PEMBAIKAN SISTEM KRIPTOGRAFI MULTI RSA

MUHAMAD GHAZALI BIN KAMARDAN

UNIVERSITI KEBANGSAAN MALAYSIA

PENGAKUAN

Saya akui karya ini adalah hasil kerja saya sendiri kecuali nukilan dan ringkasan yang tiap-tiap satunya telah saya jelaskan sumbernya.

5 Mei 2005

MUHAMAD GHAZALI BIN KAMARDAN
P28318

PENGHARGAAN

Bismillahirahmanirrahim,

Alhamdulillah, saya bersyukur ke hadrat ilahi kerana dengan limpah kurnia dan petunjuk daripadanya, kajian ilmiah saya ini dapat diselesaikan walaupun masih terdapat banyak kekurangan dan kelemahannya.

Jutaan perhargaan dan terima kasih yang teramat sangat saya ucapkan kepada penyelia saya, Dr. Eddie Shahril bin Ismail yang telah banyak memberi tunjuk ajar yang tidak ternilai harganya sehingga kajian ini dapat disempurnakan.

Begitu juga kepada semua pensyarah dan rakan-rakan yang terlibat secara langsung atau tidak langsung dalam kajian ini. Tidak lupa buat semua warga Pusat Pengajian Matematik, Fakulti Sains dan Teknologi, UKM yang banyak menghulurkan bantuan menjayakan kajian ini terutama sekali juruteknik En. Effendi dan En. Jamal. Tanpa anda semua tidak mungkin projek dapat dijayakan.

Teristimewa buat keluarga tersayang terutama ibu saya, isteri dan anak serta ahli keluarga yang banyak berdoa serta memberi bantuan, sokongan dan dorongan.

Jasa kalian amat besar nilainya dan tidak dapat saya lupakan.

Sekian, terima kasih.

MUHAMAD GHAZALI BIN KAMARDAN
UKM, BANGI.

ABSTRAK

Kajian ini mencadangkan satu pembaikan sistem kriptografi Multi RSA. Sistem ini tidak memerlukan seorang Ketua Sistem (KS), maka kita tidak perlu risau kejujuran KS. Sistem ini juga dibina berdasarkan modulo RSA yang berasingan untuk setiap kunci pelanggan. Oleh itu, setiap kunci rahsia pelanggan adalah terpisahkan. Sistem ini dijangka dapat mempertahankan keselamatannya daripada sebarang bentuk serangan musuh. Sistem ini juga mempunyai kelebihan seperti bersifat lebih fleksibel dan mudah digunakan. Adalah diharapkan supaya sistem ini menjadi titik mula kepada pembinaan sistem yang lebih efisien dan selamat.

IMPROVEMENT ON THE MULTI RSA CRYPTOGRAPHY SYSTEM

ABSTRACT

This research is proposing an improvement on multi RSA cryptography system. This system doesn't need any dealer, therefore we do not worry about the honesty of the dealer. This system is built on different RSA modulo for the keys of every player. Thus, every secret key is separated. This system is expected to retain its invulnerability from any attacks. This system also has some advantages such as its flexibility and it is easier to be used. It is hoped that this will be a starting point to the development of more efficient and safe systems.

KANDUNGAN

Halaman

SENARAI JADUAL

SENARAI RAJAH

SENARAI SIMBOL

$\prod$	hasil darab
(a,b)	faktor sepunya terbesar
$a = b \pmod{n}$	kongruen
$\phi(n)$	fungsi phi Euler
M	maklumat asli
C	maklumat tersembunyi
S	tandatangan
e	kunci enkripsi
d	kunci dekripsi
$E\ (e, M)$	transformasi enkripsi
$D\ (d, C)$	transformasi dekripsi
$S\ (d, M)$	transformasi tandatangan
$P\_(e, S)$	transformasi pengesahan

BAB I

PENGENALAN

1.1 PENGENALAN

Kriptografi adalah satu bidang untuk merekacipta suatu sistem yang dapat mengubah suatu maklumat asal menjadi satu maklumat tersembunyi kecuali oleh pengirim dan penerima sahaja. Sistem yang menggunakan kaedah kriptografi dinamakan sebagai sistem kriptografi (Buchmann 2000).

