DAFTAR PUSTAKA

Angriani, H., & Saharaeni, Y. (2019). Implementasi Algoritma Caesar Cipher pada Keamanan Data Sistem e-voting Pemilihan Ketua Organisasi Kemahasiswaan. *Inspiration: Jurnal Teknologi Informasi Dan Komunikasi*, *9*(2), 123. https://doi.org/10.35585/inspir.v9i2.2499

Cecep Kurnia Sastradipraja, & Munawar, Z. (2002). *Konsep Dasar Teknologi Web*.

Chafid, N., & Soffiana, H. (2022). Impelementasi Algoritma Kriptografi Klasik Caesar Untuk Rancang Bangun Aplikasi E-Voting Berbasis Web (Studi Kasus : Sman 10 Tangerang). *Jurnal Ilmiah Sains Dan Teknologi*, *6*(2), 133–145. https://doi.org/10.47080/saintek.v6i2.2249

Dony Ariyus. (2008). *Pengantar Ilmu Kriptografi : Teori Analisis & Implementasi*. 345. https://books.google.co.id/books?id=3SSTJONEmX0C&lpg=PP1&hl=id&pg=PP1#v=onepage&q&f=false

García-Zamora, C., Rodríguez-Henríquez, F., & Ortiz-Arroyo, D. (2005). SELES: An e-voting system for medium scale online elections. *Proceedings of the Mexican International Conference on Computer Science, 2005*, 50–57. https://doi.org/10.1109/ENC.2005.40

Ibrahim, A. A. (2017). *Perancangan Pengamanan Data Menggunakan Algoritma AES (Advanced Encyption Standard)*. *III*(1), 53–60.

Lingkup, R., Untuk, K., & Data, M. (2004). *Ruang Lingkup Kriptografi*. *IX*(2).

Menezes, A. J., Oorschot, P. C. van, & Vanstone, S. A. (1996). Applied Cryptography. *Electrical Engineering*, *1*([32), 429–455. https://doi.org/10.1.1.99.2838

Purbo, W, O., & Wahyudi, A. A. (2000). *Mengenal eCommerce*. Elex Media Komputindo.

Sakur, S. B. (2004). *Aplikasi web database dengan dreamweaver MX 2004 (versi Mysql dan PHP)*.

Simarmata, J., Sriadhi, & Rahim, R. (2019). *Kriptografi Teknik Keamanan Data & Informasi*.

Zafar, C. N., & Pilkjaer, A. (2007). E-Voting in Pakistan. *Systems Science*, 111.

Indrawanti, A. S., Azinar, A. W., & Firdiansyah, M. A. (2018). SECURE E-VOTING MENGGUNAKAN METODE RSA DAN AUTENTIKASI RFID. *Network Engineering Research Operation*, *4*(1), 67-75.

Hardjaloka, L., & Simarmata, V. M. (2016). E-voting: Kebutuhan vs. kesiapan (menyongsong) e-demokrasi. *Jurnal Konstitusi*, *8*(4), 579-604.

Irawan, C., Rachmawanto, E. H., Sari, C. A., & Sugianto, C. A. (2021, February). SUPER ENKRIPSI FILE DOKUMEN MENGGUNAKAN BEAUFORT CIPHER DAN TRANSPOSISI KOLOM. In *PROSIDING SEMINAR NASIONAL LPPM UMP* (pp. 556-563).

Nuraeni, F., & Agustin, Y. H. (2020). The IMPLEMENTASI CAESAR CIPHER & ADVANCED ENCRYPTION STANDAR (AES) PADA PENGAMANAN DATA PAJAK BUMI BANGUNAN. *Jurnal Ilmiah MATRIK*, *22*(2), 187-194.

Rachmat, N., & Samsuryadi, S. (2017, November). Studi Awal Penggunaan Algoritma C4. 5 dan Logika Fuzzy pada Klasifikasi Enkripsi Transaksi Keuangan Bebasis XML. In *Annual Research Seminar (ARS)* (Vol. 3, No. 1, pp. 255-260).

Marsal, R. U., Arnia, F., & Adriman, R. (2018). Enkripsi dan Dekripsi Citra Menggunakan Modifikasi Algoritma Vigenere Cipher. *Jurnal Komputer, Informasi Teknologi, dan Elektro*, *3*(3).

Ibrahim, A. A. (2017). Perancangan Pengamanan Data Menggunakan Algoritma AES (Advanced Encyption Standard). *Jurnal Teknik Informatika*, *3*(1), 53-60.

SASKARA, G. A. J. DESAIN DAN IMPLEMENTASI DETEKSI KERANDOMAN ALGORITMA KRIPTOGRAFI MENGGUNAKAN ALGORITMA CHAOS.

Sikumbang, A. H., Haryanto, E. V., & Saleh, A. (2020). Kombinasi Metode Stream Cipher Dan Caesar Cipher Dalam Pengamanan Data Kredit Customer (Studi Kasus: PT. ACE HARDWARE). *Jurnal Mahasiswa Fakultas Teknik dan Ilmu Komputer*, *1*(1), 693-706.

Syam, F. A., Darmayunata, Y., & Afriansyah, A. (2019). Perancangan Sistem E-Voting Untuk Pemilihan Ketua OSIS SMP Negeri 10 Pekanbaru. *ZONAsi:*

Jurnal Sistem Informasi, *1*(2), 75-85.

Subagio, N., Sari, W. E., & Yulianto, Y. (2020). Perancangan Sistem E-voting berbasis Web untuk Ketua Himpunan Mahasiswa Teknologi Rekayasa Perangkat Lunak. *Buletin Poltanesa*, *21*(2), 42-49.

Istiqamah, N., & Subiyanto, S. (2016). Sistem Keamanan E-Voting Menggunakan Fungsi Hash dan Algoritma One Time Pad. *Edu Komputika Journal*, *3*(1), 11-11.

Santoso, K. I., & Priyoatmoko, W. (2016). Pengamanan Data Mysql pada E-Commerce dengan Algoritma AES 256. SESINDO 2016, 2016.

Widodo, M. A. A., Thasandra, M., Sutra, S. O., Nasution, A. B., & Ikhwan, A. (2023). Pemanfaatan Kriptografi dalam Mewujudkan Keamanan Informasi pada E-Voting di Kota Medan dengan Menggunakan Algoritma AES. Journal on Education, 5(3), 6780-6787.

Permadi, R. B. (2014). SISTEM E-VOTING MENGGUNAKAN PROTOKOL TWO CENTRAL FACILITIES DENGAN MENGGABUNGKAN ALGORITMA AES DAN RSA SEBAGAI KOMBINASI KEAMANAN (Doctoral dissertation, Universitas Pendidikan Indonesia).

Darwis, D., Wamiliana, W., & Junaidi, A. (2017). Proses Pengamanan Data Menggunakan Kombinasi Metode Kriptografi Data Encryption Standard dan Steganografi End Of File. In Prosiding Seminar Nasional METODE KUANTITATIF 2017 (Vol. 1, No. 1, pp. 228-240). Jurusan Matematika FMIPA Unila.

Bhaudhayana, G. W., & Widiartha, I. M. (2015). Implementasi algoritma kriptografi aes 256 dan metode steganografi lsb pada gambar bitmap. J. Ilmu Komput, 8(2), 15-25.

Sadewa, T. (2015). Enkripsi Citra Digital Yang Mengandung Pesan Teks Menggunakan Metode Hill Cipher (Doctoral dissertation, Universitas Brawijaya).

LAMPIRAN

Cek Login

```php
<?php

session_start();
require_once('conf/conf.php');
require_once('libs/aes-encrypt/function.php');
header("Access-Control-Allow-Origin: *");
$username = isset($_POST["username"]) ? $_POST["username"] : null;
$pass = isset($_POST["password"]) ? $_POST["password"] : null;
$chiper_past_post = Encipher($pass, 12);

// pastikan username dan password adalah berupa huruf atau angka.
$user = fetch_array(bukaquery("SELECT data_user.id_user,
data_user.nama, data_user.instansi, user.akses,
AES_DECRYPT(user.password,'tangguhbencana!!') as key_pass
FROM data_user INNER JOIN user ON user.id_user=data_user.id_user
WHERE user.username='$username' AND user.password =
AES_ENCRYPT('$chiper_past_post','tangguhbencana!!')"));
$cekUser = isset($user['id_user']) ? $user['id_user'] : '';
// Apabila username dan password ditemukan
if (isset($_POST['csrf_token'])) {
    if (!empty($cekUser)) {
        if (cek_csrf_token($_POST['csrf_token'] == true)) {
            if ($chiper_past_post == $user['key_pass']) {
                $_SESSION['csrf_token'] = $_POST['csrf_token'];
                $_SESSION['userid'] = $user['id_user'];
                $_SESSION['instansi'] = $user['instansi'];
                $_SESSION['nama_user'] = $user['nama'];
                $_SESSION['akses'] = $user['akses'];
                $results = array(
                    "state" => 'success',
                    "token" => "" .
paramEncrypt('page=home&act=dashboard')
                );
                echo json_encode($results);
            } else {
                echo json_encode(array("state" => 'error',
"massage" => 'Not Allowed Origin, Invalid Access !!'));
            }
        } else {
            echo json_encode(array("state" => 'error', "massage"
=> 'Not Allowed Origin, Invalid Access !!'));
```

```
        }
    } else {
        unset($_SESSION['csrf_token']);
        echo json_encode(array("state" => 'error', "massage" =>
'Username dan Password Invalid !!! '));
    }
} else {
    unset($_SESSION['csrf_token']);
    header('location:login');
}
```

