Sains dan Komputer (SAINTIKOM)
Vol.18, No.2, Agustus 2019, pp. 104~110
P-ISSN: 1978-6603 E-ISSN : 2615-3475

Pengamanan Data *Clien Test Urine* Pada BNN Kabupaten Deli Serdang Menggunakan Metode Merkle Hellman

Badrul Anwar, Azanuddin, Nurcahyo Budi Nugroho
*Sistem Informasi, STMIK Triguna Dharma

Article Info
Article history:
Received May 31th, 2019
Revised June 12th, 2019
Accepted Augs 07th, 2019

Keyword:
Kriptografi,
Merkle Hellman,
Pengamanan Data Client Test Urine,
Keamanan Data

ABSTRACT
Data client test urine sangat penting yang hanya boleh diketahui pihak tertentu saja. Pengiriman, penginputan dan penyimpanan data atau informasi tanpa dilakukan pengamanan akan bersiko terhadap manipulasi data. Dalam hal ini maka perlu dibutuhkan keamanan, salah satunya dengan melakukan keamanan data pada komputer untuk melidungi akses data dari pihak yang tidak berkepentingan tersebut maka sangat diperlukan enkripsi dan dekripsi. Algoritma yang digunakan disini adalah algoritma merkle hellman, dimana algoritma merekle merupakan cryptosystem asimetris kunci yang memiliki 2 (dua) kunci yaitu public key dan private key. Dengan menerapkan metode merkle hellman ini mampu memberikan pengamanan terhadap data clent test urine, sehingga data tersebut memiliki tingkat keamanan yang tinggi. Algoritma merkle hellman dalam mengamankan data client test urine dapat dilakukan menggunakan bahasa pemprograman visual basic 2008.

First Author
Nama :Badrul Anwar
Kantor :STMIK Triguna Dharma
Program Studi :SistemInformasi
E-Mail :Badrul@trigunadharma.ac.id

1. PENDAHULUAN

Badan Narkotika Nasioanal (BNN) Kabupaten Deli Serdang adalah sebuah Lembaga Pemerintah Non Kementrian (LPNK) Indonesia yang mempunyai tugas dibidang pencegahan, pemberantasan penyalahgunaan dan peredaran gelap narkotika di wilayah Kabupaten Deli Serdang. Badan Narkotika Nasional (BNN) Kabupaten Deli Serdang terdapat klinik yang difungsikan untuk *client* yang ingin melakukan *test urine*.

Dalam sebuah pelayanan *test urine*, data *client test urine* adalah data yang sangat penting dan dijaga kerahasiaannya. Data *client test urine* pada BNN Kabupaten Deli Serdang belum menerapkan sebuah sistem pengamanan data, sehingga data *client test urine* tersebut berpotensi untuk diubah dan dimanipulasi oleh pihak-pihak yang tidak bertanggung jawab untuk keperluan pribadi seperti pencemaran nama baik, penipuan, dan sebagainya. Untuk menjaga kerahasiaan dan keamanan data dari pihak-pihak yang ingin merubah dan memanipulasi data tersebut, maka diperlukan sebuah sistem keamanan data.

Karena data *client test urine* berupa data *text*, maka dari masalah yang telah diuraikan akan dibangun sebuah sistem keamanan untuk mengamankan data *client test urine* menggunakan metode Merkle Hellman pada kriptografi berbasis *dekstop.* Kriptografi adalah ilmu yang mempelajari tentang bagaimana cara penyandian/penyamaran data yang digunakan untuk keamanan informasi seperti kerahasiaan, keutuhan, dan otentikasi entitas data. Agar dapat dilakukan enkripsi dan deskripsi dengan baik dibutuhkan suatu algoritma untuk mengenkripsi dan deskripsi data, salah satunya metode Merkle Hellman. Metode Merkle Hellman merupakan *cryptosystem asimetris* kunci, yang berarti mengunakan kunci ganda yaitu, kunci publik dan kunci pribadi.

