PENGGUNAAN *VOICE RECOGNITION* DALAM KRIPTOGRAFI KUNCI-PUBLIK

Magdalena Marlin Amanda – NIM: 13506042

Program Studi Teknik Informatika, Institut Teknologi Bandung
Jl. Ganesha 10, Bandung
E-mail : if16042@students.if.itb.ac.id

Abstrak

Makalah ini membahas tentang implementasi teknologi *voice recognition* dalam kriptografi kunci publik. Dalam makalah ini akan dibahas mengenai bagaimana implementasi dilakukan, analisis mengenai perbedaan sebelum dan sesudah penerapan *voice recognition* serta keuntungan yang ditawarkan oleh implementasi teknologi baru ini kepada penggunanya.

***Kata kunci**: voice recognition*, kriptografi kunci-publik, pembangkitan bilangan acak

1. Pendahuluan

Kriptografi kunci-publik adalah salah satu metode kriptografi modern yang tingkat keamanannya cukup tinggi sehingga penggunaanya dalam berbagai aplikasi cukup banyak, termasuk di dalamnya penggunaan kriptografi kunci-publik dalam tanda tangan digital.

Penerapan *voice recognition* dalam kriptografi kunci publik, selain untuk lebih memusingkan kriptanalis dengan metode pembangkitan kunci yang sedikit berbeda, juga dapat digunakan untuk membantu pengguna yang memiliki kekurangan dalam penglihatan. Dengan menggunakan *voice recognition* pembangkitan kunci tidak perlu dilakukan dengan menggunakan papan kunci lagi, sehingga dapat digunakan pula oleh pengguna yang memiliki masalah penglihatan.

2. Kriptografi Kunci-Publik

Kriptografi kunci-publik pertama kali dipublikasikan oleh dua ilmuwan dari Stanford University, Whitefield Diffie dan Martin Hellman pada tahun 1976. Secara sederhana, konsep kriptografi ini adalah mengumumkan secara publik kunci yang digunakan untuk enkripsi pesan (kunci publik) namun merahasiakan kunci yang digunakan untuk dekripsi pesan (kunci privat).\

Algoritma kriptografi kunci-publik yang paling populer dan banyak digunakan adalah RSA, karya Ron Rivest, Adi Shamir, dan Leonard Adleman. Keamanan algoritma kriptografi mereka terletak pada pembangkitan kunci yang didasarkan pada bilangan prima yang dibangkitkan secara acak dan berukuran cukup besar.

Penggunaan kriptografi kunci-publik cukup beragam, di antaranya untuk kerahasiaan data yang dikirimkan, tanda tangan digital untuk mencegah penyangkalan, dan untuk pertukaran kunci kriptografi simetri.

Perhitungan dan besaran yang digunakan untuk membangkitkan kunci publik dan kunci simetri adalah:

- p dan q : bilangan prima yang berbeda, bersifat rahasia
- n : bilangan hasil perkalian p dan q, tidak bersifat rahasia
- $\phi(n) = (p-1)(q-1)$; bersifat rahasia

Setelah melakukan penghitungan di atas, dipilih kunci publik e yang nilainya ralatif prima terhadap $\phi(n)$ dan kunci privat d diturunkan berdasarkan persamaan:

$$e \cdot d \equiv 1 \pmod{\phi(n)}$$

Untuk proses enkripsi dan dekripsinya, digunakan rumus sebagai berikut:

$$E_e(m) = c \equiv m^e \bmod n$$

$$D_d(m) = m \equiv c^d \bmod n$$

Kelebihan utama yang ditawarkan oleh algoritma kriptografi ini adalah sukarnya mencoba menghitung kunci privat dan kunci publik hanya dengan mengetahui nilai *n*. Untuk memperkuat algoritma ini, biasanya kriptografer atau pembuat aplikasi membuat suatu struktur data baru yang dapat menampung suatu bilangan yang besarnya lebih daripada bilangan *integer* biasa pada komputer. Dengan demikian, pemfaktoran akan semakin mustahil untuk dilakukan.

