Algoritma Kriptografi Klasik Berbasis Pencitraan Sidik Jari

Amalfi Yusri Darusman

Program Studi Teknik Informatika
Sekolah Teknik Elektro dan Informatika, Institut Teknologi Bandung
Jalan Ganesha 10 Bandung
e-mail : if17023@students.if.itb.ac.id

ABSTRAK

Permasalahan keamanan, kerahasiaan dan keaslian suatu berkas merupakan permasalahan yang amat penting melihat maraknya kegiatan "pembobolan" keamanan oleh *cracker*. *Cracker* adalah seseorang yang secara ilegal melakukan enkripsi terhadap suatu berkas untuk mendapat informasi, keuntungan, maupun bentuk berkas lain yang memberikan keuntungan kepadanya. Oleh karena pentingnya keamanan dan kerahasiaan suatu informasi, perkembangan ilmu kriptografi sangat pesat untuk "mengimbangi" tingkat "pembobolan" yang terjadi sekarang ini. Seraya perkembangan ilmu kriptografi, produk yang dihasilkan dari ilmu inipun semakin banyak dan beragam. Penggabungan dan inovasi dengan berbagai macam teknik sudah dilakukan dan terus dikembangkan. Pada makalah ini akan dideskripsikan rancangan pemanfaatan biometrika, dalam hal ini adalah penggunaan sidik jari. Hasil pencitraan sidik jari akan diubah menjadi sebuah kunci untuk melakukan enkripsi, begitu pula dengan dekripsi.

Kata kunci : pembobolan, *cracker*, enkripsi, dekripsi, kriptografi, biometrika.

1. PENDAHULUAN

Suatu berkas dengan informasi rahasia dan ekslusif harus dijaga keamanan, kerahasiaan dan keasliannya agar terjamin informasi yang disampaikan adalah benar. Penyimpanan informasi pribadipun sangat penting, misalnya seseorang ingin menyimpan informasi pin ATM pada suatu berkas dijital (agar tidak lupa), informasi tersebut tentu harus terjamin keamanannya. Marak dan berkembangnya kriptanalis yang bekerja secara ilegal untuk mendapatkan suatu informasi, membuat ilmu kriptografi terus berkembang. Mengapa demikian? Karena metode-metode yang ada pada keilmuan kriptografi lama kelamaan mungkin terpecahkan, misalnya pada periode waktu 50 tahun lalu, penggunaan metode kriptografi A adalah aman dan tidak mungkin terpecahkan, namun pada kenyataannya saat ini metode A sudah dapat dipecahkan. Begitu juga dengan metode yang ada pada periode waktu sekarang, mungkin pada periode waktu selanjutnya metode ini sudah tidak dapat digunakan lagi, karena mudahnya untuk melakukan dekripsi.

2. SISTEM BIOMETRIKA

Penggunaan identifikasi seseorang menggunakan sidik jari pada *fingerprint reading*, retina mata pada *retina scan*, dan lainnya tidak lain adalah untuk menjaga keamanan suatu tempat atau benda. Penggunaan anggota tubuh sebagai input untuk identifikasi seseorang dalam keamanan disebut penggunaan sistem *biometric*.

Sistem *biometric* adalah studi tentang metode otomatis untuk mengenali manusia berdasarkan satu atau lebih bagian tubuh manusia atau kelakuan dari manusia itu sendiri yang meiliki keunikan. Tujuan utama dari penggunaan sistem *biometric* adalah untuk menjaga keaslian keunikan kunci, karena hampir tidak mungkin pembacaan input sidik jari atau retina orang yang berbeda menghasilkan hasil pembacaan yang sama.

Gambar 1 fingerprint reader

Gambar 2 retina scanner

Penggunaan sistem *biometric* memungkinkan keunikan untuk menjaga keamanan suatu tempat atau benda. Hal inilah yang menimbulkan gagasan

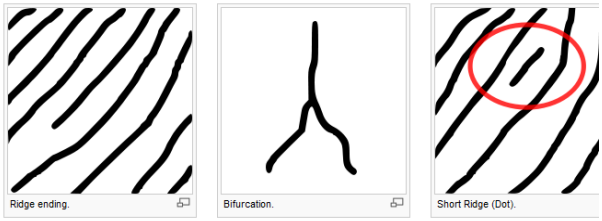
untuk menggabungkan sistem *biometric* dan salah satu algoritma kriptografi, yang dibahas pada makalah ini adalah algoritma kriptografi klasik.

