MEANS (Media Informasi Analisa dan Sistem)
p-ISSN : 2548-6985, e-ISSN : 2599-3089

Implementasi Algoritma Merkle-Hellman Knapsack dalam Penyandian Record Database

[1)] Reni Rahmadani
Universitas Negeri Medan, Jl. Willlem Iskandar Pasar V Medan Estate, Indonesia
E-Mail: renirahmadani@unimed.ac.id

[2)] Harvei Desmon Hutahaean
Universitas Negeri Medan, Jl. Willlem Iskandar Pasar V Medan Estate, Indonesia
E-Mail: harvei.hutahaean@gmail.com

[3)] Ressy Dwitias Sari
Universitas Negeri Medan, Jl. Willlem Iskandar Pasar V Medan Estate, Indonesia
E-Mail: ressy@unimed.ac.id

ABSTRACT
A lot of data is misused without the data owner being aware of it. Software developers must ensure the security user data on their system. Due to the size of the market that houses data, the security of record databases must be of great concern. Cryptographic systems or data encryption can be used for data security. The Merkle-Hellman Knapsack algorithm is included in public-key cryptography because it uses different keys for the encryption and decryption processes. This algorithm belongs to the NP-complete algorithm which cannot be solved in polynomial order time. This algorithm has stages of key generation, encryption, and decryption. The results of this study secure database records from theft by storing records in the form of ciphertext/password. Ciphertext generated by algorithmic encryption has a larger size than plaintext.

Keyword : **cryptography, public key cryptography, merkle-hellman knapsack algorithm**

PENDAHULUAN

Di era 4.0 saat ini, semua orang bergantung pada jaringan internet untuk melakukan hampir semua kegiatan. Banyak orang yang memasukkan data pribadi tanpa memperhatikan keamanan database yang digunakan sistem tersebut. Sehingga banyak data yang disalahgunakan tanpa disadari oleh si pemilik data. Data yang disalahgunakan saat ini tidak hanya data sensitif seperti password dan pin. Data lainnya yang tidak dianggap sensitif juga sering disalahgunakan seperti nomor handphone, alamat, hingga hobi dan kegemaran pengguna. Menurut penelitian yang dilakukan Arpita Ghosh dan Aron Roth perusahaan besar seperti Google, Yahoo, Microsoft, dan Facebook juga terlibat secara implisit melakukan pembelian informasi pribadi dengan imbalan non-moneter kompensasi[1]. Namun saat ini pengguna mulai melihat keamanan dari sistem yang digunakan dan akan meninggalkan sistem yang tidak menjamin keamanan datanya. Banyak pengembang software yang menyadari hal ini dan berusaha membangun sistem yang dapat menjamin keamanan data pengguna yang menggunakan sistemnya.

Data yang dimasukkan pengguna kedalam sistem disimpan di database. Saat ini keamanan record database sangat diperhatikan mengingat besarnya pasar yang akan menampung data. Bahkan Lisa K. Fleischer dan Yu-Han Lyu merancang model Bayesian, sebuah mekanisme yang kompatibel untuk menentukan besarnya insentif dan menjaga privasi yang menjamin keakuratan dan melindungi privasi biaya dan data pengguna[2]. Salah satu bentuk keamanan yang bisa diterapkan pada databasae adalah kriptogtafi. Kriptografi merupakan ilmu yang mempelajari metode penyandian data. Proses dalam kriptografi terdiri dari dua tahap yaitu enkripsi dan dekripsi[3][4]. Dalam kriptografi ada beberapa algoritma yang digunakan untuk mengamankan data seperti: RSA, Pohlig-Hellman, RC4, El-Gamal, dan lainnya. Algoritma merkle-hellman knapsack merupakan salah satu algoritma kriptografi

METODE

Kriptografi berasal dari bahasa Yunani yang berarti tulisan rahasia. Secara terminologi kriptografi adalah ilmu untuk menjaga keamanan data dalam pengirimannya[5]. Enkripsi dan dekripsi adalah proses penting dalam kriptografi. Enkripsi proses yang mengubah data/pesan (plaintext) menjadi sandi (ciphertext). Dekripsi mengembalikan ciphertext menjadi plaintext[6].

