ALGORITMA ELGAMAL DALAM PENGAMANAN PESAN RAHASIA

Danang Tri Massandy - 13508051

Program Studi Teknik Informatika
Sekolah Teknik Elektro dan Informatika
Institut Teknologi Bandung
e-mail: if18051@students.if.itb.ac.id

ABSTRAK

Makalah ini membahas tentang pengamanan pesan rahasia dengan menggunakan salah satu algoritma Kryptografi, yaitu algoritma ElGamal. Tingkat keamanan algoritma ini didasarkan atas masalah logaritma diskrit pada grup pergandaan bilangan bulat modulo prima. Algoritma ini termasuk algoritma kriptografi asimetris yang menggunakan dua jenis kunci, yaitu kunci publik dan kunci rahasia. Algoritma Elgamal mempunyai kunci public berupa tiga pasang bilangan dan kunci rahasia berupa satu bilangan. Algoritma in melakukan proses enkripsi dan dekripsi pada blok-blok plainteks dan dihasilkan blok-blok cipherteks yang masing-masing terdiri dari dua pasang bilangan. Pada makalah ini membahas tentang penggunaan algoritma ElGamal dalam proses enkripsi dan dekripsi.

Kata kunci: algoritma, cipher blok, ElGamal, kriptografi, kunci public.

1. PENDAHULUAN

Dewasa ini, perkembangan teknologi yang maju membawa dampak pada hamper seluruh aspek kehidupan manusia, seperti dalam hal komunikasi dengan orang lain. Media-media komunikasi bermunculan, seperti telepon genggam dan sampai ke internet yang dapat menghubungkan kita dengan setiap orang dimanapun dia berada. Namun, lalu lintas informasi yang beredar baik dalam media telepon ataupun internet tidaklah terjamin keamanannya. media komunikasi umum yang dapat digunakan oleh siapapun sehingga sangat rawan terhadap penyadapan informasi oleh pihak-pihak yang tidak berhak mengetahui informasi tersebut. Oleh karena penggunaan internet yang sangat luas seperti pada bisnis, perdagangan, bank, industri dan pemerintahan yang umumnya mengandung informasi yang bersifat rahasia maka keamanan informasi menjadi faktor utama yang harus dipenuhi. Berbagai hal telah dilakukan untuk mendapatkan jaminan keamanan informasi rahasia ini. Salah satu cara yang digunakan adalah dengan menyandikan isi informasi menjadi suatu kode-kode yang tidak dimengerti sehingga apabila disadap maka akan kesulitan untuk mengetahui isi informasi yang sebenarnya.

Untuk itulah diperlukan ilmu kriptografi, yang mempelajari teknik-teknik menyandikan suatu pesan dengan algoritma-algoritma tertentu. Pada dasarnya ada dua metode algoritma, yaitu algoritma rahasia dan algoritma kunci. Metode algoritma rahasia adalah algoritma yang pertama kali dibuat, akan tetapi metode ini tidak efisien untuk digunakan dalam berkomunikasi. Sedangkan, metode algoritma kunci diciptakan setelah penggunaan metode algoritma rahasia yang dirasa tidak efisien untuk digunakan lagi. Metode ini tidak menumpukan keamanan pada algoritmanya, tetapi pada kerahasiaan kunci yang digunakan pada proses penyandian. Metode algoritma kunci mempunyai tingkat efisiensi dan keamanan yang lebih baik dibandingkan dengan algoritma rahasia. Sampai sekarang algoritma kunci masih digunakan secara luas di internet dan terus dikembangkan untuk mendapatkan keamanan yang lebih baik.

Algoritma ElGamal merupakan salah satu dari algoritma kunci. Algoritma ini dikembangkan pertama kali oleh Taher ElGamal pada tahun 1985. Sampai saat ini, algoritma ElGamal masih dipercaya sebagai metode penyandian, seperti aplikasi PGP dan GnuPG yang dapat digunakan untuk pengamanan e-mail dan tanda tangan digital. Pada tahun 1994 pemerintah Amerika Serikat mengadopsi *Digital Signature Standard*, sebuah mekanisme penyandian yang berdasar pada algoritma ElGamal.

