# KOMBINASI *VIGENERE* DAN *AUTOKEY CIPHER* DALAM PROSES PROTEKSI SMS BERBASIS *ANDROID*

**Chaerul Umam[1*], Lekso Budi Handoko[1], Christy Atika Sari[1], Eko Hari Rachmawanto[1], dan Lucky Arif Rahman Hakim[1]**
[1] Teknik Informatika, Universitas Dian Nuswantoro, Semarang
Jl. Imam Bonjol No 207 Semarang 50131
[*]Email: chaerul@dsn.dinus.ac.id

**Abstrak**

*Kriptografi merupakan salah satu bidang studi yang bermanfaat untuk menerapkan keamanan pada data yang dapat berupa file, gambar, ataupun text. Dengan perkembangan sistem operasi Android saat ini, media penyampaian pesan lewat text juga ikut berkembang pesat dengan munculnya berbagai aplikasi pengiriman pesan, seperti WhatsApp, Telegram ataupun Line. Namun, meski aplikasi pengirim teks mulai bermunculan, layanan pesan singkat (SMS) masih bisa eksis digunakan untuk melakukan pertukaran informasi sampai sekarang. Karena keamanan privasi dalam suatu pertukaran informasi itu sangat penting, maka melakukan enkripsi pada pesan dapat menjadi alternatif untuk meningkatkan keamanan privasi pada pesan yang dikirim. Dari berbagai teknik enkripsi yang ada, penggabungan 2 teknik enkripsi merupakan langkah yang baik untuk lebih memingkatkan keamanan pesan, diantaranya adalah Vigenere dan Autokey. Vigenere cipher merupakan algortima kriptografi klasik yang sederhana, mudah diimplementasikan dan dapat diterapkan pada objek data SMS. Autokey cipher merupakan pengembangan dari Vigenere cipher yang memanfaakan key stream dan crossover yang dinilai lebih aman dibanding vigenere. Dengan melakukan penggabungan teknik enkripsi dan pemanfaatan kunci unik, dapat meningkatkan keamanan dalam melakukan pertukaran informasi melalui SMS berbassis Android. Pengujian AE pada hasil enkripsi menunjukkan nilai Avalanche Effect (AE) mendekati 50% yaitu 53,2% pada cipher ukuran pendek. Pada cipher ukuran sedang menggunakan 1400 bit, diketahui nilai AE terbaik yang dihasilkan hanya 34,2% saja.*

***Kata kunci:*** *SMS, Enkripsi, Vigenere Cipher, Autokey Cipher, Android.*

## 1. PENDAHULUAN

Dengan perkembangan ilmu pengetahuan yang semakin pesat dalam bidang teknologi dan juga informasi saat ini, memberikan berbagai kemudahan pada masyarakat, salah satunya adalah dalam hal komunikasi atau data dengan cepat dan bebas digunakan oleh semua orang. Jika dulu dalam hal komunikasi jarak jauh masyarakat menggunakan layanan Pos untuk melakukan komunikasi jarak jauh yang tentunya memakan waktu yang begitu lama untuk menerima pertukaran informasi, maka dengan perkembangan teknologi saat ini, masyarakat sudah bisa menggunakan layanan pesan singkat atau SMS untuk bertukar informasi (Kristianto and Syarifudin, 2020). Perkembangan telepon seluler yang semakin pesat memunculkan berbagai sistem operasi baru dengan berbagai fitur di dalamnya. Salah satu dari sistem operasi yang ada sampai sekarang adalah android, yang merupakan suatu sistem operasi berbasis linux. Meski perkembangan android yang begitu pesat dan berbagai aplikasi baru bermunculan. Diantaranya adalah aplikasi dalam hal komunikasi teks seperti WhatsApp, Telegram atau Line, layanan pesan atau SMS masih menjadi aplikasi yang wajib dalam platform android, karena penggunaannya yang mudah dan tidak memerlukan jaringan internet (Syahroji and Pradana, 2018). Dalam hal komunikasi tentu ada hal-hal yang bersifat privasi atau hanya ingin diberitahukan kepada orang-orang terntentu saja. Dan hal ini dapat dihindari dengan menggunakan ilmu kriptografi, yang dapat dimanfaatkan untuk pembuatan keamanan pada pesan dengan cara merahasiakan isi pesan yang hanya dapat dimengerti oleh orang-orang tertentu saja, karena jika pesan tersebut tersebar maka akan berdampak buruk bagi si pengirim atau yang seharusnya menerima pesan tersebut. Dalam merahasiakan pesan tersebut salah satu caranya adalah melakukan enkripsi yaitu melakukan proses untuk menyamarkan atau menyandikan pesan sehingga tidak mudah dibaca atau dimengerti oleh orang lain dan hanya orang tertentu saja yang bisa paham atau mengartikan pesan tersebut (Muharram, Azis and Manga, 2018).

