KLIK: Kajian Ilmiah Informatika dan Komputer
ISSN 2723-3898 (Media Online)
Vol 2, No 4, Februari 2022
Hal 132-137
https://djournals.com/klik

Penerapan Algoritma Friefalds Untuk Pembangkit Kunci Algoritma Knapsack Pada Pengamanan Record Database

Rahmad Rahmansyah

Program Studi Teknik Informatika, Fakultas Ilmu Komputer dan Teknologi Informasi, Universitas Budi Darma,
Jalan Sisingamanganraja No. 338,Medan, Sumatera Utara, Indonesia
Email: Rahmadrahmansyah35@gmail.com

Abstrak-Algoritma Friefalds mempunyai dua kunci, yaitu kunci publik dan kunci rahasia. Algoritma ini memiliki keamanan yang terletak pada kesulitan dalam menghitung alogaritma diskrit. Baik kunci enkripsi maupun dekripsi keduanya merupakan bilangan prima. Algoritma friefalds tipe algoritma kriptografi asimetris terdiri atas dua buah kunci yaitu kunci publick untuk melakukan enkripsi sedangkan kunci pribadi untuk melakukan dekripsi. Dalam algoritma Friefalds, kunci yang didistribusikan adalah kunci publik yang tidak diperlukan kerahasiannya sedangkan kunci pribadi tetap disimpan atau tidak didistribusikan. Setiap orang yang memiliki kunci public dapat melakukan proses implementasi enkripsi tetapi hasil dari enkripsi tersebut hanya bias dibaca oleh orang yang memiliki kunci pribadi. Untuk meningkatkan kekuatan dari algoritma tersebut, maka kunci yang digunakan untuk melakukan proses enkripsi dan dekripsi akan dimodifikasi terlebih dahulu menggunakan algoritma pengacakan yaitu Algoritma Knapsack. Algoritma Knapsack adalah algoritma acak probabilistik yang digunakan untuk memverifikasi perkalian matriks. Tujuan dalam menggunakan algoritma Freifalds ini adalah agar kunci yang dihasilkan lebih sulit ditebak sehingga mempersulit kriptanalis dalam membaca pesan atau informasi tersebut.

Kata Kunci: Kriptografi; Implementasi: Kunci; Pengacakan; Algoritma Friefalds; Algoritma Knapsack

Abstract-Friefalds algorithm has two keys, namely the public key and the secret key. This algorithm has security which lies in the difficulty in calculating discrete algorithms. Both encryption and decryption keys are prime numbers. Friefalds algorithm type asymmetric cryptography algorithm consists of two keys, namely the public key for encryption while the private key for decryption. In Friefalds algorithm, the distributed key is the public key which is not required to be kept secret while the private key is kept or not distributed. Everyone who has the public key can carry out the encryption implementation process but the results of the encryption can only be read by the person who has the private key. To increase the strength of the algorithm, the key used to perform the encryption and decryption process will be modified first using a randomization algorithm, the Knapsack Algorithm. The Knapsack algorithm is a probabilistic random algorithm used to verify matrix multiplication. The purpose of using the Freifalds algorithm is to make the resulting key more difficult to guess, making it difficult for cryptanalysts to read the message or information.

Keywords: Cryptography; Implementation: Key; Randomization; Friefalds Algorithm; Knapsack Algorithm

1. PENDAHULUAN

Kriptografi merupakan ilmu sekaligus seni untuk menjaga keamanan informasi. Kriptografi terdapat dua proses utama yaitu proses mengkodekan pesan yang dapat di dibaca (*plaintext*) menjadi pesan yang tidak dapat dibaca atau sudah disandikan (*ciphertext*) yang disebut dengan proses enskripsi (*encryption*) dan proses pengembalikan *ciphertext* menjadi *plaintext* disebut merupakan proses deskripsi (*decryption*) . Sejarah dari Kriptografi ada dua jenis yaitu kriptografi modren dan kriptografi klasik dan berdasarkan kuncinya dapat dibagi menjadi kriptografi simetris dan kriptografi asimetris.[1]

Algoritma pengacakan adalah yang di hasilkan mutasi acak dari suatu himpunan terhingga, dengan kata lain untuk mengacak suatu himpunan, seperti algoritma pengacakan dapat di gunakan yaitu algoritma Freivalds Algoritma Freivalds adalah algoritma acak probabilistik yang digunakan untuk memverifikasi perkalian matriks Algoritma ini ddigunakan untuk memodifikasi algoritma Knapsack ada enkripsi yang menggunakan pasangan plaintext dengan sebuahkunci rahasia yang diperoleh secara acak. Untuk meningkatkan pengaman yg lebih kuat lagi dari algoritma tersebut, maka kunci yang digunakan untuk melakukan proses enkripsi dan deskripsi akan diubah terlebih dahulu menggunakan pengacakan kunci yaitu algoritma Freivald.[2]

