Penerapan Teori Bilangan Pada Pengamanan Surat Elektronik Dengan Protokol Secure/Multipurpose Internet Mail Extensions (S/MIME)

Gregorius Dimas Baskara - 13519190[1]
Program Studi Teknik Informatika
Sekolah Teknik Elektro dan Informatika
Institut Teknologi Bandung, Jl. Ganesha 10 Bandung 40132, Indonesia
[1]13519190@std.stei.itb.ac.id

***Abstract*—Surat Elektronik atau *email* pada zaman modern ini sudah menjadi sarana komunikasi yang lumrah dipakai oleh hampir seluruh orang pada semua bidang. Pengiriman surat elektronik, terutama dengan konten berupa informasi yang penting dan rahasia, akan sangat rentan apabila dilakukan secara langsung tanpa dienkripsi terlebih dahulu. Oleh karena itu, pengiriman *email* harus dan telah menggunakan teknik kriptografi sehingga pesan yang dikirim tidak mudah untuk diretas oleh pihak yang tidak bertanggung jawab. Salah satu metode kriptografi yang telah dipakai bertahun-tahun oleh beberapa penyedia layanan surat elektronik adalah metode kriptografi dengan protokol S/MIME (Secure/Multipurpose Internet Mail Extensions). Protokol tersebut dilakukan menggunakan penerapan teori bilangan di dalam algoritma RSA (Rivest–Shamir–Adleman), di mana digunakan kunci publik dan privat yang digabungkan pula dengan *Digital Signature*. Melalui protokol ini, pengiriman *email* dapat diamankan dan manfaatnya telah ditelah dirasakan oleh pengguna *email* di seluruh dunia.**

***Keywords*—Teori Bilangan, Surat Elektronik, Kriptografi, Protokol S/MIME**

I. PENDAHULUAN

Pada zaman mutakhir ini, komunikasi tidak lagi dilakukan melalui faksimili maupun surat-menyurat yang dikirim melalui kantor pos. Perkembangan teknologi telekomunikasi memungkinkan manusia untuk dapat berkomunikasi satu sama lain dari jarak yang jauh dengan menggunakan jaringan internet. Berkembangnya teknologi ini pun diikuti pula oleh berpindahnya pola komunikasi masyarakat apalagi setelah diikuti oleh perkembangan telepon seluler. Berdasarkan Publikasi Badan Pusat Statistik dengan judul "Statistik Telekomunikasi Indonesia 2019", persentase penduduk Indonesia yang memiliki telepon seluler pada 2019 meningkat di angka 63,53% dan kepemilikan jaringan internet di dalam rumah tangga mencapai angka 73,75%. Hal ini juga diikuti dengan pemakaian internet yang meningkat dari angka 21,98% menjadi 47,69% dan bahkan penggunaan telepon kabel pun menurun dari angka 4,01% pada 2015 menjadi 2,09% pada tahun 2019.

Perkembangan telekomunikasi itu pun juga mempengaruhi teknologi informasi dan komunikasi di berbagai belahan dunia. Salah satu media yang berkembang dari majunya teknologi tersebut adalah surat elektronik (*email*) dan media sosial. Meskipun sekarang terlihat media sosial sudah mengalahkan penggunaan surat elektronik dan sudah dipakai oleh hampir semua pengguna telepon seluluer, namun ternyata surat elektronik masih menduduki posisi pertama dalam media komunikasi dan penyebaran informasi secara daring. Menurut lembaga optinmonster, jumlah pengguna (*user*) surat elektronik di Amerika Serikat telah berada di angka 244,5 juta pengguna dan angka tersebut diproyeksikan akan meningkat menjadi 254,7 juta pada akhir 2020. Hal ini ditambah dengan fakta bahwa berdasarkan survey optinmonster, 58% responden mengaku bahwa mereka akan membuka *email* terlebih dahulu setiap harinya dibanding *platform* komunikasi lainnya (media sosial berada di angka 14%). Surat Elektronik pun juga menjadi preferensi bagi perusahaan untuk mempromosikan produk dan berkomunikasi dengan *client*. Menurut optinmonster, 61% responden memilih untuk dikontak oleh berbagai perusahaan dengan merk berbeda melalui *email* ketimbang *platform* lainnya.

Penggunaan surat elektronik itu pun juga tidak hanya membawa keuntungan terutama kepraktisan bagi para penggunanya, namun ternyata juga dapat membawa kerugian yang besar apabila surat elektronik itu tidak diamankan dengan baik. Menurut statistik yang dikompilasi oleh virtru.com, pada awal 2019, telah tercatat 4,1 miliar kasus kebocoran data, di mana 43% korbannya merupakan UMKM (Usaha Mikro, Kecil, dan Menengah). Salah satu penyebab kebocoran data itu adalah teknik enkripsi surat elektronik yang lemah dan mudah diserang *hacker* yang tidak bertanggung jawab.