e-ISSN: 2964-2531
DOI : 10.36499/psnst.v12i1.7108
p-ISSN: 2964-5131

Layanan SMS yang ada pada aplikasi bawaan dinilai tidak aman dalam melakukan pertukaran informasi karena SMS harus melewati *Short Message Service Center* (*SMSC*) yang mana itu berfungsi untuk mencatat komunikasi yang terjadi antara pengirim dan penerima (Kristianto and Syarifudin, 2020). Dengan mengetahui hal tersebut bisa dipastikan ada kemungkinan kebocoran informasi yang ingin disampaikan melalui *SMSC*. Dibutuhkan beberapa level algoritma atau metode enkripsi untuk meningkatkan tingkat keamanan dari informasi yang ingin disampaikan, atau bisa disebut juga sebagai *multiple encryption*. *Multiple Encryption* merupakan suatu metode untuk meningkatkan keamanan data atau informasi dengan melakukan proses enkripsi secara berulang menggunakan algortitma yang sama atau berbeda guna meningkatkan kompleksitas enkripsi pada data atau informasi (Sulaksono, 2016). (Wibowo, Hakim and Sugiyanto, 2018) telah membuat pengembangan algoritma *advance encryption standard* pada sistem keamanan sms dengan menggunakan algoritma *vigenere* berbasis *android*. Dengan menambahkan algoritma *vigenere* diharapkan dapat meningkatkan keamanan pada pengiriman dan penerimaan pesan yang telah menggunakan algoritma AES. Dari penelitian tersebut didapatkan kesimpulan bahwa penerapan algortima *vigenere* dan juga AES dapat mengamankan isi pesan yang dikirim ataupun diterima. Selain itu hal tersebut juga menunjukkan bahwa penggabungan 2 algoritma untuk melakukan pengamanan pesan terbukti lebih baik.Selain menggunakan kombinasi algoritma AES dan *vigenere*, penulis juga berasumsi jika menggunakan gabungan algoritma *vigenere* dan *autokey* juga akan membuat tingkat keamanan pesan yang akan dikirim atau diterima menjadi lebih baik. Dimana pesan yang akan dikirim akan dienkripsi terlebih dahulu dengan algororitma *vigenere* kemudian dilakukan enkripsi lagi dengan algoritma *autokey*, dan tentunya menggunakan *key* yang sama untuk melakukan proses enkripsi.

