Analisa Frekuensi Hasil Enkripsi Algoritma Blowfish Terhadap Keamanan Informasi

***Ferdy Riza[1], Nurmala Sridewi[2], Amir Mahmud Husein[3], Muhammad Khoiruddin Harahap[4]**

Address: Nama Institusi/Fakultas, Program Studi, Negara[1], Nama Institusi/Fakultas, Program Studi, Negara[2], Universitas Prima Indonesia, Fakultas Teknologi dan Ilmu Komputer, Teknik Informatika[3], Politeknik Ganesha, Teknik Informatika[4], Indonesia[1234]

Email: ferdyriza@logika.ac.id[1], malaketaren97@gmail.com[2], amirmahmud@unprimdn.ac.id[3], choir.harahap@yahoo.com[4]

Abstraks

Kemudahan akan pengiriman data dengan perkembangan teknologi teknologi internet saat ini menjadi perhatian, khususnya masalah kerahasiaan data, integritas dan keamanan informasi. Kriptografi merupakan salah satu teknik yang digunakan untuk menjaga kerahasiaan data dan keamanan informasi, penerapan teknik kriptografi untuk keamanan informasi dan integritas data sangat tergantung pada pembentukan kunci. Dalam penelitian ini diusulkan pendekatan analisa frekuensi untuk mengukur tingkat keamanan informasi hasil enkripsi blowfish untuk menentukan bentuk pendistribusian dari masing-masing karakter yang digunakan pada teks dan mengetahui frekuensi pasti dari masing-masing karakter yang digunakan dalam data text uji. Pengujian algoritma enkripsi dan deksripsi metode blowfish terhadap plainteks terbukti akurat, namun semakin panjang karakter kunci yang digunakan akan sangat berpengaruh terhadap tingkat keamanan informasi hasil enkripsi, hal ini didasarkan pada hasil uji coba analisa frekuensi yang dilakukan.

Keywords *– Information security frequency analysis, Blowfish, Information security, cryptography*

1. Latar Belakang

Kemudahan akan pengiriman data dengan perkembangan teknologi teknologi internet saat ini menjadi perhatian, khususnya masalah kerahasiaan data, integritas dan keamanan informasi. Kriptografi merupakan salah satu teknik yang digunakan untuk menjaga kerahasiaan data dan keamanan informasi [1], dimana setiap informasi akan di enkripsi dengan mengubah pesan asli menjadi tidak terbaca, sedangkan deksripsi merupakan teknik yang digunakan untuk mengembalikan pesan asli menjadi terbaca [2]. Secara umum, terdapat dua teknik yang digunakan dalam kriptografi, yaitu simetris dan asimetris. Kunci kriptografi simetris disebut juga sebagai *Private Key Cryptography* dengan menggunakan kunci yang sama untuk enkripsi dan dekripsi data. Algoritma blowfish merupakan salah satu kriptografi simetris yang tercepat dibandingkan dengan algoritma lainnya, namun algoritma AES aman dan lebih unggul dari DES [3]. Keamanan informasi pada kriftografi sangat tergantung pada proses pembentukan kunci untuk enkripsi dan deskripsi data [4], sehingga perlu dilakukan analisa terhadap hasil enkripsi yang digunakan.

Analisis frekuensi adalah studi tentang frekuensi huruf atau kelompok huruf dalam ciphertext. Metode ini digunakan sebagai bantuan untuk memecahkan sandi klasik. Analisis frekuensi didasarkan pada fakta bahwa, dalam setiap rentang bahasa tertulis, huruf dan kombinasi huruf tertentu terjadi dengan frekuensi yang bervariasi. Selain itu, ada distribusi karakter huruf yang yang sama untuk hampir semua sampel bahasa yang digunakan. Penerapan analisa frekuensi dalam keamanan informasi terbukti akurat digunakan untuk menganalisa kekuatan kunci enkripsi [5]-[8].