Record Database adalah kumpulan dari pembaca data dapat disimpan di komputer yang saling berhubungan satu sama lainnya yang dijadikan jalan sumber siytem informasi yang berjalan sehingga dapat diproleh data dan informasi yang optimal dan akan dibutuhkan oleh user. Record database dapat ditampilkan dalam bentuk seperti teks sebagai sebuah informasi untuk si pengguna, sebagai permudah kriptanalisis yang dapat memproses serta membagi ruang untuk melakukan pembocoran , mendistribusikan maupun mengedit record database tersebut.[3]

Permasalahan yg sering di dapat yaitu Keamanan dan kerahasiaan suatu data, keamanan dan kerahasian sangatlah penting bagi suatu instansi atau pun perusahaan. Data yang akan diguna kan ataupun disimpan agar benar-benar aman secara fisik atau sistem perlu terlebih dahulu untuk diamankan agar tidak dapat dibaca maupun dilacak oleh pihak yang tidak bertanggung jawab.

Pada penelitian sebelumnya yang dilakukan oleh Fadlan, Muhammad Adriansa, yang dipublikasikan pada jurnal teknologi informasii dan ilmu komputer yang berjudul"Rekayasa Aplikasi Kriptografi dengan Penerapan Kombinasi Algoritma Knapsack Merkle Hellman dan Affine Cipher" Vol. 4 No. 51 Tahun 2017, kesimpulan dari jurnal ini. Proses enkripsi menggunakan metode affine cipher, setelah itu cipherteks hasil dari metode tersebut kemudan dienkripsi lagi dengan algoritma knapsack merkle hellman sdapat menghasilkan cipherteks seperti baru dan

jauh berbeda dengan bentuk aslinya atau plainteks. Selain itu, pada proses dekripsi juga berhasil pengembalikan cipherteks menjadi seperti semula (plainteks) melalui tahapan dekripsi, yang diawali dengan dekripsi knapsack merkle hellman yang dilanjutkan dengan deskripsi affine cipher. Oleh sebab itu, penerapan gabungan affine dan knapsack tersebut dapat difungsikan untuk mengamankan suatu data.[2]

Penelitian lainnya yang dilakukan oleh Aminudin, Ahmad Faisal Helmi, Sofyan Arifianto yang di publikasikan pada jurna Teknologi Informasi dan Ilmu Komputer yang berjudul "Analisa Kombinasi Algoritma Merkle-Hellman Knapscak dan Logaritma Diskrit pada Aplikasi Chat" Vol. 5 No. 3 Tahun 2018, kesimpulan jurnal ini berdasarkan penerapan algoritma knapsack dan gabungan knapsack dan logaritma diskrit dapat digambarkan pada aplikasi chat. Aplikasi chat ini dapat memperkuat pesan agar pesan tersebut agar lebih aman lagi dan tidak mudah dibaca oleh orang yang tidak bertanggung jawab karena pesan ini ketika dikirim berbentuk ciphertext yang sudah terenkripsi menggunakan kunci publik dan dapat di privat oleh si pengguna.[4]

2. METODOLOGI PENELITIAN

2.1 Record Database

Record Database adalah kumpulan dari pembaca data dapat disimpan di komputer yang saling berhubungan satu sama lainnya yang dijadikan jalan sumber siytem informasi yang berjalan sehingga dapat diproleh data dan informasi yang optimal dan akan dibutuhkan oleh user. Record database dapat ditampilkan dalam bentuk seperti teks sebagai sebuah informasi untuk si pengguna, sebagai permudah kriptanalisis yang dapat memproses serta membagi ruang untuk melakukan pembocoran , mendistribusikan maupun mengedit record database tersebut[5]

