# PENGUJIAN AVALANCHE EFFECT PADA KRIPTOGRAFI TEKS MENGGUNAKAN AUTOKEY CIPHER

***Muslih[1], Lekso Budi Handoko[2]***
[1,2]Program Studi Teknik Infomatika, Fakultas Ilmu Komputer, Universitas Dian Nuswantoro
e-mail: [1]muslih@dsn.dinus.ac.id, [2]handoko@dsn.dinus.ac.id

***ABSTRAK***

*Di era informasi digital, sebuah informasi menjadi bagian dalam segala aspek kehidupan yang memiliki nilai yang tinggi apabila menyangkut tentang informasi pribadi sampai informasi keuangan dikarenakan informasi tersebut sangat diminati oleh beberapa pihak yang memiliki kepentingan dengan informasi tersebut. Salah satu ancaman yang sering terjadi di era infromasi digital ini adalah pembobolan data dikarenakan data tersebut memiliki nilai yang tinggi untuk memperkuat keamanan data yang kita kirimkan salah satunya adalah menggunakan kriptografi. Kriptografi memiliki banyak jenis metode dalam menyadikan pesan salah satunya adalah metode kriptografi Autokey Cipher, peneliti menggunakan metode Autokey Cipher dikarenakan metode tersebut memiliki kelebihan dalam bentuk kunci yang lebih baik dari metode pendahulunya yaitu menghasilkan hasil yang memiliki frekuensi kemunculan huruf yang sama lebih sedikit dan akan diuji menggunakan metode pengujian Avalanche Effect (AE) dan Character Error Rate (CER) untuk melihat presentase keamanan data yang disandikan. Dalam pengujian menunjukkan hasil yang cukup memuaskan dengan nilai rata-rata Avalanche Effect lebih lebih dari 50% menandakan bahwa metode Autokey Cipher memiliki nilai Avalanche Effect yang bagus dikarenakan perubahan kecil pada plainteks dapat berdampak ke cipherteks sebab terdapat beberapa bit yang berubah yang mengakibatkan perubahan yang membuat lebih aman.*

***Kata Kunci**: Kriptografi, Autokey cipher, Avalanche Effect, Character Error Rate*

## 1. PENDAHULUAN

Kemajuan teknologi di era industri 4.0 atau sering disebut era infromasi digital ini sebuah informasi menjadi bagian dalam segala aspek kehidupan yang memiliki nilai yang tinggi apabila menyangkut tentang informasi pribadi sampai informasi pendidikan, keuangan dan perbankan dikarenakan informasi tersebut sangat diminati oleh beberapa pihak yang memiliki kepentingan dengan informasi tersebut [1]–[4]. Sebuah informasi sekarang ini sangat cepat dan mudah untuk didapatkan dikarenakan kemajuan teknologi yang sangat pesat dalam berbagai aspek kehidupan tetapi dari kemajuan teknologi tersebut terdapat dampak baik juga terdapat dampak buruk seperti berbagai ancaman yang muncul dari yang berdampak kecil sampai besar dikarenakan semua orang dimana pun dapat terhubung satu sama lain melalui dunia maya.

Salah satu ancaman yang sering terjadi di era infromasi digital ini adalah kejahatan di dunia maya atau bisa disebut cybercrime yaitu menggunakan teknologi komputer dan jaringan internet untuk melakukan kejahatan yang merugikan orang lain, salah satunya adalah pembobolan data dikarenakan data tersebut memiliki informasi yang bernilai tinggi dan dapat ditukar atau dibanter dengan sesuatu [5]–[7]. Pembobolan data adalah sebuah kejahatan yang dilakukan dengan mengambil sebuah data dengan secara paksa dengan tujuan untuk mengambil, mengubah atau menghapus data tersebut oleh sebab itu diperlukan keamanan untuk melindungi kerahasiaan data tersebut agar orang yang memiliki niat jahat tidak akan mudah untuk membobol data yang anda miliki untuk memperkuat keamanan data yang kita kirimkan salah satunya adalah menggunakan kriptografi [2], [8], [9].

Kriptografi [2] adalah sebuah teknik, pengetahuan ataupun seni yang mempelajari ssebuah cara mengamankan pesan atau kata oleh pemberi pesan kepada penerima pesan secara rahasia dengan berbagai cara agar orang yang tidak berkepentingan tidak dapat mengerti isi dari pesan tersebut. Kriptografi terbagi menjadi beberapa bagian yaitu pesan awal (plainteks) adalah pesan yang semua orang dapat membacanya, kunci adalah sebuah infromasi atau tanda untuk mengubah sebuah pesan menjadi bentuk lain agar tidak mudah dibaca oleh seseorang yang tidak berhak membukanya, pesan terubah (cipherteks) adalah pesan yang telah diubah mengunakan kunci dalam mengubah atau menyamarkan plainteks ke cipherteks disebut enkripsi dan mengembalikan ke pesan semula disebut dekripsi.

