E-ISSN: 2985-7406

PERBANDINGAN KINERJA ALGORITMA KANDIDAT AES DALAM ENKRIPSI DAN DEKRIPSI FILE DOKUMEN

M Bima Putra Sansaya[1*)], Ahmad Farisi[2]
[1,2]Pogram Studi rnformatika, Fakultas Ilmu Komputer dan Rekayasa, Universitas Multi Data Palembang
[1]sansayabima00@mhs.mdp.ac.id, [2]ahmadfarisi@mhs.mdp.ac.id

Kata kunci:
dokumen; kinerja; rijndael; serpent; twofish;

Abstract: *Document file is one of valueable information format which needed security to prevent unauthorized party to access. using cryptography. Cryptography can be implemented on android device because of how mobile it is, however it has performance issues. Performance-friendly cryptography algorithm is needed to encrypt document on android platformed devices. This study compares the performances of AES candidates algorithms while encrypting and decrypting document file on android platform. This experiments measures times, memory usages, CPU percentages, file sizes, speeds, and avalanche effect. Results shows the fastest encryption time is 196.51 ms and decryption on 204.04 ms done by Rijndael. The most efficient memory usages are 1547.9 KB and 1464.19 KB done by Serpent. The most efficient CPU percentages are 6.43% and 4.28% both done by Rijndael. Rijndael are the fastest with 9825.68 KB/s encryption and 9241.42 KB/s decryption speed. The highest average of avalanche effect are 49.99% done by Twofish.*

Abstrak: File dokumen adalah salah satu bentuk informasi yang berharga sehingga diperlukan sistem keamanan untuk menjaga agar informasi didalamnya tidak dapat diakses oleh pihak yang tidak berwenang dengan kriptografi. Teknologi yang dapat menerapkan kriptografi adalah android yang dikenal memiliki mobilitas tinggi, dengan keterbatasan kinerja. Untuk itu dibutuhkan algoritma kriptografi dengan kinerja efisien untuk melakukan kriptografi file dokumen pada platform android. Penelitian ini bertujuan untuk membandingkan kinerja algoritma kriptografi Kandidat AES dalam enkripsi dan dekripsi file dokumen di perangkat android. Pengujian akan mengukur waktu, penggunaan memori, persentase CPU, ukuran file, kecepatan enkripsi, dan *avalanche effect*. Hasil pengujian menunjukkan waktu enkripsi tercepat adalah 196.51 ms, waktu dekripsi tercepat 204.04 ms, oleh Rijndael. Penggunaan memori peling efisien 1547.9 KB dan 1464.19 KB oleh Serpent. Persentase penggunaan CPU paling efisien 6.43% dan 4.28%, oleh Rijndael. Kecepatan enkripsi tertinggi 9825.68 KB/detik dan kecepatan dekripsi 9241.42 KB/detik oleh Rijndael. Rata-rata *avalanche effect* tertinggi 49.99% oleh algoritma Twofish.

Sansaya. Farisi. (2023). Perbandingan Kinerja Algoritma Kandidat AES Dalam Enkripsi dan Dekripsi File Dokumen. *MDP Student Conference* 2023

PENDAHULUAN

Latar Belakang

Pada era digital ini, informasi sering kali dipertukarkan melalui media internet sehingga menjadi salah satu sumber daya yang bernilai tinggi dan membutuhkan sistem keamanan agar tidak dapat diakses oleh pihak yang tidak diinginkan [1]. Sarana perubahan bentuk informasi yang sangat penting baik di kehidupan sehari-hari, organisasi, maupun bisnis adalah file dokumen, dimana dokumen-dokumen seperti dokumen negara, dokumen persidangan, dokumen ujian, dan dokumen lain yang sifatnya penting dan rahasia membutuhkan peningkatan keamanan selain dari yang disediakan aplikasi pengolah file, mengingat file dokumen saat ini memiliki format digital seperti .doc. dan .pdf [2]. Bidang keilmuan yang mempelajari cara mengamankan pesan maupun informasi adalah kriptografi melalui teknik enkripsi untuk mengubah pesan menjadi teks sandi agar tidak dapat dibaca oleh orang yang tidak memiliki hak [3], teknik mengembalikan informasi sehingga dapat dibaca oleh pihak yang berwenang disebut dekripsi [4]. Teknologi yang penting untuk mengimplementasi kriptografi karena banyak digunakan masyarakat luas adalah Android karena sifatnya yang mudah, cepat, dan memiliki mobilitas tinggi, namum dinyatakan memiliki masalah pada kinerja karena keterbatasan *resource*, sehingga kinerja perlu diperhatikan ketika mengimplementasikan kriptografi pada *platform* Android [5].