Pada penelitian ini kami menggunakan pendekatan analisa frekuensi hasil enkrpsi menggunakan algoritma blowfish terhadap keamanan informasi, Blowfish alias "OpenPGP.Cipher.4" merupakan enkripsi yang termasuk dalam golongan *Symmetric Cryptosystem*, metoda enkripsinya mirip dengan DES (DES-like Cipher) diciptakan oleh seorang *Cryptanalyst* bernama Bruce Schneier Presiden perusahaan Counterpane Internet Security, Inc (Perusahaan konsultan tentang kriptografi dan keamanan Komputer) dan dipublikasikan tahun 1994. Sejak saat itu telah dilakukan berbagai macam analisis, dan perlahan - lahan mulai mendapat penerimaan sebagai algoritma enkripsi yang kuat (Ibrahim, 2012)..

2. Metode

2.1 Analisa Frekuensi

Dalam cipher substitusi sederhana, setiap huruf dari plaintext diganti dengan yang lain, dan huruf tertentu dalam plaintext akan selalu diubah menjadi huruf yang sama dalam ciphertext. Misalnya, jika semua kemunculan huruf e berubah menjadi huruf X, pesan ciphertext yang mengandung banyak contoh huruf X akan menyarankan kepada cryptanalyst yang X mewakili e.

Penggunaan dasar dari analisis frekuensi adalah pertama menghitung frekuensi huruf ciphertext dan kemudian mengaitkan huruf-huruf plainteks yang ditebak. Lebih banyak Xs di ciphertext dari yang lain menunjukkan bahwa X berhubungan dengan e dalam plaintext, tetapi ini tidak pasti; t dan a juga sangat umum dalam bahasa Inggris, jadi X mungkin salah satu dari bagian huruf juga. Hal ini tidak mungkin menjadi plaintext z atau q yang kurang umum. Dengan demikian, cryptanalyst mungkin perlu mencoba beberapa kombinasi pemetaan antara huruf ciphertext dan plaintext.

Penggunaan statistik yang lebih kompleks dapat dipahami, seperti mempertimbangkan jumlah pasangan huruf (bigrams), kembar tiga (trigram), dan seterusnya. Hal ini dapa dilakukan untuk memberikan informasi lebih banyak kepada cryptanalyst, misalnya, Q dan U hampir selalu terjadi bersama-sama dalam urutan plainteks, meskipun Q itu sendiri jarang [10].

Misalkan Eve mengirim pesan yang dienkripsi menggunakan cipher substitusi sederhana sebagai berikut:

```
LIVITCSWPIYVEWHEVSRIQMXLEYVEOIEWHRXEXIPFEMVEWHKVSTYLXZIXLIKIIXPIJVSZEYP
ERRGERIMWQLMGLMXQERIWGPSRIHMXQEREKIETXMJTPRGEVEKEITREWHEXXLEXXMZITWAWSQ
WXSWEXTVEPMRXRSJGSTVRIEYVIEXCVMUIMWERGMIWXMJMGCSMWXSJOMIQXLIVIQIVIXQSVS
TWHKPEGARCSXRWIEVSWIIBXVZMXFSJXLIKEGAEWHEPSWYSWIWIEVXLISXLIVXLIRGEPIRQI
VIIBGIIHMWYPFLEVHEWHYPSRRFQMXLEPPXLIECCIEVEWGISJKTVWMRLIHYSPHXLIQIMYLXS
JXLIMWRIGXQEROIVFVIZEVAEKPIEWHXEAMWYEPPXLMWYRMWXSGSWRMHIVEXMSWMGSTPHLEV
HPFKPEZINTCMXIVJSVLMRSCMWMSWVIRCIGXMWYMX
```

Untuk contoh diatas, huruf besar digunakan untuk menunjukkan ciphertext, huruf kecil digunakan untuk menunjukkan plaintext (atau tebakan), dan X ~ t digunakan untuk menyatakan dugaan bahwa ciphertext huruf X mewakili huruf plaintext t.