## 2. TINJAUAN PUSTAKA

### 2.1. Vigenere Cipher

Enkripsi merupakan suatu proses yang berguna untuk melakukan pengamanan pada data atau informasi, dengan kata lain menyandikan data atau mengacak data supaya bisa dibaca oleh orang tertentu. Selain menyandikan pesan atau informasi, Kriptografi juga bisa melakukan konversi pesan atau *plaintext* menjadi sebuah *ciphertext* yang bisa dikembalikan ke dalam bentuk awal sebelum disandikan, inilah yang disebut dengan proses dekripsi (Maricar and Sastra, 2018; Isfahani and Nugraha, 2019; Vittal Kumar Mittal | Manish Mukhija, 2019). *Vigenere Cipher* merupakan algoritma kriptografi klasik yang ditemukan oleh Battisa Bellaso pada tahun 1553, diambil dari namanya sendiri Blaise de Vigenere (Mulyono *et al.*, 2018). Alasan pengambilan nama *vigenere* adalah karena beliau menemukan kunci yang lebih kuat lagi untuk algoritma ini dengan menggunakan algoritma *autokey cipher* meskipun algoritma ini dasarnya sudah ditemukan oleh Giovan Battista Bellaso terlebih dahulu. Pada tahun 1917 algoritma *vigenere cipher* menjadi terkenal karena sulit dipecahkan, bahkan hal tersebut juga didukung oleh matematikawan Charles Utwidge Dodgson dan juga ilmuan Amerika yang menyatakan bahwa *vigenere* merupakan suatu algoritma yang tidak mungkin dipecahkan. Akan tetapi Kasiski berhasil membantah pernyataan tersebut dengan berhasil memecahkan algoritma *vigenere* pada abad ke-19. Dalam penelitian ini pesan yang dienkripsi hanya karakter huruf abjad saja, itu artinya penggunaan nomor ataupun tanda baca tidak dihitung (Maricar and Sastra, 2018). Maka dengan ketentuan tersebut dapat ditulisakan pada persamaan (1) dan (2), dimana Ci adalah nilai desimal karakter ciphertext ke-I, Pi adalah nilai desimal karakter plaintext ke-I, Ki dan Ci adalah nilai desimal karakter kunci ke-i.

$$Enkripsi \rightarrow Ci = (Pi + Ki) \bmod 26 \quad (1)$$

$$Dekripsi \rightarrow Pi = (Ci - Ki) \bmod 26 \quad (2)$$

### 2.2. Autokey Cipher

Autokey merupakan variasi dari *vigenere cipher*. Dalam melakukan enkripsi sendiri *autokey* ini sangat mirip dengan *vigenere cipher* yang membedakannya hanya pada bagian *keystream*. Dimana *keystream* ini dibuat dengan awalan kata kunci atau frase kunci, lalu menambahkan lalu menambahkannya pada akhir teks. *Tabula Recta* yang digunakan untuk menentukan *keystream*

adalah bagian atas, kemudian untuk *plaintext* di sebelah kiri, dan menggunakan *crossover* untuk menentukan huruf ciphertextnya, kemudian untuk melakukan dekripsi dengan *autokey*, pertama kali yang dilakukan adalah menggunakan huruf pertama dari kunci pada bagian atas, kemudian menentukan huruf ciphertext pada bagian kolomnya, lalu diambil huruf plaintext pada bagian kiri baris.

## 3. METODE PENELITIAN

### 3.1. Alur Kerja Proses Enkripsi Dekripsi

Proses enkripsi dan deskripsi akan dijelaskan menggunakan gambar *flowchart*. Proses enkripsi bisa dilihat pada Gambar 1. Dimana pada Gambar 1 pengirim pesan akan menginputkan pesan dan juga kunci yang akan digunakan untuk menginkripsi pesan, selanjutnya pengirim pesan bisa menginputkan nomor yang akan dituju. Jika berhasil maka akan muncul notifikasi pesan berhasil dikirim.