Algoritma yang paling umum digunakan saat ini adalah algoritma AES dimana banyak penelitian terdahulu menunjukkan bahwa Algoritma AES memiliki performa paling unggul dan tingkat keamanan terbaik dibandingkan metode lainnya [6]. AES atau *Advanced Encryption Standard* merupakan algoritma kriptografi yang didesain pada tahun 2000 khusus untuk menggantikan DES atau *Data Encryption Standard* yang pada masa itu sudah dinyatakan tidak aman lagi [7]. AES dipilih oleh *National Institute of Standards and Technologi* (NIST) melalui sayembara. Tiga algoritma dengan peringkat teratas secara berturut-turut adalah Rijndael yang terpilih sebagai AES, Serpent, dan Twofish [8].

Beberapa penelitian sebelumnya melakukan analisis kinerja pada algoritma kandidat AES dan menemukan kinerja Rijndael sebagai algoritma AES terpilih berada di bawah algoritma Kandidat AES lainya. Beberapa diantaranya bahkan mencoba melakukan modifikasi pada Rijndael untuk meningkatkan kinerja tersebut. Algoritma Serpent dan Twofish sebagai sesama peringkat tiga besar dibandingkan dengan algoritma Rijndael untuk mengetahui perbandingan kinerja dari ketiganya.

Penelitian [8] melakukan analisis perbandingan kinerja algoritma Kandidat AES untuk mengenkripsi teks pada smartphone Android dan IOS. Penelitian ini menggunakan algoritma Rijndael, Serpent, dan Twofish untuk mengenkripsi berbagi kombinasi karakter sepeti alfabet, numerik, alfanumerik, dan kombinasi alfanumerik dan simbol. Hasil penelitian ini menunjukkan bahwa algoritma Serpent unggul pada rata-rata kecepatandan penggunaan CPU, sedangkan algoritma Twofish dan Rijndael lebih unggul dalam penggunaan memori.

Penelitian lainnya yang juga melakukan analisis kinerja dari algoritma Kandidat AES adalah penelitian [9]. Penelitian ini membandingkan algoritma Rijndael, Serpent, dan Twofish pada panjang kunci 256-bit untuk mengenkripsi teks pada *platform* android. Hasil penelitian menunjukkan bahwa ukuran file berpengaruh terhadap waktu enkripsi dan dekripsi dengan algoritma Serpent memiliki waktu tercepat.Algoritma Serpent dan Twofish unggul pada penggunaan memori dan Rijndael unggul pda penggunaan CPU.