Pada makalah ini, pembahasan yang dilakukan dibatasi pada biometrika sidik jari, sehingga perangkat keras yang digunakan adalah *fingerprint reader*, metode yang digunakanpun sesuai dengan hasil pembacaan biometrika sidik jari.

Prinsip pemrosesan pencitraan sidik jari menggunakan *fingerprint reader* tergolong rumit, namun sudah banyaknya perangkat keras yang digunakan membuat *constraint* tersebut menjadi kabur. Prinsip-prinsip pencitraan tersebut diantara lain adalah *pattern based* dan *minutiae based*. Pada pattern based fingerprint recognition, pola sidik jari dikelompokkan menjadi 3, yaitu arch, loop dan whorl. Sedangkan pada minutiae based juga terdapat 3 klasifikasi pola yaitu ridge ending, bifurfication, dan dot(short ridge).

(diambil dari wikipedia.org)

Gambar 3 klasifikasi *pattern based*



Gambar 4 klasifikasi *minutiae based*

Selain prinsip yang digunakan untuk klasifikasi pola di atas, terdapat juga berbagai sistem sebagi sensor fingerprint. Sistem-sistem sensor fingertpint tersebut antara lain optical, ultrasonic dan capacitance sensors.

(diambil dari wikipedia.org)

Pada sensor optical, pencitraan sebuah sidik jari didasarkan pada pembacaan sidik jari menggunakan "sinar terlihat". Cara kerjanya bisa dianalogikan seperti sebuah digital camera yang menangkap gambar melalui sensor. Namun sensor pada sistem optical ini memiliki beberapa layer(tidak akan dibahas lebih lanjut).

(diambil dari wikipedia.org)

Pada sensor ultrasonic, prinsip kerja yang digunakan sama seperti prinsip kerja ultrasonography pada dunia kedokteran, menggunakan gelombang suara frekuensi tinggi untuk pencitraan lapisan epidermal kulit.

(diambil dari wikipedia.org)

Pada sensor capacitance, pencitraan sidik jari didasarkan pada kapasitansi lapisan sidik jari. Lapisan dermal yang bersifat konduktif dan lapisan epidermal yang bersifat non-konduktif memberikan perbedaan untuk dicitrakan pada sistem sensor ini.

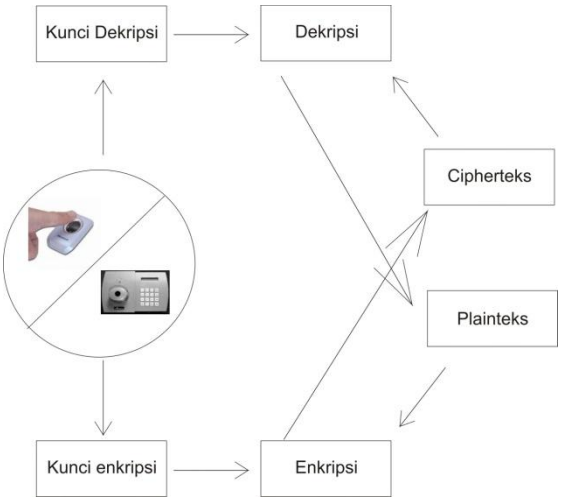
(diambil dari wikipedia.org)

$$C = \frac{Q}{V}$$

$$C = \varepsilon_0 \varepsilon_r \frac{A}{d}$$

Pada makalah ini permasalahan sistem tersebut tidak akan dibahas terlalu dalam melihat pokok pembahasan dari makalah ini adalah pembangkitkan kunci dari sebuah sistem biometrika, yang dalam hal ini adalah sidik jari. Pada makalah ini sistem sensor yang digunakan tidak dispesifikkan, namun keluaran dari sistem biometrika tersebut adalah berupa sebuah *image* seperti pada gambar 3. Gambar ini bisa berbentuk format lain namun intinya adalah sebuah image yang merepresentasikan sidik jari orang.