AES

```
public function __construct($strength = self::AES128)
    {
        switch ($strength) {
            case self::AES256:
                $this->key_size = 8;
                $this->block_size = 4;
                $this->number_of_rounds = 14;
                break;
            case self::AES192:
                $this->key_size = 6;
                $this->block_size = 4;
                $this->number_of_rounds = 12;
                break;
            case self::AES128:
            default:
                $this->key_size = 4;
                $this->block_size = 4;
                $this->number_of_rounds = 10;
                break;
        }
        $this->createSBox();
        $this->createInvertedSBox();
        $this->createRoundConstants();
        $this->createLogarithmicArray();
        $this->createExpotecialArray();
        $this->state = array();
    }

private function createSBox()
    {
        $this->s_box = array(
```

```
            0x63, 0x7C, 0x77, 0x7B, 0xF2, 0x6B, 0x6F, 0xC5, 0x30,
0x01, 0x67, 0x2B, 0xFE, 0xD7, 0xAB, 0x76,
            0xCA, 0x82, 0xC9, 0x7D, 0xFA, 0x59, 0x47, 0xF0, 0xAD,
0xD4, 0xA2, 0xAF, 0x9C, 0xA4, 0x72, 0xC0,
            0xB7, 0xFD, 0x93, 0x26, 0x36, 0x3F, 0xF7, 0xCC, 0x34,
0xA5, 0xE5, 0xF1, 0x71, 0xD8, 0x31, 0x15,
            0x04, 0xC7, 0x23, 0xC3, 0x18, 0x96, 0x05, 0x9A, 0x07,
0x12, 0x80, 0xE2, 0xEB, 0x27, 0xB2, 0x75,
            0x09, 0x83, 0x2C, 0x1A, 0x1B, 0x6E, 0x5A, 0xA0, 0x52,
0x3B, 0xD6, 0xB3, 0x29, 0xE3, 0x2F, 0x84,
            0x53, 0xD1, 0x00, 0xED, 0x20, 0xFC, 0xB1, 0x5B, 0x6A,
0xCB, 0xBE, 0x39, 0x4A, 0x4C, 0x58, 0xCF,
            0xD0, 0xEF, 0xAA, 0xFB, 0x43, 0x4D, 0x33, 0x85, 0x45,
0xF9, 0x02, 0x7F, 0x50, 0x3C, 0x9F, 0xA8,
            0x51, 0xA3, 0x40, 0x8F, 0x92, 0x9D, 0x38, 0xF5, 0xBC,
0xB6, 0xDA, 0x21, 0x10, 0xFF, 0xF3, 0xD2,
            0xCD, 0x0C, 0x13, 0xEC, 0x5F, 0x97, 0x44, 0x17, 0xC4,
0xA7, 0x7E, 0x3D, 0x64, 0x5D, 0x19, 0x73,
            0x60, 0x81, 0x4F, 0xDC, 0x22, 0x2A, 0x90, 0x88, 0x46,
0xEE, 0xB8, 0x14, 0xDE, 0x5E, 0x0B, 0xDB,
            0xE0, 0x32, 0x3A, 0x0A, 0x49, 0x06, 0x24, 0x5C, 0xC2,
0xD3, 0xAC, 0x62, 0x91, 0x95, 0xE4, 0x79,
            0xE7, 0xC8, 0x37, 0x6D, 0x8D, 0xD5, 0x4E, 0xA9, 0x6C,
0x56, 0xF4, 0xEA, 0x65, 0x7A, 0xAE, 0x08,
            0xBA, 0x78, 0x25, 0x2E, 0x1C, 0xA6, 0xB4, 0xC6, 0xE8,
0xDD, 0x74, 0x1F, 0x4B, 0xBD, 0x8B, 0x8A,
            0x70, 0x3E, 0xB5, 0x66, 0x48, 0x03, 0xF6, 0x0E, 0x61,
0x35, 0x57, 0xB9, 0x86, 0xC1, 0x1D, 0x9E,
            0xE1, 0xF8, 0x98, 0x11, 0x69, 0xD9, 0x8E, 0x94, 0x9B,
0x1E, 0x87, 0xE9, 0xCE, 0x55, 0x28, 0xDF,
            0x8C, 0xA1, 0x89, 0x0D, 0xBF, 0xE6, 0x42, 0x68, 0x41,
0x99, 0x2D, 0x0F, 0xB0, 0x54, 0xBB, 0x16
        );
    }

private function createInvertedSBox()
    {
        $this->s_box_inverted = array(
            0x52, 0x09, 0x6A, 0xD5, 0x30, 0x36, 0xA5, 0x38, 0xBF,
0x40, 0xA3, 0x9E, 0x81, 0xF3, 0xD7, 0xFB,
            0x7C, 0xE3, 0x39, 0x82, 0x9B, 0x2F, 0xFF, 0x87, 0x34,
0x8E, 0x43, 0x44, 0xC4, 0xDE, 0xE9, 0xCB,
            0x54, 0x7B, 0x94, 0x32, 0xA6, 0xC2, 0x23, 0x3D, 0xEE,
0x4C, 0x95, 0x0B, 0x42, 0xFA, 0xC3, 0x4E,
```

```
            0x08, 0x2E, 0xA1, 0x66, 0x28, 0xD9, 0x24, 0xB2, 0x76,
0x5B, 0xA2, 0x49, 0x6D, 0x8B, 0xD1, 0x25,
            0x72, 0xF8, 0xF6, 0x64, 0x86, 0x68, 0x98, 0x16, 0xD4,
0xA4, 0x5C, 0xCC, 0x5D, 0x65, 0xB6, 0x92,
            0x6C, 0x70, 0x48, 0x50, 0xFD, 0xED, 0xB9, 0xDA, 0x5E,
0x15, 0x46, 0x57, 0xA7, 0x8D, 0x9D, 0x84,
            0x90, 0xD8, 0xAB, 0x00, 0x8C, 0xBC, 0xD3, 0x0A, 0xF7,
0xE4, 0x58, 0x05, 0xB8, 0xB3, 0x45, 0x06,
            0xD0, 0x2C, 0x1E, 0x8F, 0xCA, 0x3F, 0x0F, 0x02, 0xC1,
0xAF, 0xBD, 0x03, 0x01, 0x13, 0x8A, 0x6B,
            0x3A, 0x91, 0x11, 0x41, 0x4F, 0x67, 0xDC, 0xEA, 0x97,
0xF2, 0xCF, 0xCE, 0xF0, 0xB4, 0xE6, 0x73,
            0x96, 0xAC, 0x74, 0x22, 0xE7, 0xAD, 0x35, 0x85, 0xE2,
0xF9, 0x37, 0xE8, 0x1C, 0x75, 0xDF, 0x6E,
            0x47, 0xF1, 0x1A, 0x71, 0x1D, 0x29, 0xC5, 0x89, 0x6F,
0xB7, 0x62, 0x0E, 0xAA, 0x18, 0xBE, 0x1B,
            0xFC, 0x56, 0x3E, 0x4B, 0xC6, 0xD2, 0x79, 0x20, 0x9A,
0xDB, 0xC0, 0xFE, 0x78, 0xCD, 0x5A, 0xF4,
            0x1F, 0xDD, 0xA8, 0x33, 0x88, 0x07, 0xC7, 0x31, 0xB1,
0x12, 0x10, 0x59, 0x27, 0x80, 0xEC, 0x5F,
            0x60, 0x51, 0x7F, 0xA9, 0x19, 0xB5, 0x4A, 0x0D, 0x2D,
0xE5, 0x7A, 0x9F, 0x93, 0xC9, 0x9C, 0xEF,
            0xA0, 0xE0, 0x3B, 0x4D, 0xAE, 0x2A, 0xF5, 0xB0, 0xC8,
0xEB, 0xBB, 0x3C, 0x83, 0x53, 0x99, 0x61,
            0x17, 0x2B, 0x04, 0x7E, 0xBA, 0x77, 0xD6, 0x26, 0xE1,
0x69, 0x14, 0x63, 0x55, 0x21, 0x0C, 0x7D
        );
    }

private function createRoundConstants()
    {
        $this->round_constants = array(
            0x01000000, 0x02000000, 0x04000000, 0x08000000,
0x10000000, 0x20000000, 0x40000000, 0x80000000,
            0x1B000000, 0x36000000, 0x6C000000, 0xD8000000,
0xAB000000, 0x4D000000, 0x9A000000, 0x2F000000,
            0x5E000000, 0xBC000000, 0x63000000, 0xC6000000,
0x97000000, 0x35000000, 0x6A000000, 0xD4000000,
            0xB3000000, 0x7D000000, 0xFA000000, 0xEF000000,
0xC5000000, 0x91000000
        );
    }
private function createLogarithmicArray()
    {
        $this->log = array(
```

```
            0x00, 0xFF, 0xC8, 0x08, 0x91, 0x10, 0xD0, 0x36, 0x5A,
0x3E, 0xD8, 0x43, 0x99, 0x77, 0xFE, 0x18,
            0x23, 0x20, 0x07, 0x70, 0xA1, 0x6C, 0x0C, 0x7F, 0x62,
0x8B, 0x40, 0x46, 0xC7, 0x4B, 0xE0, 0x0E,
            0xEB, 0x16, 0xE8, 0xAD, 0xCF, 0xCD, 0x39, 0x53, 0x6A,
0x27, 0x35, 0x93, 0xD4, 0x4E, 0x48, 0xC3,
            0x2B, 0x79, 0x54, 0x28, 0x09, 0x78, 0x0F, 0x21, 0x90,
0x87, 0x14, 0x2A, 0xA9, 0x9C, 0xD6, 0x74,
            0xB4, 0x7C, 0xDE, 0xED, 0xB1, 0x86, 0x76, 0xA4, 0x98,
0xE2, 0x96, 0x8F, 0x02, 0x32, 0x1C, 0xC1,
            0x33, 0xEE, 0xEF, 0x81, 0xFD, 0x30, 0x5C, 0x13, 0x9D,
0x29, 0x17, 0xC4, 0x11, 0x44, 0x8C, 0x80,
            0xF3, 0x73, 0x42, 0x1E, 0x1D, 0xB5, 0xF0, 0x12, 0xD1,
0x5B, 0x41, 0xA2, 0xD7, 0x2C, 0xE9, 0xD5,
            0x59, 0xCB, 0x50, 0xA8, 0xDC, 0xFC, 0xF2, 0x56, 0x72,
0xA6, 0x65, 0x2F, 0x9F, 0x9B, 0x3D, 0xBA,
            0x7D, 0xC2, 0x45, 0x82, 0xA7, 0x57, 0xB6, 0xA3, 0x7A,
0x75, 0x4F, 0xAE, 0x3F, 0x37, 0x6D, 0x47,
            0x61, 0xBE, 0xAB, 0xD3, 0x5F, 0xB0, 0x58, 0xAF, 0xCA,
0x5E, 0xFA, 0x85, 0xE4, 0x4D, 0x8A, 0x05,
            0xFB, 0x60, 0xB7, 0x7B, 0xB8, 0x26, 0x4A, 0x67, 0xC6,
0x1A, 0xF8, 0x69, 0x25, 0xB3, 0xDB, 0xBD,
            0x66, 0xDD, 0xF1, 0xD2, 0xDF, 0x03, 0x8D, 0x34, 0xD9,
0x92, 0x0D, 0x63, 0x55, 0xAA, 0x49, 0xEC,
            0xBC, 0x95, 0x3C, 0x84, 0x0B, 0xF5, 0xE6, 0xE7, 0xE5,
0xAC, 0x7E, 0x6E, 0xB9, 0xF9, 0xDA, 0x8E,
            0x9A, 0xC9, 0x24, 0xE1, 0x0A, 0x15, 0x6B, 0x3A, 0xA0,
0x51, 0xF4, 0xEA, 0xB2, 0x97, 0x9E, 0x5D,
            0x22, 0x88, 0x94, 0xCE, 0x19, 0x01, 0x71, 0x4C, 0xA5,
0xE3, 0xC5, 0x31, 0xBB, 0xCC, 0x1F, 0x2D,
            0x3B, 0x52, 0x6F, 0xF6, 0x2E, 0x89, 0xF7, 0xC0, 0x68,
0x1B, 0x64, 0x04, 0x06, 0xBF, 0x83, 0x38
        );
    }

private function createExpotecialArray()
    {
        $this->exp = array(
            0x01, 0xe5, 0x4c, 0xb5, 0xfb, 0x9f, 0xfc, 0x12, 0x03,
0x34, 0xd4, 0xc4, 0x16, 0xba, 0x1f, 0x36,
            0x05, 0x5c, 0x67, 0x57, 0x3a, 0xd5, 0x21, 0x5a, 0x0f,
0xe4, 0xa9, 0xf9, 0x4e, 0x64, 0x63, 0xee,
            0x11, 0x37, 0xe0, 0x10, 0xd2, 0xac, 0xa5, 0x29, 0x33,