Kriptografi memiliki banyak metode dalam menyadikan pesan dan terbagi menjadi kriptografi klasik dan kriptografi modern penulis menggunakan kriptografi klasik salah satunya adalah metode kriptografi Autokey Cipher, peneliti menggunakan metode Autokey Cipher dikarenakan metode tersebut mudah dalam pengimplementasiannya dan memiliki kelebihan dalam bentuk kunci yang lebih baik dari metode sebelumnya yaitu dengan menghasilkan enkripsi yang memiliki frekuensi kemunculan huruf yang sama lebih sedikit [2] oleh karena itu metode ini menjadi lebih sulit dan rumit untuk dipecahkan [10]. Autokey cipher merupakan salah satu kriptografi

klasik dengan sedikit modifikasi menggunakan pesan berupa ASCII 256 akan meningkatkan keamanan dengan cara meningkatkan kemungkinan untuk dipecahkan mengakibatkan menambahnya waktu pemecahan [6] suatu enkripsi dan autokey cipher masih digunakan sekarang ini dikarenakan diera teknologi yang cepat ini membutuhkan keamanan yang cepat atau realtime oleh karena itu autokey cipher cocok digunakan karena metode autokey cipher memiliki waktu enkripsi dan dekripsi yang cukup cepat dan pengujian akan dilakukan dengan menggunakan dua pengujian yaitu Avalanche Effect dan Character Error Rate untuk melihat presentase keamanan data yang disandikan [11], [12].

## 2. METODE PENELITIAN

### *2.1 Kriptografi*

Kriptografi atau cryptography menurut catatan masa lampau berasal dari Bahasa Yunani kuno yang lebih dari 400 tahun Masehi yang terdiri dari dua kata yaitu "cryptos" yang bermakna rahasia dan "graphein" yang bermakna menulis apabila kedua kata tersebut digabungkan memiliki arti menulis rahasia [10]. Kriptografi adalah sebuah teknik, pengetahuan ataupun seni yang mempelajari ssebuah cara mengamankan pesan atau kata oleh pemberi pesan kepada penerima pesan secara rahasia dengan berbagai cara agar orang yang tidak berkepentingan tidak dapat mengetahui pesan tersebut. Kriptografi memiliki beberapa komponen penting dalam melakukan pengubahan yaitu plaintext (pesan awal), kunci(alat untuk mengubah dan mengembalikan) seiring perkembangan zaman kerahasiaan kunci dimodifikasi semakin kuat dikarenakan ciphertext dipengaruhi oleh kunci yang digunakan, dan ciphertext(pesan yang terubah) [13]–[15].

### *2.2 Autokey Cipher*

Autokey Cipher atau juga bisa disebut Autoclave Cipher adalah salah satu metode kriptografi klasik. Autokey Cipher ditemukan pada tahun 1586 oleh blaise de Vinegere yang populer dengan menggunakan tabula recta dan kotak tabel 26 huruf alfabet dimulai dari A sampai Z [2], [8], [9]. Autokey Cipher ini adalah pengembangan dari caesar cipher dan vinegere cipher dengan cara menggeser karakter ke kanan tergantung kepada karakter key yang ditambahkan pengembangan tersebut terlihat pada bagian kunci yang berbeda dengan metode Vinegere Cipher dengan menambahkan kunci dengan pesan yang akan disandikan secara langsung oleh karena itu Autokey lebih baik daripada metode sebelumnya [1], [2], [16], sesuai pada persamaan (1) dan persamaan (2).

$$Enkripsi\ Cipherteks = Plainteks + Kunci\ \%\ 256 \quad (1)$$

$$Dekripsi\ Plainteks = Cipherteks - Kunci\ \%\ 256 \quad (2)$$

### *2.3 ASCII*

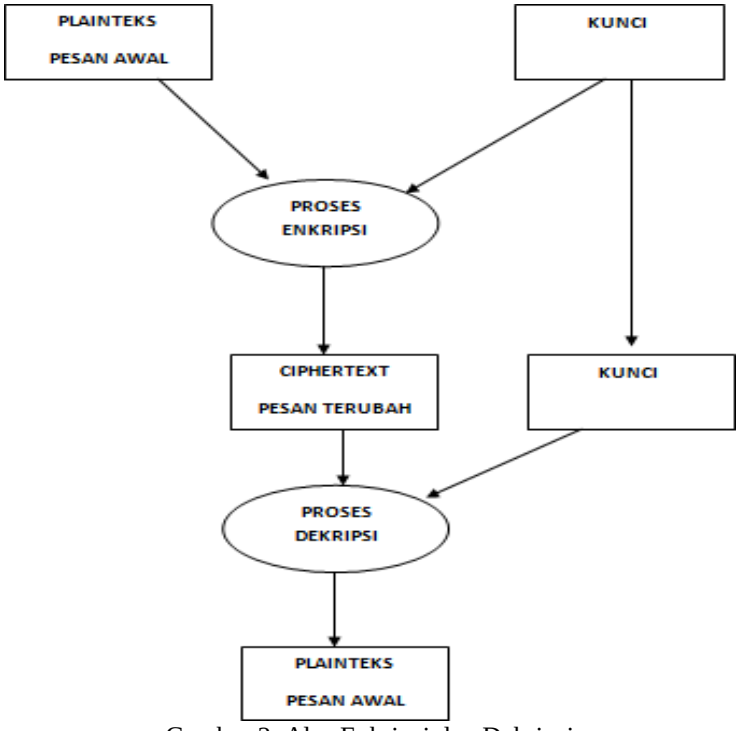
American Standard Code for Information Interchange(ACII) adalah acuan atau mewakili dalam melakukan pengkodean karakter untuk karakter dalam komunikasi yang mewakili huruf sampai simbol-simbol pada perangkat telekomunikasi dan perangkat lain- lainnya. Kode ASCII memliki 256 buah kode terbagi menjadi beberapa bagian kode yang pertama yatu ASCII 0 sampai 127 merupakan kode ASCII untuk pengkodean karakter lalu kode ASCII 128 sampai 255 merupakan kode ASCII untuk pengkodean simbol-simbol. Kode ASCII sendiri dapat dikelompokkan lagi kedalam beberapa bagian [10], [13], [17].

