Beberapa Teknik Memperkuat Algoritma RSA untuk Mengatasi Chosen-Plaintext Attack

Arief Pratama [1)]

1) Jurusan Teknik Informatika Sekolah Teknik Elektro dan Informatika ITB, Bandung, email: if14070@students.if.itb.ac.id

Abstrak *-- RSA merupakan salah satu algoritma kunci public yang paling popular. Kekuatan algoritma ini terletak pada sulitnya memfaktorkan bilangan-bilangan besar menjadi factor-faktor prima. Namun algoritma ini telah terbukti dapat dipecahkan dengan chosen-plaintext attack.*

Kata kunci*: RSA, CBC, chosen-plaintext attack, kriptanalisis*

1. PENDAHULUAN

Chosen-plaintext attack merupakan jenis serangan di mana kriptanalis memiliki plaintext, kemudian plaintext tersebut dienkripsi dengan kunci publik dan disimpan dalam kamus. Hasil enkripsinya dibandingkan dengan ciphertext yang ada. Jika terdapat kesamaan, maka kamus tersebut dapat digunakan kriptanalis untuk mempelajari isi pesan.

Kriptanalis telah dapat menghasilkan plaintext dari ciphertext yang ada, namun kuncinya sendiri belum ditemukan [2]. Pada serangan jenis ini kriptanalis dapat memilih plaintext tertentu untuk dienkripsikan, yaitu plaintext yang lebih mengarahkan penemuan kunci. Kriptanalis berusaha untuk menemukan kunci pembangun ciphertext dengan membandingkan keseluruhan ciphertext dengan plaintext yang ada.

Dimiliki:

$C_1 = E_k(P_1)$ *dan* P_1

$C_2 = E_k(P_2)$ *dan* P_2

....

$C_i = E_k(P_i)$ *dan* P_i

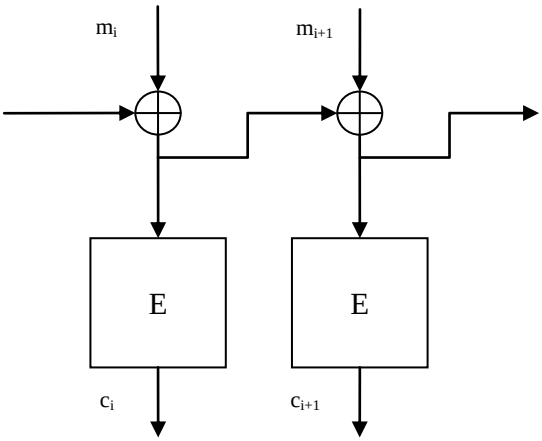
Informasi tersebut dapat digunakan kriptanalis dalam mencari kelemahan dalam cryptosystem RSA, dan dalam kasus terburuk kunci dapat dideduksi.

2. MODE-MODE OPERASI ENKRIPSI

Dalam makalah ini, penulis mengusulkan beberapa teknik untuk memperkuat algoritma ini, sehingga dapat mengatasi kelemahan tersebut. Salah satu teknik yang diusulkan di sini adalah dengan menambah kerumitan pada plaintext sehingga para kriptanalis sulit menemukan pasangan ciphertext pada dari *chosen plaintext*.

2.1. Mode enkripsi dengan menggunakan plainteks sebelumnya

Pada mode ini, proses enkripsi dapat digambarkan sebagai berikut:



Gambar 1 Alur proses enkripsi

Persamaan enkripsi:

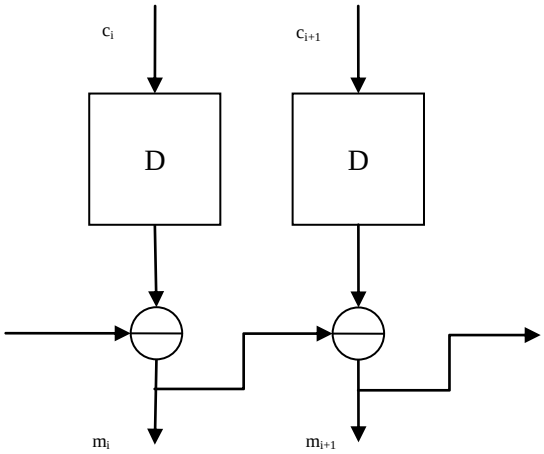
$c_1 = m_1{}^e \ mod \ n$

$c_2 = (m_2 \oplus m_1)^e \ mod \ n$

$c_3 = (\ m_3 \oplus m_2 \oplus m_1)^e \ mod \ n$

...