3. *Voice Recognition*

Teknologi *voice recognition* atau *speech recognition* adalah teknologi yang memungkinkan komputer menerima masukan berupa suara. *Voice recognition* menggunakan pencocokan antara masukan dengan kata atau kalimat yang telah terlebih dahulu dimasukkan ke dalam program, setelah itu komputer mengubah masukan tersebut menjadi bentuk yang dikenal oleh sistem.

Sebenarnya teknologi *voice recognition* dapat diperumit dengan adanya pengenalan pola frekuensi suara dan amplitudo, tapi hal tersebut malah memberikan kesukaran baru, terutama apabila suara pengguna tengah mengalami gangguan suara karena sakit atau hal lainnya.

Hingga saat ini, *voice recognition* dapat menerima masukan suara berdasarkan kata-kata dari berbagai negara, tidak hanya bahasa Inggris saja.

4. Implementasi

Ada dua variasi yang mungkin dibuat sebagai implementasi penggunaan *voice recognition* pada kriptografi kunci-publik. Variasi pertama adalah pembangkitan kunci berupa angka, sesuai dengan proses pembangkitan kunci publik dan kunci privat pada algoritma kriptografi kunci-publik, tapi cara memasukkan kunci dilakukan dengan menggunakan *voice recognition*. Variasi kedua adalah penggunaan suatu kata yang dikenal untuk mengaktifkan kunci. Dari kedua variasi ini, sebenarnya dapat pula diimplementasikan hanya salah satu kunci saja yang menggunakan *voice recognition*, tergantung preferensi pengguna.

4.1 Pengucapan Kunci Asli

Pada variasi ini, kunci masih tetap berupa angka, hanya saja pengguna dapat memasukkan kunci tersebut dengan mengetikkan dari papan kunci atau menggunakan *voice recognition*.

Untuk lebih mempermudah penggunaannya, pemasukan kunci yang berupa angka dilakukan satu persatu, dengan umpan balik berupa suara untuk pengguna yang memiliki kekurangan secara fisik. Alasan mengapa pemasukan kunci dilakukan satu persatu adalah agar komputer dapat melakukan pemrosesan lebih akurat. Pemasukan angka secara beruntun dapat menyebabkan bias pada sistem pengenalan yang akan memperlambat proses pengaktifan kunci.

Setiap satu kata yang diterima oleh komputer, program akan mencocokkan kata yang diterima dengan kata yang telah ada dalam basis datanya, terbatas hanya tersimpan pengucapan bilangan dari angka nol hingga sembilan dengan asumsi pengguna sudah tahu bahwa sistem hanya menerima masukan berupa bilangan yang diucapkan.

Setelah didapat kecocokan antara kata yang diucapkan dengan data yang tersimpan, sistem akan mengubah masukan tersebut menjadi bentuk yang dikenali oleh sistem dan menyimpannya dalam memori sementara. Proses pemasukan kunci berulang hingga semua angka dimasukkan dan kunci dapat diproses lebih lanjut.

4.2 Pengaktifan Kunci dengan Kata Sandi

Pembangkitan kunci publik dan kunci privat pada variasi kedua ini sama dengan

algoritma pembangkitan kunci yang diterapkan, hanya saja sebagai pengamanan tambahan, kunci tersebut "dilapis" dengan suatu kata yang dibangkitkan secara acak oleh sistem.

Seperti yang sudah diketahui, komputer tidak dapat benar-benar menghasilkan suatu bilangan acak, tapi dengan akses ke suatu basis data kamus bahasa, komputer dapat mengambil satu kata dari ribuan kata yang tersedia untuk dijadikan kata kunci. Hal ini dapat digunakan untuk keamanan tambahan atau mempermudah proses pembangkitan kunci apabila tidak ingin menggunakan bilangan prima yang terlalu besar.

Variasi ini dapat digabungkan dengan variasi sebelumnya, di mana selain menggunakan *voice recognition* untuk memasukkan kata kunci, *voice recognition* juga digunakan untuk memasukkan angka-angka dari kunci.