Dari pembahasan ini diharapkan sistem yang dibangun dapat membantu pihak BNN untuk melindungi data *client test urine* dari pihak-pihak yang tidak bertanggung jawab, maka dilakukan penelitian untuk pengamanan data *client test urine* dengan menerapkan kriptografi algoritma Merkle Hellman yang diberi judul **"Pengamanan Data Client Test Urine Pada BNN Kabupaten Deli Serdang Menggunakan Metode Merkle Hellman".**

2. METODE PENELITIAN

2.1 Keamanan Data

Keamanan data sangatlah penting dalam proses pengiriman ataupun penerimaan data yang dilakukan melalui media komputer. Pengamanan data ini dilakukan dalam rangka menjaga kerahasiaan, keutuhan, keabsahan dan ketersediaan data. Sehingga untuk memenuhi hal tersebut diperlukan adaya upaya dalam pengamanan data yakni dengan enkripsi dan dekripsi. (Asriyanik, 2017)

2.2 Kriptografi

Kriptografi berasal dari Bahasa Yunani, menurut bahasa tersebut kata "kriptografi"dibagi menjadi dua, yaitu kripto dan graphia. Kripto berarti *secret* (rahasia) dan Graphia berarti *writing* (tulisan). Menurut terminologinya, kriptografi adalah ilmu dan seni untuk menjaga keamanan pesan ketika pesan dikirim dari suatu tempat ke tempat yang lain (Ariyus, 2006 :77).

2.3 Data *Client Test Urine*

Data *client* merupakan informasi tentang seseorang yang berisi data pribadi seperti nama, alamat, tanggal lahir, nomor telepon, dan sejenisnya. Data ini berfungsi untuk mengetahui informasi dari seorang *client.*

Test urine adalah suatu metode pemerikasaan menggunakan *urine* (air seni) guna mendeteksi adanya gangguan dalam tubuh. Dalam pemeriksaan *test urine* yang dilakukan BNN bertujuan untuk mendeteksi adanya penggunaan obat-obatan terlarang pada seseorang. Jadi, data *client test urine* merupakan informasi dari seorang *client* yang melakukan *test urine* untuk keperluan tertentu.

2.4 Metode Merkle Hellman

Algoritma kriptografi *Merkle Hellman* atau pada umumnya dikenal dengan sebutan merupakan *chiper* yang ide awalnya dari algoritma kriptografi *One Time Pad*, yaitu kunci yang dibangkitkan secara *random* dan panjang kunci sepanjang plainteks yang akan dienkripsi. Tetapi pada algoritma kriptografi pembangkitan kunci-kunci tersebut secara otomatis dengan teknik berantai.(Siregar, 2013)

Rumus Proses Enkripsi:

$$c = \sum_{i=1}^{n} \propto_i \beta_i \quad \ldots\ldots [1]$$

Keterangan:

c = *Chiper Text*

β = *Public Key*

$\propto$ = Pesan / *Plaintext*

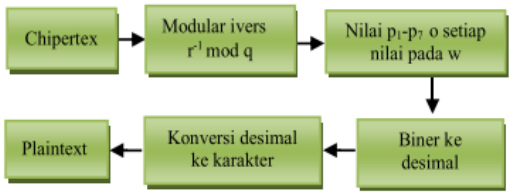
Rumus Private Key:

$$q > \sum_{i=1}^{n} w_i \quad \ldots\ldots [2]$$

Rumus *Public Key :*

$\beta = w * r \ mod \ q$ . . . . . [3]

Proses Dekripsi:



Rumus Modular *Invers:*

M = (r * M mod p = 1) . . . . . [4]

Rumus *Chipper* Data Mod q :

$K = C. \ r^{-1} \ mod \ q$. . . . . [6]

3. ANALISIS DAN HASIL

3.1 Algoritma Sistem

Adapun algoritma dalam metode Merkle Hellman yang akan digunakan untuk menyelesaikan permasalahan adalah:

1. Menentukan kunci
2. Melakukan enkripsi
3. Melakukan dekripsi

3.2 Proses Enkripsi

3.2.1 Membuat *Private Key* (w,q,r)

Tabel 3.1 *Private Key*

w	{2, 7, 11, 21, 42, 89, 180, 354} = $\sum w$ = 706
q	881
r	588

3.2.2 Membuat *Public Key*

Tabel 3.2 *Public Key*

w	**$\beta = (r * w_i) \bmod q$**	
2	588 * 2 mod 881	295
7	588 * 7 mod 881	592
11	588 * 11 mod 881	301
21	588 * 21 mod 881	14
42	588 * 42 mod 881	28
89	588 * 89 mod 881	353
180	588 * 180 mod 881	120
354	588 * 354 mod 881	236

3.2.3 Merubah *Plaintext* ke Biner 8 Digit

Tabel 3.3 Data Biner

Plainteks	**ASCII**	**Binary (z)**
S	**83**	**01010011**
u	**117**	**01110101**
s	**115**	**01110011**
a	**97**	**01100001**
n	**110**	**01101110**
t	**116**	**01110100**
i	**105**	**01101001**

3.2.4 Perhitungan Data *Chiper*

Tabel 3.4 Perhitungan Data *Chiper*

Binary (z)	**$\sum z * \beta_i$**	**Chippertext**
01010011	(0x295) + (1x592) + (0x301) + (1x14) + (0x28) + (0x 353) + (1x120) + (1x236)	962
01110101	(0x295) + (1x592) + (1x301) + (1x14) + (0x28) + (1x 353) + (0x120) + (1x236)	1496
01110011	(0x295) + (1x592) + (1x301) + (1x14) + (0x28) + (0x 353) + (1x120) + (1x236)	1263

01100001	(0x295) + (1x592) + (1x301) + (0x14) + (0x28) + (0x 353) + (0x120) + (1x236)	1129
01101110	(0x295) + (1x592) + (1x301) + (0x14) + (1x28) + (1x 353) + (1x120) + (0x236)	1394
01110100	(0x295) + (1x592) + (1x301) + (1x14) + (0x28) + (1x 353) + (0x120) + (0x236)	1260
01101001	(0x295) + (1x592) + (1x301) + (0x14) + (1x28) + (0x 353) + (0x120) + (1x236)	1157

3.3 Proses Dekripsi

3.3.1 Tabel *Modular Invers*

Tabel 3.5 *Modular Invers*

M	**(r * M) mod q**	
1	588 * 1 mod 881	588
2	588* 2 mod 881	295
3	588* 3 mod 881	2
....	.....	....
442	588* 442 mod 881	1

3.3.2 Perhitungan Data *Chiper* Mod q

Tabel 3.6 Perhitungan Data *Chiper* Mod q

***Cipher* (C)**	**M**	**K= (c * M) mod q**	
962	442	962 * 442 mod 881	**562**
1496	442	1496 * 442 mod 881	**482**
1263	442	1263 * 442 mod 881	**92**
1129	442	1129 * 442 mod 881	**573**
1394	442	1394 * 442 mod 881	**329**
1260	442	1260 * 442 mod 881	**128**
1157	442	1157 * 442 mod 881	**414**

3.3.3 Pengurangan Data Dengan Nilai w

*P*1 = 562–354 = 208**(1)** | 208–180 = 28**(1)** | 28-89 = 28**(0)** | 28-42 = 28**(0)** | 28-21 = 7**(1)** | 7-11 = 7**(0)** | 7-7 = 0**(1)** | 0-2 = 0**(0)**

Maka diperoleh hasil **01010011 = S**

*P*2 = 482–354 = 128**(1)** | 128–180 = 128**(0)** | 128-89 = 39**(1)** | 39-42 = 39**(0)** | 39-21 =18**(1)** | 18-11 = 7**(1)** | 7-7 = 0**(1)** | 0-2 = 0**(0)**