2. KRIPTOGRAFI

Kriptografi (*cryptography*) berasal dari bahasa Yunani, terdiri dari dua suku kata yaitu kripto dan graphia. Kripto artinya menyembunyikan, sedangkan graphia artinya tulisan. Kriptografi adalah ilmu yang mempelajari teknik-teknik matematika yang berhubungan dengan aspek keamanan informasi, seperti kerahasiaan data, keabsahan data, integritas data, serta autentikasi data. Tetapi tidak semua aspek keamanan informasi dapat diselesaikan dengan kriptografi. Kriptografi dapat pula diartikan sebagai ilmu atau seni untuk menjaga keamanan pesan. Ketika suatu pesan dikirim dari suatu tempat ke tempat

lain, isi pesan tersebut mungkin dapat disadap oleh pihak lain yang tidak berhak untuk mengetahui isi pesan tersebut. Untuk menjaga pesan, maka pesan tersebut dapat diubah menjadi suatu kode yang tidak dapat dimengerti oleh pihak lain.

Enkripsi adalah sebuah proses penyandian yang melakukan perubahan sebuah kode (pesan) dari yang bisa dimengerti (plainteks) menjadi sebuah kode yang tidak bisa dimengerti (cipherteks). Sedangkan proses kebalikannya untuk mengubah cipherteks menjadi plainteks disebut dekripsi. Proses enkripsi dan dekripsi memerlukan suatu mekanisme dan kunci tertentu.

Kriptoanalisis (*cryptanalysis*) adalah kebalikan dari kriptografi, yaitu suatu ilmu untuk memecahkan mekanisme kriptografi dengan cara mendapatkan kunci dari cipherteks yang digunakan untuk mendapatkan plainteks. Kriptologi (*cryptology*) adalah ilmu yang mencakup kriptografi dan kriptoanalisis.

Ada empat tujuan mendasar dari kriptografi yang juga merupakan aspek keamanan informasi, yaitu

1. *Kerahasiaan*, adalah aspek yang berhubungan dengan penjagaan isi informasi dari siapapun kecuali yang memiliki otoritas atau kunci rahasia untuk membuka informasi yang telah dienkripsi.
2. *Integritas data*, adalah aspek yang berhubungan dengan penjagaan dari perubahan data secara tidak sah. Untuk menjaga integritas data, sistem harus memiliki kemampuan untuk mendeteksi manipulasi data oleh pihak-pihak yang tidak berhak, antara lain penyisipan, penghapusan, dan pensubsitusian data lain kedalam data yang sebenarnya.
3. *Autentikasi*, adalah aspek yang berhubungan dengan identifikasi atau pengenalan, baik secara kesatuan sistem maupun informasi itu sendiri. Dua pihak yang saling berkomunikasi harus saling memperkenalkan diri. Informasi yang dikirimkan harus diautentikasi keaslian, isi datanya, waktu pengiriman, dan lain-lain.
4. *Non-repudiation* (menolak penyangkalan), adalah usaha untuk mencegah terjadinya penyangkalan terhadap pengiriman suatu informasi oleh yang mengirimkan, atau harus dapat membuktikan bahwa suatu pesan berasal dari seseorang, apabila ia menyangkal mengirim informasi tersebut.

3. ALGORITMA KRIPTOGRAFI

Menurut Bruce Schneier, *Algoritma kriptografi* atau sering disebut dengan *cipher* adalah suatu fungsi matematis yang digunakan untuk melakukan enkripsi dan dekripsi. Ada dua macam algoritma kriptografi, yaitu *algoritma simetris* (*symmetric algorithms*) dan *algoritma asimetris* (*asymmetric algorithms*).

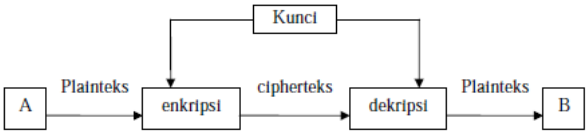
3.1 Algoritma Simetris

Algoritma simetris adalah algoritma kriptografi yang menggunakan kunci enkripsi yang sama dengan kunci dekripsinya. Algoritma ini mengharuskan pengirim dan penerima menyetujui suatu kunci tertentu sebelum mereka saling berkomunikasi. Keamanan algoritma simetris tergantung pada kunci, membocorkan kunci berarti bahwa orang lain dapat mengenkripsi dan mendekripsi pesan. Agar komunikasi tetap aman, kunci harus tetap dirahasiakan.