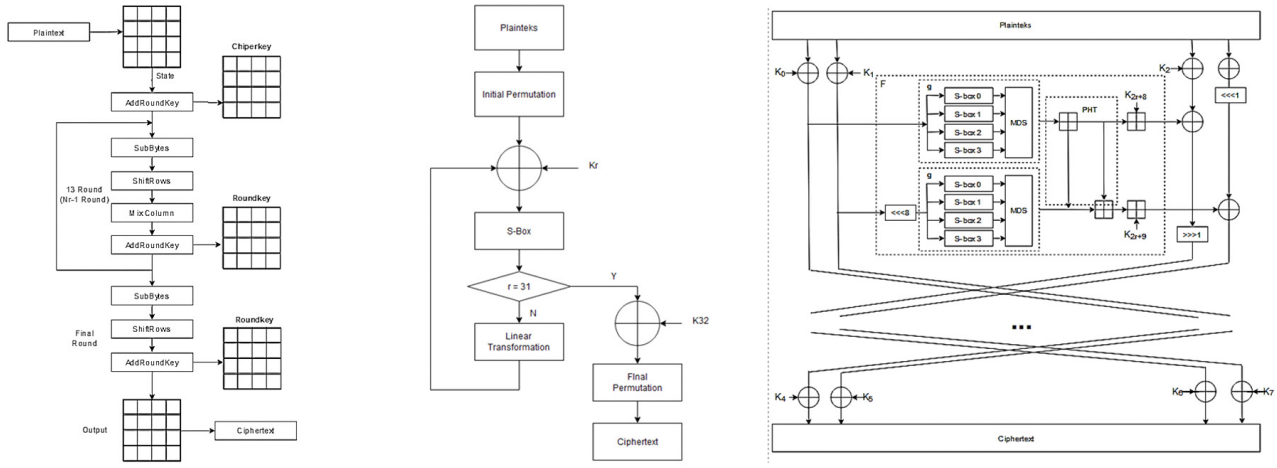
Penelitian lainnya melakukan perbandingan kinerja antara Algoritma Serpent dan Twofish. Penelitian [7] membandingkan kecepatan dan besar ukuran file yang dihasilkan. Penelitian ini mengenkripsi file dataset menggunakan semua ukuran panjang kunci yaitu 128-bit, 192-bit, dan 256-bt. Hasil penelitian menunjukkan Twofish lebih efisien dalam kecepatan enkripsi. Ukuran file terenkripsi juga selalu lebih besar daipada ukuran file aslinya. Penelitian ini juga mengukur kinerja berupa kekuatan enkripsi berdasarkan ketahanan *ciphertext* terhadap serangan *brute force* dimana Twofish lebih unggul dibandingkan Serpent.

Penlitian lainnya yang juga mengukur dan membandingkan kekuatan enkripsi antara salah satu Kandidat AES yaitu Rijndael dengan algoritma RSA adalah penelitian [10]. Kekuatan enkripsi diukur melalui *avalanche effect*. Hasil penelitian menunjukkan bahwa algoritma AES tidak lebih unggul daripada algoritma RSA dalam kinerja kekuatan enkripsi.

Berdasarkan kajian literatur yang dilakukan pada beberapa penelitian yang telah dijabarkan, penelitian ini akan meneruskan penelitian [8] dan penelitian [9] yang mengukur dan membandingkan kinerja algoritma Kandidat AES 128-bit pada perangkat android, namun penelitian ini akan melakukan enkripsi pada file dokumen dan menambahkan beberapa kinerja yang akan diukur yaitu ukuran file dan kecepatan enkripsi seperti penelitian [7] dan *avalanche effect* seperti pada penelitian [10]. Penelitian ini penting dilakukan untuk menemukan algoritma mana yang paling efisien untuk mengimplementasikan kriptografi pada file dokumen di perangkat android berdasarkan kebutuhan kinerjanya, sehingga membantu pengembang aplikasi android untuk memilih metode kriptografi yang paling sesuai.

METODE

Metode yang akan digunakan adalah tiga algoritma Kandidat AES peringkat teratas yaitu algoritma (1) Rijndael terdiri dari 13 *round* transformasi *bytes*, yaitu *Sub Bytes, Shift Rows, Mix Collumn,* dan *Add Roundkey*, (2) Serpent, terdiri atas lapisan permutasi yaitu *initial permutation*, *substitution permutation*, dan *final permutation*, dan (3) Twofish, terbentuk dari 16 round jaringan feistel, dimana fungsi F terdiri atas *Sub Bytes*, matriks *Maximum Distance Seperable* atau MDS, *Psuedo-Hadamart Transformation* atau PHT, dan rotasi *bitwise*. Ketiga algoritma tersebut mengikuti sayembara pemilihan algoritma AES oleh NIST dan memenuhi kriteria seperti panjang kunci, blocksize, dan rancangan dengan tingkat keamanan tinggi [7]. Alur prooses ketiga algoritma ditunjukkan pada Gambar 1.