2.2 Algoritma Freivalds

Algoritma Freivalds, dinamai Rūsiņš Mārtiņš Freivalds adalah algoritma acak probabilistik yang digunakan untuk memverifikasi perkalian matriks. Diberikan tiga n × n matriks A, B, dan C, masalah umum adalah memverifikasi apakah AxB=C. Algoritma naïf akan menghitung produk AxB secara eksplisit dan membandingkan istilah peristilah apakah produk ini sama dengan C. Namun, algoritma multi aplikasi matriks paling dikenal berjalan di $0(n^{2.3729})$ waktu[7]. Algoritma Freivalds menggunakan pengacakan untuk mengurangi batas waktu ini dengan probabilitas tinggi. Di waktu algoritma dapat memverifikasi produk matriks dengan probabilitas kegagalan kurang dari 2^{-K}. Langakah-langkah algoritma Freivaldsyaitu:

Hasilkanvektor n/ 1 acak 0/1

$$P=A \text{ x } (Br)-C\begin{bmatrix}1\\0\\1\end{bmatrix} \quad (2)$$

P = adalah hasil pengacakan
r = adalah nilai pektor pengacakan
A = adalah nilai variable acak matrik a
B = adalah nilai variable acak matrik b
C = adalah hasil perkalian matrik A x B

2.3 Algoritma Knapsak

Knapsack dapat diartikan sebagai sebuah karung yang dapat digunakan untuk memasukan sejumlah barang. Karungtersebutmemiliki kapasitas yang terbatas, sehingga tidak semua barang dapat masuk ke dalam karung[8]. . Untuk mengoptimalkan penggunaan kapasitas karung yang terbatas, maka perlu pemilihan yang tepat terhadap jenis barang yang dimasukkan. Optimasi pada penelitian ini dapat dihitung dengan menggunakan persamaan (1):

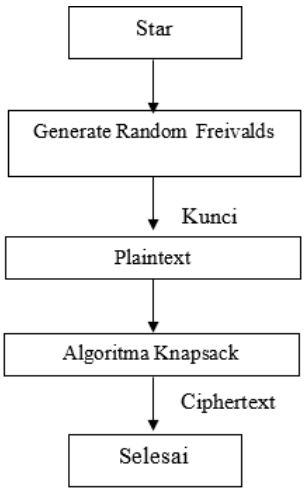
$$M=b_1w_1+b_2w_2+\cdots+b_nw \quad (3)$$

Keterangan
M = Problem Knapsack
b_n= biner plainteks
w_n= himpunan kunci
n = banyak deret Knapsack.

3. HASIL DAN PEMBAHASAN

Pembangkit kunci dilakukan dengan menggunkana algoritma yang menggunakan bilangan random. Dapat dimasukkan kata atau bilangan acak, yang dianggap 133yst menghilangkan dan berkemungkinan penyerang menerka hasil dengan memahami algoritmanya. Banyak Algoritma bilangan acak yang direncanakan dan di pergunakan hingga sampai saat ini. Algoritma tersebut menggunakan berbagai pendekatan yang berbeda-beda dan dapat diperoleh bilangan acak secararandom. Salah satu algoritma tersebut yaituAlgoritma Knapsack. Algoritma Knapsack bisadisebut sperti suatu karung yang dapat digunakan untuk memasukan sejumlah barang. Suatu karungmemiliki jumlah yang dibatasan, dapat simpul bahwa tidak semua barang dapat memuat ke dalam karung.Dengan mengulangi algoritma dasar ini beberapa kali, pemotongan minimum dapat ditemukan dengan probabilitas tinggi.

Proses Implementasi pengunjian algoritma Freivalds dengan menggunakan Algoritma Knapsack diuraikan sebagai penambahan 134ystem rancangan Implementasi pada metode kriptografi yang diteliti. Oleh sebab itu, proses yang diproleh pada penelitian digambarkan seperti bagan diagram berikut:



Gambar 1. Diagram Modifikasi Kunci Algoritma Freivalds

Proses pembentukan kunci algoritma Frievalds dengan menggunkan algoritma Knapsack dijelaskan. Dimisalkan Database atau plainteks dengan Text ASCII "**RAHMADRAHMAN**" menggunakan implementasi kunci algoritma Frievalds denganmenggunkan algoritma Knapsack. Adapun Proses Pembentukan kode Kunci Dengan menggunkan Algoritma Frievalds dengan algoritma Knapsack mempunyai dua sandi kunci, yaitu sandi kunci publik dan sandi kunci private.

