ada pada perangkat lunak. Penekanan pada diagram aktivitas adalah menggambarkan aktivitas sistem atau aktivitas yang dapat dilakukan oleh sistem, bukan apa yang dilakukan aktor. *Class diagram* menggambarkan struktur sistem dari segi pendefinisian kelas-kelas yang akan dibuat untuk membangun sistem. Kelas juga memiliki apa yang dinamakan atribut dan metode atau operasi [9].

Keamanan pengiriman informasi dan data merupakan hal yang penting, apabila dalam pengiriman informasi tersebut bocor dan informasi atau data tersebut jatuh ke tangan orang yang tidak bertanggung jawab, maka akan berdampak besar kerugian materil dan imaterilnya. Penggunaan keamanan informasi ini ditujukan agar tidak dapat dicuri oleh orang asing yang tidak berkepentingan dalam informasi tersebut. Ada beberapa metode yang dapat dilakukan untuk mengamankan pesan atau berkas yaitu dengan menggunakan *watermarking*, steganografi, kriptografi dan tanda tangan digital [10].

Kriptografi merupakan salah satu studi yang bertujuan untuk mengamankan dan merahasiakan dengan melakukan proses enkripsi dan dekripsi pada data yang akan diamankan. Enkripsi merupakan suatu proses pengubahan data menjadi bentuk sandi yang tidak dipahami dan dibaca, sedangkan dekripsi merupakan proses pengembalian data dalam bentuk sandi ke dalam bentuk semula yang dapat dipahami dan memiliki makna [11].

AES merupakan salah satu algoritma kriptografi yang menjadi standar algoritma enkripsi kunci simetris pada saat ini. *Advanced Encryption Standard* (*AES*) dipublikasikan oleh *National Institute of Standard and Technology* (*NIST*) sebagai pengganti algoritma *DES* yang sudah berakhir masa penggunaannya pada tahun 2001. *Input* dan *output* dari algoritma *AES* terdiri dari urutan data sebesar 128 bit. Urutan data yang sudah terbentuk dalam satu kelompok 128 *bit* tersebut dinamakan juga sebagai blok data atau *plaintext* yang nantinya akan dienkripsi menjadi *ciphertext*. *Cipher key* dari *AES* terdiri dari *key* dengan panjang 128 bit, 192 bit, atau 256 bit. Perbedaan panjang kunci akan mempengaruhi jumlah *round* yang akan diimplementasikan pada algoritma *AES* [12].

CBC sendiri merupakan salah satu mode operasi dalam mode-mode operasi pada blok *cipher* selain *Electronic Codebook* (*ECB*), *Cipher Feedback* (*CFB*), *Output Feedback* (*OFB*), *Galois*/*counter* (*GCM*), *Liskov*, *Rivest*, and *Wagner* (*LRW*), dan *Xor–Encrypt–Xor* (*XEX*). Mode *CBC* yang dipatenkan oleh William Friedrich Ehrsam, Carl H. W. Meyer, John Lynn Smith, dan Leonard Tuchman pada tanggal 26 April 1976 ini merupakan salah satu mode yang di mana pada enkripsi, blok *plaintext* XOR dengan suatu nilai variabel yang bernama vektor inisialisasi (IV), dan hasil *ciphertext* dijadikan IV untuk blok berikutnya. Dan pada dekripsi, IV XOR dengan "calon" *plaintext* untuk menghasilkan *plaintext* murni.

Lebih lengkapnya pada proses enkripsi, yang pertama memerlukan IV atau sering disebut *cipher* awal (C_0) dimana Jumlah *bit* C_0 harus sama dengan jumlah *bit* kunci. Biner *cipher* yang dihasilkan dari setiap blok dipindahkan (*shift*) sebesar n-*bit* ke kanan atau kiri, kemudian melakukan proses enkripsi pada setiap blok n-*bit plaintext* yang di-XOR-kan dengan blok n-*bit ciphertext* sebelumnya [13], [14].