Gambar 1. Proses Algoritma Kandidat AES [1] [8] [7]

Penelitian ini akan melakukan beberapa pengujian, dimana parameter kinerja dan metode pengukuran yang akan dipakai adalah (1) Waktu eksekusi yang diukur menggunakan metode *currentTimeMillis*() pada kelas *System* dan (2) Penggunaan Memori menggunakan metode *totalMemory* dan *freeMemory* pada kelas *Runtime,* keduanya mengacu pada penelitian [11], (3) Persentase CPU menggunakan CPU Profiler seperti pada penelitian [8], (4) ukuran file setelah enkripsi dan (5) Kecepatan enkripsi seperti penelitian [12], serta *avalanche effect* seperti pada penelitian [10] dan [13].

Perangkat yang akan digunakan pada penelitian ini ditunjukkan pada Tabel 1.

Tabel 1. Perangkat yang Digunakan

Nama Perangkat	Spesifikasi	Sistem Operasi
Xiaomi Redmi Note 10 Pro	CPU Octa-core 2.3 Ghz Kryo 470 Gold 8 GB RAM *Internal Memory* 128 GB	Android 11
Oppo Reno 2F	Octa-core 2.0 Ghz Cortex-A53 8 GB RAM *Internal Memory* 128 GB	Android 11
Oppo A96	Octa-core 2.4 Ghz Kryo 265 Gold 8 GB RAM *Internal Memory* 256 GB	Android 11
Oppo Reno 4	Octa-core 1.8 Ghz Kryo 465 Silver 8 GB RAM *Internal Memory* 128 GB	Android 11
Oppo A16	Octa-core 2.3 Ghz Cortex-A53 3 GB RAM *Internal Memory* 32 GB	Android 11
Samsung Galaxy Tab A 10.1	Octa-core 1.6 Ghz Cortex-A53 2 GB RAM *Internal Memory* 16 GB	Android 7.1.1

Menggunakan perangkat yang dicantumkan pada tabel 1, penelitian ini akan melakukan skenario percobaan, dimana setiap perangkat akan melakukan enkripsi atau dekripsi pada masing-masing 10 file .doc. dan ,pdf, dan setiap file akan diproses menggunakan algoritma Rijndael, Serpent, dan Twofish, serta menggunakan karakter kunci alfabet, numerik, alfanumerik, dan alfanumerik beserta simbol. Percobaan yang akan diujikan adalah (1) percobaan 1-A, yaitu enkripsi file .doc. (720 percobaan), (2) percobaan 2-A, yaitu enkripsi file .pdf. (720 percobaan), (3) percobaan 1-B, yaitu dekripsi file .doc. (720 percobaan), dan (4) percobaan 2-A, yaitu dekripsi file .pdf. (720 percobaan).

Adapun beberapa batasan masalah yang ditetapkan pada penelitian ini antara lain, (1) algoritma yang digunakan menggunakan panjang kunci 128- bit, (2) file pengujian adalah file *sample* yang bersifat public untuk digunakan pada penelitian, diakses dari beragam sumber.

HASIL DAN PEMBAHASAN

Berdasarkan serangkaian percobaan yang telah dilakukan, kinerja dicatat berupa waktu, penggunaan memori, penggunaan CPU, ukuran file, kecepatan, dan avalanche effect. Hasil pengujian yang diperoleh dirangkum dalam tabel-tabel berikut, Rata-rata waktu, kecepatan, penggunaan memori dan penggunaan CPU ketika enkripsi ditunjukkan pada Tabel 2 untuk algoritma Rijndael, Tabel 3 menunjukkan hasil algoritma serpent, dan Twofish ditunjukkan pada Tabel 4.

