ISSN 2356-4407

www.STIKI.ac.id

Bersama memajukan ICT Indonesia

PROCEEDING

IC - ITECHS 2014

The 1st International Conference on Information Technology and Security

Malang, November 27, 2014

Published by:

Lembaga Penelitian dan Pengabdian pada Masyarakat

Sekolah Tinggi Informatika dan Komputer Indonesia

PROCEEDING

The 1st International Conference on Information Technology and Security (IC-ITechs)

November 27, 2014

Editors & Reviewers:

Tri Y. Evelina, SE, MM Daniel
Rudiaman, S.T, M.Kom Jozua
F. Palandi, M.Kom

Layout Editor:

Eka Widya Sari

LEMBAGA PENELITIAN & PENGABDIAN KEPADA MASYARAKAT
Sekolah Tinggi Informatika & Komputer Indonesia (STIKI) – Malang
Website: itechs.stiki.ac.id E-mail: itechs@stiki.ac.id

PROCEEDING

The 1st International Conference on Information Technology and Security (IC-ITechs) November 27, 2014

ISSN 2356 - 4407

viii + 276 hlm; 21 X 29,7 cm

Reviewers & Editors:

Tri Y. Evelina, SE, MM
Daniel Rudiaman, S.T, M.Kom
Jozua F. Palandi, M.Kom

Layout Editor:

Eka Widya Sari

Published by:
LEMBAGA PENELITIAN & PENGABDIAN KEPADA MASYARAKAT
Sekolah Tinggi Informatika & Komputer Indonesia (STIKI) – Malang
Jl. Raya Tidar 100 Malang 65146, Tel. +62-341 560823, Fax. +62-341 562525
Website: itechs.stiki.ac.id E-mail: itechs@stiki.ac.id

GREETINGS

Head of Committee IC-Itechs

For all delegation participants and invited guest, welcome to International Conference on Information Technology and Security (IC-Itechs) 2014 in Malang, Indonesia.

This conference is part of the framework of ICT development and security system that became one of the activities in STIKI and STTAR. this forum resulted in some references on the application of ICT. This activity is related to the movement of ICT development for Indonesia.

IC-Itechs aims to be a forum for communication between researchers, activists, system developers, industrial players and all communications ICT Indonesia and abroad.

The forum is expected to continue to be held continuously and periodically, so we hope this conference give real contribution and direct impact for ICT development.

Finally, we would like to say thanks for all participant and event organizer who involved in the held of the IC-Itechs 2014. We hope all participant and keynote speakers got benefit from this conference.

ISSN 2356 - 4407
The 1st International Conference
on Information Technology and Security

LIST OF CONTENT

Perangkat Lunak Keamanan Informasi Pada Mobile Menggunakan Metode Stream Dan Generator Cipher

Asep Budiman Kusdinar, Mohamad Ridwan
Universitas Muhammadiyah Sukabumi
Asep.budiman.k@gmail.com, mr_ridthone@yahoo.co.id

Abstract

Integration method of stream and generator cipher can used to randomizing message information. Delivery of message information through email or mobile is required a good security and safety system. So can protect message information that be acceptable by receiver carefully and precise. In this article methodologies which will be applied for randomize message information is processing encryption and descryption to apply stream and generator cipher. The software of this can be used to send message information applicable to information in character secret by using key stream and generator cipher as introduction lock of message information. So with existence of this stream and generator cipher is locking authentication message information become safe and is well ensured.

Keywords : *stream cipher, generator cipher, key stream cipher, key generator cipher, message information.*

1. PENDAHULUAN

Keamanan informasi, kondisi ini sangat diperlukan bagi Dunia Teknologi Informasi dan Telekomunikasi. Keamanan tidak hanya terbatas pada data tetapi kepada situasi dan kondisi Pribadi dan lingkungan yang nyaman serta terkendali [Anaiba, 2004]. Perkembangan dunia informatika baik software maupun hardware, sudah tidak dapat dihindari lagi, merambah pada aspek-aspek yang tidak hanya terbatas pada dunia komputer. Namun sudah masuk ke Dunia mobile. Oleh karena itu, penggunaan computer maupun mobile bisa menghasilkan nilai positif ataupun sebaliknya tergantung kepada tujuan penggunaannya [Du, 2006].