Eve dapat menggunakan analisis frekuensi untuk membantu memecahkan pesan di sepanjang baris berikut: jumlah huruf dalam kriptogram menunjukkan bahwa plainteks adalah huruf tunggal yang paling umum, XL bigram yang paling umum, dan XLI adalah trigram yang paling umum. e adalah huruf yang paling umum, th adalah bigram yang paling umum, dan merupakan trigram yang paling umum. Ini menunjukkan bahwa X ~ t, L ~ h dan I ~ e. Huruf paling umum kedua dalam cryptogram adalah E; karena huruf pertama dan kedua yang paling sering, e dan t diperhitungkan, Eve menebak bahwa E ~ a, huruf paling sering ketiga. Sementara membuat asumsi ini, pesan dekripsi parsial berikut ini diperoleh.

```
heVeTCSWPeYVaWHaVSReQMthaYVaOeaWHRtatePFaMVaWHKVSTYhtZetheKeetPeJVSZaYP
aRRGaReMWQhMGhMtQaReWGPSReHMtQaRaKeaTtMJTPRGaVaKaeTRaWHatthattMZeTWAWSQ
WtSWatTVaPMRtRSJGSTVReaYVeatCVMUeMWaRGMeWtMJMGCSMWtSJOMeQtheVeQeVetQSVS
TWHKPaGARCStRWeaVSWeeBtVeZMtFSJtheKaGAaWHaPSWYSWeWeaVtheStheVtheRGaPeRQ
eVeeBGeeHMWYPFhaVHaWHYPSRRFQMthaPPtheaCCeaVaWGeSJKTVWMRheHYSPHtheQeMYht
SJtheMWReGtQaROeVFVeZaVAaKPeaWHtaAMWYaPPthMWYRMWtSGSWRMHeVatMSWMGSTPHha
VHPFKPaZeNTCMteVJSVhMRSCMWMSWVeRCeGtMWYMt
```

Dengan menggunakan tebakan awal ini, Eve dapat menemukan pola yang mengonfirmasi pilihannya, seperti "itu". Selain itu, pola lain menunjukkan dugaan lebih lanjut. "Rtate" mungkin "status", yang berarti R ~ s. Demikian pula "atthattMZe" dapat ditebak sebagai "atthattime", menghasilkan M ~ i dan Z ~ m. Selanjutnya, "heVe" mungkin "di sini", memberikan V ~ r. Sehingga menghasilkan tebakan sebagai berikut:

```
hereTCSWPeYraWHarSseQithaYraOeaWHstatePFairaWHKrSTYhtmetheKeetPeJrSmaYP
assGaseiWQhiGhitQaseWGPSseHitQasaKeaTtiJTPsGaraKaeTsaWHatthattimeTWAWSQ
WtSWatTraPistsSJGSTrseaYreatCriUeiWasGieWtiJiGCSiWtSJOieQthereQeretQSrS
TWHKPaGAsCStsWearSWeeBtremitFSJtheKaGAaWHaPSWYSWeWeartheStherthesGaPesQ
ereeBGeeHiWYPFharHaWHYPSssFQithaPPtheaCCearaWGeSJKTrWisheHYSPHtheQeiYht
SJtheiWseGtQasOerFremarAaKPeaWHtaAiWYaPPthiWYsiWtSGSWsiHeratiSWiGSTPHha
rHPFKPameNTCiterJSrhisSCiWiSWresCeGtiWYit
```

Pada gilirannya, dugaan ini menyarankan yang lain (misalnya, "remarA" bisa menjadi "komentar", menyiratkan A ~ k) dan seterusnya, dan relatif mudah untuk menyimpulkan sisa huruf, akhirnya menghasilkan plaintext.

```
hereuponlegrandarosewithagraveandstatelyairandbroughtmethebeetlefromagl
asscaseinwhichitwasencloseditwasabeautifulscarabaeusandatthattimeunknow
ntonaturalistsofcourseagreatprizeinascientificpointofviewthereweretworo
undblackspotsnearoneextremityofthebackandalongoneneartheotherthescalesw
ereexceedinglyhardandglossywithalltheappearanceofburnishedgoldtheweight
oftheinsectwasveryremarkableandtakingallthingsintoconsiderationicouldha
rdlyblamejupiterforhisopinionrespectingit
```

Pada titik ini, akan lebih baik bagi Eve untuk memasukkan spasi dan tanda baca, sehingga menghasilkan seperti berikut:

```
Hereupon Legrand arose, with a grave and stately air, and brought me the
beetle from a glass case in which it was enclosed. It was a beautiful
scarabaeus, and, at that time, unknown to naturalists—of course a great
prize in a scientific point of view. There were two round black spots
near one extremity of the back, and a long one near the other. The scales
were exceedingly hard and glossy, with all the appearance of burnished
gold. The weight of the insect was very remarkable, and, taking all things
into consideration, I could hardly blame Jupiter for his opinion
respecting it.
```