0x59, 0x3b, 0x30, 0x6d, 0xef, 0xf4, 0x7b,
```

```
            0x55, 0xeb, 0x4d, 0x50, 0xb7, 0x2a, 0x07, 0x8d, 0xff,
0x26, 0xd7, 0xf0, 0xc2, 0x7e, 0x09, 0x8c,
            0x1a, 0x6a, 0x62, 0x0b, 0x5d, 0x82, 0x1b, 0x8f, 0x2e,
0xbe, 0xa6, 0x1d, 0xe7, 0x9d, 0x2d, 0x8a,
            0x72, 0xd9, 0xf1, 0x27, 0x32, 0xbc, 0x77, 0x85, 0x96,
0x70, 0x08, 0x69, 0x56, 0xdf, 0x99, 0x94,
            0xa1, 0x90, 0x18, 0xbb, 0xfa, 0x7a, 0xb0, 0xa7, 0xf8,
0xab, 0x28, 0xd6, 0x15, 0x8e, 0xcb, 0xf2,
            0x13, 0xe6, 0x78, 0x61, 0x3f, 0x89, 0x46, 0x0d, 0x35,
0x31, 0x88, 0xa3, 0x41, 0x80, 0xca, 0x17,
            0x5f, 0x53, 0x83, 0xfe, 0xc3, 0x9b, 0x45, 0x39, 0xe1,
0xf5, 0x9e, 0x19, 0x5e, 0xb6, 0xcf, 0x4b,
            0x38, 0x04, 0xb9, 0x2b, 0xe2, 0xc1, 0x4a, 0xdd, 0x48,
0x0c, 0xd0, 0x7d, 0x3d, 0x58, 0xde, 0x7c,
            0xd8, 0x14, 0x6b, 0x87, 0x47, 0xe8, 0x79, 0x84, 0x73,
0x3c, 0xbd, 0x92, 0xc9, 0x23, 0x8b, 0x97,
            0x95, 0x44, 0xdc, 0xad, 0x40, 0x65, 0x86, 0xa2, 0xa4,
0xcc, 0x7f, 0xec, 0xc0, 0xaf, 0x91, 0xfd,
            0xf7, 0x4f, 0x81, 0x2f, 0x5b, 0xea, 0xa8, 0x1c, 0x02,
0xd1, 0x98, 0x71, 0xed, 0x25, 0xe3, 0x24,
            0x06, 0x68, 0xb3, 0x93, 0x2c, 0x6f, 0x3e, 0x6c, 0x0a,
0xb8, 0xce, 0xae, 0x74, 0xb1, 0x42, 0xb4,
            0x1e, 0xd3, 0x49, 0xe9, 0x9c, 0xc8, 0xc6, 0xc7, 0x22,
0x6e, 0xdb, 0x20, 0xbf, 0x43, 0x51, 0x52,
            0x66, 0xb2, 0x76, 0x60, 0xda, 0xc5, 0xf3, 0xf6, 0xaa,
0xcd, 0x9a, 0xa0, 0x75, 0x54, 0x0e, 0x01
        );
    }

public function encrypt($content, $key)
    {
        $expand_key = $this->keyExpansion($this-
>convertToWords($key));
        $this->state = $this->convertToWords($content);
        $this->addRoundKey($this->createRoundKey(0, $expand_key));
        for ($round = 1; $round < $this->number_of_rounds;
$round++) {
            $this->subBytes();
            $this->shiftRows();
            $this->mixColumns();
            $this->addRoundKey($this->createRoundKey($round,
$expand_key));
        }
        $this->subBytes();
        $this->shiftRows();
```

```
        $this->addRoundKey($this->createRoundKey($this-
>number_of_rounds, $expand_key));
        return $this->convertToHexString();
    }
public function decrypt($content, $key)
    {
        $expand_key = $this->keyExpansion($this-
>convertToWords($key));
        $this->state = $this->convertToWords($content);
        $this->addRoundKey($this->createRoundKey($this-
>number_of_rounds, $expand_key));
        for ($round = $this->number_of_rounds - 1; $round > 0;
$round--) {
            $this->invShiftRows();
            $this->invSubBytes();
            $this->addRoundKey($this->createRoundKey($round,
$expand_key));
            $this->invMixColumns();
        }
        $this->invShiftRows();
        $this->invSubBytes();
        $this->addRoundKey($this->createRoundKey(0, $expand_key));
        return $this->convertToHexString();
    }

private function subBytes()
    {
        for ($i = 0; $i < $this->block_size; $i++) {
            $this->state[$i] = $this->subWord($this->state[$i]);
        }
    }

private function invSubBytes()
    {
        for ($i = 0; $i < $this->block_size; $i++) {
            $this->state[$i] = $this->subWord($this->state[$i],
true);
        }
    }
private function shiftRows()
    {
        for ($i = 1; $i < self::WORD_LENGTH; $i++) {
            $buffer = array();
            for ($j = $this->block_size - 1; $j >= 0; $j--) {
                $pos = ($i + $j) % $this->block_size;
```

```
                $buffer[$j] = $this->getByteFromWord($this-
>state[$j], $i);
                $byte = isset($buffer[$pos]) ? $buffer[$pos] :
$this->getByteFromWord($this->state[$pos], $i);
                $this->state[$j] = $this->putByteIntoWord($byte,
$this->state[$j], $i);
            }
        }
    }

private function invShiftRows()
    {
        for ($i = 1; $i < self::WORD_LENGTH; $i++) {
            $buffer = array();
            for ($j = 0; $j < $this->block_size; $j++) {
                $pos = ($i + $j) % $this->block_size;
                $buffer[$pos] = $this->getByteFromWord($this-
>state[$pos], $i);
                $byte = isset($buffer[$j]) ? $buffer[$j] : $this-
>getByteFromWord($this->state[$j], $i);
                $this->state[$pos] = $this->putByteIntoWord($byte,
$this->state[$pos], $i);
            }
        }
    }

private function mixColumns()
    {
        $mul1 = array();
        $mul2 = array();
        $mul3 = array();
        for ($i = 0; $i < $this->block_size; $i++) {
            for ($j = 0; $j < self::WORD_LENGTH; $j++) {
                $mul1[$j] = $this->getByteFromWord($this-
>state[$i], $j);
                $mul2[$j] = $this-
>galoisFieldMultiplication($mul1[$j], 0x02);
                $mul3[$j] = $mul2[$j] ^ $mul1[$j];
            }
            for ($j = 0; $j < self::WORD_LENGTH; $j++) {
                $byte = $mul2[$j] ^ $mul1[($j + 3) % $this-
>block_size] ^ $mul1[($j + 2) % $this->block_size] ^ $mul3[($j +
1) % $this->block_size];
                $this->state[$i] = $this->putByteIntoWord($byte,
$this->state[$i], $j);
```

```
            }
        }
    }

private function invMixColumns()
    {
        $mulE = array();
        $mulD = array();
        $mulB = array();
        $mul9 = array();
        for ($i = 0; $i < $this->block_size; $i++) {
            for ($j = 0; $j < self::WORD_LENGTH; $j++) {
                $temp = $this->getByteFromWord($this->state[$i],
$j);
                $mulE[$j] = $this-
>galoisFieldMultiplication($temp, 0x0E);
                $mulD[$j] = $this-
>galoisFieldMultiplication($temp, 0x0D);
                $mulB[$j] = $this-
>galoisFieldMultiplication($temp, 0x0B);
                $mul9[$j] = $this-
>galoisFieldMultiplication($temp, 0x09);
            }
            for ($j = 0; $j < self::WORD_LENGTH; $j++) {
                $byte = $mulE[$j] ^ $mul9[($j + 3) % $this-
>block_size] ^ $mulD[($j + 2) % $this->block_size] ^ $mulB[($j +
1) % $this->block_size];
                $this->state[$i] = $this->putByteIntoWord($byte,
$this->state[$i], $j);
            }
        }
    }

private function addRoundKey($key)
    {
        for ($i = 0; $i < $this->block_size; $i++) {
            $this->state[$i] ^= $key[$i];
        }
    }

private function keyExpansion($key)
    {
        $expanded_key = array();
        for ($i = 0; $i < $this->key_size; $i++) {
            $expanded_key[$i] = $key[$i];
```

```
        }
        for ($i = $this->key_size; $i < $this->block_size *
($this->number_of_rounds + 1); $i++) {
            $temp = $expanded_key[$i - 1];
            if ($i % $this->key_size == 0)
                $temp = $this->subWord($this->rotWord($temp)) ^
$this->round_constants[$i / $this->key_size - 1];
            else if ($this->key_size > 6 && $i % $this->key_size
== 4)
                $temp = $this->subWord($temp);
            $expanded_key[$i] = $expanded_key[$i - $this-
>key_size] ^ $temp;
        }
        return $expanded_key;
    }

private function createRoundKey($round, $key)
    {
        return array($key[self::WORD_LENGTH * $round],
$key[self::WORD_LENGTH * $round + 1], $key[self::WORD_LENGTH *
$round + 2], $key[self::WORD_LENGTH * $round + 3]);
    }
```