**Gambar 1. Alur Enkripsi**


**Gambar 2. Alur Dekripsi**

Berdasarkan tahapan enrkripsi pada Gambar 1, pengguna memasukkan pesan dan juga kunci yang akan digunakan. Setelah itu pengirim pesan bisa menginkripsi pesan terlebih dahulu untuk melihat hasil pesan enkripsi sebelum dikirim. Pesan akan dienkripsi dengan algoritma *vigenere cipher* setelah itu sistem akan melanjutkan enkripsi lagi dengan menggunakan algoritma *autokey cipher* dan masih menggunakan kunci yang sama. Setelah hasil pesan dienkripsi muncul, pengirim pesan bisa menginputkan nomor tujuan. Pesan yang berhasil dikirim akan memunculkan pemberitahuan jika pesan berhasil dikirim. Sementara untuk mendeskripsi pesan seperti pada Gambar 2, pengguna memasukkan pesan dan juga kunci yang diterima. Setelah itu penerima pesan bisa melakukan dekripsi terhadap pesan dan juga kunci yang diterima. Pesan akan didekripsi dengan algoritma *autokey cipher* terlebih dahulu, setelah itu sistem akan melanjutkan dekripsi lagi dengan menggunakan algoritma *vigenere cipher* dan masih menggunakan kunci yang sama. Setelah itu pesan yang didekripsi tadi akan muncul.

### 3.2. Avalanche Effect (AE)

Secara harfiah *Avalanche* dapat diartikan sebagai longsoran salju. Dengan istilah tersebut *Avalanche Effect* bisa muncul karena prosesnya yang mirip dengan *Avalanche* atau longsoran salju yang mana hanya dengan longsoran kecil bisa menimbulkan longsoran yang lebih *Avalanche Effect* merupakan salah satu teknik yang digunakan untuk menggambarkan tingkat keamanan dari suatu proses kriptografi kunci simetris dan juga fungsi hash (Sermeno, Secugal and Mistio, 2021). Dan jika suatu algoritma mendapatkan 45%-60% dari *Avalanche Effect* maka bisa dikatakan baik. Avalanche Effect dapat dihitung dengan menggunakan persamaan berikut:

$$Avalanche\ Effect = \left(\frac{jumlah\ bit\ flip}{total\ bit}\right) \times 100\% \quad (3)$$

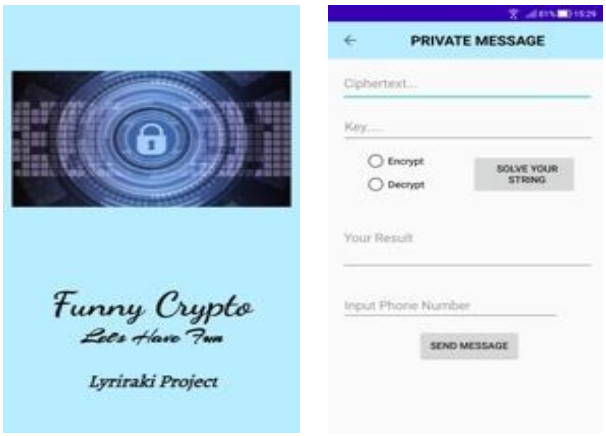
**DOI : 10.36499/psnst.v12i1.7108**
**e-ISSN: 2964-2531**
**p-ISSN: 2964-5131**

## 4. HASIL DAN PEMBAHASAN

Aplikasi ini dirancang untuk membuat layanan pesan (SMS) yang sebelum dikirimkan akan dienkripsi terlebih dahulu untuk merahasiakan isi pesan dari orang lain. Dan dalam melakukan proses enkripsi, pesan akan dienkripsi sebanyak 2x dengan algoritma yang berbeda untuk membuat pesan menjadi sulit untuk dipecahkan. Kemudian pesan yang telah di enkripsi tadi akan dikirimkan langsung melalui aplikasi tanpa menggunakan aplikasi pihak ke-3. Dengan begitu, pesan yang akan diterima sudah berbentuk enkripsi, sehingga penerima pesan harus melakukan dekripsi menggunakan kunci untuk mengubah isi pesan tadi supaya bisa diterjemahkan ke pesan aslinya.