2.2 Algoritma Blowfish

Blowfish merupakan salah satu metode enkripsi yang termasuk dalam golongan *Symmetric Cryptosystem*. Algoritma kunci simetrik cipher blok yang dirancang pada tahun 1993 oleh Bruce Schneider untuk menggantikan DES (*Data Encryption Standard*). Blowfish merupakan cipher blok, proses enkripsi dan dekripsi, Blowfish membagi pesan menjadi blok-blok dengan ukuran yang sama panjang, yaitu 64 bit.

Algoritma ini terdiri dari dua bagian yaitu perluasan kunci (*key expansion*) dan enkripsi data. Key expansion merupakan tahapan untuk memperluas kunci yang panjangnya 32-bit sampai 448-bit menjadi beberapa array subkunci (*subkey*) dengan total 4168 byte. Enkripsi data terjadi pada jaringan feistel sebanyak 16 putaran dimana setiap putaran terdiri dari permutasi kunci dan subtitusi data. Semua operasi yang digunakan adalah penambahan dan XOR pada variabel 32 bit. Tambahan

operasi lainnya hanyalah empat penelusuran tabel (table lookup) untuk setiap putaran. Blowfish menggunakan subkunci yang besar dimana setiap kunci harus dihitung sebelum enkripsi atau dekripsi data di mulai. Kunci tersebut terdiri dari:

a. Array P, terdiri dari delapan belas 32 bit subkunci: P1, P2, P3, . . . ,P18
b. Empat 32 bit S-box, masing-masing mempunyai 256 entri :
   S1[0], S1[1], . . . , S1[255], S2[0], S2[1], . . . , S2[255]
   S3[0], S3[1], . . . , S3[255], S4[0], S4[1], . . . , S4[255]

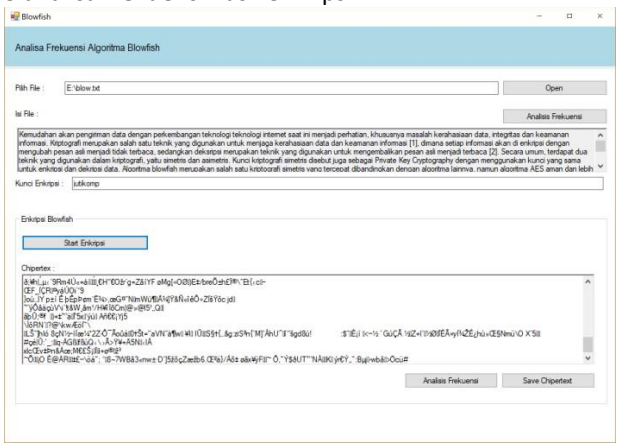
Nilai awal dari array P dan 4 S-box secara berurutan adalah string yang tetap, yang terdiri dari digit hexadesimal dari phi (π) [11].