Komputer dan mobile yang dapat menghasilkan tujuan negatif atupun positif biasanya memiliki kepentingan-kepentingan tertentu diantaranya untuk ketenaran, hiburan atau iseng, atau bahkan merusak. Disinilah perlunya pengamanan informasi yang secara signifikan, setidaknya bisa mengatasi hal tersebut. Konsep dan metoda pengamanan informasi begitu banyak yang biasanya terkumpul dalam keilmuan tertentu yang dikenal saat ini dengan kriptologi *(Cryptology)* yang mencakup kriptograpi *(Cryptography)* [Kahn, Katz and Pister, 1999]. Metoda inilah yang banyak digunakan oleh kalangan pemrogram maupun praktisi komputer untuk membuat pengamanan informasi secara berkala.

Keamanan informasi sangat diperlukan khususnya di jalur PC dan mobile, sebab me- nyangkut kebutuhan sistem dan keamanan sistem serta keamanan identitas pengguna computer pribadi dan mobile. Keamanan identitas pengguna tersebut terletak pada kerahasiaan *(confidentiality)* informasi yang memang dibutuhkan oleh pengguna. Informasi yang dikirim maupun yang diterima dicek terlebih dulu keabsahannya (validasi) oleh bagian operator. Bagian operator inilah yang mengetahui identitas pengguna tersebut. Sehingga dibutuhkan untuk menjaga kerahasiaan informasi dengan cara enkripsi dan dekripsi

sms. Pada penelitian ini enkripsi dan deskripsi sms akan menggunakan algoritma stream cipher dan key generator yang merupakan pengembangan dari metoda OTP (One Time Pad) yang tergolong dalam unbreakable cipher (cipher yang tidak mudah dipecahkan) karena kunci yang digunakan pada setiap pengiriman hanya sekali pakai saja.

2. KRIPTOGRAFI

Kriptograpi merupakan bagian dari ilmu matematika tingkat tinggi yang dapat dipakai untuk keamanan data biasanya data dapat di samarkan (cipher/ text/encryption) dan sebaliknya di (plaintext/decryption). Dengan adanya konsep ini, lubang-lubang kebocoran dari konstruksi dan konfigurasi perangkan lunak, perangkat keras, dan jaringan seminimal mungkin dapat diata secara maksimal.

Generator Cipher

Generator cipher merupakan cara mengenkripsi dan mengdekripsi data pada sejumlah data yang besar; menggunakan prinsip kerja pem- balikan (*Exclusive OR / XOR*) dari buah masukan teks asli dengan teks kunci dan hasilnya berupa teks samar enkripsi. Begitu pun sebaliknya. Teknik ini, lebih baik dibandingkan dengan teknik sebelumnya (One Time Pad).

Teknik pengembangan OTP yang diperkenalkan oleh Vernam. Prinsipnya bahwa masukan dua buah input teks asli dengan teks kunci berupa karakter dikonversi kedalam bentuk bit (64 bit).

Rumus[Schneiner, 2006] :
ci = (pi + ki) mod 2 atau ci = pi $\oplus$ ki (untuk enkripsi).
pi = (ci – ki) mod 2 atau pi = ci $\oplus$ ki (untuk dekripsi).

Contoh :
Diambil dari contoh diatas :
ci = (C + O) mod 2 = (2 + 14) mod 2
= 0 = (0000) = A,
ci = (O + T) mod 2 = (14 + 19) mod 2
= 1 = (0001) = B, dan seterusnya.

kenyataanya dalam implementasi yang paling banyak dipakai adalah dengan teknik exclusive OR untuk OTP. Misalnya terdapat bit teks asli 0001dan bit kunci 0010, maka proses enkripsinya adalah sebagai berikut :

1 = 0001 (Teks Asli)
2 = 0010 (Kunci)
---------- $\oplus$
3 = 0011 (Hasil Enkripsi), dan seterusnya

3. METODOLOGI

Dalam penelitian ini, kami menggunakan metoda linier sequential, yang terdiri atas pengumpulan informasi, analisis masalah dan kebutuhan pembangunan program enkripsi dan deskripsi yang akan disimpan sebagai fitur tambahan di PC dan Mobile, perancangan modul aplikasi, pengkodean modul dalam bentuk aplikasi, dan pengujian aplikasi.