| DC | AC | AS+UC | DC | All | DC | All | DC | All | DC | AC | UC | EA | DC | AC | UC | EA | DC | AC | UC | EA | DC | AC | UC | EA |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| NUL | NUL | NUL | 32 | SP | 64 | @ | 96 | ` | 128 | € | xxx | Ç | 160 | | nbsp | á | 192 | À | À | └ | 224 | à | à | Ó |
| 1 | ☺ | SOH | 33 | ! | 65 | A | 97 | a | 129 | | xxx | ü | 161 | ¡ | ¡ | í | 193 | Á | Á | ┴ | 225 | á | á | ß |
| 2 | ☻ | STX | 34 | " | 66 | B | 98 | b | 130 | ‚ | BPH | é | 162 | ¢ | ¢ | ó | 194 | Â | Â | ┬ | 226 | â | â | Ô |
| 3 | ♥ | ETX | 35 | # | 67 | C | 99 | c | 131 | ƒ | NBH | â | 163 | £ | £ | ú | 195 | Ã | Ã | ├ | 227 | ã | ã | Ò |
| 4 | ♦ | EOT | 36 | $ | 68 | D | 100 | d | 132 | „ | IND | ä | 164 | ¤ | ¤ | ñ | 196 | Ä | Ä | ─ | 228 | ä | ä | õ |
| 5 | ♣ | ENQ | 37 | % | 69 | E | 101 | e | 133 | … | NEL | à | 165 | ¥ | ¥ | Ñ | 197 | Å | Å | ┼ | 229 | å | å | Õ |
| 6 | ♠ | ACK | 38 | & | 70 | F | 102 | f | 134 | † | SSA | å | 166 | ¦ | ¦ | ª | 198 | Æ | Æ | ã | 230 | æ | æ | µ |
| 7 | • | BEL | 39 | ' | 71 | G | 103 | g | 135 | ‡ | ESA | ç | 167 | § | § | º | 199 | Ç | Ç | Ã | 231 | ç | ç | þ |
| 8 | ◘ | BS | 40 | ( | 72 | H | 104 | h | 136 | ˆ | HTS | ê | 168 | ¨ | ¨ | ¿ | 200 | È | È | ╚ | 232 | è | è | Þ |
| 9 | ○ | HT | 41 | ) | 73 | I | 105 | i | 137 | ‰ | HTJ | ë | 169 | © | © | ® | 201 | É | É | ╔ | 233 | é | é | Ú |
| 10 | ◙ | LF | 42 | * | 74 | J | 106 | j | 138 | Š | VTS | è | 170 | ª | ª | ¬ | 202 | Ê | Ê | ╩ | 234 | ê | ê | Û |
| 11 | ♂ | VT | 43 | + | 75 | K | 107 | k | 139 | ‹ | PLD | ï | 171 | « | « | ½ | 203 | Ë | Ë | ╦ | 235 | ë | ë | Ù |
| 12 | ♀ | FF | 44 | , | 76 | L | 108 | l | 140 | Œ | PLU | î | 172 | ¬ | ¬ | ¼ | 204 | Ì | Ì | ╠ | 236 | ì | ì | ý |
| 13 | ♪ | CR | 45 | - | 77 | M | 109 | m | 141 | | RI | ì | 173 | - | - | ¡ | 205 | Í | Í | ═ | 237 | í | í | Ý |
| 14 | ♫ | SO | 46 | . | 78 | N | 110 | n | 142 | Ž | SS2 | Ä | 174 | ® | ® | « | 206 | Î | Î | ╬ | 238 | î | î | ¯ |
| 15 | ☼ | SI | 47 | / | 79 | O | 111 | o | 143 | | SS3 | Å | 175 | ¯ | ¯ | » | 207 | Ï | Ï | ¤ | 239 | ï | ï | ´ |
| 16 | ► | DLE | 48 | 0 | 80 | P | 112 | p | 144 | | DSC | É | 176 | ° | ° | ░ | 208 | Ð | Ð | ð | 240 | ð | ð |  |
| 17 | ◄ | DC1 | 49 | 1 | 81 | Q | 113 | q | 145 | ‘ | PU1 | æ | 177 | ± | ± | ▒ | 209 | Ñ | Ñ | Ð | 241 | ñ | ñ | ± |
| 18 | ↕ | DC2 | 50 | 2 | 82 | R | 114 | r | 146 | ’ | PU2 | Æ | 178 | ² | ² | ▓ | 210 | Ò | Ò | Ê | 242 | ò | ò | ‗ |
| 19 | ‼ | DC3 | 51 | 3 | 83 | S | 115 | s | 147 | “ | STS | ô | 179 | ³ | ³ | │ | 211 | Ó | Ó | Ë | 243 | ó | ó | ¾ |
| 20 | ¶ | DC4 | 52 | 4 | 84 | T | 116 | t | 148 | ” | CCH | ö | 180 | ´ | ´ | ┤ | 212 | Õ | Õ | È | 244 | ô | ô | ¶ |
| 21 | § | NAK | 53 | 5 | 85 | U | 117 | u | 149 | • | MW | ò | 181 | µ | µ | Á | 213 | Õ | Õ | ı | 245 | õ | õ | § |
| 22 | ▬ | SYN | 54 | 6 | 86 | V | 118 | v | 150 | – | SPA | û | 182 | ¶ | ¶ | Â | 214 | Ö | Ö | Í | 246 | ö | ö | ÷ |
| 23 | ↨ | ETB | 55 | 7 | 87 | W | 119 | w | 151 | — | EPA | ù | 183 | · | · | À | 215 | × | × | Î | 247 | ÷ | ÷ | ¸ |
| 24 | ↑ | CAN | 56 | 8 | 88 | X | 120 | x | 152 | ˜ | SOS | ÿ | 184 | ¸ | ¸ | © | 216 | Ø | Ø | Ï | 248 | ø | ø | ° |
| 25 | ↓ | EM | 57 | 9 | 89 | Y | 121 | y | 153 | ™ | xxx | Ö | 185 | ¹ | ¹ | ╣ | 217 | Ù | Ù | ┘ | 249 | ù | ù | ¨ |
| 26 | → | SUB | 58 | : | 90 | Z | 122 | z | 154 | š | SCI | Ü | 186 | º | º | ║ | 218 | Ú | Ú | ┌ | 250 | ú | ú | · |
| 27 | ← | ESC | 59 | ; | 91 | [ | 123 | { | 155 | › | CSI | ø | 187 | » | » | ╗ | 219 | Û | Û | █ | 251 | û | û | ¹ |
| 28 | ∟ | FS | 60 | < | 92 | \ | 124 | \| | 156 | œ | ST | £ | 188 | ¼ | ¼ | ╝ | 220 | Ü | Ü | ▄ | 252 | ü | ü | ³ |
| 29 | ↔ | GS | 61 | = | 93 | ] | 125 | } | 157 | | OSC | Ø | 189 | ½ | ½ | ¢ | 221 | Ý | Ý | ¦ | 253 | ý | ý | ² |
| 30 | ▲ | RS | 62 | > | 94 | ^ | 126 | ~ | 158 | ž | PM | × | 190 | ¾ | ¾ | ¥ | 222 | Þ | Þ | ▌ | 254 | þ | þ | ■ |
| 31 | ▼ | US | 63 | ? | 95 | _ | 127 | DEL | 159 | Ÿ | APC | ƒ | 191 | ¿ | ¿ | ┐ | 223 | ß | ß | ▀ | 255 | ÿ | ÿ | nbsp |