Rumus Matematika

$$O_{3,i} = \bar{w}_i = \frac{w_i}{w_1 + w_2}, \text{ dengan i=1,2} \quad (1)$$

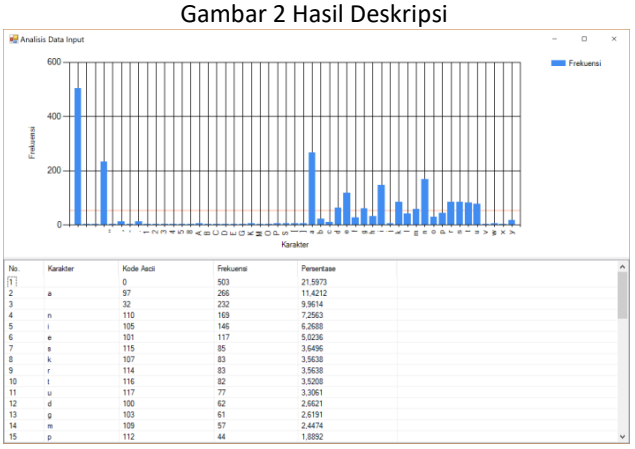
3. Hasil

Pada penelitian ini kami melakukan pengujian analisa frekuensi hasil enkripsi pada algoritma blowfish untuk keamanan informasi. Percobaan dilakukan dengan spesifikasi platform intel core i5 2,5 GHz CPU, 8 Gb RAM dan menggunakan sistem operasi WIN 10 64 bits, aplikasi dibuat menggunakan VB 2010, dengan tahapan pengujian menggunakan file teks yang akan dienkripsi menggunakan algoritma blowfish, kemudian dilakukan analisa frekuensi hasil enkripsi algoritma blowfish, tampilan aplikasi ditunjukan pada gambar 1 proses enkripsi dan gambar 2 hasil deskripsi, sedangkan gambar 3 analisa frekuensi hasil enkripsi.



Gambar 1 Proses Enkripsi

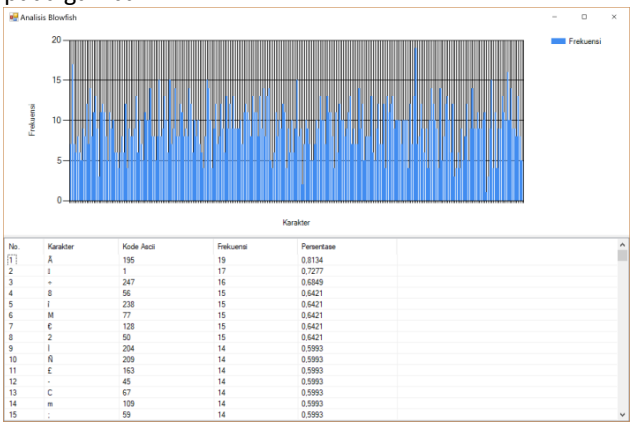
Gambar 2 Hasil Deskripsi



No.	Karakter	Kode Ascii	Frekuensi	Persentase
1		0	503	21,5973
2	a	97	266	11,4212
3		32	232	9,9614
4	n	110	169	7,2563
5	i	105	146	6,2688
6	e	101	117	5,0236
7	s	115	85	3,6496
8	k	107	83	3,5638
9	r	114	83	3,5638
10	t	116	82	3,5208
11	u	117	77	3,3061
12	d	100	62	2,6621
13	g	103	61	2,6191
14	m	109	57	2,4474
15	p	112	44	1,8892

Gambar 3 Analisa Frekuensi Plainteks

Analisa frekuensi plainteks yang akan dienkripsi ditunjukkan pada gambar 3 dimana karakter “a” sebagai karakter dengan kemunculan paling tinggi dengan 14.169%. analisa frekuensi hasil enkripsi ditunjukkan pada gambar 4.



No.	Karakter	Kode Ascii	Frekuensi	Persentase
1	A	195	19	0,8134
2	I	1	17	0,7277
3	-	247	16	0,6849
4	8	56	15	0,6421
5	i	238	15	0,6421
6	M	77	15	0,6421
7	€	128	15	0,6421
8	2	50	15	0,6421
9	l	204	14	0,5993
10	Ñ	209	14	0,5993
11	E	163	14	0,5993
12	-	45	14	0,5993
13	C	67	14	0,5993
14	m	109	14	0,5993
15	:	59	14	0,5993

Gambar 4 Analisa Frekuensi Hasil Enkripsi

Pada gambar 4 merupakan hasil pengujian enkripsi metode blowfish yang bertujuan untuk menentukan bentuk pendistribusian dari masing-masing karakter yang digunakan pada teks dan mengetahui frekuensi pasti dari masing-masing karakter yang digunakan dalam data text uji.