Tabel 2. Kinerja Enkripsi Rijndael

Skenario	Waktu (ms)	Penggunaan Memori (KB)	Penggunaan CPU (%)	Kecepatan (KB/s)
1-A	145.9	1599.57	5.68	9322.2
2-A	247.11	2133.09	7.18	10329.16
Rata-rata	**196.51**	**1866.33**	6.43	**9825.68**

Tabel 3. Kinerja Enkripsi Serpent

Skenario	Waktu (ms)	Penggunaan Memori (KB)	Penggunaan CPU (%)	Kecepatan (KB/s)
1-A	10911.64	1368.66	40.97	96.83
2-A	22455.68	1727.14	34.12	84.38
Rata-rata	16683.66	**1547.9**	**37.55**	**90.61**

Tabel 4. Kinerja Enkripsi Twofish

Skenario	Waktu (ms)	Penggunaan Memori (KB)	Penggunaan CPU (%)	Kecepatan (KB/s)
1-A	1419.8	2066.89	26	1085.86
2-A	1280.38	2407.81	22.22	769.27
Rata-rata	**1350.09**	**2237.35**	**24.11**	**927.57**

Berdasarkan Tabel 2, Tabel 3, dan Tabel 4, dari dilakukannya skenario pengujain 1-A dan 2-A, didapatkan hasil bahwa algoritma yang paling efisien dalam waktu enkripsi adalah Rijndael (196.91 ms), dibandingkan algoritma Serpent (16683.66 ms) dan Twofish (1350.09 ms). Sementara dalam penggunaan memori, algoritma Serpent unggul (1547.9 KB) dibandingkan algortima Twofish (2237.35 KB) dan Rijndael (1866.33 KB). Penggunaan CPU paling efisien adalah algoritma Rijndael (6.43%) dibandingkan algoritma Serpent (37.55%) dan Twofish (24.11%). Proses enkripsi tercepat dilakukan algoritma Rijndael (9825.68 KB/s) dibandingkan algoritma Twofish (927.57 KB/s) dan Serpent (90.61 KB/s)

Untuk hasil pengujian pada saat dekripsi, hasil pengujian yang mencatat rata-rata waktu, kecepatan, penggunaan memori dan penggunaan CPU ketika dekripsi ditunjukkan pada Tabel 5 untuk algoritma Rijndael, Tabel 6 menunjukkan hasil algoritma serpent, dan Twofish ditunjukkan pada Tabel 7.

Tabel 5. Kinerja Dekripsi Rijndael

Skenario	Waktu (ms)	Penggunaan Memori (KB)	Penggunaan CPU (%)	Kecepatan (KB/s)
1-B	103.94	1620.37	4.61	11264.31
2-B	304.13	2135.99	4.74	7218.52
Rata-rata	**204.04**	**1878.18**	**4.68**	**9241.42**

Tabel 6. Kinerja Dekripsi Serpent

Skenario	Waktu (ms)	Penggunaan Memori (KB)	Penggunaan CPU (%)	Kecepatan (KB/s)
1-B	14080.11	1412.05	40.36	92.2
2-B	531964.36	1516.32	34.88	101.49
Rata-rata	**273022.24**	**1464.19**	**37.62**	**96.85**

Tabel 7. Kinerja Dekripsi Twofish

Skenario	Waktu (ms)	Penggunaan Memori (KB)	Penggunaan CPU (%)	Kecepatan (KB/s)
1-B	1191.1	2068.47	22.55	920.33
2-B	1547.82	2322.06	21.13	636.61
Rata-rata	**1369.46**	**2195.27**	**21.84**	**778.47**

Berdasarkan Tabel 5, Tabel 6, dan Tabel 7, dari dilakukannya skenario pengujian 1-B dan 2-B, didapatkan hasil bahwa algoritma yang paling efisien dalam waktu dekripsi adalah Rijndael (204.04 ms), dibandingkan algoritma Serpent (273022.24 ms) dan Twofish (1369.46 ms). Sementara dalam penggunaan memori, algoritma Serpent unggul (1464.19 KB) dibandingkan algortima Twofish (2195.27 KB) dan Rijndael (1878.18 KB). Penggunaan CPU paling efisien adalah algoritma Rijndael (4.68%) dibandingkan algoritma Serpent (37.62%) dan Twofish (21.84%). Proses enkripsi tercepat dilakukan algoritma Rijndael (9241.42 KB/s) dibandingkan algoritma Twofish (778.47 KB/s) dan Serpent (96.85 KB/s).