Suatu sistem kriptografi yang baik bukan sahaja dapat berfungsi dengan baik tetapi juga cekap dan selamat. Cekap bermakna mudah digunakan manakala selamat bermakna maklumatnya tidak dapat diketahui atau dibongkar oleh pihak ketiga. Pihak ketiga juga dikenali sebagai penyerang sistem. Penyerang bermaksud individu yang membuat analisis untuk memecahkan maklumat tersembunyi tersebut (Buchmann 2000).

Sistem kriptografi telah digunakan sejak zaman dahulu lagi terutama dalam bidang diplomasi dan ketenteraan. Julius Ceaser, seorang penakluk Rom, misalnya telah menghantar maklumat kepada tenteranya menggunakan suatu sistem kriptografi yang dipanggil sebagai sistem kriptografi satu abjad atau sistem monogafi. Tujuan beliau berbuat demikian adalah kerana beliau tidak mempercayai pembawa maklumat beliau yang mungkin membocorkannya kepada pihak musuh. Bagaimanapun sistem tersebut didapati tidak kebal kepada penyerang. Penyerang dapat memecahkan sistem kriptografi ini berdasarkan kepada kekerapan muncul huruf-huruf dalam maklumat tersembunyi (Rosen 1992).

Hill (1931) memperkenalkan sistem kriptografi blok atau sistem poligrafi untuk mengatasi masalah ini. Walau bagaimanapun sistem ini juga mudah ditembusi oleh seorang penyerang. Ini kerana kunci untuk menukar maklumat asli kepada maklumat tersembunyi dan kunci untuk menukarkan maklumat tersembunyi kembali kepada maklumat asli mempunyai satu perhubungan modulo linear. Maka penyerang akan dapat mencari kunci dekripsi sekiranya beliau mengetahui kunci enkripsi (Rosen 1992).

Diffie dan Hellman (1976) telah memperkenalkan konsep sistem kriptografi tidak simetri atau lebih dikenali sebagai sistem kriptografi kunci awam. Dalam sistem ini kunci enkripsi diumumkan kepada awam kerana kunci enskripsi dan kunci dekripsi adalah terasing. Oleh itu, tidak mudah untuk penyerang mendapatkan kunci dekripsi daripada kunci enskripsi.

Rivest, Shamir dan Adleman (1978) telah memperkenalkan suatu sistem kunci awam yang dinamakan sistem RSA. Sistem ini adalah berasaskan kepada pengguaan dua nombor perdana yang berbeza dan bersaiz besar. Sistem ini juga merupakan sistem kriptografi yang pertama memperkenalkan skema tandatangan digital. Tandatangan digital telah membuka satu dimensi baru kepada perkembangan pesat komunikasi elektronik. Tandatangan digital digunakan dengan meluas dalam pelbagai bidang yang menggunakan media elektronik, seperti perbankan elektronik, sistem kawalan keselamatan, kewangan elektronik dan hakcipta (Buchmann 1992).

Shamir (1979) pula memperkenalkan teori berkongsi rahsia. Skema berkongsi rahsia beliau adalah berasaskan kepada persamaan polinomial. Skema ini bersesuaian dengan keperluan kebanyakan organisasi yang memerlukan satu sistem kriptografi secara berkumpulan. Tujuan kriptografi berkumpulan adalah untuk menurunkan kesenangan melakukan dekripsi maklumat tersembunyi dan menambah halangan kepada penyerang. Sistem kriptografi awam berkumpulan sangat penting tetapi sukar untuk dihasilkan. Beberapa kajian telah dilakukan sehingga kini dan banyak sistem sebegini telah dibangun. Malangnya kebanyakan sistem-sistem yang telah dibangunkan ini mempunyai beberapa

kelemahan yang tertentu. Kami akan membentangkan kajian-kajian tersebut di dalam bahagian yang seterusnya.

1.2 KAJIAN-KAJIAN LEPAS

Dalam bahagian ini kami akan membentangkan beberapa kajian berkenaan sistem kriptografi berkumpulan RSA sekitar tahun 1995 sehingga tahun 2005.

Frankel, MacKenzie & Yung (1995) mencadangkan satu kaedah sistem kriptografi RSA berkumpulan. Dalam sistem ini seseorang perlu dilantik untuk menjana kunci rahsia dan kunci awam bagi setiap pelanggan. Penjana kunci ini dikenali sebagai ketua sistem (KS). Masalah yang dihadapi dalam sistem ini adalah untuk mendapatkan seorang KS yang jujur dan boleh dipercayai. Namun mereka berjaya mencipta sistem yang kebal daripada KS yang tidak jujur. Walau bagaimanapun sistem mereka didapati tidak cekap dan sukar digunakan.