5. Analisis

5.1 Kelebihan

Kelebihan yang ditawarkan oleh penggunaan *voice recognition* dalam kriptografi kunci-publik adalah memberikan kesempatan bagi pengguna komputer yang berkekurangan secara fisik, terutama penglihatan, untuk mendapat kemudahan dalam pemakaian aplikasi kriptografi.

Selain itu, dalam pembangkitan kuncinya, dengan menggunakan pelapis tambahan untuk keamanan, pembuat aplikasi kriptografi tidak perlu membuat suatu struktur data baru untuk menampung bilangan prima yang besar dan tidak perlu mengkhawatirkan pembangkitan bilangan acak yang bersifat semu. Kata-kata yang diambil oleh aplikasi, apabila tidak dibatasi bahkan dapat diambil dari berbagai bahasa yang telah dikenal oleh perangkat *voice recognition*.

5.2 Kelemahan

Penggunaan *voice recognition* untuk mengaktifkan kunci sangat rentan pada pencurian karena menggunakan suara. Teknologi *voice recognition* yang ada saat ini rentan terhadap gangguan suara dari luar sehingga aplikasi yang menggunakan *voice recognition* lebih efektif digunakan di tempat yang cukup sepi. Apabila pihak kriptanalis mengetahui langsung di mana target mereka akan menggunakan aplikasi kriptografinya, mereka dapat memasang alat penyadap atau bahkan langsung mencuri dengar kata kunci yang tengah dimasukkan. Cara tersebut bahkan lebih mudah daripada berusaha menghitung kunci privat yang digunakan dalam aplikasi.

Selain itu, perangkat *voice recognition* yang beredar saat ini membutuhkan masukan yang benar-benar sesuai dari pengguna, baik intonasi maupun pelafalannya. Hal tersebut membuat masukan berupa suara sering kali sukar diterima dan diproses dengan tepat oleh komputer. Bagi pengguna yang tidak mengetahui batasan tersebut, hal ini bisa sangat mengganggu dan membuat aplikasi terasa sukar digunakan atau tidak *user-friendly*.

5.3 Hambatan Implementasi

Dalam kriptografi kunci-publik, kunci privat dan kunci publik dibangkitkan berdasarkan perhitungan matematis atas dua buah bilangan prima yang dibangkitkan secara acak di awal pembangkitan kunci. Kunci publik dan kunci privat yang sama sekali tidak memiliki kesamaan, tapi jika digunakan untuk memproses pesan menjadi chiperteks dan juga sebaliknya dapat menghasilkan hasil yang serupa, memerlukan perhitungan matematis khusus.

Beberapa kendala yang mengakibatkan kunci publik dan kunci privat tidak dapat dibangkitkan tanpa bilangan:

- Hanya ada beberapa kata yang setelah diubah bentuknya ke dalam bit dan kemudian menjadi angka, akan membentuk bilangan prima.
- Apabila dilakukan penambahan pada bilangan yang didapatkan dari kata yang menjadi masukan, penambahan tersebut

harus disimpan agar dapat digunakan kembali nantinya.
- Hasil dari perhitungan awal, mungkin tidak menghasilkan suatu kata yang bermakna setelah proses pembangkitan kunci privat dan kunci publik.

6. Kesimpulan

Implementasi teknologi baru untuk menerima masukan dapat memperluas penggunaan kriptografi dan menawarkan cara baru meningkatkan keamanannya. Tapi selain memiliki berbagai keunggulan dan menawarkan kelebihan-kelebihan, implementasi tersebut memiliki celah keamanan yang cukup fatal, tidak sebanding dengan kelebihan yang ditawarkan.

Daftar Pustaka

Munir, Rinaldi. 2006. *Diktat Kuliah IF5054 Kriptografi*. Program Studi Teknik Informatika. Institut Teknologi Bandung.

Hakim, Hasanul. 2008. Voice Recognition *Menggunakan RIPEMD-128.* Program Studi Teknik Informatika. Institut Teknologi Bandung.

http://en.wikipedia.org/wiki/Speech_recognition Waktu akses: 6 Mei 2009, 10.19 WIB

http://en.wikipedia.org/wiki/Cryptography Waktu akses: 6 Mei 2009, 10.19 WIB