Tabel 8. Ukuran file .doc.

Algoritma	Ukuran File Asli (KB)	Ukuran file Terenkripsi (KB)	Ukuran File Terdekripsi (KB)
Rijndael	1074.02	1074.04	1074.02
Serpent	1074.02	1074.02	1074.02
Twofish	1074.02	1074.04	1074.02

Tabel 9. Ukuran file .pdf.

Algoritma	Ukuran File Asli (KB)	Ukuran File Terenkripsi (KB)	Ukuran File Terdekripsi (KB)
Rijndael	1280.67	1281.39	1280.67
Serpent	1280.67	1281.39	1280.67
Twofish	1280.67	1281.39	1280.67

Berdasarkan Tabel 8 dan Tabel 9, ukuran file yang telah dienkripsi akan menjadi lebih besar karena adanya *padding*. Ukuran file akan kembali sesuai ukuran file asli setelah dilakukan dekripsi. Hal ini berlaku pada semua algoritma dengan pengecualian untuk algoritma Serpent pada file .doc. yang ukuran file tidak berubah atau bertambah, hal ini mengindikasikan bahwa file dengan format .doc. tidak dilakukan *padding* saat enkripsi menggunakan algoritma Serpent.

File yang telah dienkripsi kemudian dibuatkan file enkripsi baru menggunakan kunci yang sedikit diubah, keduanya kemudian dihitung jumlah bit yang berbeda pada indeks yang sama, jumlah ini disebut *hamming distance*. Persentase antara *hamming distance* dan ukuran file inilah yang dinamakan *Avalanche effect* yang dicatat dan dirangkum pada Tabel 10.

Tabel 10. Avalanche Effect

Jenis file	Avalanche Effect (%)		
	Rijndael	Serpent	Twofish
.doc.	49.03	50	49.99
.pdf.	49.04	49.06	49.99
Rata-rata	49.04	49.53	49.99

Tabel 10 menunjukkan bahwa algoritma dengan *avalanche effect* terbaik untuk enkripsi file. doc. adalah algoritma Serpent (50%) dibandingkan algoritma Twofish (49.99%) dan Rijndael (49.03%). Untuk enkripsi file .pdf. yang paling unggul adalah algoritma Twofish (49.99%) dibandingkan algoritma Serpent (49.06%) dan Twofish (49.04%). Rata-rata *avalanche effect* tertinggi diraih oleh algoritma Twofish (49.99%) dibandingkan algoritma Serpent (49.53%) dan Twofish (49.04%).

SIMPULAN

Berdasarkan rangkaian percobaan yang telah diujikan untuk membandingkan Kinerja algoritma Kandidat AES dalam enkripsi dan dekripsi file, waktu tercepat untuk enkripsi (196.51 ms) dan dekripsi (204.04 ms) dilakukan oleh algoritma Rijndael. Penggunaan memori paling efisien untuk enkripsi (1547.9 KB) dan dekripsi (1464.19 KB) diraih oleh algoritma Serpent. Pada penggunaan CPU, persentase paling efisien saat enkripsi (6.43%) dan dekripsi (4.28%) dimiliki oleh algoritma Rijndael. Ukuran file dapat berubah setelah enkripsi dan akan kembali ke ukuran file asli setelah dekripsi. Algoritma tercepat untuk enkripsi (9825.68 KB/s) dan dekripsi (9241.42 KB/s) adalah algoritma Rijndael. Sementara untuk algoritma dengan *avalanche effect* tertinggi untuk enkripsi file .doc. (50%) adalah algoritma Serpent, sedangkan untuk enkripsi file .pdf. dan seluruh file secara rata-rata (49.90%) diraih oleh algoritma Twofish.

Algoritma Rijndael unggul pada 3 dari 6 parameter kinerja, yaitu waktu, penggunaan CPU, dan kecepatan enkripsi, menjadikan Rijndael sebagai pilihan optimal jika mengutamakan efisiensi kinerja pada ketiga poin tersebut. Untuk fokus pada efisiensi memori, maka algoritma Serpent lebih unggul dibandingkan Rijndael atau Twofish, serta memiliki *avalanche effect* tertinggi untuk enkripsi file. doc. Algoritma Twofish unggul pada *avalanche effect* file .pdf. dan secara rata-rata, menjadikan Twofish pilihan terbaik untuk fokus pada kekuatan enkripsi agar semakin sulit untuk ditembus oleh penyerang.

