Pengunaan Algoritma Pertukaran Kunci Diffie-Hellman dalam SMS

Jonathan (13516058)
Program Studi Teknik Informatika
Institut Teknologi Bandung
Institut Teknologi Bandung, Jl. Ganesha 10 Bandung 40132, Indonesia
jonathantjandra.98@outlook.com

***Abstract*—Kriptografi yang dipakai dalam dunia modern yang terhubung dengan dunia internet sekarang ini adalah kriptografi dengan kunci asimetrik. Pengunaan kriptografi semakin meningkat dalam dunia komunikasi di perangkat mobile, namun di antara banyak cara komunikasi terdapat salah satu cara komunikasi yang kurang aman yaitu SMS. Pengunaan Diffie-Hellman dan kombinasi dengan enkripsi diharapkan akan dapat membantu mengamankan komunikasi melalui SMS.**

Keywords—kriptografi, kunci publik, SMS, Diffie-Hellman.

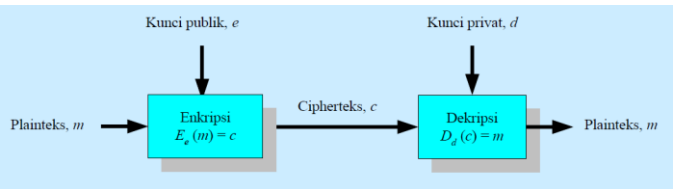
I. PENDAHULUAN

Dunia modern adalah dunia yang bergantung pada komunikasi melalui perangkat mobile. Salah satu jalur komunikasi melewati mobile adalah SMS. SMS sendiri dalam pengirimannya tidak dienkripsi, sehingga bisa disadap saat melalui jaringan operator, sehingga diperlukan adanya modifikasi agar SMS bisa dikirimkan dengan enkripsi sehingga konten tidak mudah untuk disalahgunakan serta pertukaran kunci sehingga SMS bisa didekripsi oleh pihak penerima. Makalah ini akan lebih focus terhadap aspek pertukaran kunci menggunakan algoritma Diffie-Hellman untuk SMS..

II. KRIPTOGRAFI KUNCI PUBLIK

Kriptografi kunci public merupakan bentuk dari kriptografi kunci asimetrik. Kunci pada kriptografi kunci public merupakan sebuah pasangan kunci. Satu kunci untuk mengdekripsi yaitu *private key* dan satu kunci untuk menenkripsi.yaitu *public key*.

Misalkan D adalah fungsi dekripsi, E adalah fungsi enkripsi, e sebagai kunci public dan d sebagai kunci privat. Maka diagram dari bekerjanya kriptografi kunci public dapat dinyatakan sebagai berikut:



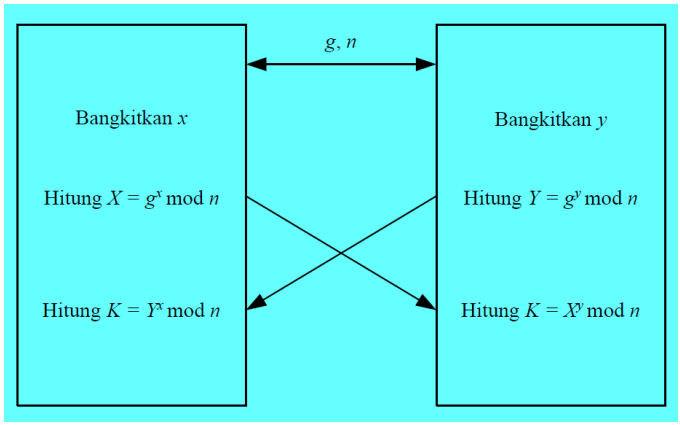
Gambar 1. Diagram Kriptografi Kunci Publik

Sumber : Slide Kriptografi Kunci Publik. Rinaldi Munir. 2018.

Dari Gambar 1 terlihat bahwa proses enkripsi dilakukan dengan $E_e(m) = c$ dan fungsi dekripsi dilakukan dengan $D_d(c) = m$ atau $D_d(E_e(m)) = m$. Dari persamaan ini dapat terlihat meskipun public key dan private key terlihat maka belum tentu plaintext akan bisa didekripsi. Selain itu juga hampir tidak mungkin untuk menemukan secara komputasi private key dari public key. (Munir dkk, 2006).

III. ALGORITMA DIFFIE-HELLMAN

Algoritma Diffie-Hellman adalah algoritma pertukaran kunci yang memungkinkan dua orang dapat saling bertukar kunci dengan aman dan dapat digunakan untuk berbagai pesan, tidak hanya satu kali. Diagram dari algoritma tersebut adalah :



Gambar 2: Pertukaran Kunci Diffie-Hellman

Sumber : Slide Algoritma Diffie-Hellman, Rinaldi Munir. 2018.