3. RANCANGAN SISTEM



Gambar 5 rancangan sistem

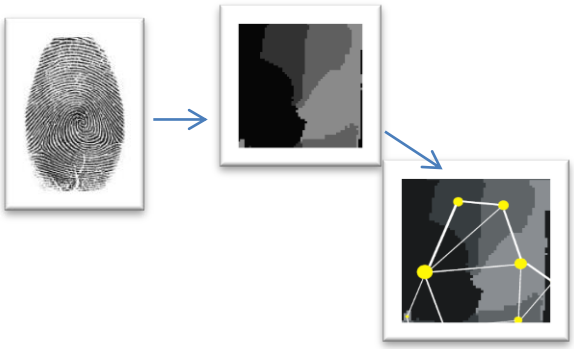
Pada gambar 3, diperlihatkan rancangan sistem enkripsi dan dekripsi menggunakan sistem biometrika. Pembacaan dari perangkat keras sistem biometrika yang unik untuk tiap orang akan menghasilkan satu kunci yang unik pula. Kunci ini akan dikonversi sedemikian hingga menghasilkan sebuah kunci untuk melakukan enkripsi plainteks

menjadi cipherteks. Untuk proses dekripsipun juga demikian, kunci unik yang diperoleh dari pembacaan sistem biometrika digunakan sebagai kunci untuk dekripsi cipherteks menjadi plainteks.

Jika dilihat dari cara kerja sistem ini, perubahan kunci yang dibaca dari sistem biometrika tersebut menjadi sebuah string atau bentuk lain adalah sama dengan algoritma enkripsi dan dekripsi biasa. Misalnya enkripsi vigenere cipher menggunakan kunci "apple", kunci ini dapat dicari menggunakan analisis frekuensi dan teknik lainnya. Pembacaan unik dari sistem biometrika ini juga akan dikonversi menjadi bentuk string pula, namun tidak berbentuk kata-kata yang sering ditemui, bentuknya akan berupa hasil konversi bit-bit dari ascii yang dibaca dari garis-garis sidik jari maupun retina mata. Misalnya, hasil pembacaan sistem biometrika tidak berupa kata-kata namun berbentuk abstrak atau bentuk lain yang sulit dipahami dan dilihat *pattern*-nya.

4. RANCANGAN SISTEM ENKRIPSI DAN DEKRIPSI

Keluaran dari sistem pencitraan sidik jari adalah berupa sebuah *image*. *Image* ini tidak langsung digunakan sebagai kunci(misalnya dengan dikonversi ke dalam bentuk string, karena sangat sulit untuk menghasilkan hasil pembacaan yang sama), namun dikonversi dulu menjadi sebuah graf berbobot yang masing-masing *node*-nya memiliki "berat" masing-masing. "Berat" inilah yang menurut rancangan pada makalah ini, digunakan sebagai kunci untuk enkripsi dan dekripsi.



Gambar 6 proses konversi dari pencitraan sidik jari ke graf berbobot

Pada gambar 6 diperlihatkan proses konversi sebuah citra sidik jari menjadi sebuah graf berbobot dengan "berat" node yang berbeda-beda. Graf berbobot didefinisikan sebagai G= (V, E, μ, υ) dengan V adalah jumlah nodes, E adalah jumlah sisi, μ adalah berat node, dan υ adalah berat sisi.

Penentuan berat sisi dan nodes sendiri adalah berdasarkan beberapa parameter seperti titik tengah gravitasi untuk masing-masing region, jarak antar 2 titik tengah gravitasi, garis batas tiap region, dan lainnya.

$$Wn = Area(Ri)\ , i= 1, 2, 3, \ldots, n$$

Persamaan di atas menunjukkan rumus untuk mencari sebuah berat dari node dengan menggunakan parameter-parameter yang telah disebutkan di atas. Berat tiap region ini yang akan digunakan untuk membuat sebuah kunci.

Dapat juga digunakan berat sebuah sisi untuk menentukan kunci, parameter yang digunakan adalah :

- Adj-P adalah batas antara 2 region yang bersinggungan atau saling bertetangga
- Node-d adalah jarak antarnodes yang dihubungkan oleh sebuah sisi
- Diff-v adalah perbedaan direction dari dua region

Dari parameter diatas, dibuat persamaan untuk sebuah sisi adalah

$$We = Adj - p \times Node - d \times Diff - v$$

Untuk detail penurunan kedua persamaan tidak akan dibahas pada makalah ini. Namun disinilah proses pembuatan kunci unik yang didapat dari sistem biometrika yang digunakan. Himpunan solusi salah satu dari 2 persamaan tersebut digunakan untuk membuat kunci enkripsi dan dekripsi.