3. HASIL DAN PEMBAHASAN

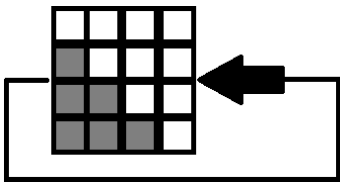
Pertama yang dilakukan adalah melakukan pengujian metode dengan cara dan hasil sebagai berikut: menentukan *plaintext*, kunci, dan IV. Masing-masing merupakan YalsonNP17620TI2, STIKOMPOLTEKCRBN, dan KriptoAES128-CBC. Selanjutnya mengubah nilai *plaintext*, kunci, dan IV di atas ke dalam bentuk heksadesimal, yaitu: 59616C736F6E4E503137363230544932, 5354494B4F4D504F4C54454B4352424E, dan 4B726970746F4145533132382D434243 dan kemudian melakukan tahap CBC, dengan XOR nilai heksadesimal *plaintext* dan IV, sehingga menghasilkan *plaintext*CBC, yaitu 59616C736F6E4E503137363230544932⊕4B726970746F4145533132382D434243 = 121305031B010F156206040A1D170B71.

Setelah itu, melakukan penjadwalan nilai heksadesimal kunci dengan mengambil setiap 8 nilai heksadesimal yang terakhir pada kunci. Dalam pengujian ini yang diambil adalah nilai heksadesimal 4352424E, kemudian digeser ke sebelah kiri sekali, sehingga menghasilkan 52424E43. Kemudian hasil di atas diganti dengan konstanta Rijndael S-BOX dan menghasilkan 002C2F1A. Selanjutnya hasil di atas dilakukan XOR dengan konstanta penjadwalan ekspansi kunci AES yang sesuai panjang *bit* dengan perhitungan, yaitu: 002C2F1A⊕01000000 = 012C2F1A. Lalu hasil di atas di XOR dengan 8 nilai heksadesimal pertama pada kunci dengan perhitungannya, yaitu 5354494B⊕012C2F1A = 52786651. Hasil ini di XOR dengan 8 nilai heksadesimal kedua pada kunci 4F4D504F⊕52786651 = 1D35361E. Selanjutnya hasil di atas di XOR Kembali dengan 8 nilai heksadesimal ketiga pada kunci 4C54454B⊕1D35361E = 51617355. Kemudian hasil di atas di XOR dengan 8 nilai heksadesimal keempat (terakhir) 4352424E⊕51617355 = 51617355. Kemudian hasil ini di XOR sebelumnya digabung, sehingga kunci ronde 1 yang dihasilkan adalah 527866511D35361E516173551233311B. Ulangi sampai 10 kali yang dimana kunci ronde 10 adalah DAC9B7BB6C655C9E55ECD05E540D117B untuk sebagai kunci ronde 1 pada proses dekripsi.

Pada tahapan *AES*, yang pertama dilakukan adalah *AddRoundKey*, dengan XOR nilai heksadesimal *plaintext*CBC bersama dengan nilai heksadesimal kunci tersebut 121305031B010F156206040A1D170B71⊕5354494B4F4D504F4C54454B4352424E = 41474C48544C5F5A2E5241415E45493F, sedangkan pada tahapan *SubBytes*, yaitu menukar hasil tahap *AddRoundKey* sebelumnya dengan konstanta Rijndael S-BOX, sehingga menghasilkan 83A029522029CFBE31008383586E3B75.

Pada tahapan *ShiftRows*, yaitu menggeser nilai ke sebelah kiri sekali (pada baris kedua), dua kali (pada baris ketiga), dan tiga kali (pada baris keempat). Hasilnya dapat ditunjukkan dengan matriks di bawah ini:

$$\begin{bmatrix} 83 & 20 & 31 & 58 \\ A0 & 29 & 00 & 6E \\ 29 & CF & 83 & 3B \\ 52 & BE & 83 & 75 \end{bmatrix}$$



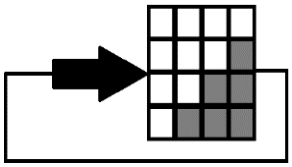
$$\begin{bmatrix} 83 & 20 & 31 & 58 \\ 29 & 00 & 6E & A0 \\ 83 & 3B & 29 & CF \\ 75 & 52 & BE & 83 \end{bmatrix}$$

Pada tahapan *InverseMixColumns*, sama dengan tahap *MixColumns* pada enkripsi, akan tetapi dengan nilai konstanta yang berbeda dan hasil perhitungannya sebagai berikut:

$$\begin{bmatrix} 0E & 0B & 0D & 09 \\ 09 & 0E & 0B & 0D \\ 0D & 09 & 0E & 0B \\ 0B & 0D & 09 & 0E \end{bmatrix} \begin{bmatrix} 41 & EF & 47 & 73 \\ C4 & 6C & 52 & 35 \\ 66 & 6D & C4 & 05 \\ 5B & 3F & F7 & DC \end{bmatrix} = \begin{bmatrix} C3 & CF & 5A & 37 \\ DE & 3A & CA & D7 \\ 8F & F4 & 95 & 64 \\ 2A & D0 & 23 & 1B \end{bmatrix}$$