Modifikasi disini ditujukan untuk Kunci Private yaitu:

Dimana:

$$r = \begin{bmatrix}1\\1\\1\end{bmatrix}$$

$$A = \begin{bmatrix}2 & 7 & 13\\7 & 13 & 2\\13 & 2 & 7\end{bmatrix}$$

$$B = \begin{bmatrix}3 & 5 & 11\\5 & 11 & 2\\11 & 3 & 5\end{bmatrix}$$

$$P=A \text{ x } (Br)\text{-}C\begin{bmatrix}1\\0\\1\end{bmatrix}$$

P = adalah hasil pengacakan
r = adalah nilai pektor pengacakan
A = adalah nilai variable acak matrik a
B = adalah nilai variable acak matrik b
C = adalah hasil perkalian matrik A x B

$$P=A \text{ x } (Br)\text{-}C\begin{bmatrix}1\\0\\1\end{bmatrix}$$

$$C=\begin{bmatrix}2 & 7 & 13\\7 & 13 & 2\\13 & 2 & 7\end{bmatrix} \text{ X } \begin{bmatrix}3 & 5 & 11\\7 & 13 & 3\\13 & 2 & 7\end{bmatrix}$$

$$C=\begin{bmatrix}2x3+7x7+13x13 & 2x5+7x13+13x2 & 2x11+7x3+13x7\\7x3+13x7+2x13 & 7x5+13x13+2x2 & 7x11+13x3+2x7\\13x3+2x7+7x13 & 13x5+2x13+7x2 & 13x11+2x3+7x7\end{bmatrix}$$

$$C=\begin{bmatrix}224 & 127 & 134\\138 & 208 & 130\\144 & 105 & 198\end{bmatrix}$$

$$P=A \text{ x } (Br)\text{-}C\begin{bmatrix}1\\0\\1\end{bmatrix}$$

$$P=\begin{bmatrix}2 & 7 & 13\\7 & 13 & 2\\13 & 2 & 7\end{bmatrix} x \left(\begin{bmatrix}3 & 5 & 11\\7 & 13 & 3\\13 & 2 & 7\end{bmatrix} x \begin{bmatrix}1\\1\\1\end{bmatrix} \right) - \begin{bmatrix}224 & 127 & 134\\138 & 208 & 130\\144 & 105 & 198\end{bmatrix} x \begin{bmatrix}1\\0\\1\end{bmatrix}$$

$$P\begin{bmatrix}2 & 7 & 13\\ 7 & 13 & 2\\ 13 & 2 & 7\end{bmatrix}\left(\begin{bmatrix}3+5+11\\ 7+13+3\\ 13+2+7\end{bmatrix}\right)-\begin{bmatrix}224 & 0 & 134\\ 138 & 0 & 130\\ 144 & 0 & 198\end{bmatrix}$$

$$P=\begin{bmatrix}2 & 7 & 13\\ 7 & 13 & 2\\ 13 & 2 & 7\end{bmatrix}x\begin{bmatrix}19\\ 23\\ 22\end{bmatrix}-\begin{bmatrix}358\\ 268\\ 342\end{bmatrix}$$

$$P=\begin{bmatrix}38+161+286\\ 133+299+44\\ 247+46+154\end{bmatrix}-\begin{bmatrix}358\\ 268\\ 342\end{bmatrix}$$

$$P=\begin{bmatrix}485\\ 476\\ 447\end{bmatrix}-\begin{bmatrix}358\\ 268\\ 342\end{bmatrix}$$

$$P=\begin{bmatrix}127\\ 208\\ 105\end{bmatrix}$$

Sehingga di dapat kan untuk nilai kunci adalah (127,208,105). Sehingga pada proses pembentukkan kunci algoritma friefalds di dapat nilai pengacakan algoritma *freifald* adalah 127, 208, 105 sehingga di peroleh kunci nya adalah 2, 3, 5, 7, 11, 13, 127, 208,105 sehingga di peroleh kunci privatnya adalah 2, 3, 5, 7, 11, 13, 105, 127,208.Adapun Proses Pembentukan enkripsi algoritma Algoritma Frievalds dengan algoritma Knapsack sebagai berikut :

1. Menentukan nilai kunci publik algoritma Knapsack berdasarkan kunci privat yang didapat dari algoritma freivald.
   Diketahui nilai m= 256 dan n= 11
   Sehingga bisa dihitung hasilnya adalah sebagai berikut:
   (2 * 11) mod 256= 22
   (3 * 11) mod 256 = 33
   (5 * 11) mod 256= 55
   (7 * 11) mod 256= 77
   (11 * 11) mod 256= 121
   (13 * 11) mod 256= 143
   (105 * 11) mod 256= 131
   (127 * 11) mod 256= 117
   (208 * 11) mod 256= 240
   Hasil perkalian akan menjadi kunci publik sedangkan barisan *superincreasing* semula menjadi kunci privat sehingga diperoleh:
   Kunci publik = {22, 32, 55, 77, 121, 143, 131, 117, 240}
   Kunci privat = {2, 3, 5, 7, 11, 13, 105, 127,208}
2. Setelah proses pembentukan kunci selesai dilakukan, maka tahap selanjutnya adalah melakukan proses enkripsi. Adapun data teks yang akan diubah kedalam proses enkripsi menggunakan algoritma *Knapsack* yaitu "RAHMADRAHMAN" adalah sebagai berikut:
   a. Ubah karakter plainteks menjadi bilangan biner 9 bit. Seperti yang terlihat di tabel 1.