Skripsi Ganjil 22/23

ORIGINALITY REPORT

21%	20%	8%	10%
SIMILARITY INDEX	INTERNET SOURCES	PUBLICATIONS	STUDENT PAPERS

PRIMARY SOURCES

1	docplayer.info Internet Source	2%
2	repositori.usu.ac.id Internet Source	2%
3	ejournal.antarbangsa.ac.id Internet Source	1%
4	id.scribd.com Internet Source	1%
5	text-id.123dok.com Internet Source	1%
6	repository.its.ac.id Internet Source	1%
7	Submitted to Universitas Pamulang Student Paper	1%
8	digilib.uns.ac.id Internet Source	1%
9	www.researchgate.net Internet Source	1%

Jurnal Ganjil 22/23

ORIGINALITY REPORT

14%	13%	8%	9%
SIMILARITY INDEX	INTERNET SOURCES	PUBLICATIONS	STUDENT PAPERS

PRIMARY SOURCES

1	Submitted to Universitas Nahdlatul Ulama Surabaya Student Paper	5%
2	id.scribd.com Internet Source	2%
3	Submitted to Sriwijaya University Student Paper	1%
4	Submitted to Universitas Brawijaya Student Paper	1%
5	Dayat Subekti. "PEMANFAATAN TEKONOLOGI WEB UNTUK PEMBUATAN APLIKASI LAPORAN KEUANGAN DI BANK SAMPAH LINTAS WINONGO YOGYAKARTA", Jurnal Aplikasi Teknologi Informasi dan Manajemen (JATIM), 2022 Publication	<1%
6	pdfs.semanticscholar.org Internet Source	<1%
7	pt.scribd.com Internet Source	<1%

JURNAL INFORMATIKA, Vol.10 No.1 April 2023, Halaman 1-8
ISSN: 2355-6579 | E-ISSN**:** 2528-2247

Sistem *Voting* Pemihan Ketua Organisasi Menggunakan Algoritma Kriptografi *Caesar Chiper* dan AES

Veranisa Tya Cahyani [1], Fauziah [2], Ira Diana Sholihati [3]
[1,2,3] Universitas Nasional, Jakarta, Indonesia

e-mail: [1] veranisatya@gmail.com, [2] fauziah@civitas.unas.ac.id, [3] ira.diana@civitas.unas.ac.id

Informasi Artikel | Diterima: 00-00-2023 | Direvisi: 00-00-2023 | Disetujui: 00-00-2023

Abstrak

Dalam pemilihan ketua sebuah organisasi masih banyak ditemui prosesnya dilakukan secara konvensional menggunakan kertas. Hal tersebut menjadikan proses perhitungan suara akan memakan waktu yang tidak sebentar. Dalam masa pandemi COVID-19, dimana kegiatan yang melibatkan banyak orang juga dibatasi, sehingga memiliki kendala juga jika melakukan *voting* secara konvensional yang harus mengumpulkan banyak orang. Di zaman sekarang, kemajuan teknologi mendukung manusia untuk menciptakan inovasi terbaru yang dapat membantu manusia dalam kehidupan sehari-hari, salah satunya yaitu sistem *voting* pemilihan ketua organisasi menggunakan algoritma kriptografi *caesar chiper* dan AES. Tujuan dibuatnya sistem *voting* ini adalah sebagai pengambilan keputusan yang transparan, tidak ada kecurangan dan efisien. Metode yang digunakan adalah kriptografi *Caesar Chiper* dan AES yang digunakan untuk pengamanan *password* dan juga kode kandidat. Hasil dari penelitian ini adalah hasil *entropy* dari *plaintext* ke *chipertext* terjadi peningkatan dari data sampel yang digunakan rata-rata selisihnya adalah sebesar 1,0178. Nilai tersebut akan terus meningkat jika *plaintext* yang digunakan semakin bervariasi dan akan semakin aman juga sistem yang dibuat.

Kata Kunci: Kriptografi, *Caesar Chiper*, AES

Abstract

In selecting the chairman of an organization, there are still many processes that are carried out conventionally using paper. This makes the vote counting process take a long time. During the COVID-19 pandemic, activities involving many people were also limited, so there were also obstacles to voting conventionally where many people had to gather. Nowadays, technological advances support humans to create the latest innovations that can help humans in everyday life, one of which is the voting system for selecting the head of the organization using the caesar cipher cryptographic algorithm and AES. The purpose of this voting system is to make decisions that are transparent, free of fraud and efficient. The method used is Caesar Chiper and AES cryptography which is used to secure passwords and also candidate codes. The results of this study are that the entropy results from plaintext to ciphertext have increased from the sample data used, the average difference is 1.0178. This value will continue to increase if the plaintext used is more varied and the more secure the system will be.

Keywords*: Cryptographic, Caesar Chiper, AES*

1. Pendahuluan

Proses pemilihan ketua sebuah organisasi biasanya dilakukan melalui *voting* yang bisa dilakukan secara manual menggunakan kertas. Pemilihan yang dilakukan secara manual tentu saja harus dilaksanakan secara langsung yaitu seluruh pemilih harus hadir langsung dalam kegiatan pemungutan suara. Namun dalam masa pandemi COVID-19 segala jenis kegiatan yang mengumpulkan banyak orang dibatasi. Sehingga proses pemilihan suatu ketua organisasi dilaksanakan secara *hybrid*, 50 % offline dan 50% *online*.

Terdapat beberapa aplikasi *voting online* yang dapat dengan mudah dicari pada internet, namun masih terdapat kelemahan dalam keamanan datanya. Beberapa kelemahannya antara lain adalah para pemilih dapat melihat suara pemilih lain, para pemilih dapat menghapus suara pemilih lain dan juga *voting* dilakukan dengan membagikan link voting yang dapat dibuka oleh siapa saja tanpa bisa membatasi jumlah pemilih.