Boneh dan Franklin (1997) mencadangkan suatu protokol untuk berkongsi modulus RSA. Sistem yang dicadangkan oleh mereka adalah lebih cekap daripada kaedah Frankel et. al (1995). Bagaimanapun protokol ini tidak dapat menjanakan suatu modulus yang selamat.

Poupard dan Stern (1998) pula mencadangkan suatu protokol sistem kriptografi RSA yang menjanakan modulus perkongsian untuk dua individu. Kemudian Gilboa (1999) telah memperluaskan protokol Poupard dan Stern (1998). Walau bagaimanapun, didapati sistem ini tidak cekap seperti sistem yang dicadangkan oleh Boneh dan Franklin (1997).

Shoup (2000) menganjurkan skema tandatangan RSA berkumpulan yang praktikal. Skema ini memerlukan satu modulus RSA (nombor perdana) yang selamat. Skema tandatangan RSA ini mempunyai beberapa ciri-ciri yang menarik. Pertamanya, skema ini adalah selamat dan kebal dalam model rawak, dengan mengandaikan

penyelesaian kepada masalah RSA adalah sukar. Keduanya, gabungan tandatangan tiada perhubungan langsung dengan pengesahannya dan akhir sekali, saiz tandatangan setiap individu yang digabungkan adalah terbatas oleh satu pemalar yang didarabkan dengan saiz modulus RSA. Bagaimanapun sistem ini memerlukan seorang KS untuk menjanakan kunci di antara penggunanya.

How, Yahya dan Eddie. (2001) mencadangkan suatu sistem kriptografi multi RSA yang setiap pengguna mempunyai kunci dalam modulo yang sama. Sistem ini juga memerlukan seorang KS untuk menjana kunci-kunci setiap pengguna. Sistem ini juga mempunyai beberapa kelemahan. Kami akan bentangkan kelemahan sistem ini dalam Bab IV nanti.

Damgård dan Koprowski (2001) pula mengasingkan protokol RSA bagi penjanaan kunci-kunci pengguna daripada protokol tandatangan dan dekripsi. Hal yang sama dilakukan oleh Fouque dan Stern (2001) dengan meletakkan satu andaian piawai. Ini dapat mengelakkan daripada perkongsian kunci-kunci di dalam modulo yang sama.

Kawauchi dan Tada (2003) pula mencadangkan satu skema tandatangan RSA yang lain yang juga menggunakan konsep pengasingan. Damgård dan Dupont (2005) telah membentangkan suatu tandatangan RSA berkumpulan yang cekap tanpa perlu sebarang andaian tentang keselamatannya. Jarecki dan Saxena (2005) pula membentangkan suatu tandatangan RSA yang lebih mudah dan ringkas.

1.3 SKOP KAJIAN

Kajian kami adalah untuk merekacipta suatu sistem kriptografi multi RSA. Kami mencadangkan kaedah menjanakan kunci pengguna dengan menggunakan modulo RSA yang berasingan. Kemudian kami cadangkan satu skema untuk membina maklumat tersembunyi oleh pengirim dan kaedah untuk dekripsi maklumat tersebut secara berkumpulan oleh penerima. Kami juga akan membentangkan kaedah untuk

menandatangani tandatangan digital secara berkumpulan dan prosedur penerima untuk mengesahkan kebenaran tandatangan tersebut.

Bagi sistem penghantaran maklumat tersembunyi, kajian kami mengambil kira kefleksibelan bilangan penerima dan individu yang sepatutnya menerima maklumat. Dalam keadaan tertentu sesuatu maklumat perlu dihantar kepada beberapa individu tertentu. Sebagai contohnya, maklumat perlu dihantar kepada satu unit dalam sebuah organisasi. Sebagai langkah keselamatan, unit-unit dalam organisasi tersebut telah menetapkan individu yang terlibat dalam proses dekripsi. Bilangan individu untuk proses dekripsi mungkin berbeza di antara unit-unit yang berlainan. Oleh itu, kita perlu satu sistem maklumat tersembunyi yang hanya membenarkan individu-individu ini untuk melakukan dekripsi.

