Metode Enkripsi RSA dan Blowfish Pada Aplikasi File Sharing Berbasis Socket Server-Client

Diajukan Sebagai Syarat Untuk Menyelesaikan
Pendidikan Program Strata-1 Pada
Jurusan Teknik Informatika

Oleh:

Diaz Rachmadannisa Erichel
NIM : 09021281924061

Jurusan Teknik Informatika
FAKULTAS ILMU KOMPUTER UNIVERSITAS SRIWIJAYA
2023

LEMBAR PENGESAHAN SKRIPSI

Metode Enkripsi RSA dan Blowfish Pada Aplikasi File Sharing Berbasis Socket Server-Client

Oleh:

Diaz Rachmadannisa Erichel
NIM : 09021281924061

Palembang, 28 Juni 2023

Mengetahui, Ketua Jurusan Teknik Informatika	Pembimbing
Alvi Syahrini Utami, M.Kom. NIP 197812222006042003	Mastura Diana Marieska, M.T. NIP 198603212018032001

TANDA LULUS UJIAN KOMPREHENSIF SKRIPSI

Pada hari Senin tanggal 19 Juni 2023 telah dilaksanakan ujian komprehensif skripsi oleh Jurusan Teknik Informatika Fakultas Ilmu Komputer Universitas Sriwijaya.

Nama	:	Diaz Rachmadannisa Erichel
NIM	:	09021281924061
Judul	:	Metode Enkripsi RSA dan Blowfish Pada Aplikasi *File Sharing* Berbasis *Socket Server-Client*

dan dinyatakan **LULUS.**

1. Ketua

   Yunita, M. Cs. .....
   NIP 198306062015042002

2. Penguji

   Osvari Arsalan, M.T. .....
   NIP 198806282018031001

3. Pembimbing

   Mastura Diana Marieska, M.T. .....
   NIP 198603212018032001

Mengetahui,
Ketua Jurusan Teknik Informatika

Alvi Syahrini Utami, M.Kom.
NIP 197812222006042003

HALAMAN PERNYATAAN BEBAS PLAGIAT

Yang bertanda tangan di bawah ini:

Nama	:	Diaz Rachmadannisa Erichel
NIM	:	09021281924061
Program Studi	:	Teknik Informatika Reguler
Judul Skripsi	:	Metode Enkripsi RSA dan Blowfish Pada Aplikasi *File Sharing* Berbasis *Socket Server-Client*

Hasil Pengecekan *iThenticate/Turnitin*: 17%

Menyatakan bahwa laporan proyek saya merupakan hasil karya sendiri dan bukan hasil penjiplakan/plagiat. Apabila ditemukan unsur penjiplakan/plagiat dalam laporan proyek ini, maka saya bersedia menerima sanksi akademik dari Universitas Sriwijaya sesuai dengan ketentuan yang berlaku.

Demikian, pernyataan ini saya buat dengan sebenarnya dan tidak ada paksaan oleh siapapun.

Palembang, 8 Juli 2023

Diaz Rachmadannisa Erichel

NIM. 09021281924061

MOTTO DAN PERSEMBAHAN

"And now that you don't have to be perfect, you can be good."

— **John Steinbeck, *East of Eden***

Kupersembahkan karya tulis ini kepada :

- Orang tua yang telah membesarkan
- Sahabat-sahabat yang telah mewarnai hari
- Mereka yang membutuhkan referensi

RSA AND BLOWFISH ENCRYPTION METHODS ON SERVER-CLIENT SOCKET-BASED FILE SHARING APPLICATION

DIAZ RACHMADANNISA ERICHEL
09021281924061

ABSTRACT

Increase in internet usage is directly proportional to the increase in cyber attacks every year. One of the increasing factors is criminal groups targeting collaboration tools such as OneDrive or Google Drive. Data security on the internet network is needed for designing network-based applications, one of which is by securing data before sending it via the internet. Testing speed and increasing file size is needed to determine which encryption method is more suitable to be implemented in network-based applications, in this case socket-based file sharing applications. RSA and Blowfish were chosen as test algorithms for asymmetric and symmetric key algorithms respectively. The test is carried out with 5 attempts of encryption and decryption for each test sample and then sent via the intranet network between two PCs, then the average speed of the 5 trials will be taken. The test results show that Blowfish is more suitable to be implemented in socket-based file sharing applications because the resulting increase in file size is much smaller than RSA, and the encryption and decryption speed is below 0 seconds.