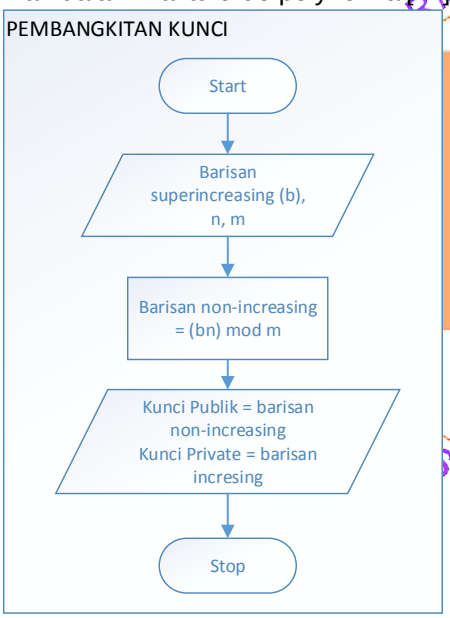
2.1. Kriptografi Kunci Publik

Terdapat dua pemisahan algoritma kriptografi berdasarkan pembagian kunci. Algoritma

kriptografi simetris menggunakan kunci yang sama untuk proses enkripsi dan dekripsi[7]. Algoritma kunci simetris lemah dalam melawan serangan brute force pada kuncinya. Pendistribusian kunci pada algoritma ini bersifat rahasia[8]. Algortima kunci asimetris menggunakan kunci yang berbeda untuk proses enkripsi dan dekripsi[9]. Kunci yang digunakan pada proses enkripsi disebut publik key dan dapat diketahui orang lain[10]. Algoritma merkle-hellman knapsack masuk kedalam algoritma kriptografi kunci asimetris yang sering disebut juga algoritma kunci publik[11].

2.2. Algoritma Merkle-Hellman Knapsack

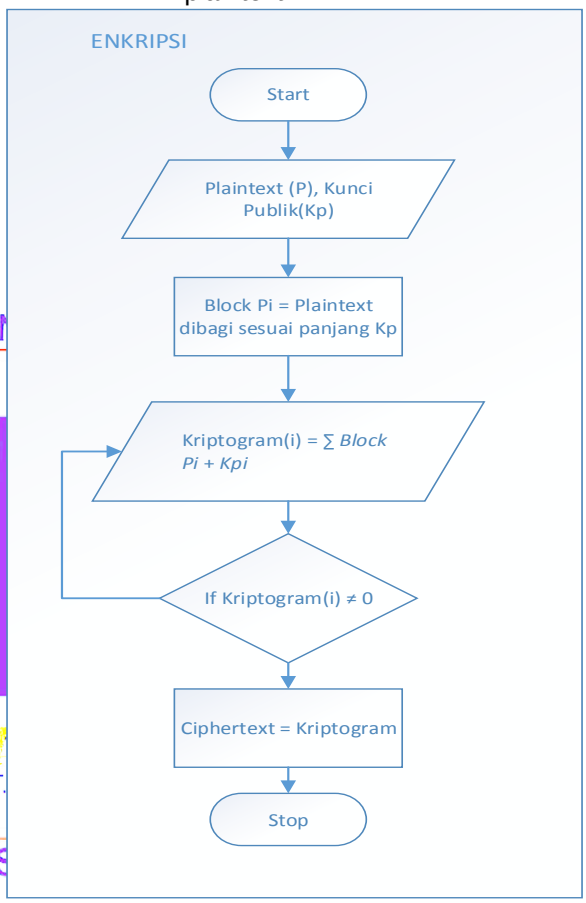
Algoritma Merkle-Hellman Knapsack termasuk kedalam kriptografi kunci publik karena menggunakan kunci yang berbeda untuk proses enkripsi dan dekripsi. Algoritma ini termasuk kedalam algortima NP-complete yang tidak dapat dipecahkan dalam waktu orde polynomial[12].



Gambar 1. *Flowchart* pembangkitan kunci

Terdapat tiga tahap dalam yang dilakukan dalam algoritma ini[13]:

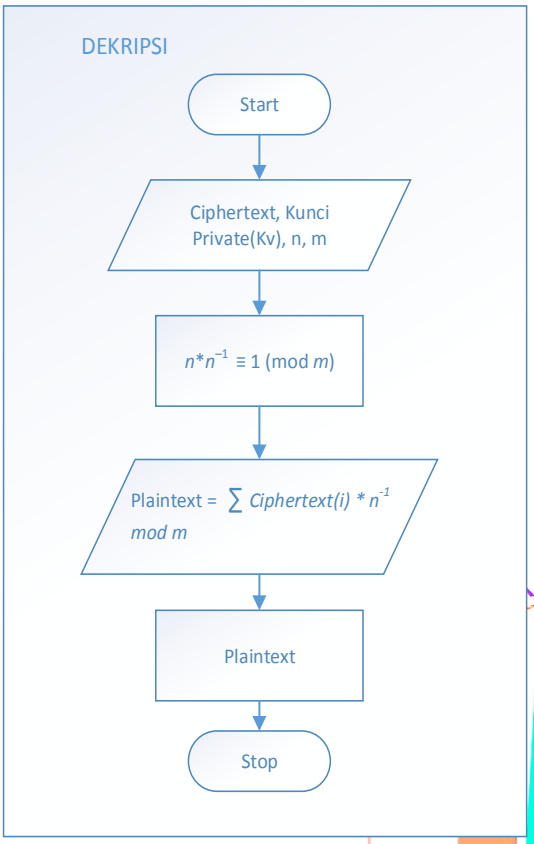
1. Proses Pembangkitan Kunci
   a. Tentukan kunci private, kunci ini merupakan barisan superincreasing dimana elemen dalam deret harus lebih besar daripada jumlah elemen sebelumnya.
   b. Tentukan bilangan prima m dan n, dimana m harus lebih besar dari elemen terakhir pada deretan dan n relatif prima dengan m.
   c. Bangkitkan kunci publik dengan persamaan:
      $Kpi = si * n \bmod m$……(1)
      dimana Kp adalah kunci publik
      s adalah elemen dalam deretan
      i adalah indeks dari deretan
      Kunci publik memiliki panjang elemen yang sama dengan deretan superincreasing
2. Proses Enkripsi
   a. Pesan/Plaintext dipecah menjadi block bit yang panjanganya samadengan panjang elemen kunci publik
   b. Tentukan ciphertext dengan persamaan:
      $c = b1*Kp_1 + b_2*Kp_2 + ... + b_n*Kp_n$…..(2)
      dimana: c adalah ciphertext
      b adalah bentuk biner dari block plaintext



Gambar 2. *Flowchart* proses enkripsi

3. Proses Dekripsi
   a. Proses dekripsi dilakukan dengan menggunakan kunci private
   b. Hitung nilai plaintext dengan persamaan
      $Pi = c * n^{-1} \bmod m$ ……(3)
      dimana: n^{-1} nilai invers dari m
   c. Hitung nilai biner Pi dengan mengurangi Pi dengan nilai elemen yang besarnya mendekati nilai Pi. Proses dilanjutkan sampai hasil = 0 atau 1.
   d. Gabungkan nilai yang didapat dengan syarat: jika hasil 0 nilai biner dimasukkan jika hasil 1 maka nilai tidak dimasukkan.

MEANS (Media Informasi Analisa dan Sistem)
p-ISSN : 2548-6985, e-ISSN : 2599-3089



Gambar 3. *Flowchart* proses dekripsi

HASIL DAN PEMBAHASAN

Record database yang digunakan dalam penelitian ini adalah record data mahasiswa UNIMED prodi Teknologi Informatika dan Komputer angkatan 2019 yang berisi IPK.

Tabel 1. Record database mahasiswa

Nama	Nim	Sem1	Sem2
SITI HAPSAH	5191151006	3,45	3,46
YOSUA SITEPU	5192451003	3,54	3,90
JAFAR SIDIK	5192451007	3,72	3,55
FIYA MONALISA	5193151005	3,63	3,58
RIZKY NABILA	5193351005	3,54	3,55

Dari record dalam database di atas diambil contoh plaintext dari field nama yaitu “SITI HAPSAH”. Tahapan pertama adalah menentukan kunci private. Kunci private merupakan deretan super increasing yang digunakan dalam proses ini adalah 2, 5, 11, 23, 47, 95, 191, 378. Tentukan kunci publik dengan nilai m = 479 dan n = 73. Hitung dengan persamaan (1) dan didapatkan kunci publik 146, 365, 324, 242, 78, 229, 52, 291. Setelah didapatkan kunci maka akan dilakukan proses enkripsi dimulai dengan menentukan block plaintext yang sesuai dengan panjang kunci yaitu 8 bit.

Enkripsi block plaintext

Block-1 = S = 01010011
Kunci publik = 146, 365, 324, 242, 78, 229, 52, 291
Kriptogram = (1x365) + (1x242) + (1x52) + (1x291) = 950

Block-2 = I = 01001001
Kunci publik = 146, 365, 324, 242, 78, 229, 52, 291
Kriptogram = (1x365) + (1x78) + (1x291) = 734

Block-3 = T = 01010100
Kunci publik = 146, 365, 324, 242, 78, 229, 52, 291
Kriptogram = (1x365) + (1x242) + (1x229) = 836

Block-5 = Space = 00100000
Kunci publik = 146, 365, 324, 242, 78, 229, 52, 291
Kriptogram = (1x324) = 324