5. VIGENERE CIPHER

Pada sistem ini digunakan vigenere cipher untuk enkripsi dan dekripsi. Contoh sederhana yang mendeskripsikan vigenere cipher adalah sebagai berikut :

Plainteks : THIS PLAINTEXT

Kunci : sony sonysonys
Cipherteks : **LVVQ HZNGFHRVL**

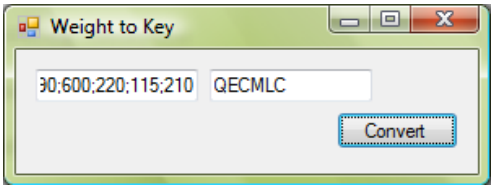
Pada dasarnya, setiap enkripsi huruf adalah *Caesar cipher* dengan kunci yang berbeda-beda.

c('T') = ('T' + 's') mod 26 = L
c('H') = ('H' + 'o') mod 26 = V, dst

6. MEKANISME ENKRIPSI

Hasil konversi pencitraan sidik jari menjadi sebuah himpunan integer seperti yang disebutkan di atas akan digunakan sebagai kunci untuk enkripsi. Misalkan dari hasil konversi tersebut dihasilkan himpunan berat node atau berat sisi h = {120, 290, 600, 220, 115, 210}, angka-angka ini dapat diubah menjadi sebuah karakter sesuai dengan ASCIInya sehingga membentuk sebuah string kunci yang bentuknya tidak jelas (tidak merepresentasikan sebuah kata ataupun pattern string yang biasanya).

Untuk konversi dari himpunan integer menjadi key digunakan sebuah aplikasi yang telah dibuat yaitu Weight to Key. Aplikasi ini mengkonversi himpunan berat yang ada menjadi sebuah kunci. Pemisah tiap berat menggunakan karakter titik koma (;). Misal digunakan himpunan h pada contoh di atas :



Gambar 7 weight to key untuk konversi kunci

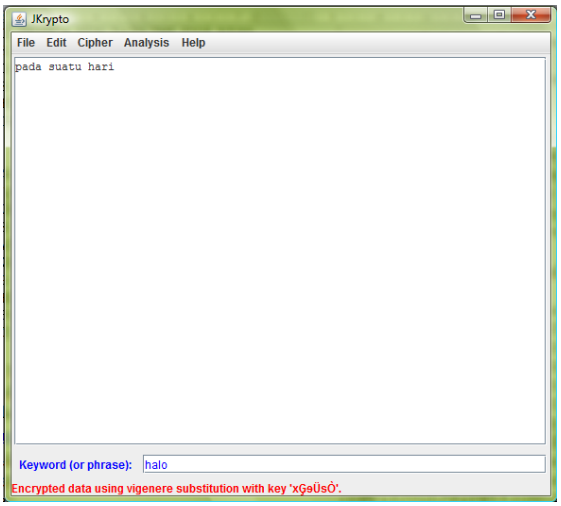
```
int[] a;
string input = textBox1.Text;
string[] inputInd;
string output = "";
inputInd = input.Split(';');
a = new int[inputInd.Length];
for (int i = 0; i < a.Length; i++)
    {
    a[i] = (int.Parse(inputInd[i]) % 26) + 65;
    output += ("" + (char)a[i]);
    }
textBox2.Text = output;
```

Dari masukan himpunan h di atas dihasilkan kunci "QECMLC", kunci inilah yang digunakan untuk enkripsi. Pada rancangan sistem sebenarnya, aplikasi weight to key seharusnya terintegrasi dengan sistem biometrika, bukan merupakan aplikasi terpisah seperti ini, namun untuk memudahkan simulasi dan karena sistem ini masih berupa rancangan dibuatlah aplikasi weight to key.

Misalkan diberikan sebuah string masukan untuk enkripsi menggunakan kunci tersebut, masukan tersebut adalah sebagai berikut :