Informasi yang dapat diambil adalah jumlah karakter yang digunakan, persentasi kemunculan karakter, dan juga jumlah kemunculan karakter pada data text uji. Pross analisis ini akan mengarahkan pada karakter dengan jumlah kemunculan yang paling banyak dan

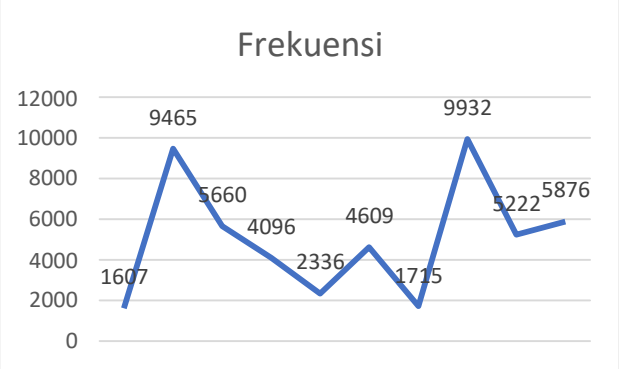
diikuti dengan karakter dengan jumlah kemunculan paling sedikit. Karakter "Â" adalah pemilik frekuensi kemunculan yang paling tinggi yaitu 19 kali dengan persentasi kemunculan sebesar 0.8134 % dan "(spasi)" sebagai karakter dengan kemunculan paling sedikit yaitu 120 dengan persentasi kemunculannya pada data text uji sebesar 1.6811 %. Untuk pengukuran tingkat frekuensi kemunculan huruf menggunakan persamaan (2).

$$Frekuensi\ Relatif = \frac{jumlah\ huruf}{total\ jumlah\ huruf} x100 \quad (2)$$

Pada tabel 1 merupakan hasil pengujian analisa frekuensi hasil enkripsi algoritma blowfish, sedangkan pada gambar 5 merupakan hasil dalam bentuk grafik.

Tabel 1 Hasil Analisa Frekuensi

Nama File	Jumlah Kunci	Frekuensi	Persentase
Percobaan 1	8 Karakter	5182	0,7371
Percobaan 2	10 Karakter	9314	0,4019
Percobaan 3	12 Karakter	7528	0,9665
Percobaan 4	14 Karakter	1630	0,7948
Percobaan 5	16 Karakter	9547	0,8721
Percobaan 6	18 Karakter	3171	0,5818
Percobaan 7	20 Karakter	9841	0,6122
Percobaan 8	22 Karakter	6032	0,3823
Percobaan 9	24 Karakter	8232	0,7181
Percobaan ..	26 Karakter	2407	0,9942



Gambar 5 Grafik Frekuensi

Dari hasil pada tabel 1 menunjukkan bahwa semakin panjang karakter kunci yang digunakan pada algoritma blowfish, maka akan menghilangkan karakter pendistribusian data dari plainteks sehingga dapat mengaburkan bentuk asli dari data asli.

4. Kesimpulan

Pada penelitian ini pendekatan analisa frekuensi hasil enkripsi algoritma blowfish untuk mengukur tingkat keamanan informasi menghasilkan kesimpulan bahwa ketergantungan kunci pada algoritma blowfish terhadap keamanan informasi sangat berpengaruh secara signifikan, hal ini didasarkan pada hasil pengujian enkripsi plainteks, namun masih perlu dilakukan pengujian lebih lanjut untuk menghasilkan tingkat akurasi analisa yang lebih baik dengan membandingkan dengan metode kriptografi lainnya.

References

[1] Mahmud H, A., Angga W, B., Tommy, Marwan E, A., & Siregar, R. (2018). Performance analysis of AES-Blowfish hybrid algorithm for security of patient medical record data. *Journal of Physics: Conference Series*, *1007*, 012018. https://doi.org/10.1088/1742-6596/1007/1/012018

[2] Novelan, M. S., Husein, A. M., Harahap, M., & Aisyah, S. (2018). SMS Security System on Mobile Devices Using Tiny Encryption Algorithm. *Journal of Physics: Conference Series*, *1007*(1), 12037. Retrieved from http://stacks.iop.org/1742-6596/1007/i=1/a=012037

[3] Apdilah, D., Harahap, M. K., Khairina, N., Husein, A. M., & Harahap, M. (2018). A Comparison of One Time Pad Random Key Generation using Linear Congruential Generator and Quadratic Congruential Generator. *Journal of Physics: Conference Series*, *1007*(1). https://doi.org/10.1088/1742-6596/1007/1/012006

[4] P Shaikh, V. Kaul. Enhanced Security Algorithm using Hybrid Encryption and ECC, IOSR Journal of Computer Engineering (IOSR-JCE), Volume 16, Issue 3; 2014, pp 80-85

[5] Shadi R. Masadeh, Hamza A. Al_Sewadi, Mohammad A. Wadi, A Novel Paradigm for Symmetric Cryptosystem, International Journal of Advanced Computer Science and Applications, Vol. 7, No. 3, 2016.