Skema tandatangan digital yang kami cadangkan juga mempunyai beberapa kelebihan. Bilangan penandatangan untuk sesuatu tugasan biasa mungkin telah ditetapkan oleh organisasi tetapi untuk sesuatu tugasan khas, organisasi mungkin akan menetapkan bilangan individu yang berlainan. Oleh itu, skema tandatangan digital yang dapat disesuaikan bilangan penandatangan adalah amat perlu kepada organisasi sebegini. Penerima perlu mengetahui individu yang menandatangai maklumat tersebut supaya dapat mengesahkan tandatangan-tandatangan mereka.

Sistem-sistem yang dibina menggunakan unsur-unsur dalam bidang teori nombor yang akan ditunjukkan di dalam Bab II. Dalam Bab III, kami akan persembahkan sistem kriptografi simetri dan sistem kriptografi tidak simetri (sistem kunci awam). Kami juga akan membentangkan serangan ke atas sistem kriptografi dan ciri-ciri sistem kriptografi yang kuat ataupun selamat. Dalam Bab IV kami akan bentangkan sistem kriptografi multi RSA yang dicadangkan oleh How et al. (2001) serta kelemahan-kelemahan sistem ini. Kemudian, kami akan persembahkan sistem kriptografi multi RSA yang kami bina dan berikan analisis keselamatannya. Akhir sekali, dalam Bab V kami akan membuat 9rumusan kepada sistem yang kami cadangkan ini.

BAB II

ASAS-ASAS MATEMATIK DALAM KRIPTOGRAFI

2.1 PENGENALAN

Teori nombor adalah antara alat paling penting di dalam pembangunan sesuatu sistem kriptografi. Kita menggunakan teori nombor untuk membentuk algoritma sistem kriptografi. Oleh itu, kita perlu mengetahui beberapa asas takrifan dan teorem kepada kaedah yang digunakan ini. Bab ini membentangkan takrifan dan teorem dalam teori nombor yang digunakan dalam sistem kriptografi (Burton 1979; Dudley 1978; Rosen 1992).

2.2 UNSUR-UNSUR TEORI NOMBOR

Satu daripada takrifan yang penting dalam pembinaan sistem kriptografi adalah keboleh bahagian. Takrifan ini adalah asas kepada beberapa takrifan dan teorem yang digunakan dalam sistem kriptografi. Di bawah ini kami persembahkan takrifan tersebut.

Takrif 2.2.1: Andaikan a dan b adalah integer yang $a \neq 0$. Kita katakan bahawa a boleh dibahagi b jika wujud integer c sehinggakan $b = ac$. Jika a boleh dibahagi b, kita juga katakan bahawa a adalah pembahagi atau faktor bagi b. Jika a boleh dibahagi b, kita tandakan sebagai $a \mid b$ dan jika a tidak boleh dibahagi b kita tandakan sebagai $a \nmid b$.

Nombor perdana adalah kunci utama kepada sistem kriptografi RSA. Maka perlu kita memahami takrifan nombor tersebut. Takrifan nombor perdana adalah diberikan sebagai berikut:

***Takrif 2.2.2*:** Satu nombor perdana adalah satu integer positif lebih besar daripada 1 dan tidak boleh membahagi sebarang nombor positif lain kecuali 1 dan nombor itu sendiri.

Suatu nombor yang tidak memiliki sifat nombor perdana di atas dipanggil sebagai nombor gubahan. Takrifan nombor gubahan diberikan seperti di bawah ini:

***Takrif 2.2.3*:** Satu nombor gubahan adalah satu integer positif lebih besar daripada 1 dan bukan nombor perdana.

Nombor gubahan boleh didapati daripada hasil darab beberapa nombor perdana. Misalnya, $4 = 2.2$, $6 = 2.3$ dan $1001 = 7.11.13$ adalah contoh-contoh nombor gubahan. Kunci kerahsiaan dalam sistem RSA adalah hasil darab dua nombor perdana yang besar, p dan q untuk menghasilkan satu nombor gubahan n, iaitu $n = pq$.