Maka diperoleh hasil **01110101 = u**

*P*3 = 573–354 = 219**(1)** | 219–180 = 39**(1)** | 39-89 = 39**(0)** | 39-42 = 39**(0)** | 39-21 = 18**(1)** | 18-11 = 7**(1)** | 7-7 = 0**(1)** | 0-2 = 0**(0)**

Maka diperoleh hasil **01110011 = s**

*P*4 = 372–354 = 18**(1)** | 18–180 = 18**(0)** | 18-89 = 18**(0)** | 18-42 = 28**(0)** | 18-21 = 18**(0)** |18-11 = 7**(1)** | 7-7 = 0**(1)** | 0-2 = 0**(0)**

Maka diperoleh hasil **01100001 = a**

*P*5 = 329–354 = 329**(0)** | 329–180 = 149**(1)** | 149-89 = 60**(1)** | 60-42 = 18**(1)** | 18-21 = 18**(0)** | 18-11 = 7**(1)** | 7-7 = 0**(1)** | 0-2 = 0**(0)**

Maka diperoleh hasil **01101110 = n**

*P*6 = 128–354 = 128**(0)** | 128–180 = 128**(0)** | 128-89 = 39**(1)** | 39-42 = 28**(0)** | 39-21 = 18**(1)** | 18-11 = 7**(1)** | 7-7 = 0**(1)** | 0-2 = 0**(0)**

Maka diperoleh hasil **01110100 = t**

*P*7 = 414–354 = 60**(1)** | 60–180 = 60**(0)** | 60-89 = 60**(0)** | 60-42 = 18**(1)** | 18-21 = 18**(0)** | 18-11 = 7**(1)** | 7-7 = 0**(1)** | 0-2 = 0**(0)**

Maka diperoleh hasil **01101001 = i**

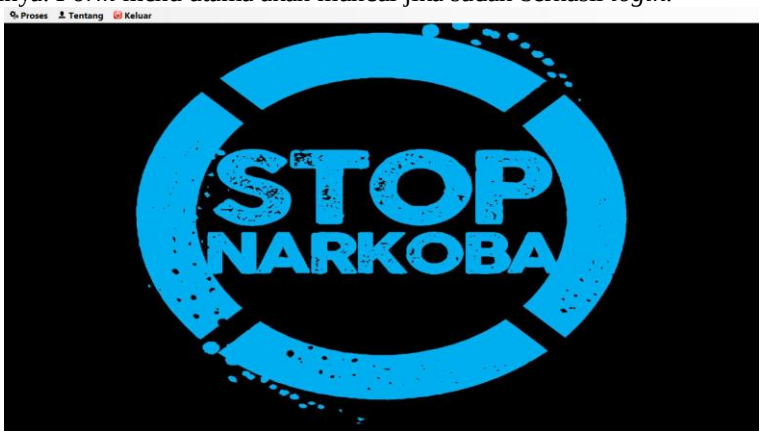
4. IMPLEMENTASI DAN UJI COBA

4.1 *Form Login*

Form Login berfungsi untuk menghubungkan user ke Menu Utama. *User* diharuskan memasukkan nama *user* beserta *password* dengan benar. Jika salah maka Menu Utama tidak akan ditampilkan. Berikut ini tampilan *form* menu *login*:

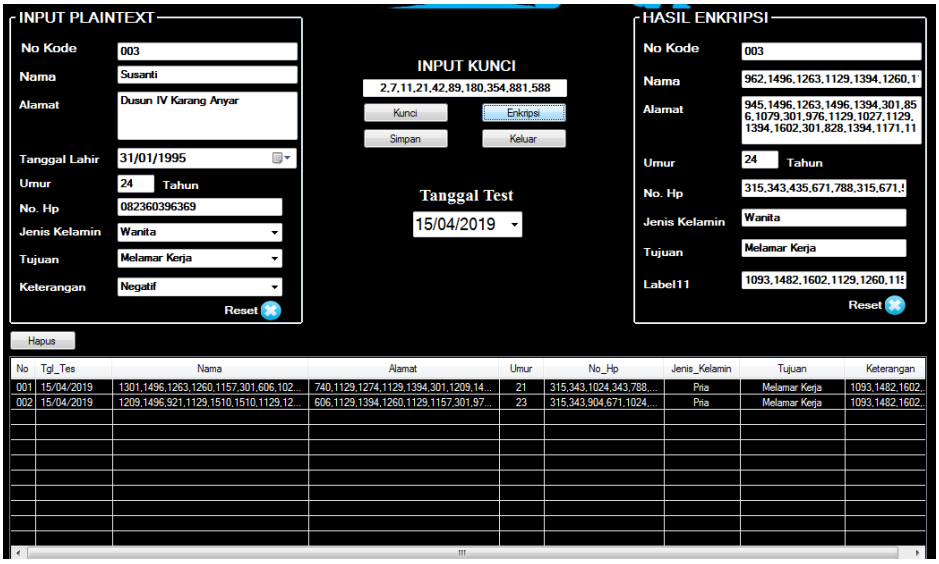
4.2 *Form* Menu Utama

Form menu utama adalah tampilan navigasi. Di mana di dalamnya terdapat menu-menu untuk membuka *form* lainnya. *Form* menu utama akan muncul jika sudah berhasil *login.*



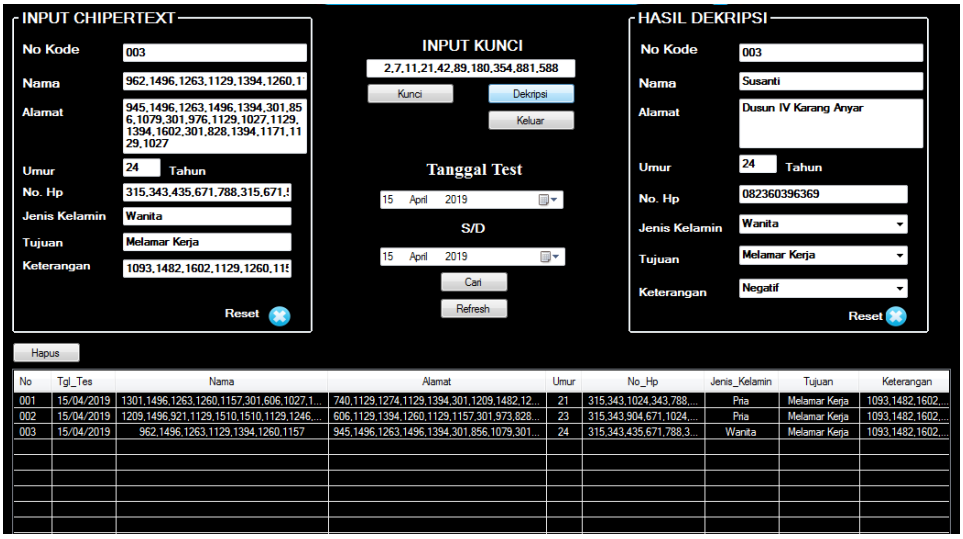
4.3 *Form* Enkripsi

Form Enkripsi digunakan untuk melakukan *input* data *client* yang akan dilakukan proses pengamanan.



4.4 *Form* Dekripsi

Form dekripsi digunakan untuk mengembalikan data yang telah dienkripsi sebelumnya dan dapat dicetak menjadi sebuah lembar laporan.