Gambar 1 ASCII

*2.4 Proses Enkripsi dan Dekripsi*

Berdasarkan Gambar 2, proses enkripsi dimulai dengan memasukan pesan awal atau plainteks dan kunci lalu dilakukan proses enkripsi sebuah pesan dan menghasilkan pesan tersandi atau cipherteks dan untuk melakukan dekripsi dibutuhkan pesan tersandi dan kunci yang ditentukan diawal lalu dilakukan proses dekripsi dan mengembalikan ciphertkes kembali ke plainteks.




Gambar 2. Alur Enkripsi dan Dekripsi

*2.5 Avalache Effect (AE)*

Avalanche Effect adalah sebuah metode untuk mencari dan mengetahui berapa persen pengubahan pesan pada saat proses enkripsi dilakukan dengan melihat rasio antara jumlah bit dari cipherteks yang berubah dan jumlah bit dari plainteks sebelum dirubah dalam proses enkripsi [11], [18]–[21] semakin besar persen yang dihasilkan semakin bagus juga enkripsi yang dihasilkan dan sebaliknya. Pengujian Avalanche Effect dianggap baik apabila terjadi perubahan bit yang menunjukkan antara 45-60% (50 % adalah hasil yang dianggap baik dalam pengujian). Perubahaan sebesar 50% akan mengakibatkan masalah yang cukup sulit untuk para pembobol melakukan serangan terhadap data yang dimiliki sesuai pada persaman (3).