### 4.1. Pengujian Black Box

Implementasi dari desain *flowchart* pada tampilan *user interface* ketika dibuka akan menampilkan animasi awal seperti Gambar 3 (a). Setelah animasi aplikasi selesai, maka akan diarahkan ke form input untuk melakukan inputan pesan, *key*, nomer telepon dan juga pemilihan proses enkripsi ataupun dekripsi pada pesan yang bisa dilihat pada Gambar 3 (b). Hasil pengujian untuk aplikasi pengiriman pesan akan dilakukan dengan pengujian *blackbox* yang dapat dilihat pada Tabel 1 untuk proses enkripsi dan Tabel 2 untuk dekripsi. Beberapa skenario Tabel 1 yang akan diuji diantara lain adalah form input pesan kosong, form input key kosong, fom input key dan pesan kosong, tidak melakukan pemilihan proses enkripsi, melakukan proses enkripsi, form nomor telepon tidak diisi, semua form diisi dengan lengkap dan benar, tampilan pesan yang dikirim. Kemudian untuk skenario pada Tabel 2 yang akan diuji diantara lainnya yaitu form input pesan kosong, form input key kosong, fom input key dan pesan kosong, tidak melakukan pemilihan proses dekripsi, dekripsi dengan key yang berbeda dan dekripsi dengan key yang sesungguhnya

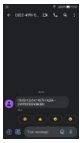



(a) (b)

**Gambar 3. (a) Tampilan Awal Aplikasi, (b) Tanpilan Form Enkripsi-Dekripsi**

**Tabel 1. Pengujian Enkripsi**

| Skenario Pengujian | Test Case | Keterangan | Skenario Pengujian | Test Case | Keterangan |
|---|---|---|---|---|---|
| Form input pesan kosong. |  | Berjalan dengan baik, tidak terdapat eror | Melakukan proses enkripsi |  | Berjalan dengan baik, tidak terdapat eror |
| Form input key kosong. |  | Berjalan dengan baik, tidak terdapat eror | Form nomor telepon tidak diisi. |  | Berjalan dengan baik, tidak terdapat eror |

| Skenario Pengujian | Test Case | Keterangan |
|---|---|---|
| Fom input key dan pesan kosong. |  | Berjalan dengan baik, tidak terdapat eror |
| Tidak melakukan pemilihan proses enkripsi. |  | Berjalan dengan baik, tidak terdapat eror |
| Semua form diisi dengan lengkap dan benar. |  | Berjalan dengan baik, tidak terdapat eror |
| Tampilan pesan yang dikirim |  | Berjalan dengan baik, tidak terdapat eror |

**Tabel 2. Pengujian Dekripsi**

| Skenario Pengujian | Test Case | Keterangan |
|---|---|---|
| Form input pesan kosong. . |  | Berjalan dengan baik, tidak terdapat eror |
| Form input key kosong. |  | Berjalan dengan baik, tidak terdapat eror |
| Fom input key dan pesan kosong. |  | Berjalan dengan baik, tidak terdapat eror |
| Tidak melakukan pemilihan proses dekripsi. |  | Berjalan dengan baik, tidak terdapat eror |
| Dekripsi dengan key yang berbeda. |  | Berjalan dengan baik, tidak terdapat eror |
| Dekripsi dengan key yang sesunggu |  | Berjalan dengan baik, tidak terdapat eror |

## 4.2. Pengujian Evalanche Effect

Avalnche Effect yang akan diimplementasikan adalah dengan mengganti karakter pertama dari kunci atau *key* dengan karakter lain supaya menghasilkan hasil enkripsi yang berbeda, kemudian akan dibandingkan untuk dengan rumus Avalanche Effect seperti pada Tabel 3 untuk mengilustrasikan plainteks ukuran kecil. Hasil perhitungan rata-rata yang didapatkan dari *Avalanche Effect* pada percobaan pertama yaitu 45,75%. Perolehan ini cukup baik, mengingat nilai AE yang baik yaitu mendekati 50%. Diketahui bahwa jumlah perubahan bit yang kecil dalam pesan yang panjang tentu akan berpengaruh pada nilai AE yang optimal. Pada percobaan kedua dengan ukuran pesan lebih panjangyaitu 1400 bit, dihasilkan nilai rata-rata AE sebesar 47,33%. Dilihat dari segi waktu eksekusi enkripsi maupun dekripsi tidak menemui kendala.