Terdapat penelitian sebelumnya yaitu sistem *e-voting* dibuat dengan mengimplementasikan algoritma *caesar chiper* pada proses memasukan data ke *database*, jadi

seluruh data yang dimasukan kedalam *database* dienkripsi dan proses dekripsi dilaksanakan pada saat data hasil pemilihan diumumkan. Sehingga dapat mengurangi penyalahgunaan data hasil pemilihan. Terdapat saran dari penelitian ini yaitu bisa dilakukan penggabungan beberapa algoritma untuk memberikan hasil yang lebih aman sehingga sulit menemukan pola dekripsi.(Angriani & Saharaeni, 2019)

Pada penelitian sebelumnya oleh Nurul Chafid dan Herlina Soffiana yaitu membuat aplikasi *e-voting* berbasis web dengan mengimplemantasikan algoritma kriptografi klasik *caesar chiper* yang diimplementasikan pada proses login aplikasi. Terdapat saran dari penelitian ini yaitu dapat menambahkan fitur ekspor data menjadi PDF dan Excel untuk mempermudah admin merekap data hasil *voting*.(Chafid & Soffiana, 2022)

Berkaitan dengan latar belakang penelitian ini difokuskan pada permasalahan keamanan data dalam proses voting pemilihan ketua organisasi agar terjaga keamanan datanya yang diberi judul "Sistem *Voting* Pemilihan Ketua Organisasi Berbasis Web Menggunakan Algoritma Kriptografi *Caesar Chiper* dan AES"

2. Metode Penelitian

2.1 *E-Voting*

Voting merupakan salah satu cara pengambilan keputusan dengan penentuan dari suara terbanyak dari seluruh anggota di suatu organisasi. Dalam *e-voting* (*voting* secara elektronik) proses pemungutan suaranya dilakukan dengan cara pemilih memberikan suara melalui Internet atau Intranet. *E-Voting* merupakan suatu aplikasi atau sistem yang digunakan untuk melakukan *voting* secara elektronik. Pelaksanaan *voting menggunakan e-voting* dilakukan dengan melakukan pembuatan akun untuk para pemilih, kegiatan pemilihan, perhitungan perolehan suara dan menampilkan hasil perolehan suara secara elektronik. Hasil perolehan suara pada *e-voting* biasanya disajikan secara digital berbentuk diagram.

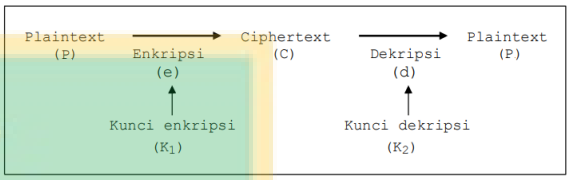
Electronic election system harus mengutamakan kerahasiaan dan keamanan. Jika kerahasiaan dan keamanan dapat terjamin, maka *e-voting* sudah tepat untuk digunakan. (García-Zamora et al., 2005) Terdapat beberapa aspek manfaat dari penerapan *e-voting* yaitu sebagai berikut. (Zafar & Pilkjaer, 2007)

a. Biaya: sumber daya yang lebih menghemat dibandingkan dengan *voting* manual yang kurang efisien.
b. Waktu: waktu pelaksanaan yang lebih cepat dibandingkan *voting* manual.
c. Hasil: hasil perolehan suara yang lebih tepat, akurat dan mengurangi risiko terjadinya human *error* denagn sistem yang baik.

2.2 Kriptografi

Kriptografi merupakan suatu disiplin keilmuan yang dipakai mengamankan pesan ketika pesan tersebut dikirim dari pengirim ke penerima. (Dony Ariyus, 2008)

Pada Gambar 2.1 dijelaskan proses enkripsi dan dekripsi yang terjadi dengan menggunakan kunci(*key*).(Lingkup et al., 2004)



Gambar 2. 1 Enkripsi dan Dekripsi Dengan Kunci

Proses enkripsi dapat ditulis dengan :

$$eK1\ (P) = C \quad (2.1)$$

Proses dekripsi dapat ditulis dengan :

$$dK2\ (C) = P \quad (2.2)$$

Proses pengujian dapat dilakukan dengan :

$$dK2\big(eK1(P)\big) = P \quad (2.3)$$

2.3 *Caesar Chiper*

Algortima *Caesar Chiper* termasuk teknik substitusi yaitu setiap huruf yang ada dalam *plaintext* diubah dengan huruf berbeda yang terdapat perbedaan posisi dalam alfabet. Dalam algoritma *Caesar Cipher*, huruf pada *plaintext* diganti dengan huruf ketiga setelahnya dari susunan alfabet yang sama. Berikut susunan alfabet yang telah digeser sejauh 3 huruf :

Alfabet Biasa: A B C D E F G H I J K L M N O P Q R S T U V W X Y Z
Alfabet Sandi: D E F G H I J K L M N O P Q R S T U V W X Y Z A B C

Dalam melakukan penyandian pesan dapat dilakukan dengan mencocokan huruf yang akan dienkripsi pada alfabet biasa, setelah itu tulis huruf yang ada pada alfabet sandi. Dalam mengubah pesan sandi menjadi pesan yang asli, dapat menggunakan cara sebaliknya. Contohnya adalah sebagai berikut.

Plaintext : JAKARTA KOTA KOLABORASI
Chipertext : MDNDU WDNRW DNROD ERUDVL

Persamaan matematikanya sebagai berikut

$$C = E(P) = (P + 3)\ mod\ 26 \qquad (2.4)$$

Terdapat 26 huruf yang ada pada alfabet. Penerima pesan akan mengembalikan cipherteks dengan rumus kebalikannya, yang dapat dijabarkan pada persamaan berikut

$$P = D(C) = (C - 3)\ mod\ 26 \qquad (2.5)$$

Fungsi D merupakan invers dari fungsi E, yaitu :

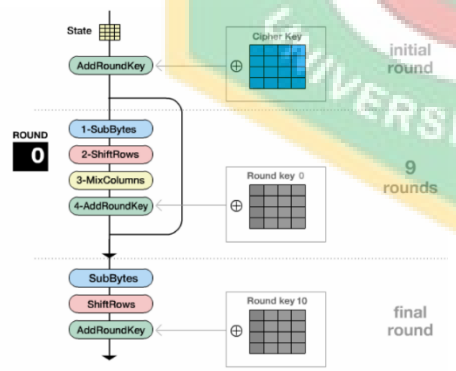
$$D(C) = E - 1(P) \qquad (2.6)$$

2.4 AES (*Advanced Encryption Standard)*

Advanced Encryption Standard (AES) termasuk blok *chipertext* simetrik yang bisa memproses enkripsi dan dekripsi data. Enkripsi adalah sebuah proses merubah data awal (*plaintext*) menjadi data yang disandikan (*chipertext*), kebalikannya proses dekripsi merupalan proses merubah *ciphertext* menjadi bentuk data awal yang disebut sebagai *plaintext*. Pada penggunaan algoritma AES terdapat kunci kriptografi 128, 192, dan 256 bits untuk proses enkripsi dan dekripsi data pada blok 128 bits.(Ibrahim, 2017)

2.4.1 Proses Enkripsi

Proses enkripsi pada yang terjadi pada AES terdapat 4 jenis, antara lain *SubBytes, ShiftRows, Mixcolumns,* dan *AddRoundKey*. Proses enkripsi pada AES dapat diperhatikan pada Gambar 2.2.

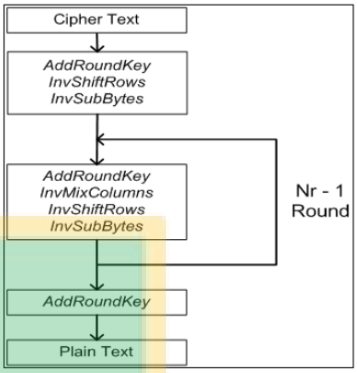


Gambar 2. 2 Alur Proses Enkripsi Algortima AES

Gambar 2.2 menjelaskan bagaimana proses enkripsi algoritma AES, tahapan pertama adalah *initial round* yaitu proses *AddRoundKey*. Tahapan selanjutnya adalah 9 rounds yaitu proses *SubBytes, ShiftRows, MixColums* dan *AddRoundKey*. Tahapan yang terakhir adalah *final round* yaitu proses *Round Key* 10. Pada *Round Key* 10 hanya tidak melewati proses *MixColumns*.

2.4.2 Proses Dekripsi

Perubahan cipher dapat dikembalikan dengan arah yang berkebalikan untuk mendapatkan *invers cipher* yang mudah dipahami. Proses dekripsi pada algoritma AES dapat dilihat pada Gambar 2.3.(Ibrahim, 2017)



Gambar 2. 3 Dekripsi AES

Gambar 2.3 menjelaskan mengenai alur proses dekripsi pada algoritma AES. Prosesnya yaitu kebalikannya dari proses enkripsi. Pada tahap awal, *chipertext* akan melewati proses *AddRoundKey, InvShiftRows* dan *InvSubBytes* setelah itu dapat dilanjutkan ke tahapan berikutnya.

