Seminar Nasional Sains & Teknologi Informasi (SENSASI)
SENSASI 2019

ISBN: 978-602-52720-2-8
Juli 2019
Hal: 296 – 299

Implementasi Metode Merkle Hellman Untuk Keamanan Informasi Daftar Pencarian Orang (DPO) Polda Sumatera Utara

Badrul Anwar*, Azanuddin

Program Studi Sistem Komputer, STMIK Triguna Dharma, Medan, Indonesia
Email : [1]badrul_anwar@trigunadharma.ac.id, [2]azdin.bpc@gmail.com,

Abstrak

Di masa sekarang ini hampir semua komunikasi data serba digital mulai dari pengiriman file - file baik dokumen - dokumen berbasis teks, gambar, suara, maupun video. Berbagai macam cara menyembunyikan file telah banyak kita temui salah satunya yang paling populer adalah dengan cara menghidden. Perkembangan penyembunyian file itu sendiri semakin hari semakin pesat. Dengan kata lain file yang disembunyikan tersebut sudah tentu banyak orang sudah mengetahui cara untuk membukanya hal ini membuat setiap orang yang akan menyembunyikan data/file merasa bahwa ini sudah tidak aman lagi. Salah satu cara untuk melindungi data dari pihak yang tidak berkepentingan, adalah dengan melakukan kriptografi menggunakan Salah satu metode keamanan komputer yaitu dengan menggunakan Algoritma Merkle Hellman . penelitian ini diharapkan data/file dapat terjaga dengan baik tanpa dapat dimanipulasi oleh orang lain untuk merusak maupun mencuri informasi yang ada. Hasil dari penelitian ini akan diimplementasikan dalam sebuah program aplikasi untuk dapat memberikan kemudahan bagi setiap orang yang akan mengamankan file-file penting.

Kata Kunci: Kriptografi, Merkle Hellman, Daftar Pencarian Orang (DPO), Keamanan Informasi, Enkripsi, Deskripsi

1. PENDAHULUAN

DPO (Daftar pencarian orang) adalah sebuah istilah dibidang hukum atau kriminalitas yang merujuk kepada daftar orang-orang yang dicari atau yang menjadi target oleh pihak aparat penegak hukum, secara umum DPO merujuk kepada dua hal, yaitu orang hilang dan pelaku kriminal.Sumber informasi dalam mengimplementasikan DPO ini bervariasi, tergantung tingkat kriminalitas yang dilakukan objek DPO ataupun kerja sama antar intansi penegak hukum. Adapun prosedur DPO di tingkat penyidik haruslah mengacu pada pengetahuan sesuai hukum.

Berdasarkan penelitian yang dilaksanakan pada Bareskrim Polda Sumut, ternyata bidang ini memiliki kelemahan dalam mengamankan data DPO, dimana data hanya diarsipkan didalam sebuah folder komputer tanpa memiliki keamanan lebih untuk mengamankan setiap data dan setiap orang dapat mengakses atau membuka data tersebut. Dengan penyimpanan data seperti itu memungkinkan untuk orang lain dapat mencuri atau memanipulasi data. Dengan perkembangan teknologi komputer, kerahasiaan data dapat diminimalisir dengan ilmu kriptografiKriptografi merupakan ilmu matematika yang memiliki banyak fungsi dalam mengamankan data. Kriptografi terdiri dari dua proses utama yakni proses enkripsi dan dekripsi. Proses enkripsi adalah mengubah Plaintext menjadi Ciphertext (dengan menggunakan kunci tertentu) sehingga informasi pada data tersebut susah untuk dimengerti. Salah satu metode kriptografi yang digunakan dalam pengamanan data adalah metode Merkle Hellman

2. METODOLOGI PENELITIAN

"Kriptografi berasal dari bahasa Yunani yaitu kripto yang artinya "secret" (rahasia) dan graphia yang artinya "writting" (tulisan). Menurut teminologinya kriptografi adalah ilmu dan seni untuk menjaga keamanan pesan ketika pesan di kirim dari suatu tempat ke tempat yang lain"[1].