THE JAPANESE HAVE ALWAYS LOVED FRESH FISH. BUT THE WATERS CLOSE TO JAPAN HAVE NOT HELD MANY FISH FOR DECADES. SO TO FEED THE JAPANESE POPULATION, FISHING BOATS GOT BIGGER AND WENT FARTHER THAN EVER.THE FARTHER THE FISHERMEN WENT,THE LONGER IT TOOK TO BRING IN THE FISH. IF THERE TURN TRIP TOOK MORE THAN A FEW DAYS,THE FISH WERE NOT FRESH. THE JAPANESE DID NOT LIKE THE TASTE. TO SOLVE THIS PROBLEM, FISHING COMPANIES INSTALLED FREEZERS ON THEIR BOATS. THEY WOULD CATCH THE FISH AND FREEZE THEM AT SEA. FREEZERS ALLOWED THE BOATS TO GO FARTHER AND STAY LONGER. HOWEVER, THE JAPANESE COULD TASTE THE DIFFERENCE BETWEEN FRESH AND FROZEN AND THEY DID NOT LIKE FROZEN FISH. THE FROZEN FISH BROUGHT A LOWERPRICE. SO FISHING COMPANIES INSTALLED FISH TANKS. THEY WOULD CATCH THE FISH AND STUFF THEM IN THE TANKS, FIN TO FIN. AFTER A LITTLE THRASHING AROUND,THE FISH STOPPED MOVING.THEY WERE TIRED AND DULL,BUT ALIVE. UNFORTUNATELY, THE JAPANESE COULD STILL TASTE THE DIFFERENCE.

Masukan tersebut akan dienkripsi menjadi cipherteks dengan kunci di atas menggunakan aplikasi lain yaitu JKrypto (terdapat di www.informatika.org/~rinaldi). Aplikasi JKrypto inipun seharusnya merupakan bagian dari sistem keseluruhan enkripsi dengan biometrika.



Gambar 8 aplikasi JKrpto untuk simulasi

Masukan string di atas setelah dienkripsi menggunakan aplikasi JKrypto menggunakan kunci yang telah didapatkan sebelumnya menjadi :

JLG VLRQRGEP JQZG MWYQCU XZXUH HDPUX JKES. DKX VTP YQXGDD EBSUQ EQ ZERMY JQZG ZZV XINP XCDC HUDJ VST PPEQHGE. DQ JS HQPF JLG VLRQRGEP RETWXLVYSP, RTUXMPS MQQXU SZV RMISPT QRF IPPJ JCDEJUV VTLP UZGD.EJU JCDEJUV VTP HYWJQCOUR YQYV,JLG XZPWIT UE VESM FZ DHMPS TP JLG RTUX. MH FSGHI VGCP JVKB EQEO OACG JLCZ L HUA FMJU,JLG RTUX AGDP PEX HDPUX. XJQ UCFEPQDG TMF ZZV BMMQ EJU XCEEG. JS UAWXU XJUD RHSDXPO, VMUTTPW GQYACDMGE TPIXCXWGT JTQPBUVU AY VXIKD MQQXU. FSGO AQGWF SEVOS VXI HUDJ QRF RCGUDG FSGC EV EPC. VVGQKGHW CXWQMIF FSG RSCFD VE KQ RLTJLGD LPT WVMJ NERIQC. JEAGHPT, JLG VLRQRGEP EEYNP ECIXG FSG TMHRPTUREQ MGJAGQY HHIUT LPT JTAKGD EPP EJUC FUO PEX NUVG VVQLPP VMUT. EJU JTAKGD JKES DHSWSSV Q PQIPTFVKOP. UE JKESKDK EAXRQRKQD KDWVMWNUH HUDJ JEPWD. VXIA IZWBH EMEEX XJQ QKIL CZO UJYHR EJUQ KZ EJU XCZVU, VMP FZ HYR. CREGH E NUEVBI VTCCILKZR CHSWZO,VXI HUDJ IXQBAGT QQHTPW.XJQJ YUVG FTTUH CZO FKPN,NFV QPKHP. WDJQDEWDEVQWA, JLG VLRQRGEP EEYNP DVYPN FLUJI VTP FYJHQCGDGG.

Hasil keluaran dari sistem enkripsi menggunakan kunci pencitraan biometrika adalah seperti string di atas.

7. MEKANISME DEKRIPSI

Pada mekanisme dekripsi, prinsip yang digunakan adalah sama, dengan menggunakan kunci yang diperoleh dari pembacaan sidik jari kemudian dari pembacaan tersebut akan dikonversi menjadi himpunan integer-integer yang merepresentasikan berat dari node-node, setelah itu dari himpunan integer tersebut dikonversi lagi menjadi sebuah string dengan representasi ASCII himpunan integer tersebut. Kunci yang digunakan untuk dekripsi adalah kunci yang terbentuk dari konversi ke string tersebut. Dengan masukan cipherteks pada bab sebelumnya (hasil enkripsinya), digunakan kunci yang hasil pembacaan sidik jari oleh orang yang sama, maka kunci yang dihasilkan sama kemudian berimbas kepada proses dekripsi cipherteks menjadi plainteks yang sama pula.