2.5 *MySQL*

MySQL adalah sistem *database* yang bisa diandalkan. Pertamanya, *SQL* dipergunakan untuk bahasa yang mehubungkan program *database* dengan bahasa program. Berkat terbentuknya *SQL* maka dari itu programmer jaringan dan aplikasi tidak menemukan permasalahan yang berarti dalam mengintergrasikan aplikasi yang dibuat. pengguna *MySQL* dapat menggunakan sistem secara bersama-sama. *MySQL* merupakan perangkat lunak gratis yang dapat diunduh pada laman resminya. *MySQL* juga merupakan sebuah sistem manajemen *database*, relasional sistem *database* dan *software open source*.(Sakur, 2004)

2.6 *Apache*

Apache adalah *software web server* yang terkenal yang dikembangkan pada tahun 1995. *Server Apache* telah dikembangkan oleh *Apache Software Foundation*, yang anggotanya terus menambahkan fungsionalitas baru yang bermanfaat, dengan tujuan menyediakan *platform server* yang sangat aman dan dapat diperluas yang memastikan pengiriman layanan HTTP sesuai dengan standar HTTP. Versi asli *Apache* ditulis untuk UNIX, tetapi saat ini versi yang berjalan di bawah OS/2, *Windows* dan *platform* lainnya. Pada *Server Apache* terdapat berbagai fitur *web server*, termasuk CGI, SSL,

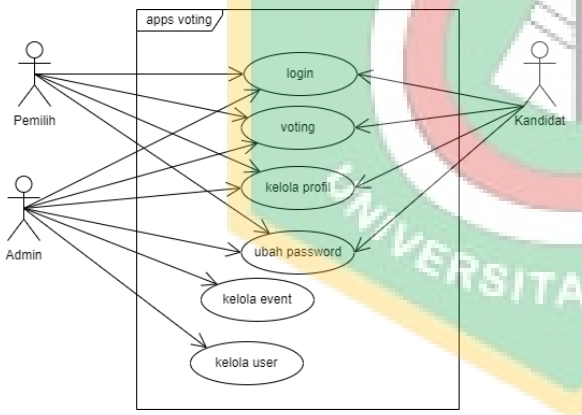
dan *domain virtual*. *Apache* sangat mendukung *modul plug-in*. Disebut *Apache* karena dikembangkan dari kode NCSA yang sudah ditambah berbagai *patch*, oleh karena itu dinamakan *server patchy* atau *server Apache*.(Cecep Kurnia Sastradipraja & Munawar, 2002)

2.7 Metode Pengujian

Untuk melihat kualitas enkripsi dari aplikasi yang dibuat pada hal ini adalah proses *login* dengan melakukan enkripsi pada *password user* dan pada proses *voting* dengan melakukan enkripsi pada kode kandidat maka dilakukan pengujian yaitu dengan melakukan perhitungan *entropy*. Semakin tinggi nilai *entropy* maka semakin aman sistem enkripsi yang dibuat. (Simarmata et al., 2019)

Pada penelitian yang dilakukan beberapa tahapan seperti menyusun kerangka pemikiran yang diawali dari merumuskan masalah, lalu membuat solusi dengan penerapan algoritma sebagai penyelesaiannya dan untuk memperoleh hasil penelitian.

Fokus pada penelitian ini yaitu pembuatan sistem *voting* pemilihan ketua organisasi menggunakan algortima kriptografi *Caesar Chiper* dan AES pada *password* serta penggunaan algoritma AES pada kode kandidat. Berikut rancangan *usecase* diagramnya :



Gambar 2.4 *Usecase* Diagram Sistem *Voting*

Pada Gambar 2.4 *usecase* diagram dijelaskan bahwa terdapat 3 aktor yaitu admin, pemilih dan kandidat serta terdapat enam proses dalam *usecase* diatas. Pada *usecase* digambarkan bahwa pemilih dapat melakukan *login, voting*, kelola profil dan ubah *password*. Kemudian admin dapat melakukan *login, voting*, kelola profil, ubah *password*, kelola *event* dan kelola *user*. Sedangkan kandidat dapat melakukan *login, voting*, kelola profil dan ubah *password*.

Teknik yang dipergunakan dalam penelitian ini untuk pengumpulan datanya yaitu teknik kuantitatif yang mana merupakan data yang dapat terukur dan dihitung.

3. Hasil dan Pembahasan

Dalam bab ini akan dijelaskan terkait sistem yang sudah dibangun dan juga proses pengujian sesuai dengan penggunaan metodenya. Dimana dalam sub bab pembahasan akan dijelaskan terkait apa-apa saja yang bisa dilakukan dalam sistem oleh admin dan user (pemilih dan kandidat).

Lalu pada sub bab pengujian akan menghitung perbandingan nilai *entropy* pada *plaintext* dan *chipertext* untuk melihat keamanan sistem yang dibuat.

3.1 Pembahasan

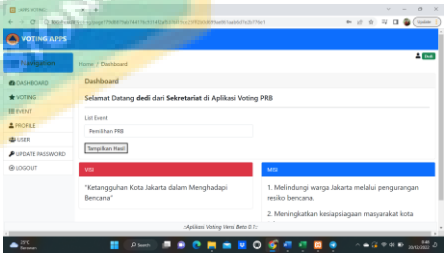
Pada bagian ini akan dijelaskan terkait apa saja yang dapat dilakukan pada sistem beserta *screenshoot* tampilannya pada sistem.

Login

Gambar 3. 1 Tampilan Form Login

Gambar 3.1 adalah *Form Login* untuk *user* yang dapat digunakan admin, pemilih dan kandidat pada sistem untuk melakukan *Login*.

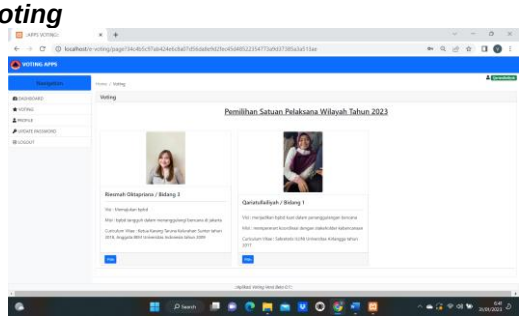
Dashboard



Gambar 3. 2 Tampilan Halaman *Dashboard*

Gambar 3.2 adalah *Dashboard* pada admin dan *user*. Pada halaman *dashboard* terdapat *list* hasil perolehan suara dari *event* yang pernah berlangsung. Dan juga terdapat visi dan misi organisasi.

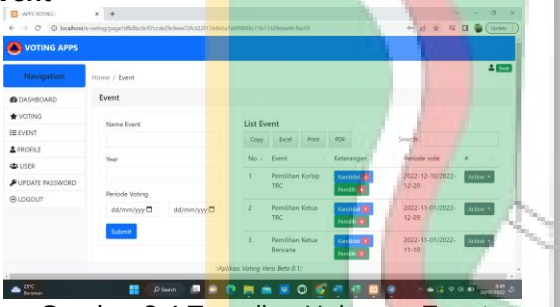
Voting



Gambar 3.3 Tampilan Halaman *Voting*

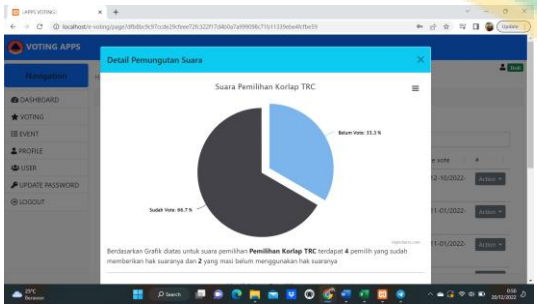
Gambar 3.3 adalah halaman *Voting* pada admin dan *user*. Pada halaman ini menampilkan kandidat jika ada *event* yang sedang berlangsung. Admin juga dapat melakukan *voting* jika sudah ditambahkan menjadi pemilih dalam *event* yang sedang berlangsung. Jika tidak terdapat *event* yang sedang berlangsung, maka halaman ini akan kosong dan akan tampil tulisan “Maaf saat ini sedang tidak *event* yang berlangsung”.

Event



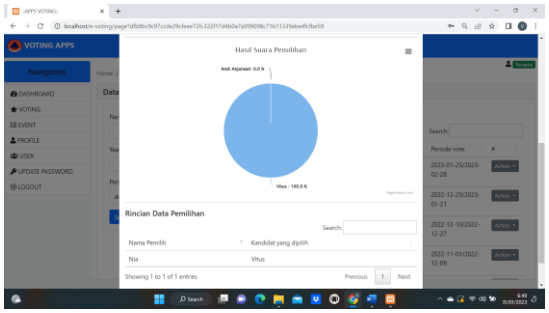
Gambar 3.4 Tampilan Halaman *Event*

Gambar 3.4 merupakan halaman *Event* pada admin, untuk pemilih dan kandidat tidak terdapat halaman ini. Dalam halaman *event*, admin dapat melakukan CRUD terkait *event*, menambahkan pemilih, menambahkan kandidat, dan melihat detail *event*.



Gambar 3.5 Tampilan Detail Event Hasil Suara

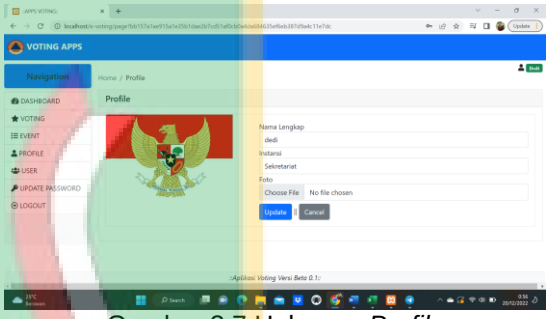
Pada Gambar 3.5 diperlihatkan tampilan *detail event* pada *Detail* Pemungutan Suara yang merupakan *pie chart* untuk mengetahui presentase pemilih yang sudah melakukan *vote* dan yang belum melakukan *vote*.



Gambar 3.6 Tampilan *Detail Event* Perolehan Suara dan Rincian Data Pemilih

Pada Gambar 3.6 adalah tampilan halaman *Detail Event* yang hanya dapat dilihat oleh admin. Terdapat *pie chart* hasil suara pemilih dan rincian data pemilihan yang memperlihatkan suara pemilih.