Keywords: Socket, File Sharing, Blowfish, RSA, Processing Speed

Approved,
Head of Informatics Engineering Department

Alvi Syahrini Utami, M.Kom.
NIP. 197812222006042003

Supervisor

Mastura Diana Marieska, M.T.
NIP. 198603212018032001

METODE ENKRIPSI RSA DAN BLOWFISH PADA APLIKASI FILE SHARING BERBASIS SOCKET SERVER-CLIENT

DIAZ RACHMADANNISA ERICHEL
09021281924061

ABSTRAK

Peningkatan penggunaan internet berbanding lurus dengan peningkatan cyber attack setiap tahunnya. Faktor peningkatan tersebut salah satunya adalah kelompok kriminal yang menargetkan alat kolaborasi seperti OneDrive atau Google Drive. Pengamanan data pada jaringan internet dibutuhkan untuk perancangan aplikasi berbasis jaringan, salah satunya dengan mengamankan data sebelum dikirimkan melalui internet. Pengujian kecepatan dan pertambahan ukuran file dibutuhkan untuk menentukan metode enkripsi mana yang lebih cocok untuk diimplementasikan pada aplikasi berbasis jaringan, dalam kasus ini aplikasi file sharing berbasis socket. RSA dan Blowfish dipilih sebagai algoritma uji untuk masing-masing algoritma kunci asimetris dan simetris. Pengujian dilakukan dengan 5 kali percobaan enkripsi dan dekripsi untuk setiap sampel uji lalu dikirim lewat jaringan intranet antar dua PC, kemudian akan diambil rata-rata kecepatan dari 5 percobaan tersebut. Hasil pengujian menunjukkan Blowfish lebih cocok diimplementasikan pada aplikasi file sharing berbasis socket dikarenakan peningkatan ukuran file yang dihasilkan jauh lebih kecil dari RSA, dan kecepatan enkripsi dan dekripsi yang berada di bawah 0 sekon.

Kata Kunci: *Socket*, *File Sharing*, Blowfish, RSA, Kecepatan Proses

Mengetahui,
Ketua Jurusan Teknik Informatika

Alvi Syahrini Utami, M.Kom.
NIP. 197812222006042003

Pembimbing

Mastura Diana Marieska, M.T.
NIP. 198603212018032001

KATA PENGANTAR

Puji dan syukur penulis panjatkan kehadirat Allah Ta'ala yang telah memberikan nikmat kesehatan dan kesempatan sehingga proses penulisan skripsi Metode Enkripsi RSA dan Blowfish Pada Aplikasi *File Sharing* Berbasis *Socket Server-Client* ini dapat terlaksana dengan baik.

Di balik penulisan skripsi ini tentu saja ada banyak pihak yang telah berkontribusi untuk membantu kelancaran penulisan skripsi ini. Dengan demikian, penulis ingin mengucapkan terima kasih kepada pihak-pihak tersebut, yaitu :

1. Almarhum Dr. Jaidan Jauhari, M.T. selaku Dekan Fakultas Ilmu Komputer.
2. Ibu Alvi Syahrini Utami, M.Kom. selaku Ketua Jurusan Teknik Informatika.
3. Ibu Mastura Diana Marieska, M.T. selaku pembimbing skripsi penulis.
4. Bapak Qurhanul Rizqie, S.Kom, M.T. selaku pembimbing akademik penulis.
5. Orang tua dan para sahabat penulis yang selalu memberikan semangat dan doa untuk kelancaran skripsi penulis.
6. Teman-teman kelas A Teknik Informatika Angkatan 2019 yang saling membantu dalam perjalanan studi di jurusan ini.

Semoga Allah Ta'ala memberikan pahala yang melimpah kepada mereka semua. Penulis juga berharap agar skripsi ini dapat bermanfaat bagi para pembaca terutama bagi mereka yang memiliki minat untuk melakukan riset di bidang yang sama.