5. KESIMPULAN

Dari hasil pembahasan pada bab sebelumnya dan pengamatan yang telah dilakukan maka dapat diambil kesimpulan diantaranya sebagai berikut:

1. Dengan menerapkan metode *Merkle Hellman* ini mampu untuk memberikan pengamanan terhadap data *client test urine*, sehingga data tersebut memiliki tingkat keamanan yang tinggi.
2. Mengimplementasikan aplikasi pengamanan data *client test urine* dilakukan pemprogramanan dengan menerapkan Metode *Merkle Hellman*. Dilakukan menggunakan bahasa pemprograman *Visual Basic* 2008. Dengan terlebih dahulu masuk login menu utama, kemudian masuk ke *form* Proses Enkripsi lalu input data *client*, kemudian proses dengan enkripsi dilanjutkan dengan menyimpan ke dalam *database*. Selanjutnya untuk proses dekripsi, masuk ke *form* proses dekripsi dengan memilih no kode *client* yang telah tersimpan lalu data diproses menggunakan perhitungan metode *merkle hellman*.
3. Pembangunan aplikasi pengamanan dapat dilakukan dengan pengkodean menggunakan bahasa pemrograman berbasis *Dekstop Programming*.
4. Aplikasi yang dirancang dapat menjadi solusi pemecahan masalah dalam hal pengamanan data *client test urine* pada BNN Kabupaten Deli Serdang

DAFTAR PUSTAKA

Ariyus, Dony. 2006. *Computer Security*. Yogyakarta:C.V Andi Offset

Ariyus, Dony. 2006 *Kriptografi Keamanan Data dan Komunikasi*, Yogyakarta : Graha Ilmu

Ariyus, Dony. 2009. *Keamanan Multimedia*. Yogyakarta: C.V Andi Offset

Asriyanik. (2017). Studi Terhadap Advanced Encryption Standard (Aes) Dan Algoritma Knapsack Dalam Pengamanan Data. *Sains Dan Teknologi*, *7*(1), 554–561.

Fadlan, M., & Hadriansa, H. (2017). Rekayasa Aplikasi Kriptografi Dengan Penerapan Kombinasi Algoritma Knapsack Merkle Hellman Dan Affine Cipher. *Jurnal Teknologi Informasi Dan Ilmu Komputer*, *4*(4), 286–274. https://doi.org/10.25126/jtiik.201744468

Hendrayudi. 2011. *Dasar-Dasar Pemrograman Microsoft Visual Basic 2008*. Bandung: CV Yrama Widya.

Kharisma, R. S., & Rachman, M. A. F. (2017). Pembuatan Aplikasi Notes Menggunakan Algoritma Kriptografi Polyalphabetic Subtitution Cipher Kombinasi Kode Asii Dan Operasi Xor Berbasis Android. *Jurnal Teknologi Informasi*, *35*, 1–7. https://doi.org/10.1016/j.clnu.2014.08.012

Komputer, Wahana. 2010. *The Best Encryption Tools.* Jakarta: PT Elex Media Komputindo

Mardalius. (2018). Implementasi Aplikasi Enkripsi dan Dekripsi Text Pada Visual Basic. Net Menggunakan Algoritma Merkle Hellman Knapsack, *9986*(September), 249–252.

Murdani. (2017). Perancangan Aplikasi Keamanan Data Teks Menggunakan Algoritma Merkle Hellman Knapsack. *Pelita Informatika*, *16*(3), 302–305.

Rosa, A S., & Shalahuddin, M. 2013. *Rekayasa Perangkat Lunak Terstruktur dan Berorientasi Objek*. Bandung: Informatika Bandung.

Siregar, M. (2013). Analisa Dan Perancangan Aplikasi Pengamanan Data Teks Menggunakan Algoritma Merkle Hellman, *V*(3), 122–126.

Sulianta, Feri. 2017 *Teknik Perancangan Arsitektur Sistem Informasi*, Yogyakarta: Penerbit Andi

Sulindawati, & Fathoni, M. (2011). Pengantar Analisa Perancangan " Sistem ". *Jurnal Saintikom*, *9*(2), 1–19. https://doi.org/10.1097/AOG.0b013e3181660c1b

Ukar, K., & Pratama, B., G. 2010. Seri Penuntun Praktis Microsoft Access 2010. Jakarta: PT Elex Media Komputindo

Yasin, Verdi. 2012, *Rekayasa Perangkat Lunak Berorientasi Obyek*. Penerbit

Mitra Wacana Media.