**Tabel 3. Pengujian AE pada Plainteks Ukuran Kecil**

| Keterangan | Percobaan ke- | | |
|---|---|---|---|
| | 1 | 2 | 3 |
| Plainteks | Work From Home | Belajar untuk masa depan yang lebih cerah | Tidak menyerah untuk menggapai impian dengan selalu giat belajar dan berdoa |
| Key | Semangat | Semangat | Semangat |
| Hasil Enkripsi | GWPK FDOY NKBO | LMJAJMR GYFDK VMJG AFHKZ KSZT XRBVR CDHTJ | DQBAK YEZBUSAR SRSCW BEUMTFTSS MZHOMM LKVSBV EBWCYA SVEH UCWUBID GJP MEMDRN |
| Modifikasi Key | Zemangat | Zemangat | Zemangat |
| Hasil Enkripsi | UWPK FDOY BKBO | ZMJAJMR GMFDK VMJG OFHKZ KSZH XRBVR CDVTJ | RQBAK YEZPUSAR SRSQW BEUMTFHSS MZHOMA LKVSBV EPWCYA SVEV UCWUBID UJP MEMDRB |
| Total bit | 96 | 280 | 520 |
| Perubahan bit | 4 | 4 | 22 |
| Lama Waktu Eksekusi | 0.005 detik | 0.006 detik | 0.007 detik |
| Avalanche effect | 41,6% | 53,2% | 42,3% |
| Rata-rata AE | | | 45,7% |