Dalam Algoritma Diffie-Hellman, kedua pihak (Alice dan Bob) melakukan hal sebagai berikut:

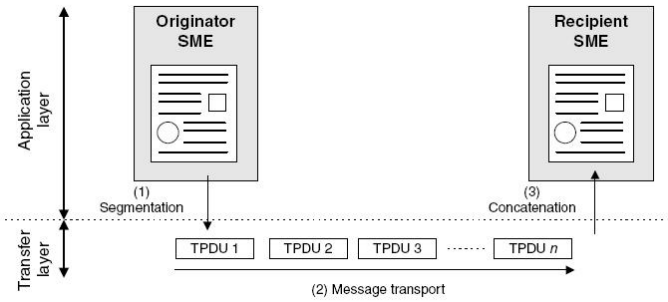
1. Menentukan dua buah bilangan prima (n dan g, dengan syarat g < n)
2. Alice, dengan kunci privat/bilangan acak x menghitung $X = g^x \bmod n$, sedangkan Bob dengan kunci privat/.bilangan acak y menghitung $Y = g^y \bmod n$
3. Kemudian saat terjadi pertukaran, maka Alice akan menghitung $Y^x \bmod n$, dan Bob akan menghitung $X^y \bmod n$. Hasilnya akan benar jika sama, yaitu $g^{xy} \bmod n$.

IV. SMS (SHORT MESSAGE SERVICE)

SMS adalah sebuah layanan pesan teks singkat yang dapat diakses dari sebuah perangkat seluler dan internet. SMS pertama kali dikirim pada tahun 1992. Pengunaan SMS didukung oleh seluruh perangkat GSM dan standarisasi oleh 3GPP.

Struktur pesan dari SMS dapat terdiri dari macam-macam isinya misalnya lagu, gambar, dsb. Dalam transfer maka tentu saja tidak semua dapat dikirim dalam 1 SMS saja, sehingga aplikasi SMS akan membagi pesan-pesan tersebut menjadi beberapa bagian, dan kemudian akan digabungkan kembali saat transfer selesai. (Herdansyah dan Wardoyo, 2011, mengutip dari Bodic, 2005)

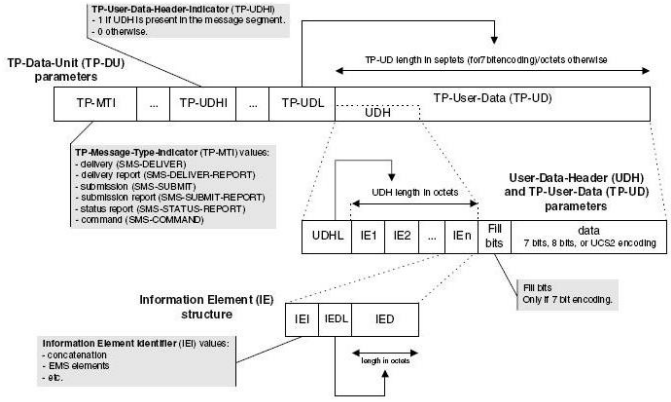
Diagram pengiriman pesan adalah sebagai berikut:



Gambar 3. Pengiriman Pesan dari SMS.

Sumber: Mobile Messaging Technologies and Services SMS,EMS and MMS Second Edition. Gwenaël Le Bodic. 2005

Dalam TPDU (Transport Protocol Data Unit), maka terjadi pemrosesan header dan parameter dari SMS tersebut sehingga dapat dikirimkan dengan tepat.



Gambar 4. Transfer Protocol Data Unit

Sumber: Mobile Messaging Technologies and Services SMS,EMS and MMS Second Edition. Gwenaël Le Bodic. 2005

V. RANCANGAN PENERAPAN

Dalam implementasinya diperlukan sebuah aplikasi SMS khusus yang mampu menangani input untuk pembentukan kunci privat masing-masing pihak, dengan kunci public masing-masing pihak adalah nomor telepon, serta penentukan kunci bersama, serta mengetik isi konten SMS. Diagram rancangan dasar adalah sebagai berikut:

Gambar 5. Diagram Rancangan Sistem Pertukaran Kunci

Asumsi :

Dua bilangan yang diketahui (n dan g) adalah nomor telepon masing-masing pihak tanpa kode negara.

Algoritma enkripsi pada SMS harus disesuaikan dengan formatting serta pertimbangan kecepatan enkripsi, akan tetapi tetap aman. Penelitian terkait yaitu oleh Hendarsyah dan Wardoyo pada tahun 2011 mengemukakan ide untuk memodifikasi RC4 cipher dalam enkripsi SMS.

VI. KESIMPULAN

Pengunaan algoritma pertukaran kunci Diffie-Hellman mendukung pengiriman kunci yang lebih aman setelah sebuah SMS dienkripsi karena SMS dikirimkan melalui protocol jaringan tanpa enkripsi, sehinga kontennya berupa plaintext. Namun setelah dilakukan enkripsi, maka konten SMS tersebut adalah berupa ciphertext dan dapat bisa didecode hanya oleh perangkat yang dituju.

Akan tetapi, kelemahan dari algoritma enkripsi yang digunakan dalam SMS perlu diperhatikan, karena bergantung pada jenis serangan yang bisa dilakukan, enkripsi dan pertukaran kunci tidak akan bisa melindungi. Selain itu, penentuan keamanan algoritma Diffle-Hellman yang bergantung pada bilangan prima perlu diperhatikan untuk cost dalam pemrosesan pada perangkat.

REFERENCES

[1] Hendarsyah, D. dan Wardoyo, R, 2011. Implementasi Protokol Diffie-Hellman Dan AlgoritmaRC4 Untuk Keamanan Pesan SMS

[2] Munir, R. 2018. Slide Kuliah Kriptografi Kunci Publik.

[3] Munir, R. 2018. Slide Kuliah Algoritma Diffle-Hellman..

[4] ETSI TS 151 010-1 V12.5.0 (2015-09) . (Diakses di http://www.etsi.org/deliver/etsi_ts/151000_151099/15101001/12.05.00_60/ts_15101001v120500p.pdf#page=3419