Sifat kunci yang seperti ini membuat pengirim harus selalu memastikan bahwa jalur yang digunakan dalam pendistribusian kunci adalah jalur yang aman atau memastikan bahwa seseorang yang ditunjuk membawa kunci untuk dipertukarkan adalah orang yang dapat dipercaya. Masalahnya akan menjadi rumit apabila komunikasi dilakukan secara bersama-sama oleh sebanyak n pengguna dan setiap dua pihak yang melakukan pertukaran kunci, maka akan terdapat sebanyak

$$C_2^n = \frac{n!}{(n-2)!\,.2!} = \frac{n.(n-1)}{2}$$

kunci rahasia yang harus dipertukarkan secara aman.

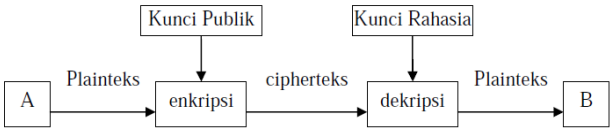


Gambar 1. Skema Algoritma Simetris

3.2 Algoritma Asimetris

Algoritma asimetris, sering juga disebut dengan *algoritma kunci publik*, menggunakan dua jenis kunci, yaitu *kunci publik* (*public key*) dan *kunci rahasia* (*secret key*). Kunci publik merupakan kunci yang digunakan untuk mengenkripsi pesan. Sedangkan kunci rahasia digunakan untuk mendekripsi pesan.

Kunci publik bersifat umum, artinya kunci ini tidak dirahasiakan sehingga dapat dilihat oleh siapa saja. Sedangkan kunci rahasia adalah kunci yang dirahasiakan dan hanya orang-orang tertentu saja yang boleh mengetahuinya. Keuntungan utama dari algoritma ini adalah memberikan jaminan keamanan kepada siapa saja yang melakukan pertukaran informasi meskipun di antara mereka tidak ada kesepakatan mengenai keamanan pesan terlebih dahulu maupun saling tidak mengenal satu sama lainnya.



Gambar 2. Skema Algoritma Asimetris

Contoh dari algoritma asimetris adalah RSA, ElGamal, McEliece, LUC dan DSA (*Digital Signature Algorithm*).

Dalam melakukan proses enkripsi, sering digunakan plainteks berupa data ataupun pesan yang besar, sehingga membutuhkan waktu yang lama apabila dilakukan proses sekaligus pada plainteks tersebut. Oleh karena itu, plainteks dapat dipotong-potong menjadi beberapa blok-blok yang sama panjang. Kemudian dari blok-blok yang diperoleh tersebut dilakukan proses enkripsi, dan hasil cipherteksnya dapat didekripsi dan digabungkan kembali menjadi plainteks. Algoritma kriptografi yang menggunakan mekanisme seperti ini disebut dengan cipher blok (*block cipher*).

4. ALGORITMA ELGAMAL

Algoritma ElGamal merupakan algoritma kriptografi asimetris. Pertama kali dipublikasikan oleh Taher ElGamal pada tahun 1985. Algoritma ini didasarkan atas masalah logaritma diskret pada grup $\mathbb{Z}_P$*. Algoritma ElGamal terdiri dari tiga proses, yaitu proses pembentukan kunci, proses enkripsi dan proses dekripsi. Algoritma ini merupakan cipher blok, yaitu melakukan proses enkripsi pada blok-blok plainteks dan menghasilkan blok-blok cipherteks yang kemudian dilakukan proses dekripsi, dan hasilnya digabungkan kembali menjadi pesan yang utuh dan dapat dimengerti. Untuk membentuk sistem kriptografi ElGamal, dibutuhkan bilangan prima p dan elemen primitif grup $\mathbb{Z}_P$*.

Untuk lebih jelasnya mengenai algoritma ElGamal, berikut ini diberikan suatu sistem kriptografi ElGamal, yaitu sistem kriptografi yang menggunakan algoritma ElGamal, definisi himpunan-himpunan plainteks, cipherteks dan kunci, serta proses enkripsi dan dekripsi, seperti diberikan pada gambar berikut ini.

Diberikan bilangan prima p dan sebuah elemen primitif $\alpha \in \mathbb{Z}_p^*$. Ditentukan $\mathcal{P} = \mathbb{Z}_p^*$, $\mathcal{C} = \mathbb{Z}_p^* \times \mathbb{Z}_p^*$ dan $a \in \{0,1,\ldots, p-2\}$. Didefinisikan

$$\mathcal{K} = \{(p,\alpha,a,\beta) : \beta = \alpha^a \bmod p\}.$$

Nilai p, α, dan β dipublikasikan, dan nilai a dirahasiakan.