Dasar matematis yang mendasari proses enkripsi dan dekripsi adalah relasi antara dua himpunan yaitu yang berisi elemen plaintext dan yang berisi elemen ciphertext. Enkripsi dan dekripsi merupakan fungsi tranformasi antara himpunan-himpunan tersebut. Apabila elemen-elemen plaintext dinotasikan dengan P, elemen-elemen ciphertext dinotasikan dengan C, sedangkan untuk proses enkripsi dinotasikan dengan E, dekripsi dengan notasi D, maka secara matematis proses kriptografi dapat dinyatakan sebagai berikut [2]

$$\text{Enkripsi : } E(P) = C \quad (1)$$

$$\text{Dekripsi : } D(C) = P \quad (2)$$

Merkle-Hellman Knapsack merupakan Kriptosistem yang dibuat oleh Merkle dan Hellman pada tahun 1980 Walaupun sistem ini, dan beberapa variannya, telah dipecahkan sekitar awal tahun 1980, tetapi masih layak untuk dipelajari dengan berbagai alasan [3] [4].

Dalam kriptosistem Merkle-Hellman, 'penyamaran' diakhiri dengan penelusuran: diberikan s1, s2,..,sn merupakan sebuah ukuran himpunan super-increasing. Memilih suatu bilangan prima p yang lebih besar dari pada jumlah semua si, dan suatu bilangan b dengan $1 < b < p$. System ini sangat popular sejak bisa secara cepat diimplementasikan. Namun, diawal tahun 1980, Shamir, menggunakan Lenstra algoritma pemrograman linier cepat, mampu membuang jauh penyamaran ini dan memperoleh himpunan super-increasing (atau sesuatu yang ekuivalen dengan itu). Banyak metode lain untuk melakukan penyamaran himpunan super-increasing yang telah dicoba, tapi sebagian besar dari itu dapat di buka. Satu metode, diketahui sebagai kriptosistem Chor-Rivest, menggunakan nilai manipulasi berhingga dan ini masih dianggap aman untuk digunakan[2] [5] [6].

$$t_i = a * s_i \bmod p \quad (3)$$

Proses Enkripsi :

1. Pesan plaintext P bisa dituliskan dalam bentuk: P = [p1, p2,..., pk].

ISBN: 978-602-52720-2-8
Juli 2019
Hal: 296 – 299

2. Membagi pesan ke dalam blok bit-bit m , P0 = [pl, p2,..., pm], P1 = [pm+1,..., p2m], dan selanjutnya. (m adalah bilangan pembatas dalam knapsack)
3. Memilih nilai dengan mengubah dari bentuk 1 bit kedalam Pi selanjutnya Pi disajikan sebagai vector yang dipilih untuk element t.
4. Nilai ciphertext merupakan: Pi * t, target menggunakan blok Pi untuk memilih vector.

Proses Dekripsi :

1. Dengan nilai a–1 kemudian a* a–1 = 1 mod p. Dalam contoh kami, 7–1 mod 17 adalah 5, mulai 5 * 8 mod 17 = 40 mod 17 = (17 * 7) + 1 mod 17 = 1
2. Ingat bahwa H adalah knapsack sulit yang terjadi dari knapsack sederhana S. H adalah memperoleh S dengan H= w * S mod
3. Pesan ciphertext juga di dapat dari algoritma enkripsi dengan langkah-langkah sebagai berikut : C = H * P = w * S * P mod n
4. Untuk mengubah cipher, pengali C dari w–1, mulai w-1 * C = w-1 * H * P =
5. w-1 * w * S * P mod n = S * P mod n
6. Sekarang penerima dapat memecahkan masalah knapsack sederhana dengan knapsack S dan target w–1 * Ci untuk beberapa bilangan ciphertext Ci.
7. Dimulai w–1 * Ci = S * P mod n, solusi untuk target w–1 * Ci adalah blok plaintext Pi , dimana adalah pesan asli yang di enkripsi [7] [8]

3. ANALISA DAN PEMBAHASAN

3.1 Analisa

Algoritma sistem merupakan sebuah tahapan yang dilakukan untuk melakukan proses kemanan dalam mengamankan data Daftar Pencarian Orang (DPO) pada Polda Sumut. Adapun algoritma sistem dalam permasalahan ini menggunakan metode Merkle Hellman adalah sebagai berikut :

a. Membuat Private key (S, A, dan P).

S = (2,4,7,14,28,112,224,407) = ∑s = 798

A = 989

P = 578

b. Membuat Public Key

Plaintext (x) : GUNAWAN

Enkripsi :

Perhitungan Public Key (T) :

T = P * Si mod A

c. Mengubah Plaintext ke biner.

Pada Proses ini data perlu diubah menjadi bentuk biner karena perhitungan Merkle Hellman menggunakan teknik binary sebagai proses enkripsi dan dekripsinya

Plaintext : GUNAWANDimasukkan kedalam kode ASCIIX = 71 85 78 65 87 65 78

d. Menjumlahkan (perkalian biner dengan Publik key).