$c_i = (\ m_i \oplus m_{i-1} \oplus m_{i-2} \oplus \ ... \oplus m_1)^e \ mod \ n \qquad (1)$



Gambar 2 Alur proses dekripsi

$m_1 = {c_1}^d \ mod\ n$

$m_2 = ({c_1}^d \ mod\ n) \ominus m_1$

$m_2 = ({c_1}^d \ mod\ n) \ominus (m_1 \oplus m_2)$

...

$m_i = ({c_i}^d \ mod\ n) \ominus (m_{i-1} \oplus m_{i-2} \oplus ... \oplus m_1)$ (2)

Simbol $\oplus$ adalah penjumlahan terhadap digit yang berkoresponden kemudian dimodulus 10. Simbol $\ominus$ adalah pengurangan terhadap digit yang berkoresponden kemudian dimodulus 10. Setiap blok m diasumsikan memiliki panjang digit yang sama.

Contoh:

$9387 \oplus 6623$ dapat dihitung sebagai berikut:

$(9 + 6)\ mod\ 10 = 5$

$(3 + 6)\ mod\ 10 = 9$

$(8 + 2)\ mod\ 10 = 0$

$(7 + 3)\ mod\ 10 = 0$

Maka, $9387 \oplus 6623 = 5900$.

$5900 \ominus 6623$ dapat dihitung sebagai berikut:

$(5 - 6)\ mod\ 10 = 9$

$(9 - 6)\ mod\ 10 = 3$

$(0 - 2)\ mod\ 10 = 8$

$(0 - 3)\ mod\ 10 = 7$

Maka, $5900 \oplus 6623 = 9387$.

Contoh berikut akan menggambarkan proses enkripsi dan dekripsi pada mode ini.

m = HARI INI = 726 582 733 273 787 003

m_1 = 726 *m_2 = 582*

m_3 = 733 *m_4 = 273*

m_5 = 787 *m_6 = 003*

Parameter lainnya: *e = 79, d = 1019, n =3337*

Jika dengan menggunakan metode RSA konvensional, ciphertext yang dihasilkan adalah : *215 776 1743 933 1731 158*

Proses enkripsi:

c_1 = $726^{79} \ mod\ 3337$

= 215

c_2 = $(582 \oplus 726)^{79} \ mod\ 3337$

= $208^{79} \ mod\ 3337$

= 1150

c_3 = $(733 \oplus 208)^{79} \ mod\ 3337$

= $931^{79} \ mod\ 3337$

= 322

c_4 = $(273 \oplus 931)^{79} \ mod\ 3337$

= $104^{79} \ mod\ 3337$

= 2893

c_5 = $(787 \oplus 104)^{79} \ mod\ 3337$

= $881^{79} \ mod\ 3337$

= 932

c_6 = $(003 \oplus 881)^{79} \ mod\ 3337$

= $884^{79} \ mod\ 3337$

= 1450

Ciphertext yang dihasilkan : *215 1150 322 2893 932 1450*

Proses dekripsi :

m_1 = $215^{1019} \ mod\ 3337$

= 726

m_2 = $(1150^{1019} \ mod\ 3337) \ \ominus\ 726$

= $208 \ominus 726$

= 582

m_3 = $(322^{1019} \ mod\ 3337) \ominus 208$

= $931 \ominus 208$

= 733

m_4 = $(2893^{1019} \ mod\ 3337) \ominus 931$

= $104 \ominus 931$

= 273

m_5 = $(932^{1019} \ mod\ 3337) \ominus 104$

= $881 \ominus 104$

= 787

m_6 = $(1450^{1019} \ mod\ 3337) \ominus 881$

= $884 \ominus 881$

= 003

2.2. Mode enkripsi dengan mengadapsi mode CBC dari block cipher

CBC (*cipher block chaining*) adalah mode enkripsi yang memiliki persamaan sebagai berikut [1]:

$C_i = E\ (P_i \wedge C_{i-1})$

$P_i = C_{i-1} \wedge D(C_i)$

$C_0 = Initialization\ Vector$

Dengan mengadapsi mode tersebut ke persamaan RSA, maka kita dapat memperoleh :

a. Persamaan enkripsi

$$c_i = (m_i \oplus c_{i-1})^e \ mod\ n \quad (3)$$

Jika m_i dan c_{i-1} tidak memiliki panjang digit yang sama, maka modulo hanya dilakukan sepanjang digit terpendek, namun lebar digit hasil perhitungan harus sepanjang m_i.

Contoh:

$9387 \oplus 662$ dapat dihitung sebagai berikut:

$(9 + 6)\ mod\ 10 = 5$

$(3 + 6)\ mod\ 10 = 9$

$(8 + 2)\ mod\ 10 = 0$

Maka, $9387 \oplus 662 = 5907$.

b. Persamaan dekripsi

$$m_i = (c_i{}^d \ mod\ n) \ominus c_{i-1} \quad (4)$$

Dengan menggunakan plaintext dan kunci seperti contoh sebelumnya, maka proses enkripsi dan dekripsi pada mode ini dapat digambarkan sebagai berikut.

Proses enkripsi:

$c_1 = 726^{79} \ mod\ 3337$

$= 215$

$c_2 = (582 \oplus 215)^{79} \ mod\ 3337$

$= 797^{79} \ mod\ 3337$

$= 1138$

$c_3 = (733 \oplus 1138)^{79} \ mod\ 3337$

$= 846^{79} \ mod\ 3337$

$= 470$

$c_4 = (273 \oplus 470)^{79} \ mod\ 3337$

$= 643^{79} \ mod\ 3337$

$= 580$

$c_5 = (787 \oplus 580)^{79} \ mod\ 3337$

$= 264^{79} \ mod\ 3337$

$= 2937$

$c_6 = (003 \oplus 2937)^{79} \ mod\ 3337$

$= 296^{79} \ mod\ 3337$

$= 902$

Ciphertext yang dihasilkan: *215 1138 470 580 2937 902*

Proses dekripsi:

$m_1 = 215^{1019} \ mod\ 3337$

$= 726$

$m_2 = (1138^{1019} \ mod\ 3337) \ominus 215$

$= 797 \ominus 215$

$= 582$

$m_3 = (470^{1019} \ mod\ 3337) \ominus 1138$

$= 846 \ominus 1138$

$= 733$

$m_4 = (580^{1019} \ mod\ 3337) \ominus 470$

$= 643 \ominus 470$

$= 273$

$m_5 = (2937^{1019} \ mod\ 3337) \ominus 580$

$= 264 \ominus 580$

$= 787$

$m_6 = (902^{1019} \ mod\ 3337) \ominus 2937$

$= 296 \ominus 2937$

$= 003$

3. ANALISIS TERHADAP MODE OPERASI

3.1. Analisis mode enkripsi pertama

Pada contoh di atas, jika kriptanalis mengetahui bahwa plaintext mengandung blok 733, blok tersebut dapat dienkripsi menjadi :

$733^{79} \ mod\ 3337 = 1743$

Sedangkan pada ciphertext, enkripsi blok 733 akan menghasilkan 322.

Kriptanalis tidak akan menemukan blok 1743 dalam ciphertext, dan walaupun ditemukan blok tersebut bukanlah blok yang berkoresponden dengan plaintext 733.