Tabel 1. Konversi Karakter menjadi bilangan biner 9 bit

Pesan	Desimal	Biner
R	82	001010010
A	65	001000001
H	72	001001000
M	51	001001101
A	65	001000001
D	68	001000100
R	82	001010010
A	65	001000001
H	72	001001000
M	77	001001101
A	65	001000001
N	78	001001110

   b. Setiap bit *plainteks* di kalikan setiap elemen yang berkoresponden didalam kunci publik, dimana kunci publik = {22, 33, 55, 77, 121, 143, 131, 117, 240}. Seperti yang terlihat di table 2.

Tabel 2. Perkalian bit *plainteks* dengan elemen pada kunci publik

Biner	Kriptografi
001010010	(1*55) + (1*121) + (1*117) = 293
001000001	(1*55) + (1*240) = 295

001001000	(1*55) + (1*143) = 198
001001101	(1*77) + (1*121) + (1*117) + (1*240) = 569
001000001	(1*55) + (1*240) = 295
001000100	(1*55) + (1*131) = 186
001010010	(1*55) + (1*121) + (1*117) =293
001000001	(1*55) + (1*240) = 295
001001000	(1*55) + (1*143) =198
001001101	(1*55) + (1*143) + (1*131) + (1*240) = 569
001000001	(1*55) + (1*240 = 295
001001110	(1*55) + (1*143) +(1*131) + (1*117) = 506

Dengan demikian, *cipherteks_Knapsack* yang dihasilkan adalah 293, 295, 198, 569, 295, 186, 293, 295, 198, 569, 295, 506. Pada proses pembentukkan enkripsi algoritma Knapsackdi dapat nilai pengacakan di peroleh kunci privatnya adalah 2, 3, 5, 7, 11, 13, 105, 127,208. Adapun Proses Pembentukan deskripsi Algoritma Frievalds dengan algoritma Knapsack mempunyai langkah-langkah deskripsi pada algoritma knapsack adalah sebagai berikut:

1. Tentukan terlebih dahulu nilai *n* invers dengan rumus: $n^{-1} = (1+k*m)/n$, dimana nilai *k* adalah dimulai dari nol (0). Dengan *m* = 256, *n* = 11 dan menggunakan *k* = 10, maka diperoleh:$n^{-1} = (1 + 7*256) / 11 = 163$
2. Tentukan nilai transformasi masing-masing *plainteks_Base64*, lalu nyatakan hasilnya sebagai jumlah elemen sandi kunci privat untuk diperoleh *plainteks_Knapsack* dengan menggunakan suatu algoritma pencarian menjadi *superincreasing* Knapsack sehingga didapatkan plainteksdalam bentuk biner.
   Kunci privat = {2, 3, 5, 7, 11, 13, 105, 127, 208}
   293*163 Mod 256 = 143 = 5 + 11 + 127 , berkoresponden dengan 001010010
   295*163 Mod 256 = 213 = 5 + 208 , berkoresponden dengan 001000001
   198*163 Mod 256 = 18 = 5 + 13 , berkoresponden dengan 001001000
   569*163 Mod 256=331 =5+ 13 + 105 + 208, berkoresponden dengan 001001101
   295*163 Mod 256 = 213 5 + 208 , berkoresponden dengan 001000001
   186*163 Mod 256 = 246 = 5 + 208 , berkoresponden dengan 00100100
   293*163 Mod 256 = 143 = 5 + 11 + 127 , berkoresponden dengan 001010010
   295*163 Mod 256 = 213 = 5 + 208 , berkoresponden dengan 001000001
   198*163 Mod 256 = 18 = 5 + 13 , berkoresponden dengan 001001000
   569*163 Mod 256=331 =5+ 13 + 105 + 208, berkoresponden dengan 001001101
   295*163 Mod 256 = 213 = 5 + 208 , berkoresponden dengan 001000001
   506*163 Mod 256 = 250=5+ 13 + 105 +127, berkoresponden dengan 001001110
3. Ubah nilai biner 9 bit pada *plainteks Knapsack* menjadi karakter ASCII. Seperti yang terlihat di table 3.