Palembang, 29 Mei 2023

Penyusun, Diaz Rachmadannisa Erichel

DAFTAR ISI

Halaman

HALAMAN JUDUL.....i
LEMBAR PENGESAHAN SKRIPSI.....ii
TANDA LULUS UJIAN KOMPREHENSIF.....iii
HALAMAN PERNYATAAN BEBAS PLAGIAT.....iv
HALAMAN MOTTO DAN PERSEMBAHAN.....v
ABSTRACT.....vi
ABSTRAKSI.....vii
KATA PENGANTAR.....viii
DAFTAR ISI.....ix
DAFTAR GAMBAR.....xii
DAFTAR TABEL.....xiv
DAFTAR LAMPIRAN.....xv
BAB I I-1
1.1 Pendahuluan I-1
1.2 Latar Belakang Masalah I-1
1.3 Rumusan Masalah I-2
1.4 Tujuan Penelitian I-3
1.5 Manfaat Penelitian I-3
1.6 Batasan Masalah I-3
1.7 Sistematika Penulisan I-4
1.8 Kesimpulan I-5
BAB II II-1
2.1 Pendahuluan II-1
2.2 *Socket* II-1
2.3 *Server-Client* II-2
2.4 Kriptografi II-3
2.4.1. Algoritma Kriptografi Kunci Simetris II-4

2.4.2. Algoritma Kriptografi Kunci Asimetris II-5
2.5 RSA II-5
2.6 Blowfish II-9
2.7 Intranet II-15
2.8 Penelitian Lain yang Relevan II-15
2.9 Kesimpulan II-16
BAB III III-1
3.1 Pendahuluan III-1
3.2 Unit Penelitian III-1
3.3 Pengumpulan Data III-1
3.3.1. Tipe Data III-1
3.3.2. Sumber Data III-1
3.3.3. Metode Pengumpulan Data III-1
3.4 Tahapan Penelitian III-2
3.4.1. Kerangka Kerja III-2
3.4.2. Kriteria Pengujian III-3
3.4.3. Format Data Pengujian III-6
3.4.4. Alat yang Digunakan dalam Pelaksanaan Penelitian III-7
3.4.5. Pengujian Penelitian III-8
3.4.6. Analisis Hasil Pengujian dan Membuat Kesimpulan III-9
3.5 Metode Pengembangan Perangkat Lunak III-9
3.6 Manajemen Proyek Penelitian III-11
BAB IV IV-1
4.1 Pendahuluan IV-1
4.2 Metode Waterfall IV-1
4.2.1. *Requirement Analysis* IV-1
4.2.2. *System and Software Design* IV-2
4.2.3. *Implementation and Unit Testing* IV-26
4.2.4. *Integration and System Testing* IV-28
4.2.5. *Operation and Maintenance* IV-30
4.3 Kesimpulan IV-31

BAB V V-1
5.1 Pendahuluan V-1
5.2 Data Hasil Percobaan V-1
5.2.1. Konfigurasi Percobaan V-1
5.2.2. Hasil Percobaan V-2
5.3 Analisis Hasil Penelitian V-3
5.4 Kesimpulan V-7
BAB VI VI-1
6.1 Kesimpulan VI-1
6.2 Saran VI-1
DAFTAR PUSTAKA
LAMPIRAN