Seterusnya kita perlu memahami takrifan faktor sepunya terbesar bagi dua nombor. Takrifan ini adalah perlu diketahui supaya dapat memahami takrifan-takrifan yang berikutnya. Takrifan ini adalah seperti berikut:

***Takrif 2.2.4*:** Faktor sepunya terbesar bagi dua integer a dan b yang kedua-duanya bukan sifar, ialah integer terbesar yang boleh dibahagi oleh a dan b. Faktor sepunya terbesar bagi a dan b ditandakan sebagai (a, b). Takrifkan juga $(0, 0) = 0$.

Takrifan perdana relatif adalah intipati kepada takrifan kongruen linear dan teoram Euler yang akan diterangkan kemudian. Perdana relatif ditakrifkan sebagai berikut:

***Takrif 2.2.5*:** Integer a dan b dikatakan perdana relatif jika $(a, b) = 1$.

Seterusnya kita dapat kembangkan takrifan perdana relatif untuk satu set nombor integer sebagai di bawah ini.

***Takrif 2.2.6*:** Kita katakan integer $a_1, a_2, ..., a_n$ adalah saling perdana relatif jika $(a_1, a_2, ..., a_n) = 1$. Integer-integer ini dipanggil perdana relatif berpasangan jika untuk setiap pasang a_i dan a_j dalam set ini, $(a_i, a_j) = 1$, iaitu jika setiap pasang integer daripada set ini adalah perdana relatif.

Kita juga perlu mengetahui takrifan gandaan sepunya terkecil. Takrifan ini dibentang di bawah ini.

***Takrif 2.2.7*:** Gandaan sepunya terkecil bagi dua integer positif a dan b adalah integer positif terkecil yang boleh membahagi oleh a dan b.

Teorem di bawah ini menjelaskan satu kaedah untuk mendapatkan gandaan sepunya terkecil.

***Teorem 2.2.8*:** Jika a dan b adalah integer positif maka $[a,b] = ab/(a,b)$, di mana $[a,b]$ dan (a,b) adalah gandaan sepunya terkecil dan faktor sepunya terbesar masing-masing bagi a dan b.

***Bukti*:** Rujuk (Rosen 1992 : 93)

Pemahaman konsep kongruen adalah sangat penting di dalam sistem kriptografi RSA. Ini kerana kita menggunakan konsep ini dalam keseluruhan algortima sistem RSA. Takrifan kongruen adalah seperti berikut:

***Takrif 2.2.9*:** Andaikan m suatu integer positif. Jika a dan b adalah integer, kita katakan bahawa a adalah kongruen kepada b modulo m jika $m|(a-b)$.

Teorem berikut ini adalah berasaskan konsep kongruen. Teorem ini selain digunakan di dalam sistem RSA, ia juga adalah asas kepada pemahaman takrifan-takrifan dan teorem-teorem berikut.

***Teorem 2.2.10*:** Jika a dan b adalah integer, maka $a \equiv b(\bmod m)$ jika dan hanya jika wujud integer k sehinggakan $a = b + km$.

***Bukti*:** Rujuk (Burton 1979: 70; Dudley 1978: 28; Rosen 1992: 120)

Satu takrifan khusus dalam konsep kongruen ini adalah songsangan. Songsangan kongruen ditakrifkan sebagai berikut:

Takrif 2.2.11: Diberi satu integer a dengan $(a,m)=1$, penyelesaian bagi $ax \equiv 1(\bmod m)$ dipanggil satu songsangan bagi a modulo m dan ditanda sebagai $a^{-1} \bmod m$.

Seterusnya kami kemukakan satu teorem iaitu penyelesaian kepada sistem kongruen linear.

***Teorem 2.2.12*:** Jika a, b, c, d, e dan f adalah integer dan m adalah integer positif, sehinggakan $(\Delta,m)=1$ yang $\Delta = ad - bc$ maka sistem kongruen

$$ax + by \equiv e(\bmod m)$$
$$cx + dy \equiv f(\bmod m)$$

mempunyai penyelesaian unik modulo m diberikan oleh

$$x = \overline{\Delta}(de - bf)(\bmod m)$$
$$y = \overline{\Delta}(af - ce)(\bmod m)$$

***Bukti*:** Rujuk (Rosen 1992 : 147)

Selanjutnya kami akan membincangkan beberapa takrifan dan teorem kongruen yang melibatkan eksponen. Teorem berikut adalah teorem kecil Fermat yang merupakan salah satu teorem yang penting bagi konsep kongruen yang melibatkan eksponen.