Untuk $K = (p,\alpha,a,\beta)$, plainteks $m \in \mathbb{Z}_p^*$ dan untuk suatu bilangan acak rahasia $k \in \{0,1,2,\ldots, p-2\}$, didefinisikan

$$e_K(m,k) = (\gamma,\delta)$$

dengan

$$\gamma = \alpha^k \bmod p.$$

dan

$$\delta = \beta^k . m \bmod p.$$

Untuk $\gamma, \delta \in \mathbb{Z}_p^*$, didefinisikan

$$d_K(\gamma,\delta) = \delta.(\gamma^a)^{-1} \bmod p.$$

Gambar 3. Sistem Kriptografi ElGamal pada Z_p*

4. 1 Proses Pembentukan Kunci

Proses pertama adalah pembentukan kunci yang terdiri dari kunci rahasia dan kunci publik. Pada proses ini dibutuhkan sebuah bilangan prima p yang digunakan untuk membentuk grup $\mathbb{Z}_P$*, elemen primitif α dan sebarang $a \in \{0,1,\ldots, p-2\}$. Kunci publik algoritma ElGamal berupa pasangan 3 bilangan, yaitu (p, α, β), dengan

$$\beta = \alpha^a mod\ p \qquad (1)$$

Sedangkan kunci rahasianya adalah bilangan a tersebut.

Karena pada algoritma ElGamal menggunakan bilangan bulat dalam proses perhitungannya, maka pesan harus dikonversi ke dalam suatu bilangan bulat. Untuk mengubah pesan menjadi bilangan bulat, digunakan kode ASCII (*American Standard for Information Interchange*). Kode ASCII merupakan representasi numerik dari karakter-karakter yang digunakan pada komputer, serta mempunyai nilai minimal 0 dan maksimal 255. Oleh karena itu, berdasarkan sistem kriptografi ElGamal di atas maka harus digunakan bilangan prima yang lebih besar dari 255. Kode ASCII berkorespondensi 1-1 dengan karakter pesan.

Berikut ini diberikan suatu algoritma yang dapat digunakan untuk melakukan pembentukan kunci.

Algoritma Pembentukan Kunci

Input : Bilangan prima aman $p > 255$ dan elemen primitif $a \in \mathbb{Z}_P$*.
Output : Kunci publik (p, α, β) dan kunci rahasia *a*.

Langkah :

1. Pilih $a \in \{0,1,..., p-2\}$.
2. Hitung $\beta = \alpha^a mod\ p$.
3. Publikasikan nilai *p*, α, dan β , serta rahasiakan nilai *a*.

Pihak yang membuat kunci publik dan kunci rahasia adalah penerima, sedangkan pihak pengirim hanya mengetahui kunci publik yang diberikan oleh penerima, dan kunci publik tersebut digunakan untuk mengenkripsi pesan. Jadi, kentungan menggunakan algoritma kriptografi kunci publik adalah tidak ada permasalahan pada distribusi kunci apabila jumlah pengirim sangat banyak serta tidak ada kepastian keamanan jalur yang digunakan.

4.2. Proses Enkripsi

Pada proses ini pesan dienkripsi menggunakan kunci publik (*p*, a, b) dan sebarang bilangan acak rahasia *k* ϵ {0, 1, ..., *p*-2}. Misalkan *m* adalah pesan yang akan dikirim. Selanjutnya, *m* diubah ke dalam blok-blok karakter dan setiap karakter dikonversikan ke dalam kode ASCII, sehingga diperoleh plainteks m_1, m_2, ..., m_n dengan m_i ϵ {1, 2,..., p-1}, *i* =1, 2,..., *n* . Untuk nilai ASCII bilangan 0 digunakan untuk menandai akhir dari suatu teks.

Proses enkripsi pada algoritma ElGamal dilakukan dengan menghitung

$$\gamma = \alpha^k mod\ p \qquad (2)$$

dan

$$\delta = \beta^k . m\ mod\ p \qquad (3)$$

dengan rahasia *k* ϵ {0, 1, ..., *p*-2} acak. Diperoleh cipherteks (γ, δ).