Jika diasumsikan bahwa kriptanalis mengetahui bahwa blok plaintext 733 berkoresponden dengan ciphertext 322, maka :

$322 = (733 \oplus X)^{79} \ mod\ 3337$

Informasi yang didapat kriptanalis hanya terbatas pada nilai di atas. Nilai X hanya dapat ditemukan

jika menggunakan brute-force, yang memakan waktu lama untuk menyelesaikannya. Walaupun nilai X ditemukan, nilai tersebut tidak akan berarti apa-apa kecuali 733 merupakan blok kedua di mana X merupakan blok pertama. Untuk menghitung blok ketiga dan seterusnya, kriptanalis hanya dapat mengandalkan brute-force.

Berdasarkan rumus, proses enkripsi suatu blok plainteks melibatkan plainteks-plainteks sebelumnya. Namun dalam implementasinya, perhitungan modulo terhadap suatu plainteks dapat memanfaatkan perhitungan yang telah dilakukan terhadap plainteks sebelumnya. Perhitungan modulo terhadap suatu cipherteks juga dapat memanfaatkan perhitungan sebelumnya.

Hal ini tentu saja berpengaruh besar dalam performansi enkripsi/dekripsi. Namun jika implementasi seperti di atas digunakan, kesalahan perhitungan modulo pada suatu blok akan menghasilkan cipherteks/plainteks yang bersangkutan juga salah dan kesalahan itu merambat keseluruh cipherteks/plainteks berikutnya.

3.2. Analisis mode enkripsi kedua (CBC)

Dengan menggunakan contoh yang diberikan pada subbab 2.2, jika kriptanalis mengetahui bahwa plaintext mengandung blok 733, maka dengan mode enkripsi konvensional RSA didapat:

$733^{79} \bmod 3337 = 1743$

Dengan menggunakan mode ini, cipherteks dihitung dengan :

$C = (733 \oplus X)^{79} \bmod 3337$

Di mana X merupakan blok ciphertext sebelum C. Untuk mendapatkan C, kriptanalis harus menghitung rumus di atas dengan menggunakan pasangan 2 blok yang berurutan secara brute-force.

Jika diasumsikan bahwa blok plainteks 733 berkorespoden dengan cipherteks 1743, maka kriptanalis dapat mencari X dengan mudah karena X merupakan blok cipher sebelum 1743.

Dalam implementasi, kesalahan enkripsi terhadap satu blok plainteks akan menyebabkan kesalahan terhadap cipherteks yang bersangkutan dan satu blok cipherteks sesudahnya.

4. PENGEMBANGAN LEBIH LANJUT

Kedua mode tersebut dapat dikembangkan lebih lanjut. Beberapa pengembangan yang dapat dilakukan adalah:

1. Menggunakan *initialization vektor* dalam enkripsi blok pertama.
2. Kedua mode di atas dapat dikombinasikan sehingga chiper akan semakin rumit untuk dianalisis.

5. KESIMPULAN

Sebagaimana diketahui, dalam kasus-kasus tertentu chosen-plainteks attack dapat memungkinkan kriptanalis menemukan kunci RSA. Namun, kemungkinan tersebut dapat diperkecil dengan memperumit criptosystem RSA. Dengan beberapa mode enkripsi yang penulis usulkan pada makalah ini, chosen-plaintext attack akan semakin sulit untuk dilakukan dan para kriptanalis akan semakin sulit dalam mengumpulkan informasi terkait plaintext.

Kedua mode enkripsi ini memiliki kelemahan jika diimplementasikan dalam saluran komunikasi kunci publik. Untuk mode pertama, kesalahan pada operasi $\oplus$ pada suatu blok akan menyebabkan kesalahan cipherteks yang bersangkutan dan seluruh cipherteks sesudahnya. Untuk mode kedua, kesalahan enkripsi pada satu blok akan mengakibatkan kesalahan pada blok tersebut dan satu blok sesudahnya.

Mode enkripsi pada cryptosystem RSA yang penulis usulkan pada makalah ini hanyalah sebagian kecil dari berbagai mode yang dapat ditemukan.

DAFTAR REFERENSI

[1] Munir, Rinaldi, “Diktat Kuliah IF5054 Kriptografi”, Institut Teknologi Bandung, 2006.

[2] Hapsari, Anggun Dkk, “Teknik-teknik Kriptanalisis”, Departemen Teknik Informatika Institut Teknologi Bandung, 2002.