Hasil dekripsi dengan kunci sama pada contoh diatas adalah :

THE JAPANESE HAVE ALWAYS LOVED FRESH FISH. BUT THE WATERS CLOSE TO JAPAN HAVE NOT HELD MANY FISH FOR DECADES. SO TO FEED THE JAPANESE POPULATION, FISHING BOATS GOT BIGGER AND WENT FARTHER THAN EVER.THE FARTHER THE FISHERMEN WENT,THE LONGER IT TOOK TO BRING IN THE FISH. IF THERE TURN TRIP TOOK MORE THAN A FEW DAYS,THE FISH WERE NOT FRESH. THE JAPANESE DID NOT LIKE THE TASTE. TO SOLVE THIS PROBLEM, FISHING COMPANIES INSTALLED FREEZERS ON THEIR BOATS. THEY WOULD CATCH THE FISH AND FREEZE THEM AT SEA. FREEZERS ALLOWED THE BOATS TO GO FARTHER AND STAY LONGER. HOWEVER, THE JAPANESE COULD TASTE THE DIFFERENCE BETWEEN FRESH AND FROZEN AND THEY DID NOT LIKE FROZEN FISH. THE FROZEN FISH BROUGHT A LOWERPRICE. SO FISHING COMPANIES INSTALLED FISH TANKS. THEY WOULD CATCH THE FISH AND STUFF THEM IN THE TANKS, FIN TO FIN. AFTER A LITTLE THRASHING AROUND,THE FISH STOPPED MOVING.THEY WERE TIRED AND DULL,BUT ALIVE. UNFORTUNATELY, THE JAPANESE COULD STILL TASTE THE DIFFERENCE.

8. KEGAGALAN SISTEM

Pada level abstraksi rancangan, konversi kunci dari himpunan integer hasil pencitraan akan murni dikonversi ke dalam bentuk representasi karakternya, namun karena karakter tersebut tidak dapat diproses dari segi persamaan vigenere cipher maka perlu penyesuaian pada algoritma konversi dari himpunan integer menjadi representasi karakter sesuai ASCIInya.

```
int[] a;
string input = textBox1.Text;
string[] inputInd;
string output = "";
inputInd = input.Split(';');
a = new int[inputInd.Length];
for (int i = 0; i < a.Length; i++)
    {
    a[i] = (int.Parse(inputInd[i]) % 26) + 65;
    output += ("" + (char)a[i]);
    }
textBox2.Text = output;
```

Pada potongan kode diatas, bagian yang ditulis miring berwarna merah adalah bagian yang ditambahkan untuk penyesuaian. Jika bagian kode tersebut tidak ditambahkan maka kunci yang digunakan adalah hasil enkripsi dari kasus di atas adalah :

QYT ISEXETRW WXMT ZDLXPH KGKBU UQWHE WXRZ. QRK IGW LXKTQK RIFHD LD GREZF WXMT MGI EVAC EPKP UHKW CFG CWRXUTR. KD QF UDWS QYT ISEXETRW ELGJKSIFFC, EAHEZCF TDXKH FGI YZVFWG XES VWCQ WPQLWBI IGSC BMTQ.LWB WPQLWBI IGW UFJWDJBBE LDFI,QYT KGCDVG HL ILFZ SG QOZCF AC QYT EAHE. ZU SZTOV ITJC QIXO LDLB BNJT QYPM S UBN SZQH,QYT EAHE NTQW CLK UQWHE. KWD BPMRCDKT AZS MGI IZZD LWB KPRLT. QF HNDKB KWHK EOFQKWB, CZHGACD TDLHPKZTR ACPKPKDTA WGDWOBIH NF IEVXQ TDXKH. SZTV NDTDS ZRIBZ IEV UHKW XES EJTBQT SZTJ RI RWP. CITDRTOJ PKDDTVS SZT YFPSK IL XD ESGQYTQ SCA JIZQ ALEVDJ. WLNTUWG, QYT ISEXETRW RLLAC LPPKT SZT AZUEWGBERD TTQNTDF UOVHG SCA WGNRTK RCC LWBP SHV CLK AHCT CIDYWC CZHG. LWB WGNRTK WXRZ QOFJFZI X CDVWGMIXBW. HL WXRZXKX RNEEXEXDK XKJIZDABU UHKW QRCJK. IEVN VGJIU RZLRE KWD XXPY PMV HQLUE LWBD XM LWB KPMCH, CZC SG UFE. PELTO R AHLIIV IGJPPYXMY POFJMV,IEV UHKW PKDOHTA DDUACD.KWDQ LBIT SAGBU PMV SRCA,AMI XCXUW. JKWDQLJKRIDDN, QYT ISEXETRW RLLAC KIFCA SSHQV IGW SFWUDJTKTT.