Pada tahapan *InverseShiftRows* dan tahapan *InverseSubBytes* dengan hasil sebagai berikut:

$$\begin{bmatrix} C3 & CF & 5A & 37 \\ DE & 3A & CA & D7 \\ 8F & F4 & 95 & 64 \\ 2A & D0 & 23 & 1B \end{bmatrix}$$



$$\begin{bmatrix} C3 & CF & 5A & 37 \\ D7 & DE & 3A & CA \\ 95 & 64 & 8F & F4 \\ D0 & 23 & 1B & 2A \end{bmatrix} \text{ dan } \begin{bmatrix} 33 & 5F & 46 & B2 \\ 0D & 9C & A2 & 10 \\ AD & 8C & 73 & BA \\ 60 & 32 & 44 & 95 \end{bmatrix}$$

Selanjutnya proses diulangi sampai ronde ke 10 dan menghasilkan nilai heksadesimal 121305031B010F156206040A1D170B71. Kemudian masuk tahap CBC, yaitu XOR nilai heksadesimal ronde yang ke 10 di atas dengan IV, perhitungan yang dihasilkan adalah: 121305031B010F156206040A1D170B71⊕4B726970746F4145533132382D434243 = 59616C736F6E4E503137363230544932. Pada tahap akhir adalah mengubah hasil nilai heksadesimal di atas ke dalam ASCII dang menghasilkan YalsonNP17620TI2.

Ada beberapa sampel *file* berbagai format digunakan dalam pengujian ini dan hasilnya adalah: bentuk .docx ukuran asli 553793 *bytes*, dienkripsi ukurannya 658105 *bytes* dengan perbedaan 0.19% lebih besar dari aslinya, didekripsi ukurannya 320714 *bytes* dengan perbedaan 0.06% lebih kecil dari *file* enkripsinya, dengan perbedaan dekripsi 0.42% lebih kecil dari aslinya. Selanjutnya bentuk .xlsx ukuran asli 156553 *bytes*, dienkripsi ukurannya 2290199 *bytes* dengan perbedaan 13.64% lebih besar dari aslinya, didekripsi ukurannya 544358 *bytes* dengan perbedaan 0.76% lebih kecil dari *file* enkripsinya, dengan perbedaan dekripsi 2.48% lebih besar dari aslinya dan bentuk .pptx ukuran asli 1653505 *bytes*, dienkripsi ukurannya 16289608 *bytes* dengan perbedaan 8.85% lebih besar dari aslinya, didekripsi ukurannya 1653505 *bytes* dengan perbedaan 0.90% lebih kecil dari *file* enkripsinya, dengan perbedaan dekripsi 0% alias sama ukurannya dengan aslinya.

4. KESIMPULAN

Berdasarkan hasil penelitian yang telah dilakukan dimulai dari penentuan pokok permasalahan, melakukan analisis sistem sampai pengimplementasian algoritma AES128-CBC untuk pengamanan pada berkas dokumen dapat disimpulkan bahwa semua karakter yang diproses dapat dienkripsi dan didekripsi dengan baik dengan menggunakan algoritma AES128-CBC, dikarenakan *ciphertext* hasil enkripsi dapat dikembalikan menjadi *plaintext* ataupun berkas dokumen asli tanpa mengalami kerusakan data seperti perubahan, pengurangan ataupun penambahan karakter, pengimplementasian algoritma AES128-CBC telah berhasil mengamankan berkas dokumen dikarenakan berkas dokumen yang tersimpan pada *database* adalah dokumen hasil enkripsi dari algoritma AES128-CBC, dan algoritma AES128-CBC ini memberikan keamanan berlapis untuk mengamankan dokumen dikarenakan pada proses enkripsi maupun dekripsi berkas dokumen. Isi berkas dokumen akan mengalami 10 kali proses pengamanan data dengan setiap 1 kali proses mengalami 4 transformasi data sebelum disimpan ke dalam *database* atau ditampilkan pada suatu program.

DAFTAR PUSTAKA

[1] E. S. Han and A. goleman, daniel; boyatzis, Richard; Mckee, “Peranan Kriptografi Sebagai Keamanan Sistem Informasi Pada Usaha Kecil Dan Menengah,” J. Chem. Inf. Model., vol. 53, no. 9, p. 2, 2019.