***Teorem 2.2.13*:** Jika p adalah nombor perdana dan a integer positif dengan pla maka $a^{p-1} \equiv 1 \ (\bmod p)$.

***Bukti*:** Rujuk (Burton 1979: 98; Dudley 1978: 44; Rosen 1992: 187)

Dengan mendarabkan a ke dalam dua-dua belah persamaan dalam teorem kecil Fermat kita perolehi teorem yang berikut ini.

***Teorem 2.2.14*:** Jika p adalah nombor perdana dan a integer positif maka $a^p \equiv a(\bmod p)$

***Bukti*:** Rujuk (Burton 1979: 98; Dudley 1978: 45; Rosen 1992: 188)

Teorem kecil Fermat hanya melibatkan ekponen nombor perdana. Euler telah memperkenalkan beberapa teorem yang penting bagi konsep kongruen yang melibatkan eksponen nombor gubahan pula. Kita mulakan dengan menunjukkan takrifan fungsi phi Euler.

***Takrif 2.2.15*:** Andaikan n adalah integer positif, fungsi phi Euler $\phi(n)$ ditakrifkan sebagai bilangan nombor integer positif yang kurang daripada n dan perdana relatif dengan n.

Berikut ini kami kemukakan teorem Euler yang menggunakan eksponen nombor gubahan dan analog dengan teorem kecil Fermat.

***Teorem 2.2.16*:** Jika m integer positif dan a integer dengan $(a,m)=1$, maka $a^{\phi(m)} \equiv 1 \pmod{m}$.

***Bukti*:** Rujuk (Burton 1979: 143; Dudley 1978: 64; Rosen 1992: 203)

Dua teorem berikut ini adalah fungsi phi Euler bagi nombor perdana dan dua nombor yang perdana relatif. Teorem-teorem ini digunakan dalam penjanaan kunci sistem RSA.

***Teorem 2.2.17*:** Jika p adalah nombor perdana maka $\phi(p)=p-1$, sebaliknya jika p adalah integer positif dan $\phi(p)=p-1$ maka p adalah nombor perdana.

***Bukti*:** Rujuk (Rosen 1992: 208)

Kerahsiaan dalam sistem RSA terletak kepada dua nombor perdana iaitu p dan q. Oleh kerana p dan q nombor perdana maka mereka juga adalah perdana relatif. Maka teorem berikut ini dapat digunakan untuk mengira $\phi(n)$ yang $n = pq$.

***Teorem 2.2.18*:** Andaikan m dan n adalah perdana relatif maka $\phi(mn)=\phi(m)\phi(n)$.

***Bukti*:** Rujuk (Rosen 1992: 209)

Dengan menggabung teorem 2.2.17 dan toerem 2.2.18, maka kita perolehi $\phi(n)=(p-1)(q-1)$. Nilai $\phi(n)$ amat perlu dalam menjana nilai kunci awam e dan kunci rahsia d dalam sistem RSA yang akan dibincangkan dalam Bab IV nanti.

BAB III

SISTEM KRIPTOGRAFI

3.1 PENGENALAN

Sistem kriptografi yang ada kini adalah sangat berbeza daripada sistem-sistem kriptografi yang dibangun pada masa dahulu. Selari dengan perkembangan pesat sistem komunikasi elektronik maka sistem kriptografi telah mengalami evolusi untuk menambah kesukaran kepada serangan penyerang. Banyak kajian yang telah dibuat untuk merekacipta suatu sistem kriptografi yang paling cekap dan selamat.

Sistem-sistem kriptografi ini boleh dibahagikan kepada dua jenis sistem yang utama iaitu sistem kriptografi simetri dan sistem kriptografi tidak simetri. Dalam bab ini kami akan membincangkan maksud kedua-dua jenis sistem tersebut. Kemudian kami akan kemukakan bentuk-bentuk serangan ke atas sistem kriptografi oleh seorang penyerang dan ciri-ciri sistem kriptografi yang kebal.

3.1.1 Sistem Kriptografi Simetri

Jika suatu sistem kriptografi mempunyai kunci enkripsi, e dan kunci dekripsi, d yang sama atau jika d boleh dijanakan dengan mudah menggunkan e, maka sistem kriptografi ini dipanggil sistem kriptografi simetri. Jika seorang pengirim dan seorang penerima ingin menggunakan sistem kriptografi simetri, mereka perlu bertukar kunci rahsia e