DAFTAR GAMBAR

Halaman

Gambar II-1. Proses Aplikasi, *Socket*, dan Protokol Transport yang Mendasarinya……..…….II-1
Gambar II-2. Fungsi-Fungsi *Socket Client-Server* TCP……...…..…...….II-3
Gambar II-3. Kriptografi Kunci Simetris……...……II-4
Gambar II-4. Kriptografi Kunci Asimetris…….II-5
Gambar II-5. Skema Pembangkitan Kunci RSA……II-7
Gambar II-6. Skema Enkripsi RSA…….……..…….II-8
Gambar II-7. Skema Dekripsi RSA…….……..……II-9
Gambar II-8. Skema Ekspansi Kunci Blowfish…….……..……II-11
Gambar II-9. Skema Enkripsi Blowfish…….……..……II-12
Gambar II-10. Algoritma Blowfish……...……...II-13
Gambar II-11. Skema Dekripsi Blowfish……...……..II-14
Gambar II-12. Fungsi F……...…….II-15
Gambar III-1. Diagram Tahapan Penelitian……...……..III-2
Gambar III-2. Skema Enkripsi-Dekripsi RSA…….……..……...III-4
Gambar III-3. Skema Enkripsi-Dekripsi Blowfish……...……III-5
Gambar III-4. Skema Pengujian……..…..……III-7
Gambar III-5. Diagram Gantt Penjadwalan Proyek Perangkat Lunak……...III-13
Gambar IV-1. Diagram *Use Case* Sistem *File Sharing*……...…….IV-2
Gambar IV-2. *Activity* Koneksi ke *Server*…….…..……...IV-12
Gambar IV-3. *Activity Upload* dengan Blowfish……IV-13
Gambar IV-4. *Activity Upload* dengan RSA……..….……...IV-14
Gambar IV-5. *Activity Download* dengan Blowfish……..…….……IV-15
Gambar IV-6. *Activity Download* dengan RSA……...……...IV-16
Gambar IV-7. *Activity Update List* Nama *File*……..…….……...…….IV-17
Gambar IV-8. *Activity Load Directory*……...…IV-17
Gambar IV-9. *Activity* Enkripsi dengan Blowfish……..……...……...IV-18
Gambar IV-10. *Activity* Enkripsi dengan RSA……..….……IV-18
Gambar IV-11. *Activity* Dekripsi dengan Blowfish……..….…….IV-19

Gambar IV-12. *Activity* Dekripsi dengan RSA……..…...……...IV-20
Gambar IV-14. Diagram *Class Client*…….…..……..IV-21
Gambar IV-15. Diagram *Class Server*……...…….IV-22
Gambar IV-16. Diagram *Sequence Client*……..….……...IV-23
Gambar IV-17. Diagram *Sequence Server*……...……...IV-24
Gambar V-1. Grafik Perbandingan Ukuran *Ciphertext*……...……...V-3
Gambar V-2. Grafik Perbandingan Kecepatan Enkripsi……..…...…..V-3
Gambar V-3. Grafik Perbandingan Kecepatan Dekripsi……...…….V-4

DAFTAR TABEL

Halaman

Tabel II-1. Deskripsi Notasi Algoritma RSA……..II-6
Tabel III-1. Data Perubahan Ukuran *File*……..III-6
Tabel III-2. Data Kecepatan Waktu Enkripsi dan Dekripsi……...III-7
Tabel III-3. Spesifikasi *Hardware* dan *Software* Penelitian (1).....….....III-7
Tabel III-4. Spesifikasi *Hardware* dan *Software* Penelitian (2).....III-8
Tabel III-5. Penjadwalan Proyek Penelitian……III-11
Tabel IV-1. Kebutuhan Fungsional Perangkat Lunak…….……..IV-1
Tabel IV-2. Skenario Koneksi ke *Server*…….……..……IV-3
Tabel IV-3. Skenario *Upload* dengan Blowfish……..…….…….IV-3
Tabel IV-4. Skenario *Upload* dengan RSA……..……IV-4
Tabel IV-5. Skenario *Download* dengan Blowfish…….……...IV-5
Tabel IV-6. Skenario *Download* dengan RSA……..…….....IV-6
Tabel IV-7. Skenario *Update List* Nama *File*……..…..…….IV-7
Tabel IV-8. Skenario *Load Directory*……..…..…….IV-8
Tabel IV-9. Skenario Enkripsi dengan Blowfish……..…..……IV-9
Tabel IV-10. Skenario Enkripsi dengan RSA……..…..…...IV-10
Tabel IV-11. Skenario Dekripsi dengan Blowfish……..…IV-10
Tabel IV-12. Skenario Dekripsi dengan RSA…….……....IV-11
Tabel V-1. Konfigurasi Penelitian……..…..……....……..……V-1
Tabel V-2. Data Perbandingan Ukuran *Ciphertext*……..…..……..V-2
Tabel V-3. Data Perbandingan Waktu Enkripsi dan Dekripsi…..……..V-2
Tabel V-4. Ukuran *Plaintext* dan *Ciphertext* Blowfish Dalam *Byte*……..……V-4
Tabel V-5. Perbandingan Kecepatan Berdasarkan Panjang Nilai *e* RSA…..….V-6