**DOI : 10.36499/psnst.v12i1.7108**
**e-ISSN: 2964-2531**
**p-ISSN: 2964-5131**

**Tabel 3. Pengujian AE pada Plainteks Ukuran Sedang**

| Keterangan | Percobaan ke- | | |
|---|---|---|---|
| | 4 | 5 | 6 |
| Plainteks | Ketika kamu mengeluh akan banyaknya pekerjaan yang diberikan padamu saat ini ingatlah bahwa di luar sana masih banyak orang orang yang juga ingin mendapatkan pekerjaan seperti apa yang sedang kamu kerjakan | Ketika kamu mengeluh akan banyaknya pekerjaan yang diberikan padamu saat ini ingatlah bahwa di luar sana masih banyak orang orang yang juga ingin mendapatkan pekerjaan seperti apa yang sedang kamu kerjakan | Ketika kamu mengeluh akan banyaknya pekerjaan yang diberikan padamu saat ini ingatlah bahwa di luar sana masih banyak orang orang yang juga ingin mendapatkan pekerjaan seperti apa yang sedang kamu kerjakan |
| Key | Semangat | Berusaha sekuat tenaga mewujudkan impian | Teruslah berusaha |
| Hasil Enkripsi | UMRIKM KMGG<br>DMXSOXQJ KONF<br>FXRNYUNXB<br>BBQCBWKAO MSPX<br>MUBDZQVGQ JBTBCC<br>SNBT XXC AFGMMFXX<br>HNNIT AS ATAY AACS<br>FSSZL BZXSYC WKBZD<br>UPKBJ YZDC YUTS<br>GZDWU GKZLZFQEWEM<br>SQJMITAZC IYBTATU<br>NTO VCEZ MEEKTE<br>XGQY ZOMNKKYH | MMBWUA YAWC<br>GSNSQTUH MKYV<br>TOFMGENYQ NIAERVMBJ<br>SALG ZKHWEAATH<br>WMNYHN GFMZ MAG<br>YAOAXCLP JBPWB JV BPSI<br>MWVN BMVGB NGFMZM<br>BZYYQ EKLPV HOEC<br>XXYT WBXMZ<br>HEZPSVPMYFZ<br>VIYVHUKEE STDKFQO<br>XJQ GCOM MDXEAV KNUF<br>IWSEYUEU | WMBWUW KOOC<br>USXGSLQT BGUJ<br>LOBAUCKES AKZMPTJBB<br>NGVE AGPTHAWFG<br>LAEAUP MNII MQY<br>ABDLTCCB DGRWH LH<br>BKBH OTMC BJGZD<br>PDHRCY PFAOI IZGFN<br>NAMM RSEN IOOEM<br>ABTPAOOKSQJ<br>XFSUMJONE SFXFPDR<br>PHM KZKQ SFVQKS PDQU<br>NGXRBASF |
| Modifikasi Key | Zemangat | Verusaha sekuat tenaga mewujudkan impian | Ceruslah berusaha |
| Hasil Enkripsi | IMRIKM KMUG<br>DMXSOXEJ KONF<br>FXFNYUNXB<br>BPQCBWKAO ASPX<br>MUBDNQVGQ JBTPCC<br>SNBT XLC AFGMMFLX<br>HNNIT AG ATAY AACG<br>FSSZL BZLSYC WKBZR<br>UPKBJ YZRC YUTS<br>GZRWU GKZLZTQEWEM<br>SQXMITAZC IMBTATU<br>NTC VCEZ MEEYTE<br>XGQY ZCMNKKYH | AMBWUA YAWC<br>GSNSQTUH MKYV<br>TOFMGENYQ NIAERJMBJ<br>SALG ZKHWEAATH<br>WMNYHN GFMZ MAG<br>YAOAXCZP JBPWB JV BPSI<br>MWVN BMVGB NGFMZM<br>BZYYQ EKLDV HOEC<br>XXYT WBXMZ<br>HEZPSVPMYFZ<br>VIYVHUKEE SHDKFQO<br>XJQ GCOM MDXEAV KNUF<br>IWSEYUEU | OMBWUW KOOC<br>USXGSLIT BGUJ<br>LOBAUCKES ACZMPTJBB<br>NGVE AGPTZAWFG<br>LAEAUP MNII MIY<br>ABDLTCCB DGRWH LZ<br>BKBH OTMC BJGZD<br>PDZRCY PFAOI IZGFN<br>NAEM RSEN IOOEM<br>ABTPAGOKSQJ<br>XFSUMJONE SXXFPDR<br>PHM KZKQ SFVIKS PDQU<br>NGXRBASF |
| Total bit | 1400 | 1400 | 1400 |
| Perubahan bit | 48 | 13 | 21 |
| Lama Waktu Eksekusi | 0.012 detik | 0.006 detik | 0.008 detik |
| Avalanche effect | 34,2% | 92,8% | 15% |
| Rata-rata AE | | 47,33% | |

## 5. KESIMPULAN

Penggunaan gabungan algoritma Vigenere Cipher dan Autokey Cipher pada pesan mendapatkan rata-rata *Avalacnhe Effect* sudah mendekati 50%, hal ini menunjukkan bahwa gabungan ke-2 algortima tersebut cukup baik. Dari hasil rata-rata yang didapat, dapat disimpulkan bahwa rendahnya nilai rata-rata yang didapat disebabkan ke-2 algoritma *Vigenere* dan *Autokey* hanya mendukung enkripsi dan dekripsi huruf alfabet. Dari hasil penelitian yang dilakukan, adapun saran untuk pengembangan penelitian selanjutnya dapat menggunakan karakter ASCII secara lengkap dan bukan hanya huruf saja, dapat mengakses dan memilih kontak yang tersimpan di dalam daftar kontak serta dapat diterapkan untuk mengirim e-mail atau pesan elektronik lainnya atau menambahkan algoritma lain untuk membuat pesan teks lebih rumit dan meningkatkan keamanan privasi.