4. HASIL DAN PEMBAHASAN

Pembangunan Modul Program

Modul program yang dibangun untuk keamanan ini terdiri atas modul enkripsi, deskripsi, tampung kunci dan tampung teks.

Modul Program 1. Enkripsi informasi

```
// Proses Enkripsi
function Enkripsi(Teks : String):String;
var i, j, HasilEnkripsi : Integer; TampKunci : String;

begin try
 HasilEnkripsi := 0;
 edtGenKunciPub.Text := genSimpanKunci; Teks :=
 Copy(edtGenTeks.Text, 0, 255);
 TampKunci := Copy(edtGenKunciPub.Text, 0, 255);
 for i := 0 to Length(Teks)
 do begin
   for j := 0 to Length(tampkunci)
   do begin
   HasilEnkripsi := HasilEnkripsi + ord(tampKunci[j])
   xor ord(Teks[i]));
   end;
  result := result + char(HasilEnkripsi);
 end;
except end; end;
```

Modul program merupakan modul yang dibangun untuk proses enkripsi yaitu merubah plaintext menjadi ciphertext, dengan cara plaintext dan key generator ditranslate menjadi deretan biner sesuai dengan rangkaian biner dari abjad yang telah didefinisikan kemudian plaintext di-XOR–kan dengan key generator. Dan hasilnya berupa deretan angka biner yang akan ditranslate menjadi abjad.

Hasil dari transalate tersebut adalah ciphertext yang siap untuk dikirimkan. Setelah pesan berupa chipertext diterima, maka disisi pengirim melakukan deskripsi informasi dengan menggunakan modul deskripsi informasi.

Modul Program 2. Deskripsi informasi

```
// Proses Dekripsi
function Dekripsi(Teks : String):String;
var i, j, HasilDekripsi : Integer; TampKunci        : String;

begin
 HasilEnkripsi := 0;
 edtGenTeks.Text := genSimpanTeks; Teks := Copy(edtGenTeks.Text,
 0, 255);
 TampKunci := Copy(edtGenKunciPub.Text, 0, 255);
 for i := 0 to Length(Teks)
 do begin
   for j := 0 to Length(tampkunci)
   do begin
     HasilEnkripsi   :=   HasilEnkripsi   +   (ord(tampKunci[j])   xor
ord(Teks[i]) end;
  result := result + char(HasilDekripsi);
 end;
end;
```

Pada modul deskripsi ini chipertext yang berupa rangkaian abjad ditranslate menjadi deretan biner. Kemudian Ciphertext di-XOR- kan dengan key generator untuk menghasilkan deretan angka yang akan ditranslate menjadi plaintext.

Modul program 3. Proses Tampung Kunci

```
// Proses Tampung Kunci function
SimpanKunci:String;       var       i,
KunciPub : Integer;
   Kunci   : String;

begin
 kuncipub := 0;
 Kunci := Copy(edtGenKunci.Text, 0, 255);
 for i := 0 to 2*Length(Kunci)-1 do
 begin
   KunciPub := KunciPub + (ord(kunci[i]) xor

ord(kunci[i+3]));
   result := result + char(KunciPub);
 end;
end;
```

Modul program 3. Proses Tampung Teks

```
// Proses Tampung Teks function
SimpanTeks:String; var i, TeksPub : Integer;
  Teks : String;

begin
  TeksPub := 0;
    Teks := Copy(edtGenEnkripsi.Text, 0, 255);
  for i := 0 to 2*Length(Teks)-1 do begin
    TeksPub := TeksPub + (ord(kunci[i]) xor ord(kunci[i-
  3]));
    result := result + char(TeksPub);
end;
```

Tampilan hasil program

Modul proses tampung teks ini digunakan untuk menampung teks dalam bentuk abjad dan sekaligus sebagai proses translate menjadi rangkain biner, dan modul ini berperan sebagai basis data konversi huruf ke angka biner. Dimana basis data ini terdiri atas A-Z, a-z, 0..9, dan simbol-simbol khusus seperti ?,/,!,@,#,$,%,^,&,*,(,),<,>,+,=,-.