$$Avalanche\ Effect = \frac{jumlah\ bit\ berbeda}{total\ bit}\ x\ 100\% \quad (3)$$

*2.5 Character Eror Rate (CER)*

Character Error Rate adalah sebuah metode pengujian yang digunakan untuk mengukur presentase tingkat akurasi sebuah hasil enkripsi dengan cara mencocokan dan membandingkan character (huruf, angka, simbol) yang dimiliki plainteks dibandingkan dengan plainteks yang ditambah atau diubah semakin rendah presentase semakin bagus juga hasil enkripsinya dan sebaliknya [22], [23] seperti pada persamaan (4) di bawah ini.

$$Character\ Error\ Rate = \frac{jumlah\ karakter\ berbeda}{jumlah\ karakter\ yang\ dikirim}\ x\ 100\% \quad (4)$$

## 4. HASIL DAN PEMBAHASAN

Dari pembahasan diatas akan dilakukan sebuah percobaan dengan menggunakan media berbentuk pesan yaitu “Pulang keSemarang jam-8 malam!” dan perubahan 1 kata “Pulang kesemarang jam-8 malam!” dengan kunci petang tahap pertama ubah karakter pesan dan kunci ke bentuk decimal seperti P=80 dengan mencocokkannya dengan tabel ASCII 256 ulangi sampai karakter terakhir setelah itu tambahkan bentuk decimal pesan dan kunci lalu ubah kembali kebentuk karakter dengan mencocokkan kembali dengan tabel ASCII 256. Proses enkripsi pesan dapat di lihat pada Gambar 1 dan Gambar 2.

| P | u | l | a | n | g | | k | e | S |
|---|---|---|---|---|---|---|---|---|---|
| 80 | 117 | 108 | 97 | 110 | 103 | | 107 | 101 | 83 |
| p | e | t | a | n | g | P | u | l | a |
| 112 | 101 | 116 | 97 | 110 | 103 | 80 | 117 | 108 | 97 |
| À | Ú | à | Â | Ù | Î | p | à | Ñ | ´ |
| 192 | 218 | 224 | 194 | 220 | 206 | 80 | 224 | 209 | 180 |
| e | m | a | r | a | n | g | | j | a |
| 101 | 109 | 97 | 114 | 97 | 110 | 103 | | 106 | 97 |
| n | g | | k | e | S | e | m | a | r |
| 110 | 103 | 32 | 107 | 101 | 83 | 101 | 109 | 97 | 114 |
| Ó | Ô | | Ý | Æ | Á | Ì | | Ë | Ó |
| 211 | 212 | 129 | 221 | 198 | 193 | 204 | 109 | 203 | 211 |
| m | - | 8 | | m | a | l | a | m | ! |
| 109 | 45 | 56 | 32 | 109 | 97 | 108 | 97 | 109 | 33 |
| a | n | g | | j | a | m | - | 8 | |
| 97 | 110 | 103 | 32 | 106 | 97 | 109 | 45 | 56 | 32 |
| Î | | | @ | × | Â | Ù | | ¥ | A |
| 206 | 155 | 159 | 64 | 215 | 194 | 217 | 142 | 165 | 65 |

Gambar 1. Proses enkripsi pesan 1

Dari hasil enkripsi membuktikan bahwa pesan dapat disandikan dengan baik setelah itu pesan tersandi akan diubah kembali ke bentuk semula dengan cipherteks “ÀÚàÂÜÎpàÑ´ÓÔÝÆÁÌËÓÎ@×ÂÙ¥A” dan “ÀÚàÂÜÎpàÑÔÓÔÝÆáÌËÓÎ@×ÂÙŽ ¥A” dengan kunci yang sudah digunakan untuk melakukan enkripsi tahap pertama ubah karakter cipherteks dan kunci ke bentuk decimal seperti À=192 dengan mencocokkannya dengan tabel ASCII 256 pada Gambar 1, ulangi sampai karakter terakhir setelah itu kurangkan bentuk decimal pesan dan kunci lalu ubah kembali kebentuk karakter dengan mencocokkan kembali dengan tabel ASCII 256.