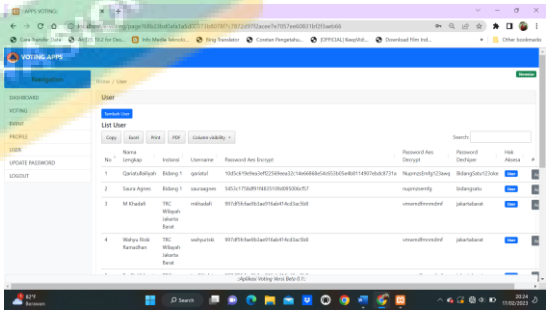
Profile



Gambar 3.7 Halaman *Profile*

Pada Gambar 3.7 ialah halaman *profile* yang ada pada admin dan *user*. Pada halaman tersebut admin dan *user* bisa meng-*update data profile*.

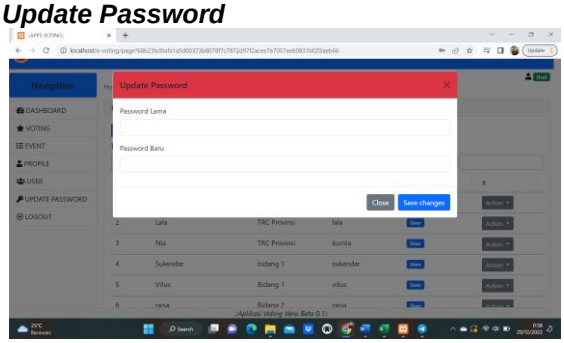
User



Gambar 3.8 Halaman *User*

Pada Gambar 3.8 adalah halaman *user* yang terdapat pada admin. Pada halaman tersebut admin dapat mengelola *user* dengan menambahkan, mengedit dan menghapus *user*. Pada halaman *user* juga admin dapat melihat *password user* dan hasil enkripsinya.

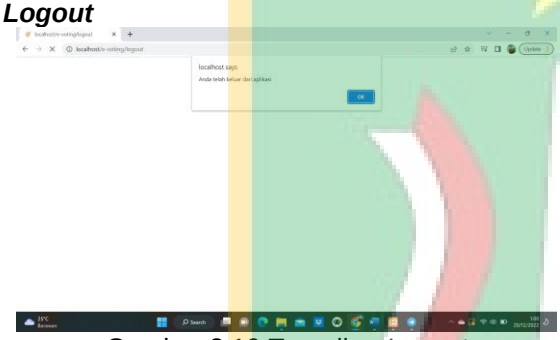
Update Password



Gambar 3.9 Tampilan Ubah *Password*

Pada Gambar 3.9 merupakan tampilan ubah *password* yang ada pada admin dan *user*. Pada halaman tersebut admin dan *user* bisa mengubah *password* dengan mengisikan *password* lama dan *password* baru.

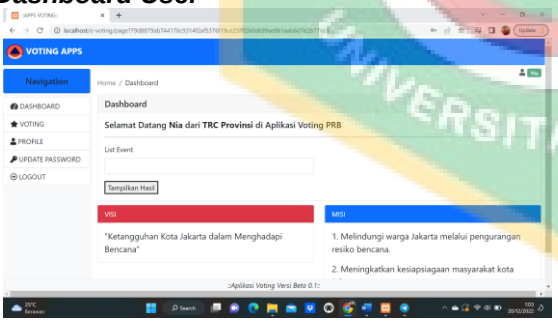
Logout



Gambar 3.10 Tampilan *Logout*

Pada Gambar 3.10 merupakan tampilan notifikasi saat sudah berhasil melakukan *logout*.

Dashboard User

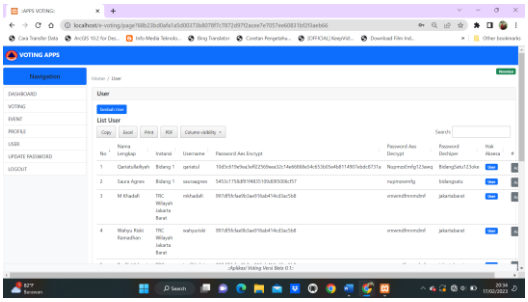


Gambar 3.11 Tampilan *Dashboard User* (pemilih dan kandidat)

Pada Gambar 3.11 merupakan tampilan *dashboard* untuk pemilih dan kandidat. Hanya terdapat beberapa menu yaitu *voting*, *profile* dan ubah *password*.

3.2 Hasil

Pengujian dilakukan pada proses *login*, yaitu data *password* dienkripsi menggunakan algoritma *Caesar Chiper* kemudian hasil *chipertext*nya dienkripsi kembali menggunakan algoritma AES. Data *user* yang ditambahkan akan disimpan kedalam database. Data *password* yang sudah terenkripsi terdapat pada Gambar 3.12.



Gambar 3. 12 Hasil Enkripsi dan Dekripsi Data *Password*

Gambar 3.12 merupakan tampilan data *user* pada admin yang menampilkan data *user* dan juga hasil enkripsi dan dekripsi dari *password user* pada sistem *voting*.

Gambar 3.13 Hasil Enkripsi Data Kode Kandidat

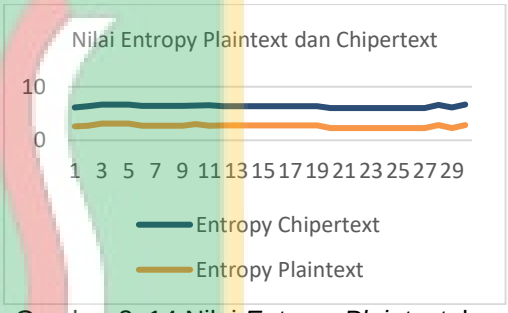
Gambar 3.13 merupakan tampilan hasil enkripsi kode kandidat pada halaman *inspect element*. Untuk melihatnya dapat menekan tombol Ctrl + U. Pada Gambar 3.13 hasil enkripsi kode kandidat dituliskan sebagai *data-whatever*.

Untuk melihat kualitas enkripsi dari aplikasi yang dibuat pada hal ini adalah proses login dengan melakukan enkripsi pada *password user* maka dilakukan pengujian yaitu dengan melakukan perhitungan *entropy* pada data sampel sebanyak 30 data yang terdapat pada Tabel 4.1. Untuk melihat kualitas enkripsi pada proses *voting* dengan melakukan enkripsi pada kode kandidat, juga dilakukan pengujian perhitungan entropy pada 3 data sampel yang terdapat pada Tabel 4.2. Semakin tinggi nilai *entropy* maka semakin aman sistem enkripsi yang dibuat. (Simarmata et al., 2019)

Tabel 3.1 Pengujian *Entropy Plaintext* dan *Chipertext* pada *Password*

User name	Plain text	Kunci	Entropy Plaintext	Entropy Chipertext	Selisih
verani satc	admin	tangguhb encana!!	2,584962501	3,525127092	0,940165
oktim el	sekret ariat	tangguhb encana!!	2,732158891	3,623508797	0,89135
vitus	bidan gsatu	tangguhb encana!!	3,121928095	3,517342901	0,395415
suken dar	bidan gsatu	tangguhb encana!!	3,121928095	3,517342901	0,395415
dadan g	bidan gsatu	tangguhb encana!!	3,121928095	3,517342901	0,395415
raisa	bidan gdua	tangguhb encana!!	2,725480557	3,682332326	0,956852
yuliaiy	bidan gtiga	tangguhb encana!!	2,721928095	3,690116518	0,968188
oryza	bidan gtiga	tangguhb encana!!	2,721928095	3,690116518	0,968188
riesm ah	bidan gtiga	tangguhb encana!!	2,721928095	3,690116518	0,968188
aulian a	pusda tin	tangguhb encana!!	3	3,480721945	0,480722
kurnia	provin si	tangguhb encana!!	2,75	3,799979385	1,049979
ajimm	jakart apusa t	tangguhb encana!!	2,751629167	3,634989959	0,883361
mprih atama	jakart apusa t	tangguhb encana!!	2,751629167	3,634989959	0,883361
adhity orp	jakart apusa t	tangguhb encana!!	2,751629167	3,634989959	0,883361
cangh ara	jakart apusa t	tangguhb encana!!	2,751629167	3,634989959	0,883361
ferryi febria	jakart apusa t	tangguhb encana!!	2,751629167	3,634989959	0,883361
nsyah dm	jakart apusa t	tangguhb encana!!	2,751629167	3,634989959	0,883361
firnan dof	jakart apusa t	tangguhb encana!!	2,751629167	3,634989959	0,883361
muha mmad ap	jakart apusa t	tangguhb encana!!	2,751629167	3,634989959	0,883361
paran dika	jakart autar a	tangguhb encana!!	2,284159128	3,735281416	1,451122
kurnia	provin si	tangguhb encana!!	2,75	3,799979385	1,049979
ajimm	jakart apusa t	tangguhb encana!!	2,751629167	3,634989959	0,883361
mprih atama	jakart apusa t	tangguhb encana!!	2,751629167	3,634989959	0,883361
adhity orp	jakart apusa t	tangguhb encana!!	2,751629167	3,634989959	0,883361
cangh ara	jakart apusa t	tangguhb encana!!	2,751629167	3,634989959	0,883361
ferryi febria	jakart apusa t	tangguhb encana!!	2,751629167	3,634989959	0,883361
nsyah dm	jakart apusa t	tangguhb encana!!	2,751629167	3,634989959	0,883361
firnan dof	jakart apusa t	tangguhb encana!!	2,751629167	3,634989959	0,883361
muha mmad ap	jakart apusa t	tangguhb encana!!	2,751629167	3,634989959	0,883361
paran dika	jakart autar a	tangguhb encana!!	2,284159128	3,735281416	1,451122
dicky mei	jakart autar a	tangguhb encana!!	2,284159128	3,735281416	1,451122
agung tri	jakart autar a	tangguhb encana!!	2,284159128	3,735281416	1,451122
ariyan to	jakart autar a	tangguhb encana!!	2,284159128	3,735281416	1,451122
brame kti	jakart autar a	tangguhb encana!!	2,284159128	3,735281416	1,451122
dimas mf	jakart autar a	tangguhb encana!!	2,284159128	3,735281416	1,451122
ezark urnia	jakart autar a	tangguhb encana!!	2,284159128	3,735281416	1,451122
fachri h	jakart autar a	tangguhb encana!!	2,284159128	3,735281416	1,451122
saabu h	jakart atimur	tangguhb encana!!	2,855388542	3,735281416	0,879893
edysu	jakart abara t	tangguhb encana!!	2,284159128	3,844384532	1,560225
agus mu	jakart aselat an	tangguhb encana!!	2,835237745	3,844384532	1,009147
Mean			2,652842077	3,670675643	1,0178