## DAFTAR PUSTAKA

Isfahani, F. Al and Nugraha, F. (2019) ‘Implementasi Steganografi LSB dengan Enkripsi Base64

Pada Citra dengan Ruang Warna CMYK', *ScientiCO : Computer Science and Informatics Journal*, pp. 1–8. doi: 10.22487/j26204118.2018.v1.i2.11221.

Kristianto, B. D. and Syarifudin, G. (2020) 'Perancangan Perangkat Lunak Enkripsi SMS Menggunakan Algoritma RC6 Dan Rijndael Pada Smartphone SMS Encryption Software Design Using RC6 and Rijndael Algorithms on Smartphones', *Jurnal Ilmiah SISFOTENIKA*, 10(1), pp. 115–126.

Maricar, M. A. and Sastra, N. P. (2018) 'Efektivitas Pesan Teks Dengan Cipher Substitusi, Vigenere Cipher, dan Cipher Transposisi', *Majalah Ilmiah Teknologi Elektro*, 17(1), p. 59. doi: 10.24843/mite.2018.v17i01.p08.

Muharram, F., Azis, H. and Manga, A. R. (2018) 'Analisis Algoritma pada Proses Enkripsi dan Dekripsi File Menggunakan Advanced Encryption Standard (AES)', *Prosiding Seminar Nasional Ilmu Komputer dan Teknologi Informasi*, 3(2), pp. 112–115.

Mulyono, I. U. W. *et al.* (2018) 'Encryption of Text Message on Audio Steganography Using Combination Vigenere Cipher and LSB (Least Significant Bit)', *Kinetik: Game Technology, Information System, Computer Network, Computing, Electronics, and Control*, 4(1), pp. 63–74. doi: 10.22219/kinetik.v4i1.701.

Sermeno, J. P., Secugal, K. A. S. and Mistio, N. E. (2021) 'Modified Vigenere cryptosystem: An integrated data encryption module for learning management system', *International Journal of Applied Science and Engineering*, 18(4), pp. 1–10. doi: 10.6703/IJASE.202106_18(4).003.

Subimawanto, D. *et al.* (2014) 'Implementasi Algoritma Kriptografi Kode Caesar, Vigenere, dan Transposisi untuk Sistem Proteksi Penggunaan Pesan Singkat (SMS) pada Smartphone Android', *Prosiding Seminar ilmiah Nasional Komputer dan Sistem Intelijen (KOMMIT 2014)*, 8(14-15 Oktober), pp. 146–154.

Sulaksono, D. H. (2016) 'MULTIPLE ENCRYPTION DENGAN MENGGUNAKAN METODE VIGENERE CHIPER DAN BLOWFISH', *SCAN : Jurnal Teknologi Informasi dan Komunikasi*, XI, pp. 25–30.

Syahroji, A. and Pradana, R. (2018) 'Vigenere Cipher dan Affine Cipher untuk Pengamanan Chatting Berbasis Android', *Skanika*, 1(3), pp. 1168–1175. Available at: https://jom.fti.budiluhur.ac.id/index.php/SKANIKA/article/view/2542.

Vittal Kumar Mittal | Manish Mukhija (2019) 'Cryptosystem Based on Modified Vigenere Cipher using Encryption Technique', *International Journal of Trend in Scientific Research and Development (IJTSRD) International Journal of Trend in Scientific Research and Development*, 3(5), pp. 1936–1939. doi: https://doi.org/10.31142/ijtsrd27878.

Wibowo, F., Hakim, D. K. and Sugiyanto, S. (2018) 'PENDUGAAN KELAS MUTU BUAH PEPAYA BERDASARKAN CIRI TEKSTUR GLCM MENGGUNAKAN ALGORITMA K-NEAREST NEIGHBORS', *Jurnal Nasional Pendidikan Teknik Informatika (JANAPATI)*, 7(1), p. 100. doi: 10.23887/janapati.v7i1.12991.