| P | u | l | a | n | g | | k | e | s |
|---|---|---|---|---|---|---|---|---|---|
| 80 | 117 | 108 | 97 | 110 | 103 | | 107 | 101 | 115 |
| p | e | t | a | n | g | P | u | l | a |
| 112 | 101 | 116 | 97 | 110 | 103 | 80 | 117 | 108 | 97 |
| À | Ú | à | Â | Ü | Î | p | à | Ñ | ´Ô |
| 192 | 218 | 224 | 194 | 220 | 206 | 80 | 224 | 209 | 212 |
| e | m | a | r | a | n | g | | j | a |
| 101 | 109 | 97 | 114 | 97 | 110 | 103 | | 106 | 97 |
| n | g | | k | e | S | e | m | a | r |
| 110 | 103 | 32 | 107 | 101 | 115 | 101 | 109 | 97 | 114 |
| Ó | Õ | | Ý | Æ | á | Ì | | Ë | Ó |
| 211 | 212 | 129 | 221 | 198 | 225 | 204 | 109 | 203 | 211 |
| m | - | 8 | | m | a | l | a | m | ! |
| 109 | 45 | 56 | 32 | 109 | 97 | 108 | 97 | 109 | 33 |
| a | n | g | | j | a | m | - | 8 | |
| 97 | 110 | 103 | 32 | 106 | 97 | 109 | 45 | 56 | 32 |
| Ì | | | @ | × | Ä | Ù | | ¥ | A |
| 206 | 155 | 159 | 64 | 215 | 194 | 217 | 142 | 165 | 65 |

Gambar 2. Proses enkripsi pesan 2

| À | Ú | à | Â | Ü | Î | p | à | Ñ | ´ |
|---|---|---|---|---|---|---|---|---|---|
| 192 | 218 | 224 | 194 | 220 | 206 | 112 | 224 | 209 | 180 |
| p | e | t | a | n | g | P | u | l | a |
| 112 | 101 | 116 | 97 | 110 | 103 | 80 | 117 | 108 | 97 |
| P | u | l | a | n | g | | k | e | S |
| 80 | 117 | 108 | 97 | 110 | 103 | 32 | 107 | 101 | 83 |
| Ó | Õ | | Ý | Æ | Á | Ì | | Ë | Ó |
| 211 | 212 | 129 | 221 | 198 | 193 | 204 | 141 | 203 | 211 |
| n | g | | k | e | S | e | m | a | r |
| 110 | 103 | 32 | 107 | 101 | 83 | 101 | 109 | 97 | 114 |
| e | m | a | r | a | n | g | | j | a |
| 101 | 109 | 97 | 114 | 97 | 110 | 103 | 32 | 106 | 97 |
| Ì | | | @ | × | Ä | Ù | | ¥ | A |
| 206 | 155 | 159 | 64 | 215 | 194 | 217 | 142 | 165 | 65 |
| a | n | g | | j | a | m | - | 8 | |
| 97 | 110 | 103 | 32 | 106 | 97 | 109 | 45 | 56 | 32 |
| m | - | 8 | | m | a | l | a | m | ! |
| 109 | 45 | 56 | 32 | 109 | 97 | 108 | 97 | 109 | 33 |

Gambar 3. Proses dekripsi pesan 1

| À | Ú | à | Â | Ü | Î | p | à | Ñ | Ô |
|---|---|---|---|---|---|---|---|---|---|
| 192 | 218 | 224 | 194 | 220 | 206 | 112 | 224 | 209 | 212 |
| p | e | t | a | n | g | P | u | l | a |
| 112 | 101 | 116 | 97 | 110 | 103 | 80 | 117 | 108 | 97 |
| P | u | l | a | n | g | | k | e | s |
| 80 | 117 | 108 | 97 | 110 | 103 | 32 | 107 | 101 | 115 |
| Ó | Õ | | Ý | Æ | á | Ì | | Ë | Ó |
| 211 | 212 | 129 | 221 | 198 | 225 | 204 | 141 | 203 | 211 |
| n | g | | k | e | s | e | m | a | r |
| 110 | 103 | 32 | 107 | 101 | 115 | 101 | 109 | 97 | 114 |
| e | m | a | r | a | n | g | | j | a |
| 101 | 109 | 97 | 114 | 97 | 110 | 103 | 32 | 106 | 97 |
| Ì | | | @ | × | Ä | Ù | | ¥ | A |
| 206 | 155 | 159 | 64 | 215 | 194 | 217 | 142 | 165 | 65 |
| a | n | g | | j | a | m | - | 8 | |
| 97 | 110 | 103 | 32 | 106 | 97 | 109 | 45 | 56 | 32 |
| m | - | 8 | | m | a | l | a | m | ! |
| 109 | 45 | 56 | 32 | 109 | 97 | 108 | 97 | 109 | 33 |

Gambar 4. Proses dekripsi pesan 2

Setelah melakukan perhitungan enkripsi dan dekripsi dari dua pesan diatas dapatdibuktikan dengan mencocokkan hasil enkripsi dan dekripsi dari aplikasi seperti pada Gambar 5.


Gambar 5. Tampilan Aplikasi

Pada pengujian ini, telah digunakan 33 buah percobaaan dengan pesan mulai dari 8 kata ditambah sampai 26 kata dengan kunci dari 1 kata ditambah sampai 3 kata juga menggunakan 6 buah angka.