Tabel 3. Konversi biner 9 bit pada *plainteks_Knapsack* menjadi karakter ASCII

Biner	**Desimal**	**Pesan**
001010010	82	R
001000001	65	A
001001000	72	H
001001101	51	M
001000001	65	A
001000100	68	D
001010010	82	R
001000001	65	A
001001000	72	H
001001101	77	M
001000001	65	A
001001110	78	N

Dengan demikian maka diperoleh kembali plainteks asli "RAHMADRAHMAN". Sehinnga hasil proses enkripsi dan deskripsi dapat dilaksanakn serta data yang di amankan dapat dikembalikan secara utuh.

4. KESIMPULAN

Berdasarkan hasil kesimpulan dari hasil dan pembahasan pada penelitian ini dimana Proses penerapan Algoritma Frievalds dengan cara melakukan pengacakan nilai untuk pembentukan kunci berdasarkan metode kriptografi Algoritma Knapsack, Proses enkripsi dapat dilakukan serta hasil pengembalian enkripsi dengan cara melakukan proses dekripsi dapat dilakukan dengan baik menggunakan Algoritma Knapsack berdasarkan kunci yang telah dibangkitkan dengan Algoritma Friefalds.

REFERENCES

[1] M. M. Amin, "Implementasi Kriptografi Klasik Pada Komunikasi Berbasis Teks," Pseudocode, vol. 3, no. 2, hal. 129–136, 2017.
[2] M. Fadlan dan H. Hadriansa, "Rekayasa Aplikasi Kriptografi dengan Penerapan Kombinasi Algoritma Knapsack Merkle Hellman dan Affine Cipher," J. Teknol. Inf. dan Ilmu Komput., vol. 4, no. 4, hal. 268, 2017.
[3] N. R. Yanti, A. Alimah, dan D. A. Ritonga, "Implementasi Algoritma Data Encryption Standard Pada Penyandian Record Database," J-SAKTI (Jurnal Sains Komput. dan Inform., vol. 2, no. 1, hal. 23, 2018.
[4] A. Aminudin, A. F. Helmi, dan S. Arifianto, "Analisa Kombinasi Algoritma Merkle-Hellman Knapscak dan Logaritma Diskrit pada Aplikasi Chat," J. Teknol. Inf. dan Ilmu Komput., vol. 5, no. 3, hal. 325, 2018.
[1] D. K. Pane, "Implementasi Data Mining Pada Penjualan Produk Elektronik Dengan Algoritma Apriori (Studi Kasus : Kreditplus)," Pelita Inform. Budi Darma, 2013.
[2] A. R. Syahputra, "Implementasi Algoritma Winnowing Untuk Deteksi Kemiripan Judul Skripsi Studi Kasus: STMIK Budi Darma," Pelita Inform. Budi Darma, vol. 12, no. 1, hal. 1–9, 2017.
[3] G. L. Ginting, P. N. Dian, dan Pristiwanto., "Perancangan Aplikasi Pendeteksi Kesalahan Perintah SQL Query Menggunakan Algoritma Knuth Morris Pratt," J. Ris. Komput. ISSN 2407-389X, 2018.
[4] D. Ariyus, "Pengantar Ilmu Kriptografi," Penerbit Andi, 2008.
[5] R. Sadikin, KRIPTOGRAFI UNTUK KEAMANAN JARINGAN. YOGYAKARTA: C.V ANDI OFFSET, 2012.
[6] S. Kromodimoeljo, Teori dan Aplikasi Kriptograf. 2009.
[7] M. Dias, C. Suhery, T. Rismawan, dan J. S. Komputer, "Penerapan Kriptografi Menggunakan Algoritma Knapsack, Algoritma Genetika, dan Algoritma Arnold's Catmap Pada Citra," J. Coding, Sist. Komput. Untan, vol. 04, no. 2, hal. 119–129, 2016.
[8] D. G. J. M. A. Sabelfeld(Eds), Computer Security-ESORICS 2006. Germany, 2006.
[9] L. A. Gordon, M. P. Loeb, W. Lucyshyn, dan R. Richardson, "2006 CSI/FBI computer crime and security survey," Comput. Secur. J., 2006.
[10] D. Ariyus, Kriptografi keamanan data dan komunikasi. Graha Ilmu.