Bilangan acak *k* ditentukan oleh pihak pengirim dan harus dirahasiakan, jadi hanya pengirim saja yang mengetahuinya, tetapi nilai *k* hanya digunakan saat melakukan enkripsi saja dan tidak perlu disimpan. Berikut adalah algoritma enkripsi.

Algoritma Enkripsi

Input : Pesan yang akan dienkripsi dan kunci publik (p, α, β).
Output : Chiperteks (γ_i, δ_i), *i* = 1, 2, …, n.

Langkah :

1. Pesan dipotong-potong ke dalam bentuk blok-blok pesan dengan setiap blok adalah satu karakter pesan.
2. Konversikan masing-masing karakter ke dalam kode ASCII, maka diperoleh plainteks sebanyak *n* bilangan, yaitu m_1, m_2, ..., m_n.
3. Untuk *i* dari 1 sampai *n* kerjakan :
   3.1. Pilih sebarang bilangan acak rahasia $k_i \in \{0,1,..., p-2\}$.
   3.2. Hitung $\gamma = \alpha^k mod\ p$.
   3.3. Hitung $\delta = \beta^k . m\ mod\ p$.
4. Diperoleh cipherteks yaitu (γ, δ), *i* = 1, 2, 3, .., n.

Salah satu kelebihan algoritma ElGamal adalah bahwa suatu plainteks yang sama akan dienkripsi menjadi cipherteks yang berbeda-beda. Hal ini dikarenakan pemilihan bilangan *k* yang acak. Akan tetapi, walaupun cipherteks yang diperoleh berbeda-beda, tetapi pada proses dekripsi akan diperoleh plainteks yang sama.

4.3. Proses Dekripsi

Setelah menerima cipherteks (γ, δ), proses selanjutnya adalah mendekripsi cipherteks menggunakan kunci publik *p* dan kunci rahasia *a*. Dapat ditunjukkan bahwa plainteks *m* dapat diperoleh dari cipherteks menggunakan kunci rahasia *a*.

Diberikan (p, α, β) sebagai kunci publik dan a sebagai kunci rahasia pada algoritma ElGamal. Jika diberikan cipherteks (γ, δ), maka

$$m = \delta . (\gamma^a)^{-1} mod\ p \qquad (4)$$

dengan *m* adalah plainteks.

Karena $\mathbb{Z}_p^*$ merupakan grup siklik yang mempunyai order *p* -1 dan *a* ϵ {0,1,..., *p* - 2}, maka $(\gamma^a)^{-1} = \gamma^{-a} = \gamma^{p-1-a}\ mod\ p$.

Algoritma Deskripsi

Input : Chiperteks (γ_i, δ_i), *i* = 1, 2, …, n, kunci publik p dan kunci rahasia a.
Output : Pesan asli.

Langkah :

1. Untuk *i* dari 1 sampai *n* kerjakan :
   1.1. Hitung $\gamma^{p-1-a}\ mod\ p$
   1.2. Hitung $m_i = \delta . (\gamma^a)^{-1} mod\ p$
2. Diperoleh plainteks m_1, m_2, ..., m_n.
3. Konversikan masing-masing bilangan m_1, m_2, ..., m_n ke dalam karakter sesuai dengan kode ASCII-nya, kemudian hasilnya digabungkan kembali.

5. CONTOH KASUS PENGGUNAAN ALGORITMA ELGAMAL DALAM MENGIRIM PESAN RAHASIA

Pada suatu hari, Irdham akan berkomunikasi tentang lokasi transaksi jual beli barang dagangannya kepada Andi yang hanya mengetahui lokasi tersebut. Akan tetapi, pesan

itu harus rahasia dan dienkripsi. Pesan itu berbunyi "kampus".