Tabel 1. Pengujian Avalanche Effect dan Character Error Rate

| Plainteks | Kunci | Rata-rata Avalanche Effect | Character Error Rate |
|---|---|---|---|
| 8 kata | 1 Kata | 56,5% | 2% |
| 8 kata | 1 Kata | 57% | 4% |
| 8 kata | 2 Kata | 58,5% | 2% |
| 8 kata | 2 Kata | 59% | 4% |
| 8 kata | 3 Kata | 56,5% | 2% |
| 8 kata | 3 Kata | 57% | 4% |
| 8 kata | 6 angka | 58% | 2% |
| 8 kata | 6 angka | 58% | 6% |
| 12 kata | 1 Kata | 55,5% | 1% |
| 12 kata | 1 Kata | 55,5% | 4% |
| 12 kata | 2 Kata | 59,5% | 1% |
| 12 kata | 2 Kata | 59,5% | 4% |
| 12 kata | 3 Kata | 56% | 1% |
| 12 kata | 3 Kata | 56% | 4% |
| 12 kata | 6 angka | 56% | 4% |
| 12 kata | 6 angka | 57% | 8% |
| 16 kata | 1 Kata | 56% | 1% |
| 16 kata | 1 Kata | 56% | 2% |
| 16 kata | 2 Kata | 58% | 1% |
| 16 kata | 2 Kata | 58% | 2% |
| 16 kata | 3 Kata | 57% | 1% |
| 16 kata | 3 Kata | 57% | 2% |
| 16 kata | 6 angka | 57% | 2% |
| 16 kata | 6 angka | 57% | 6% |

| | | | |
|---|---|---|---|
| 20 kata | 1 Kata | 56,5% | 1% |
| 20 kata | 1 Kata | 57% | 2% |
| 20 kata | 2 Kata | 58% | 1% |
| 20 kata | 2 Kata | 58,5% | 2% |
| 20 kata | 3 Kata | 57,5% | 1% |
| 20 kata | 3 Kata | 58% | 2% |
| 20 kata | 6 angka | 56% | 2% |
| 20 kata | 6 angka | 56% | 4% |
| 26 kata | 1 kata | 56% | 1% |

Berdasarkan hasil pengujian pada Tabel 1, dapat dilihat bahwa pengamanan menggunakan metode Autokey Cipher menghasilkan nilai rata-rata Avalanche Effect dari dua buah pesan sebesar 50% keatas menandakan bahwa metode Autokey Cipher memiliki nilai Avalanche Effect yang bagus dikarenakan perubahan kecil pada plainteks dapat berdampak ke cipherteks sebab terdapat beberapa bit yang berubah yang mengakibatkan perubahan yang membuat lebih aman dikarenakan membuat perbedaan waktu pemecahan suatu cipherteks satu dengan cipherteks yang lain dan penggunakan ASCII 256 gabungan antara huruf besar, huruf kecil, angka dan simbol membuat lebih banyak kemungkinan dalam waktu pemecahan cipherteks.

## 5. KESIMPULAN

Berdasarkan penelitian yang telah dilakukan dapat disimpulkan bahwa metode Autokey Cipher dapat menyandikan sebuah pesan dengan baik yang sulit dipecahkan dan dapat mengembailkannya ke bentuk awal. Pada penelitian yang telah dilakukan metode Autokey Cipher mendapatkan hasil rata-rata nilai Avalanche Effect yang baik dengan nilai diatas 50% menunjukan bahawa metode Autokey Cipher dapat menyandikan pesan dengan baik dan pengubahan panjang pesan dan kunci dapat mempengaruhi nilai Avalanche Effectnya.

## 6. SARAN

Pada penelitian selanjutnaya. media yang digunakan dapat ditingkatkan menjadi media citra atau video dengan ukuran kunci autokey yang lebih panjang. Untuk menganalisa lebih lanjut, dapat ditambahkan proses perhitungan Bit Error Rate (BER), entropy maupun histogram hasil enkripsi dekripsi pesan.

## DAFTAR PUSTAKA

[1] Muhammad Fadlan, Haryansyah, and Rosmini, "Pengamanan Data melalui Model Super Enkripsi Autokey Cipher dan Transposisi Kolom," *J. RESTI (Rekayasa Sist. dan Teknol. Informasi)*, vol. 5, no. 6, pp. 1113–1119, Dec. 2021.

[2] M. Fadlan, R. Rosmini, and H. Haryansyah, "Perpaduan Algoritma Kriptografi Atbash dan Autokey Cipher dalam Mengamankan Data," *J. MEDIA Inform. BUDIDARMA*, vol. 5, no. 3, p. 806, Jul. 2021.

[3] C. A. Sari and E. H. Rachmawanto, "Penyembunyian Data Untuk Seluruh Ekstensi File Menggunakan Kriptografi Vernam Cipher dan Bit Shiffting," *J. Appl. Intell. Syst.*, vol. 1, no. 3, pp. 179–190, 2016.

[4] T. S. Permana, C. A. Sari, E. H. Rachmawanto, D. R. I. M. Setiadi, and E. R. Subhiyakto, "Implementasi Pengamanan Citra Digital Berbasis Metode Kriptografi Vernam Cipher," *Techno.Com*, vol. 16, no. 4, pp. 337–347, 2017.

[5] E. H. Rachmawanto and C. A. Sari, "Keamanan File Menggunakan Teknik Kriptografi Shift Cipher," *Techno.COM*, vol. 14, no. 4, pp. 329–335, 2015.