Tabel 3.1 merupakan hasil perhitungan *entropy* pada *plaintext* dan *chipertext* dari algortima kriptografi *Caesar Chiper* dan AES yang digunakan, juga terdapat selisih dari kedua perhitungan *entropy* tersebut. Dapat dilihat pada tabel diatas nilai *entropy chipertext* lebih besar daripada nilai *entropy* pada *plaintext*. Nilai *entropy* tertinggi pada *plaintext* yaitu 3,121928095 dan terendahnya adalah 2,284159128. Sedangkan nilai *entropy* tertinggi pada *chipertext* yaitu 3,844384532 dan terendahnya yaitu 3,480721945.



Gambar 3. 14 Nilai *Entropy Plaintext* dan *Chipertext* pada *password*

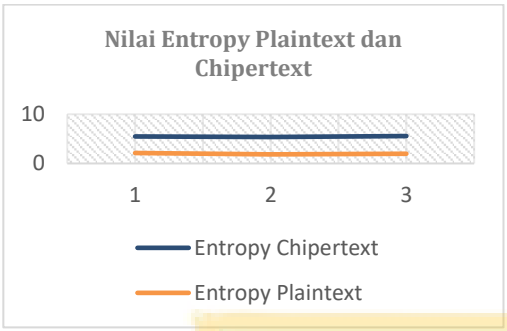
Gambar 3.14 memperlihatkan nilai *entropy* pada *plaintext* dan *chipertext* dari data sampel yang digunakan. Secara rata-rata nilai *entropy* pada *chipertext* meningkat hingga 1,0178, dengan nilai rata-rata adalah 3,670675643.

Tabel 3.2 Pengujian *Entropy Plaintext* dan *Chipertext* pada Kode Kandidat

Nama Kandidat	Plaintext	Kunci	Entropy Plaintext	Entropy Chipertext	Selisih
Riesma	2301250001	tanggu hbenc ana!!	2,121928095	3,331747563	1,2098
Qari	2301310001	tanggu hbenc ana!!	1,846439345	3,527518266	1,6811
Aulia	2302080001	tanggu hbenc ana!!	1,960964047	3,601409766	1,6404

Tabel 3.2 merupakan hasil perhitungan *entropy* pada *plaintext* dan chipertext algortima kriptografi AES yang digunakan, juga terdapat selisih dari kedua perhitungan *entropy* tersebut. Dapat dilihat pada tabel diatas nilai *entropy chipertext* lebih besar daripada nilai *entropy* pada *plaintext*. Nilai *entropy* tertinggi pada plaintext yaitu 2,121928095 dan terendahnya

adalah 1,846439345. Sedangkan nilai entropy tertinggi pada chipertext yaitu 3,601409766 dan terendahnya yaitu 3,331747563.



Gambar 3.15 Nilai *Entropy Plaintext* dan *Chipertext* pada Kode Kandidat

Gambar 3.15 memperlihatkan nilai *entropy* pada *plaintext* dan *chipertext* dari data sampel yang digunakan yaitu data kode kandidat. *Entropy* adalah nilai rerata perkiraan dari jumlah bit rerata yang dipergunakan untuk menyandikan elemen pesan. Nilai yang dikatakan tinggi dari *entropy* adalah 8. Nilai yang diperoleh dalam penelitian ini yaitu mendekati 4, maka dari itu *entropy* yang dihasilkan pada sistem ini masing sedang. Semakin bervariasi *chipertext* yang digunakan makan akan semakin tinggi *entropy* yang dihasilkan pada plaintext.

4. Kesimpulan

Sesuai dengan hasil pembahasan dan pengujian dalam penelitian ini bisa dikatakan bahwa dengan adanya sistem *voting* yang dikembangkan, proses pemilihan ketua organisasi dapat dilaksanakan secara *online* tanpa khawatir mengenai protokol kesehatan COVID-19. Sistem ini juga dapat menjamin keamanan suara pemilih, karena menggunakan metode kriptografi AES pada kode kandidatnya. Kombinasi penggunaan algoritma kriptografi AES dan *Caesar Chiper* juga berjalan dengan baik pada *password user*. Tersedianya fitur ekspor pada setiap data yang ada pada sistem, tersedia dalam berbagai format dokumen seperti pdf dan excel. Hal tersebut tentu akan mempermudah admin dalam melakukan pendataan.

Referensi

Angriani, H., & Saharaeni, Y. (2019). Implementasi Algoritma Caesar Cipher pada Keamanan Data Sistem e-voting Pemilihan Ketua Organisasi Kemahasiswaan. Inspiration: Jurnal Teknologi Informasi Dan Komunikasi, 9(2), 123. https://doi.org/10.35585/inspir.v9i2.2499

Chafid, N., & Soffiana, H. (2022). Impelementasi Algoritma Kriptografi Klasik Caesar Untuk Rancang Bangun Aplikasi E-Voting Berbasis Web (Studi Kasus : Sman 10 Tangerang). Jurnal Ilmiah Sains Dan Teknologi, 6(2), 133–145. https://doi.org/10.47080/saintek.v6i2.2249

Ibrahim, A. A. (2017). Perancangan Pengamanan Data Menggunakan Algoritma AES (Advanced Encyption Standard). III(1), 53–60.

Simarmata, J., Sriadhi, & Rahim, R. (2019). Kriptografi Teknik Keamanan Data & Informasi.

Indrawanti, A. S., Azinar, A. W., & Firdiansyah, M. A. (2018). SECURE E-VOTING MENGGUNAKAN METODE RSA DAN AUTENTIKASI RFID. Network Engineering Research Operation, 4(1), 67-75.

Irawan, C., Rachmawanto, E. H., Sari, C. A., & Sugianto, C. A. (2021, February). SUPER ENKRIPSI FILE DOKUMEN MENGGUNAKAN BEAUFORT CIPHER DAN TRANSPOSISI KOLOM. In PROSIDING SEMINAR NASIONAL LPPM UMP (pp. 556-563).

Nuraeni, F., & Agustin, Y. H. (2020). The IMPLEMENTASI CAESAR CIPHER & ADVANCED ENCRYPTION STANDAR (AES) PADA PENGAMANAN DATA PAJAK BUMI BANGUNAN. Jurnal Ilmiah MATRIK, 22(2), 187-194.

Rachmat, N., & Samsuryadi, S. (2017, November). Studi Awal Penggunaan Algoritma C4. 5 dan Logika Fuzzy pada Klasifikasi Enkripsi Transaksi Keuangan Bebasis XML. In Annual Research Seminar (ARS) (Vol. 3, No. 1, pp. 255-260)

Marsal, R. U., Arnia, F., & Adriman, R. (2018). Enkripsi dan Dekripsi Citra Menggunakan Modifikasi Algoritma Vigenere Cipher. Jurnal Komputer, Informasi Teknologi, dan Elektro, 3(3).

Sikumbang, A. H., Haryanto, E. V., & Saleh, A. (2020). Kombinasi Metode Stream Cipher Dan Caesar Cipher Dalam Pengamanan Data Kredit Customer (Studi Kasus: PT. ACE HARDWARE). Jurnal Mahasiswa Fakultas Teknik dan Ilmu Komputer, 1(1), 693-706.

Syam, F. A., Darmayunata, Y., & Afriansyah, A. (2019). Perancangan Sistem E-Voting Untuk Pemilihan Ketua OSIS SMP Negeri 10 Pekanbaru. ZONAsi: Jurnal Sistem Informasi, 1(2), 75-85.

Santoso, K. I., & Priyoatmoko, W. (2016). Pengamanan Data Mysql pada E-Commerce dengan Algoritma AES 256. SESINDO 2016, 2016.

Subagio, N., Sari, W. E., & Yulianto, Y. (2020).

Perancangan Sistem E-voting berbasis Web untuk Ketua Himpunan Mahasiswa Teknologi Rekayasa Perangkat Lunak. Buletin Poltanesa, 21(2), 42-49.

Widodo, M. A. A., Thasandra, M., Sutra, S. O., Nasution, A. B., & Ikhwan, A. (2023). Pemanfaatan Kriptografi dalam Mewujudkan Keamanan Informasi pada E-Voting di Kota Medan dengan Menggunakan Algoritma AES. Journal on Education, 5(3), 6780-6787.

Darwis, D., Wamiliana, W., & Junaidi, A. (2017). Proses Pengamanan Data Menggunakan Kombinasi Metode Kriptografi Data Encryption Standard dan Steganografi End Of File. In Prosiding Seminar Nasional METODE KUANTITATIF 2017 (Vol. 1, No. 1, pp. 228-240). Jurusan Matematika FMIPA Unila.