DAFTAR LAMPIRAN

Lampiran 1. Link Repository Kode Program

BAB I
PENDAHULUAN

1.1 Pendahuluan

Pada bab pendahuluan akan dibahas mengenai latar belakang masalah, rumusan masalah, tujuan penelitian, manfaat penelitian, batasan masalah, sistematika penulisan dan kesimpulan. Bab ini akan menjelaskan mengenai gambaran umum dari keseluruhan penelitian.

1.2 Latar Belakang Masalah

Perkembangan teknologi saat ini diiringi dengan penggunaan internet yang semakin meningkat. Hasil survey dari Asosiasi Penyelenggara Jasa Internet Indonesia (APJII) menyatakan bahwa pengguna internet di Indonesia pada periode 2022-2023 telah mencapai 215,63 juta orang, dan angka ini mengalami peningkatan 2,67% dari periode sebelumnya[1)]. Sementara itu peningkatan penggunaan ini juga berbanding lurus dengan peningkatan *cyber attack* setiap tahunnya. Security Magazine menerangkan bahwa terdapat peningkatan 38% pada frekuensi *cyber attack* secara global pada 2022 dibandingkan dengan 2021, dengan salah satu faktornya adalah kelompok kriminal yang menargetkan alat-alat kolaborasi seperti OneDrive atau Google Drive digunakan selama pandemi untuk memungkinkan kerja jarak jauh[2)].

Berdasarkan data di atas, pengamanan terhadap data yang dikirimkan ke jaringan internet sangatlah dibutuhkan untuk pertimbangan pembuatan aplikasi berbasis jaringan seperti alat-alat kolaborasi di atas. Dibutuhkan suatu metode enkripsi yang dapat mengamankan data pada jaringan internet. Salah satu hal yang dapat dilakukan adalah mengamankan data tersebut sebelum dikirimkan lewat jaringan internet ke tujuannya menggunakan metode enkripsi tersebut.

[1)] Asosiasi Penyelenggara Jasa Internet Indonesia (APJII), Survey Penetrasi Internet Indonesia, 2023

[2)] Security Magazine, Global cyberattacks increased 38% in 2022, 20 Januari 2023

Namun dalam membangun sebuah aplikasi berbasis jaringan untuk berbagi data, tdaik hanya keamanan yang perlu diperhatikan namun juga kecepatan pemrosesan dan besaran *file* yang dikirimkan. Pengguna menginginkan sebuah aplikasi yang dapat berbagi *file* dengan kecepatan yang baik sesuai dengan besaran *file* yang dikirim. Sementara itu, proses enkripsi biasanya akan menambah ukuran *file* dari ukuran asalnya. Untuk menentukan jenis algoritma enkripsi mana yang lebih cocok untuk digunakan dalam membangun aplikasi tersebut, dilakukan pengujian untuk masing-masing salah satu dari algoritma kunci simetris dan asimetris.

Untuk algoritma kunci simetris, Blowfish dipilih karena Avalance Effect pada perubahan kunci dan perubahan *plaintext* untuk 1 sampai 16 putaran, algoritma Blowfish memiliki Avalanche Effect sebesar 41% untuk putaran ke-16 pada setiap 1 bit perubahan kunci dan 42% untuk putaran ke-16 pada setiap 1 bit perubahan *plaintext* dan dinyatakan cukup aman (Manisha S. Mahindrakar, 2014).

Untuk algoritma kunci asimetris, RSA dipilih karena dengan panjang kunci 512 bit dan panjang blok 64 bit, RSA memiliki Avalanche Effect sebesar 51% untuk data yang mengandung hanya alfabet dan 56% untuk data yang mengandung alfanumerik (Rohit Verma dan Aman Kumar Sharma, 2020). Angka tersebut terbilang besar untuk ukuran kunci tersebut.