DAFTAR PUSTAKA

[1] A. Prameshwari and N. P. Sastra, *"Implementasi Algoritma Advanced Encryption Standard (AES) 128 Untuk Enkripsi dan Dekripsi File Dokumen," Eksplora Inform.*, Vol. 8, No. 1, p. 52, 2018, doi: 10.30864/eksplora.v8i1.139.

[2] A. Marpaung, P. S. Ramadhan, and A. Pranata, *"Implementasi RSA Untuk Enkripsi Dan Dekripsi File Dokumen,"* Vol. 2, pp. 39–48, 2023.

[3] S. Rubinstein-Salzedo, *Cryptography*. Springer Cham, 2018.

[4] E. Suryadi, K. Nurwijayanti, and U. T. Mataram, *"Penerapan Sistem Keamanan Video Menggunakan Kriptografi Algoritma Kunci Simetris," JATISI (Jurnal Tek. Inform. dan Sist. Informasi)*, Vol. 9, No. 3, 2022.

[5] N. S. Sibarani, G. Munawar, and B. Wisnuadhi, *"Analisis Performa Aplikasi Android pada Bahasa Pemrograman Java dan Kotlin. In Prosiding Industrial Research Workshop and National Seminar," Ind. Res. Work. Natl. Semin.*, 2018.

[6] O. G. Abood and S. K. Guirguis, *"A Survey on Cryptography Algorithms," Int. J. Sci. Res. Publ.*, Vol. 8, No. 7, 2018, doi: 10.29322/ijsrp.8.7.2018.p7978.

[7] R. S. P. Sutan, A. C. Prihandoko, and D. M. Firmansyah, *"Analisis Perbandingan Kinerja Algoritma Kriptografi Serpent dan Twofish pada Dataset 'World Bank Projects and Operations,'" Berk. Sainstek*, Vol. 8, No. 3, p. 65, 2020, doi: 10.19184/bst.v8i3.15805.

[8] A. Farisi, *"Analisis Kinerja Algoritma Kriptografi Kandidat Advanced Encryption Standard (AES) pada Smartphone," JATISI (Jurnal Tek. Inform. dan Sist. Informasi)*, Vol. 4, No. 2, pp. 199–208, 2018, doi: 10.35957/jatisi.v4i2.103.

[9] N. Rachmat and Samsuryadi, *"Performance Analysis of 256-Bit Aes Encryption Algorithm On Android Smartphone," J. Phys. Conf. Ser.*, Vol. 1196, No. 1, 2019, doi: 10.1088/1742-6596/1196/1/012049.

[10] R. Verma and A. K. Sharma, *"Cryptography: Avalanche effect of AES and RSA," Int. J. Sci. Res. Publ.*, Vol. 10, No. 4, p. p10013, 2020, doi: 10.29322/ijsrp.10.04.2020.p10013.

[11] A. Ghadbane, *"A Dissertation in Fulfillment For The Requirements of the Degree of Master By : Abderrahmen Ghadbane Benchmarking Study of Post-Quantum Schemes in Smartphones,"* 2018.

[12] A. Hidayat and D. Setiyana, *"Perbandingan Waktu dan Kecepatan Proses Enkripsi dan Dekripsi Data Teks.TXT Menggunakan Algoritma Des dan 3Des," Siliwangi, J. No, Vol Sains, Seri Teks, Data Menggunakan, T X T Des, Algoritm. Des Dan 3des*, Vol. 4, No. 2, pp. 93–99, 2018.

[13] C. Irawan and E. H. Rachmawanto, *"Keamanan Data Menggunakan Gabungan Kriptografi AES dan RSA," Proceeding SENDIU*, Vol. L, No. 2, pp. 978–979, 2021.