[6] C. A. Sari, E. H. Rachmawanto, D. W. Utomo, and R. R. Sani, "Penyembunyian Data Untuk Seluruh Ekstensi File Menggunakan Kriptografi Vernam Cipher dan Bit Shiffting," *J. Appl. Intell. Syst.*, vol. 1, no. 3, pp. 179–190, 2016.

[7] L. B. Handoko, C. Umam, and C. A. Sari, "Autentikasi Citra RGB Menggunakan Kombinasi Fungsi HASH MD5 dan RSA," in *Prosiding SNST ke-9*, 2018, pp. 28–33.

[8] D. C. Brown, "A cryptanalysis of the autokey cipher using the index of coincidence," in *Proceedings of the ACMSE 2018 Conference*, 2018, vol. 2018-Janua, pp. 1–8.

[9] O. Grošek, E. Antal, and T. Fabšič, "Remarks on breaking the Vigenère autokey cipher," *Cryptologia*, vol. 43, no. 6, pp. 486–496, Nov. 2019.

[10] A. Elmogy, Y. Bouteraa, R. Alshabanat, and W. Alghaslan, "A New Cryptography Algorithm Based on

ASCII Code," *19th Int. Conf. Sci. Tech. Autom. Control Comput. Eng. STA 2019*, pp. 626–631, 2019.
[11] M. Essaid, I. Akharraz, A. Saaidi, and et A. Mouhib, "Image encryption scheme based on a new secure variant of Hill cipher and 1D chaotic maps," *J. Inf. Secur. Appl.*, vol. 47, pp. 173–187, Aug. 2019.
[12] A. Salam, D. R. I. M. Setiadi, E. H. Rachmawanto, and C. A. Sari, "ShiftMod Cipher: A Symmetrical Cryptosystem Scheme," in *2019 International Seminar on Application for Technology of Information and Communication (iSemantic)*, 2019, pp. 1–5.
[13] E. Y. Purba, S. Efendi, P. Sirait, and P. Sihombing, "Collaboration of RSA Algorithm Using EM2B Key with Word Auto Key Encryption Cryptography Method in Encryption of SQL Plaintext Database," *J. Phys. Conf. Ser.*, vol. 1230, no. 1, p. 012009, Jul. 2019.
[14] R. Rahim *et al.*, "Combination Vigenere Cipher and One Time Pad for Data Security," *Int. J. Eng. Technol.*, vol. 7, no. 2.3, pp. 92–94, 2018.
[15] W. S. Sari, E. H. Rachmawanto, D. R. I. M. Setiadi, and C. A. Sari, "A Good Performance OTP Encryption Image based on DCT-DWT Steganography," *TELKOMNIKA (Telecommunication Comput. Electron. Control.*, vol. 15, no. 4, p. 1982, Dec. 2017.
[16] S. B. Sadkhan and S. F. Jawad, "Security Evaluation Methods and the used parameters for Some Cryptosystem," in *2020 International Conference on Computer Science and Software Engineering (CSASE)*, 2020, pp. 314–318.
[17] A. R. Tulloh, Y. Permanasari, and E. Harahap, "Kriptografi Advanced Encryption Standard ( AES ) Untuk Penyandian File Dokumen," *J. Mat. UNISBA*, vol. 2, no. 1, pp. 118–125, 2016.
[18] S. Sugiyanto and R. K. Hapsari, "Pengembangan Algoritma Advanced Encryption Standard pada Sistem Keamanan SMS Berbasis Android Menggunakan Algoritma Vigenere," *J. Ultim.*, vol. 8, no. 2, pp. 131–138, May 2017.
[19] A. Subandi, M. S. Lydia, R. W. Sembiring, M. Zarlis, and S. Efendi, "Vigenere cipher algorithm modification by adopting RC6 key expansion and double encryption process," *IOP Conf. Ser. Mater. Sci. Eng.*, vol. 420, no. 1, p. 012119, Oct. 2018.
[20] J. P. Sermeno, K. A. S. Secugal, and N. E. Mistio, "Modified Vigenere cryptosystem: An integrated data encryption module for learning management system," *Int. J. Appl. Sci. Eng.*, vol. 18, no. 4, pp. 1–10, 2021.
[21] P. Witoolkollachit, "The avalanche effect of various hash functions between encrypted raw images versus non-encrypted images : A comparison study," *J. Thai Med. Informatics Assoc.*, vol. 1, pp. 69–82, 2016.
[22] R. Damaševičius, R. Maskeliūnas, E. Kazanavičius, and M. Woźniak, "Combining Cryptography with EEG Biometrics," *Comput. Intell. Neurosci.*, vol. 2018, pp. 1–11, 2018.
[23] M. K. Samimi and T. S. Rappaport, "3-D Millimeter-Wave Statistical Channel Model for 5G Wireless System Design," *IEEE Trans. Microw. Theory Tech.*, vol. 64, no. 7, pp. 2207–2225, Jul. 2016.