[6] Ayman Al-ahwal, Sameh Farid, The Effect Of Varying Key Length On A Vigenère Cipher, IOSR Journal of Computer Engineering (IOSR-JCE). e-ISSN: 2278-0661, p-ISSN: 2278-8727, Volume 17, Issue 2, Ver. VI (Mar – Apr. 2015), PP 18-23.

[7] Narendren S, Yashas B Yathish and Chandra Mohan B, A Cryptosystem using Two Layers of Security - DNA and RSA Cryptography, International Journal of Pure and Applied Mathematics Volume 119 No. 7 2018, 217-224.

[8] Alaa E Din Riad, Hamdy K. Elminir, Alaa R. Shehata andTaha R. Ibrahim, Security Evaluation And Encryption Efficiency Analysis Of Rc4 Stream Cipher For Converged Network Applications, Journal of ELECTRICAL ENGINEERING, VOL. 64, NO. 3, 2013, 196–200.

[9] Rohmat Nur Ibrahim. Kriptografi Algoritma Des, Aes/Rijndael, Blowfish Untuk Keamanan Citra Digital Dengan Menggunakan Metode Discrete Wavelet Transformation (Dwt). Jurnal Computech

& Bisnis, Vol. 6, No. 2, Desember 2012, 82-95 ISSN 2442-4943. 2012.

[10] https://en.wikipedia.org/wiki/Frequency_analysis#Frequency_analysis_for_simple_substitution_ciphers diakses pada tanggal 10 September 2018

[11] Por, L. Y., Beh, D., Ang, T. F., Ong, S. Y. An Enhanced Mechanism for Image Steganography Using Sequential Colour Cycle Algorithm, The International Arab Journal of Information Technology, Vol. 10, 51-60. 2013.

Biografi Penulis

Ferdy Riza, M.Kom Lahir di Kabupaten 50 Kota, 3 Juni 1989. Pendidikan Strata 1 (S1) Program Studi Teknik Informatika di Sekolah Tingggi Teknik Harapan dan Strata 2 (S2) Magister Ilmu Komputer Program Studi Teknik Informatika di Pascasarjana Universitas Putra Indonesia. Saat ini mengajar di STMIK Logika dan aktif dalam bidang penelitian yang terkait dengan Kriptografi dan terapannya

Nurmala Sridewi, M.Kom. Lahir di Pancur Batu, 07 Nopember 1989. Pendidikan Diploma 1 (D1) Program Studi Manajemen Informatika di AMIK Logika, Pendidikan Strata 1 (S1) Program Studi Sistem Informasi di Sekolah Tinggi Manajemen Informatika Komputer Logika, Medan dan Strata 2 (S2) Magister Ilmu Komputer Program Studi Sistem Informasi di Pascasarjana Universitas Putra Indonesia (YPTK), Padang. Saat ini aktif mengajar di STMIK Logika.

Amir Mahmud Husein, memperoleh gelar Sarjana Komputer (S.Kom), Program Studi Sistem Informasi Sekolah Tinggi Teknik Harapan Medan yang sekarang telah menjadi Universitas Harapan Medan, lulus tahun 2008. Memperoleh gelar Magister Komputer (M.Kom) Program Pasca Sarjana Magister Ilmu Komputer Universitas Sumatera Utara, lulus tahun 2010. Saat ini aktif sebagai pengajar di Universitas Prima Indonesia Medan, Fakultas Teknologi dan Ilmu Komputer, Program Studi Teknik Informatika. Minat penelitian saat ini meliputi bidang data mining, machine learning dan big data.

Muhammad Khoiruddin Harahap, M. Kom, berprofesi Dosen Politeknik Ganesha Medan Program Studi Teknik Informatika. Minat Penelitian saat ini adalah Kriptografi, Steganografi dan pengambilan keputusan.