Pada saat dekripsi dengan kunci yang sama dihasilkan plainteks sebagai berikut :

T.+ 0A6A4+9E .A<+ AL=A?9 2O<E* ,8E9H ,/9H. (U: :.E =A:+8S)L59+ T5 JA6AN .A<+ 4O: H+2* MAN? ,/S. F58 *E)A*+9. S5 T5 ,+E* T.+ 0A6A4+9E 6O6;2A:I54, ,I9H/4-B5A:9 -O: B/--E8 A4* =E4T ,A8T.E8 :.A4 E<+8.T.E ,A8T.E8 :.E ,I9.+R3E4 =+N:,T.+ 2O4G+8 /T :O51 :O (R/4- I4 T.+ ,I9H./, :H+R+ :;R4 T8/6 T5O1 35R+ T.A4 A ,E= *AY9,T.+ ,I9H =+8E 4O: ,8E9H. :.+ JAPA4+S+ D/* 4O: L/1+ T.E :A9T+. T5 95L<E :./S 6R5(2E3, F/9.I4G)53PAN/+9 I4S:A2L+D ,8+E@E89 5N :H+/8 B5A:9. :H+Y =5;L* CA:)H :H+ ,/S. A4* ,R+E@+ :H+M A: 9EA. F8++Z+R9 A2L5W+* :H+ B5A:S :O -5 ,A8T.+8 A4D 9:AY 2O4-+R. .O=+<E8, T.+ 0A6A4+9E)O;2* TAS:+ :H+ D/,,E8E4)+ B+T=++N ,R+9. A4D ,85Z+N A4* T.E? */D 4O: 2/K+ F85@E4 F/9.. T.E ,85Z+N ,/9H (R5;-H: A 25=E8P8/)E. 9O ,/9H/N-)5M6A4/+S /N9:AL2E* ,/S. TA41S. :H+? =O;L*)AT)H :.+ F/S. A4D 9T;,, T.E3 /4 T.E :A4K9, F/4 :O ,I4. A,T+R A 2/T:L+ :.RAS./4G AR5;4D,:H+ ,/S. S:56P+D 35<I4G.:.+Y =E8+ :I8E* A4D *U22,(U: A2/<E. ;N,58T;NA:+L?, T.+ 0A6A4+9E)O;2* S:I22 :A9T+ :.E *I,,+R+N)+.

9. KESIMPULAN

Penggunaan konversi himpunan integer yang murni dikonversi menjadi string kunci sangat baik jika berhasil diimplementasikan, karena sulit untuk menentukan kunci dari bentuk string yang ada. Sedangkan penggunaan konversi himpunan integer yang sudah disesuaikan, berhasil diimplementasikan namun tingkat keamanan yang ditawarkan menjadi sama saja dengan enkripsi vigenere cipher biasa karena orang masih dapat menebak dan mencoba-coba kunci yang digunakan (masih berbentuk string terbaca).

Sistem inipun masih berupa rancangan yang masih harus dirisetkan lebih lanjut. Namun ide dasar penggunaan biometrika untuk kunci enkripsi sangat baik digunakan dan dikembangkan karena nilai keunikan yang ditawarkan.

10. DAFTAR PUSTAKA

[1] http://www.informatika.org/~rinaldi/Kriptografi/2006-2007/Algoritma%20Kriptografi%20Klasik%20(bag%203).ppt
Diakses pada 24 Maret 2010, 01.10 WIB

[2] http://www.informatika.org/~rinaldi/Kriptografi/2009-2010/kripto09-10.htm
Diakses pada 24 Maret 2010, 01.39 WIB
Penggunaan file jkrypto.jar

[3] http://en.wikipedia.org/wiki/Biometrics
Diakses pada 23 Maret 2010, 13.12 WIB