[2] M. Azhari, D. I. Mulyana, F. J. Perwitosari, and F. Ali, “Jurnal Pendidikan Sains dan Komputer Implementasi Pengamanan Data pada Dokumen Menggunakan Algoritma Kriptografi Advanced Encryption Standard (AES) Jurnal Pendidikan Sains dan Komputer,” vol. 2, no. 1, pp. 163–171, 2022.

[3] A. Eka Putri, A. Kartikadewi, and L. A. Abdul Rosyid, “Implementasi Kriptografi dengan Algoritma Advanced Encryption Standard (AES) 128 Bit dan Steganografi menggunakan Metode End of File (EOF) Berbasis Java Desktop pada Dinas Pendidikan Kabupaten Tangerang,” Appl. Inf. Syst. Manag., vol. 3, no. 2, pp. 69–78, 2021, doi: 10.15408/aism.v3i2.14722.

[4] I. A. R. Simbolon, I. Gunawan, I. O. Kirana, R. Dewi, and S. Solikhun, “Penerapan Algoritma AES 128-Bit dalam Pengamanan Data Kependudukan pada Dinas Dukcapil Kota Pematangsiantar,” J. Comput. Syst. Informatics, vol. 1, no. 2, pp. 54–60, 2020.

[5] S. Benyamin, E. Ahadi, D. P. S. Manrung, and I. Gunawan, “Pengamanan Pesan Teks Menggunakan Kriptofrafi Algoritma Vigenere Chiper Dari Serangan Eavesdropping,” J. Tek. Inform. Kaputama, vol. 4, no. 1, pp. 35–40, 2020.

[6] R. Firmansyah, “Implementasi Keamanan Pesan Teks Menggunakan Kriptografi Algoritma Rsa Dengan Metode Waterfall Berbasis Java,” Joutica, vol. 4, no. 1, p. 174, 2019, doi: 10.30736/jti.v4i1.265.

[7] R. Perwitasari, R. Afwani and S. E. Anjarwani, "PENERAPAN METODE RATIONAL UNIFIED PROCESS (RUP) DALAM PENGEMBANGAN SISTEM INFORMASI MEDICAL CHECK UP PADA CITRA MEDICAL CENTRE," *Jurnal Teknologi Informasi, Komputer dan Aplikasinya*, vol. 2, no. 1, pp. 76-88, 2020.

[8] F. Sonata and V. W. Sari, "Pemanfaatan UML (Unified Modeling Language) Dalam Perancangan Sistem Informasi E-Commerce Jenis Customer-To-Customer," *Jurnal Komunikasi, Media dan Informatika*, vol. 8, no. 1, pp. 22-31, 2019.

[9] J. Simatupang and S. Sianturi, "PERANCANGAN SISTEM INFORMASI PEMESANAN TIKET BUS PADA PO. HANDOYO BERBASIS ONLINE," *Jurnal Intra-Tech*, vol. 3, no. 2, pp. 11-25, 2019.

[10] D. Darwis, R. Prabowo and N. Hotimah, "Kombinasi GIFSHUFFLE, Enkripsi AES dan Kompresi Data huffman Untuk Meningkatkan Keamanan Data," *Jurnal Teknologi Informasi dan Ilmu Komputer*, vol. 5, no. 4, p. 389, 2018.

[11] M. I. Zulfikar, G. Abdillah and A. Komarudin, "Kriptografi untuk Keamanan Pengiriman," in *Seminar Nasional Aplikasi Teknologi Informasi (SNATI)*, Yogyakarta, 2019.

[12] F. Muharram, H. Azis and A. R. Manga', "Analisis Algoritma pada Proses Enkripsi dan Dekripsi File Menggunakan Advanced Encryption Standard (AES)," *Prosiding Seminar Nasional Ilmu Komputer dan Teknologi Informasi,* vol. 3, no. 2, pp. 112-115, 2018.

[13] D. Lombu, S. D. Tarihoran and I. Gulo, "Kombinasi Mode Cipher Block Chaining Dengan Algoritma Triangle Chain Cipher Pada Penyandian Login Website," *Jurnal Sains Komputer & Informatika (J-SAKTI),* vol. 2, no. 1, pp. 1-11, 2018.

[14] A. A. Permana and D. Nurnaningsih, "RANCANGAN APLIKASI PENGAMANAN DATA DENGAN ALGORITMA ADVANCED ENCYPTION STANDARD (AES)," *JURNAL TEKNIK INFORMATIKA,* vol. 11, no. 2, pp. 177-186, 2018.