Pengujian program

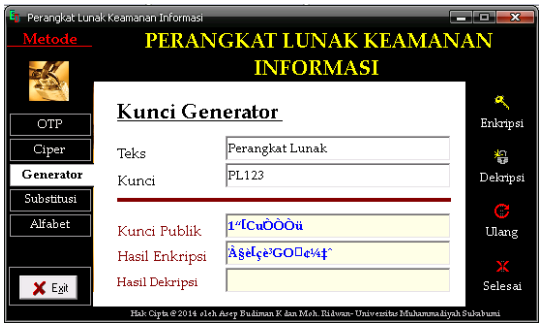
Pengujian program dilakukan untuk melihat integritas dari modul yang telah bangun. Apakah semua modul dapat berjalan dengan baik atau tidak. Pengujian pertama dilakukan adalah bentuk tampilan awal atau tampilan (lihat gambar.1) untuk melakukan enkripsi dan pengirim pesan.

Pada modul proses tampung kunci ini dibuat untuk menampung key generator yang akan digunakan, sekaligus sebagai track record untuk mengingatkan user agar tidak ada kunci yang dipakai ulang.

Gambar 1. Tampilan awal

Dari gambar1, hasil pengujian untuk menampilkan tampilan utama telah berhasil. Pada tampilan utama ini user dapat memilih menu pilihan untuk enkripsi ataupun deksripsi, dengan cara memilih algoritma yang diinginkan yaitu generator cipher dan kunci publik yang akan digunakan.

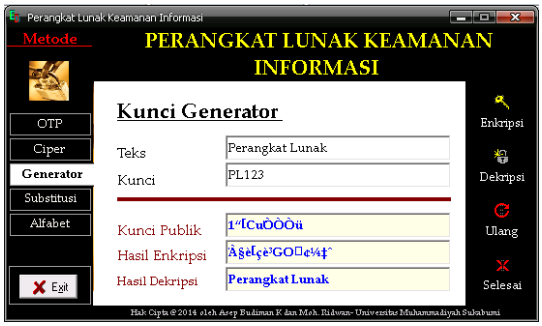
Pengujian berikutnya adalah untuk menentukan pengujian integrasi antara modul enkripsi, modul tampung kunci dan tampung teks dalam melakukan proses enkripsi. Hasil pengujian ini dapat dilihat pada gambar 2.



Gambar 2. Proses Enkripsi

Dari gambar 2, hasil enkripsi muncul dalam bentuk kalimat yang tidak memiliki arti alias proses enkripsi berhasil. Dengan kunci publik yang panjangnya tidak sama dengan plainteks.

Pengujian selanjutnya adalah pengujian integrasi untuk modul deskripsi, modul tampung kunci dan tampung teks dalam melakukan proses deskripsi. Hasil pengujian dapat dilihat pada gambar 3.



Gambar 3. Proses Deskripsi

Dari gambar 3, proses deskripsi berhasil dengan memunculkan pesan yang sebenarnya. Dengan menggunakan kunci publik yang panjangnya tidak sama dengan chiperteks.

5. KESIMPULAN

Penggunaan metoda stream dan generator cipher dengan key generator untuk keamanan informasi mempermudah dalam pengiriman informasi yang sifatnya rahasia, karena si penerima informasi tersebut harus memiliki kunci yang sama dengan si pengirim. Dengan demikian informasi yang dikirim akan aman karena kunci publik yang digunakan hanya sekali pakai dan dibuat secara random, serta panjang kunci publik tidak harus sama panjang dengan plaintext atau pun ciphertext.

DAFTAR PUSTAKA

[1] Anaiba, Adel (2004), *A Decision Support Model For Wireless Information Management Using Mobile Agent*, url : http://www.soc.staffs.ac.uk/aa11/WIDA. Pdf. diakses tanggal : 20 September 2014

[2] Du, Wenliang (2006) *A Key Management Scheme for Wireless Sensor Networks Using Deployment Knowledge*, Syracuse University, Syracuse, NY

[3] 13244-1240, USA

[4] Kahn, J.M., Katz,R.H.,and Pister,KS.J. (1999), *Next century challenges: Mobile networking for smart dust*, Proceedings of the 5th Annual ACM/IEEE

Internation Conference on Mobile Computing and Networking (MobiCom).
[5] Bruce Schneier, "*Applied Cryptography: Protocols, Algorithms, and Source Code in C*," second edition, John Wiley & Sons, Inc., 1996.