Penelitian ini akan mencoba untuk mengambil sampel data kecepatan dari kedua algoritma yang disebutkan di atas dan diimplementasikan pada aplikasi *file sharing* berbasis *socket* sebagai alat ujinya, dimana kedua algoritma tersebut diimplementasikan dalam satu aplikasi dan kemudian dibandingkan dengan satu sama lain manakah yang lebih cocok untuk digunakan pada aplikasi tersebut berdasarkan kecepatan proses yang dihasilkan.

1.3 Rumusan Masalah

Untuk membuat sebuah aplikasi berbasis *server-client* yang aman dan cepat dibutuhkan metode enkripsi yang tepat. Berdasarkan uraian latar belakang dan masalah di atas, didapatkan rumusan masalah sebagai berikut:

1. Bagaimana implementasi algoritma RSA dan algoritma Blowfish pada aplikasi *file* sharing berbasis *socket server-client*?
2. Bagaimana perbandingan kecepatan enkripsi dan dekripsi antara algoritma RSA dan algoritma Blowfish?
3. Bagaimana perbandingan ukuran pada *file* antara algoritma RSA dan algoritma Blowfish setelah dienkripsi menggunakan masing-masing algoritma tersebut?

1.4 Tujuan Penelitian

Tujuan dari penelitian ini adalah sebagai berikut:

1. Menghasilkan aplikasi *file sharing* berbasis *server-client* yang dienkripsi dengan algoritma RSA dan algoritma Blowfish
2. Mengetahui perbandingan performa algoritma RSA dan algoritma Blowfish pada aplikasi *file sharing* berbasis *server-client*.

1.5 Manfaat Penelitian

1. Sebagai referensi dalam membangun aplikasi *file sharing* sederhana berbasis *server-client* menggunakan algoritma RSA atau Blowfish.
2. Sebagai referensi performa dari algoritma RSA dan Blowfish apabila diimplementasikan pada aplikasi *file sharing* berbasis *server-client*.

1.6 Batasan Masalah

Terdapat batasan-batasan masalah untuk penelitian ini. Batasan-batasan tersebut adalah:

1. Penelitian ini memakai sebuah aplikasi berbasis *socket server-client* dengan pilihan algoritma enkripsi RSA dan Blowfish dan dibuat menggunakan bahasa pemrograman Java.
2. Penelitian ini hanya membandingkan kecepatan enkripsi-dekripsi dan penambahan pada ukuran *file* yang dienkripsi.
3. Pengujian pada pelitian ini menggunakan dua buah PC yang tersambung oleh jaringan intranet.

1.7 Sistematika Penulisan

Sistematika penulisan proposal skripsi ini adalah sebagai berikut:

BAB I. PENDAHULUAN

Pada bab ini diuraikan latar belakang, perumusan masalah, tujuan dan manfaat penelitian, batasan masalah/ruang lingkup, metodologi penelitian, dan sistematika penulisan.

BAB II. KAJIAN LITERATUR

Pada bab ini akan dibahas dasar-dasar teori yang digunakan dalam penelitian, seperti definisi *socket*, *server-client*, kriptografi, RSA, Blowfish, dan intranet.

BAB III. METODOLOGI PENELITIAN

Pada bab ini akan dibahas mengenai tahapan yang akan dilaksanakan pada penelitian ini. Masing-masing rencana tahapan penelitian dideskripsikan dengan rinci dengan mengacu pada suatu kerangka kerja. Di akhir bab ini berisi perancangan manajemen proyek pada pelaksanaan penelitian.

BAB IV. PENGEMBANGAN PERANGKAT LUNAK

Pada bab ini akan dibahas mengenai perancangan dan implementasi perangkat lunak file sharing berbasis server-client dengan metode enkripsi RSA dan Blowfish, hasil eksekusi, dan hasil pengujian.

BAB V. HASIL DAN ANALISIS PENELITIAN

Pada bab ini, hasil pengujian berdasarkan langkah-langkah yang telah direncanakan disajikan. Analisis diberikan sebagai basis dari kesimpulan yang diambil dalam penelitian ini.