Prosesnya adalah sebagai berikut,

1. Pembentukan kunci
   Irdham harus membuat kunci publik, misalkan dipilih bilangan prima aman, p = 2579 dan elemen primitive α = 2. Selanjutnya dipilih a = 765 dan dihitung,
   $$\beta = 2^{765} mod\ 2579 = 949$$
   Diperoleh kunci publik (p, α, β)=(2579,2,949) dan kunci rahasia a = 765. Irdham memberikan kunci publik ini kepada Andi. Sementara kunci rahasia tetap dipegang oleh Irdham.
2. Andi memperoleh kunci publik (p, α, β) = (2579,2,949). Dan Andi kemudian akan mengenkripsi pesan rahasia yang akan dikirimkannya. Sebelumnya, pesan itu diterjemahkan dalam kode ASCII, seperti pada tabel di bawah ini

Tabel 1 Konversi Pesan ke dalam Kode ASCII

i	Karakter	Plainteks m_i	ASCII
1	k	m_1	107
2	a	m_2	97
3	m	m_3	109
4	p	m_4	112
5	u	m_5	117
6	s	m_6	115

3. Proses selanjutnya, adalah menentukan bilangan acak rahasia k_i ϵ {0,1,…,2577}, i = 1, 2, …, 30. Kemudian dihitung, $\gamma = 2^{k_i} mod\ 2579$ dan $\delta = 949^{k_i}.m_i\ mod\ 2579$. Hasil enkripsi seperti tabel di bawah ini

Tabel 2 Proses Enkripsi

i	m_i	k_i	$\gamma = 2^{k_i} mod\ 2579$	$\delta = 949^{k_i}.m_i\ mod\ 2579$
1	107	766	1898	342
2	97	2298	520	1516
3	109	146	22	359
4	112	2483	1742	830
5	117	702	1052	1302
6	115	988	21253	2087

Berdasarkan tabel 2, diperoleh cipherteks $(\gamma_i,\ \delta_i)$, i = 1, 2, …, 6 sebagai berikut,

(1898, 342) (520, 1516)
(22, 359) (1742, 830)
(1052, 1302) (2153, 2087)

4. Kemudian cipherteks itu dikirimkan oleh Andi kepada Irdham. Saat diterima, Irdham harus mendekripsikan cipherteks tersebut agar dapat dibaca. Irdham mempunyai kunci publik p = 2579 dan kunci rahasia a = 765 untuk mendekripsikan cipherteks tersebut sesuai dengan algoritma dekripsi.

Tabel 3 Proses Dekripsi

i	$(\gamma_i,\ \delta_i)$	${\gamma_i}^{1813}\ mod\ 2579$	$m_i = \delta_i.{\gamma_i}^{1813} mod\ 2579$	Huruf
1	(1898, 342)	219	107	k
2	(520, 1516)	1771	97	a
3	(22, 359)	1825	109	m
4	(1742, 830)	286	112	p
5	(1052, 1302)	422	117	u
6	(2153, 2087)	655	115	s

Jadi, pesan rahasia yang dikirimkan Andi berbunyi, "kampus".

6. KESIMPULAN

Algoritma kriptografi asimetris, seperti algoritma ElGamal mempunyai kemampuan yang baik dalam mengatasi masalah distribusi kunci. Algoritma ini terdiri dari tiga proses, yaitu proses pembentukan kunci, proses enkrispsi, dan proses dekripsi. Saat pembentukan kunci, sang penerima pesan membuat kunci publik yang tetap dipegangnya dan kunci rahasia yang diserahkan pada sang pembuat pesan. Kemudian, pesan yang akan dikirim oleh sang pembuat pesan mengenkripsi pesannya dengan kunci publik yang diterimanya. Pesan itu sebelumnya harus dikonversikan dalam kode ASCII terlebih dahulu karena algoritma ElGamal menggunakan bilangan bulat dalam perhitungannya. Pesan yang dienkripsi tersebut kemudian dikirimkan kepada sang penerima pesan yang mempunyai kunci rahasia untuk mendekripsikan pesan yang telah dienkripsi tersebut. Pada dasarnya, dari proses pembentukan kunci sampai proses dekripsi ini, digunakan aritmatika modulo.

Kelebihan dari algoritma ElGamal adalah proses enkripsi pada plainteks yang sama diperoleh cipherteks yang berbeda-beda, namun pada proses dekripsi diperoleh plainteks yang sama.

REFERENSI

[1] Wikipedia, 2009, *Cryptography*, http://en.wikipedia.org/wiki/Cryptography , 19 Desember 2009, 13:12.

[2] _____, 2009, *ElGamal Encryption*, http://en.wikipedia.org/wiki/ElGamal_encryption , 19 Desember 2009, 13:20.

[3] _____, 2009, *Public Key Cryptography*, http://en.wikipedia.org/wiki/Public-key_cryptography , 19 Desember 2009, 13:40.