Block-6 = H = 1001000
Kunci publik = 146, 365, 324, 242, 78, 229, 52, 291
Kriptogram = (1x146) + (1x242) = 388

Block-7 = A = 01000001
Kunci publik = 146, 365, 324, 242, 78, 229, 52, 291
Kriptogram = (1x365) + (1x291) = 656

Block-7 = P = 1010000
Kunci publik = 146, 365, 324, 242, 78, 229, 52, 291
Kriptogram = (1x146) + (1x324) = 470

Ciphertext : 950734836734324656470950656388. Ukuran ciphertext yang dihasilkan lebih panjang dari ukuran plaintext. Record diatas disimpan dalam bentuk ciphertext untuk mengamankan record dari pencurian data.

KESIMPULAN

Dari penelitian yang dilakukan penulis dapat menyimpulkan bahwa, algoritma Merkle-Hellman Knapsack dapat diimplementasikan dalam pengamanan record database. Record database disimpan dalam bentuk ciphertext/sandi sehingga keamannya lebih terjaga. Algoritma Merkle-Hellman Knapsack menghasilkan ciphertext yang memiliki ukuran lebih besar daripada plaintext..

DAFTAR PUSTAKA

[1] Ghosh, Arpita, and Aaron Roth. "Selling privacy at auction." Proceedings of the 12th ACM conference on Electronic commerce. 2011.

[2] Fleischer, Lisa K., and Yu-Han Lyu. "Approximately optimal auctions for selling privacy when costs are correlated with data." Proceedings of the 13th ACM Conference on Electronic Commerce. 2012.

MEANS (Media Informasi Analisa dan Sistem)
p-ISSN : 2548-6985, e-ISSN : 2599-3089

[3] Rahmadani, R., & Hutahaean, H. D. (2020). Implementation Of Pohlig-Hellman Algorithm And Steganography Combination Of First Of File (Fof) And End Of File (EOF) For File Security. Jurnal Mantik, 4(1, May), 14-19.

[4] Budiman, M. A., & Rachmawati, D., Implementation of Super-Encryption with Trithemius Algorithm and Double Transposition Cipher in Securing PDF Files on Android Platform. Journal of Physics: Conference Series, vol. 978, pp. 012088. 2018.

[5] Purba, Wina Mariana Br. "Implementasi Algoritma Knapsack Dan Base64 Pada Pengamanan File Teks." Pelita Informatika: Informasi dan Informatika 7.4 (2019): 291-302.

[6] Asriyanik, Asriyanik. "Studi Terhadap Advanced Encryption Standard (Aes) Dan Algoritma Knapsack Dalam Pengamanan Data." SANTIKA (Jurnal Ilmiah Sains dan teknologi) 7.1 (2017): 553-561.

[7] Kester, Quist-Aphetsi. "A Hybrid Cryptosystem based on Vigenere cipher and Columnar Transposition cipher." arXiv preprint arXiv:1307.7786 (2013).

[8] Preetha, M., and M. Nithya. "A study and performance analysis of RSA algorithm." International Journal of Computer Science and Mobile Computing 2.6 (2013): 126-139.

[9] Torkaman, Mohammad Reza Najaf, Nazanin Sadat Kazazi, and Azizallah Rouddini. "Innovative approach to improve hybrid cryptography by using DNA steganography." International Journal on New Computer Architectures and Their Applications (IJNCAA) 2.2 (2012): 225-236.

[10] Rahmadani, R., Putri, T. T. A., Sriadhi, S., Sari, R. D., & Hutahaean, H. D. Data security system using hybrid cryptosystem RC4A-RSA algorithm. IOP Conference Series: Materials Science and Engineering, vol. 830, pp. 032008. 2020.

[11] Hwang, M. S., Lee, C. C., & Tzeng, S. F. (2009). A new knapsack public-key cryptosystem based on permutation combination algorithm. Information Journal of Applied Mathematics and Computer Sciences, 5(1), 33-38.

[12] Pattiasina, Timothy John. "Rancang Bangun Aplikasi Enkripsi dan Dekripsi Email Dengan Menggunakan Algoritma Advanced Encryption Standard Dan Knapsack." Teknika 3.1 (2014): 1-10.

[13] Aminudin, Aminudin, Ahmad Faisal Helm, and Sofyan Arifianto. "Analisa Kombinasi Algoritma Merkle-Hellman Knapsack Dan Logaritma Diskrit Pada Aplikasi Chat." Jurnal Teknologi Informasi dan Ilmu Komputer (JTIIK) 5.3 (2018): 325-334.