BAB VI. KESIMPULAN DAN SARAN

Pada bab ini berisi kesimpulan dari semua uraian-uraian pada bab-bab sebelumnya dan juga berisi saran-saran yang diharapkan berguna dalam penelitian ini.

1.8 Kesimpulan

Perkembangan teknologi berkembang dengan sangat pesat. Aplikasi *file sharing* saat ini banyak digunakan orang untuk berbagi dokumen digital. Namun aplikasi *file sharing* rentan terhadap serangan seperti pencurian data dan penyadapan. Untuk mencegah hal tersebut, dibutuhkan metode enkripsi yang tepat untuk mengamankan data yang akan dibagikan. RSA dan Blowfish adalah contoh dua metode enkripsi yang populer digunakan untuk mengamankan dokumen digital. Penelitian ini akan menggunakan algoritma RSA dan algoritma Blowfish pada aplikasi *file sharing* berbasis *socket server-client* dengan tujuan membandingkan kecepatan enkripsi dan pertambahan ukuran dokumen sebelum dan setelah enkripsi pada aplikasi *file sharing* yang dibuat. Penelitian ini diharapkan dapat berguna untuk kebutuhan referensi bagi penelitian serupa di masa mendatang.

DAFTAR PUSTAKA

Mahindrakar, M. S. (2014). *Evaluation of Blowfish Algorithm based on Avalanche Effect*. International Journal of Innovations in Engineering and Technology (IJIET).

Verma, R., & Sharma, A. K. (2020). *Cryptography: Avalanche effect of AES and RSA*. International Journal of Scientific and Research Publications (IJSRP), 10(4), p10013.

Arief, M., Fitriyani, & Ikhsan, N. (2015). *Kriptografi RSA Pada Aplikasi File Transfer Client-Server Based*. e-Proceeding of Engineering : Vol.2, No.1.

Bellare, M., & Rogaway, P. (2005). *Introduction to Modern Cryptography*.

Comer, D. E., & Stevens, D. L. (2000). *Internetworking with TCP IP: Client Server Programming And Applications For The Windows Tm Sockets Version*. *3*.

Kalita, L. (2014). *Socket Programming*. International Journal of Computer Science and Information Technologies (IJSIT), Vol. 5 (3).

Khatri, N & Valmik. (2015). *Blowfish Algorithm*. International Journal of Engineering Sciences & Management Research, 2(10).

Katz, J., & Lindell, Y. (2015). *Introduction to Modern Cryptography Chapman & Hall/CRC Cryptography and Network Security Series*.

Kota, C. M., & Aissi, C. (2002). *Implementation of the RSA Algorithm and Its Cryptanalysis*.

Kurose, J. F., & Ross, K. W. (2000). *Computer Networking A Top-Down Approach Featuring the Internet*.

Mu'alimin Arrijal, I., Efendi, R., & Susilo, B. (2016). *Penerapan Algoritma Kriptografi Kunci Simetris Dengan Modifikasi Vigenere Cipher Dalam Aplikasi Kriptografi Teks*. In Jurnal Pseudocode (Vol. 1).

Nita, S. L., & Mihailescu, M. I. (2022). Cryptography and Cryptanalysis in Java. In *Cryptography and Cryptanalysis in Java*. Apress.

Richard Stevens, W., Fenner, B., & Rudoff, A. M. (2003). *UNIX Network Programming The Sockets Networking API*.

Rivest, R., Shamir, A., & Adleman, L. (1978). *A Method For Obtaining Digital Signatures and Public-Key Cryptosystems*. *26*.

Rizka, M. (2021). *Perpaduan Diffie Hellman dan Blowfish sebagai Sistem Keamanan Dokumen*. In Multimedia & Jaringan (Vol. 6, Issue 2).

Schneier, B. (2015). *Applied Cryptography Protocols, Algorithms and Source Code in C*.

Wardoyo, S., Imanullah, Z., & Fahrizal, R. (2016). *Enkripsi dan Dekripsi File dengan Algoritma Blowfish pada Perangkat Mobile Berbasis Android*. Jurnal Nasional Teknik Elektro, *5*(1).