Plaintext dibagi dalam blok sesuai dengan banyak ny S, pada contoh ini banyaknya S 8 digit

01000111 : Y = (0*167)+(1*334)+(0*90)+(0*180)+(0*360)+(1*451)+(1*902) + (1*853)= 334 + 451 + 902 + 853

= 2540

Ciphertext:2540 1818 2047 1187 2720 1187 1998

Dekripsi :Hitung Z = M-1 Y mod A

e. Mengurangkan data dengan nilai S.

Proses pengurangan data dengan nilai – nilai pada elemen S. Pengurangan terus dilakukan dari elemen yang paling besar hingga yang paling kecil. Hasil akhir dari pengurangan haruslah bernilai 0. Hasil akhir dimana pengurangan tidak 0, maka proses dekripsi dinyatakan gagal. Penyebab kegagalan dapat terjadi apabila kunci S tidak dibuat dengan metode superincreasing linier.

Untuk Y 2540 = 747

ISBN: 978-602-52720-2-8
Juli 2019
Hal: 296 – 299

Untuk Y ⟶ 2540 = 747

2	4	7	14	28	112	224	407	S
							747-407	Z
						340-224	340	
					116-112	116		
				4-28	4			
			4-14					
		4-7						
	4-4							
0-2	4							
0	1	0	0	0	1	1	1	

Plaintext : 01000111

Plaintext dimasukan kedalam kode ASCII maka akan didapatkan hasil

Binary(Z)	ASCII	Plaintext
1000111	71	G
1010101	85	U
1001110	78	N
1000001	65	A
1010111	87	W
1000001	65	A
1001101	78	N

3.2 Pembahasan

Aplikasi ini dilengkapi dengan user interface yang menarik dan bertujuan untuk memudahkan pengguna dalam menggunakannya. Pada aplikasi ini memiliki interface atau desain form yang terdiri dari formlogin, form menu utama, form Data Pencarian Orang, form Enkripsi, dan form Dekripsi

Gambar 1. Form Daftar Pencarian Orang

Gambar 2. Form Enkripsi

ISBN: 978-602-52720-2-8
Juli 2019
Hal: 296 – 299

Gambar 3. Form Deskripsi

4. KESIMPULAN

Keunggulan dari metode Merkle Hellman mempunyai keamanan yang kuat dengan jumlah kunci yang lebih banyak dibanding dengan kriptosistem seperti RSA.Berdasarkan uji coba yang telah dilakukan, aplikasi ini berhasil mengimplementasikan proses enkripsi dan dekripsi untuk mengamankan data. Hal ini dibuktikan melalui pengujian yang telah dilakukan bahwa semua data yang telah di enkripsi dapat dikembalikan ke bentuk semula dalam proses dekripsi dan data tidak mengalami perubahan.

REFERENCES

[1] Shamir, A. (1984). A Polynomial-Time Algorithm for Breaking the Basic Merkle—Hellman Cryptosystem. IEEE Transactions on Information Theory. https://doi.org/10.1109/TIT.1984.1056964
[2] Adleman, L. M. (1983). On Breaking the Iterated Merkle-Hellman Public-Key Cryptosystem. In Advances in Cryptology. https://doi.org/10.1007/978-1-4757-0602-4_29
[3] Brickell, E. F., Davis, J. A., & Simmons, G. J. (1983). A Preliminary Report on the Cryptanalysis of Merkle-Hellman Knapsack Cryptosystems. In Advances in Cryptology. https://doi.org/10.1007/978-1-4757-0602-4_28
[4] Nguyen, P., & Stern, J. (1997). Merkle-Hellman revisited: A cryptanalysis of the qu-vanstone cryptosystem based on group factorizations. Lecture Notes in Computer Science (Including Subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics). https://doi.org/10.1007/BFb0052236
[5] Pargeter, A. R., & Yan, S. Y. (2007). Number Theory for Computing. The Mathematical Gazette. https://doi.org/10.2307/3620808
[6] Hellman, M. E. (2005). An overview of public key cryptography. IEEE Communications Magazine. https://doi.org/10.1109/mcom.2002.1006971
[7] Elgamal, T. (1985). A Subexponential-Time Algorithm for Computing Discrete Logarithms Over GF(p)2. IEEE Transactions on Information Theory. https://doi.org/10.1109/TIT.1985.1057075
[8] Goodman, R. M. F., & McAuley, A. J. (1985). A new trapdoor knapsack public key cryptosystem. Lecture Notes in Computer Science (Including Subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics). https://doi.org/10.1007/3-540-39757-4_15