Menanggapi banyaknya kasus kebocoran surat elektronik tersebut, penyedia layanan surat elektronik seperti Yahoo dan Gmail pun telah meningkatkan keamanan mereka secara terus-menerus. Gmail contohnya, telah menggunakan Transport Layer Security (TLS) untuk melakukan enkripsi *email* secara transit. Proses enkripsi yang dilakukan melalui *gmail* ternyata menggunakan metode serupa dengan enkripsi pada Microsoft Outlook dan perangkat berbasis IOS, yaitu dengan menggunakan metode S/MIME (Secure/Multipurpose Internet Mail Extensions). Metode S/MIME ini merupakan pengembangan dari algoritma RSA yang telah banyak digunakan pada bidang kriptografi. Melalui metode kriptografi

ini diharapkan bahwa pengiriman surat elektronik dapat berlangsung dengan aman dan dapat mengurangi tingkat kebocoran data melalui surat elektronik.

II. LANDASAN TEORI

1. *Teori Bilangan*

Bilangan dan Teori Bilangan

Terdapat berbagai jenis bilangan yang dipelajari di cabang ilmu Matematika. Jenis-jenis bilangan tersebut meliputi :

- Bilangan Asli, yaitu bilangan yang dimulai dari 1 ke atas {1, 2, 3, 4, 5, 6, 7, …}.
- Bilangan Cacah, yaitu bilangan asli yang juga meliputi angka 0 : {0, 1, 2, 3, 4, 5, 6, 7, …}.
- Bilangan Bulat (Z), yaitu bilangan cacah yang ditambahkan dengan bilangan negatif : {-4, -3, -2, -1 , 0, 1, 2, 3, 4,…}.
- Bilangan Prima, yaitu bilangan bulat yang hanya habis dibagi 1 dan bilangan itu sendiri : {2, 3, 5, 7, 11, 13, 17, …..}.
- Bilangan Pecahan, yaitu bilangan yang dapat dinyatakan dalam bentuk pecahan a/b : {1/2, 3/4, 5/6, 7/8, …}
- Bilangan Rasional, yaitu bilangan yang meliputi bilangan Bulat dan Pecahan.
- Bilangan Irasional, yaitu bilangan yang tidak dapat dinyatakan dalam bentuk pecahan a/b : {$\sqrt{2}$, $\sqrt{3}$, dan bilangan irasional lainnya}
- Bilangan Riil, yaitu bilangan yang meliputi bilangan rasional dan irasional
- Bilangan Imajiner, yaitu bilangan yang meliputi i di mana i^2 = -1, contoh $\sqrt{-1}$, $\sqrt{-2}$
- Bilangan Kompleks, yaitu bilangan yang meliputi bilangan Riil dan Imajiner.

Teori bilangan (Number Theory) sendiri mempelajari secara khusus bilangan bulat (integer) dan fungsi-fungsi yang berkaitan dengan bilangan tersebut.

Sifat Pembagian Pada Bilangan Bulat

Jika terdapat $a, b \in Z, a \neq 0$, maka dikatakan bahwa a habis membagi b jika terdapat bilangan bulat c sedemikian sehingga :

$$b = ac$$

Contoh 3 habis membagi 6 karena terdapat $c = 2$ sehingga $6 = 3\ x\ 2$. a habis membagi b dapat ditulis $a \mid b$.

Teorema Euclidean Pada Bilangan Bulat

Jika terdapat $m, n \in Z\ dan\ n > 0$, maka pembagian m/n akan menghasilkan q $(quotient)$ dengan sisa r (remainder) sedemikian sehingga

$$m = nq + r$$

di mana

$$0 \leq r < n.$$

Contoh $9/5$ dapat disajikan di dalam bentuk $9 = 5\ x\ 1 + 4$ Sehingga dapat terlihat bahwa hasil baginya adalah 1 dan sisanya (remainder) adalah 4.

Pada bilangan negatif perlu diingat bahwa $0 \leq r < n$, sehingga misalkan $-7/5$ harus disajikan sebagai $-7 = 5\ x(-2) + 3$ dan bukan $-7 = 5\ x(-1) + (-2)$ yang artinya $-7/5$ akan memiliki hasil bagi berupa -2 dengan sisa 3.

Pembagi Bersama Terbesar / PBB (Greatest Common Divisor)

Jika terdapat $a, b, c \in Z$, maka c dikatakan sebagai pembagi bersama terbesar dari a dan b, jika c adalah bilangan bulat terbesar sehingga c habis membagi a dan c habis membagi b atau dapat ditulis

$$PBB(a, b) = c \text{ di mana } c|a\ , c|b$$

Contoh, $PBB(5{,}10) = 5$ karena 5 merupakan bilangan bulat terbesar yang mana 5 | 5 dan 5 | 10.

Algoritma Euclidean Untuk Mencari Pembagi Bersama Terbesar / PBB (Greatest Common Divisor)

Jika terdapat $m, n \in Z$, sedemikian sehingga $m = nq + r$, di mana $0 \leq r < n$, maka dapat diturunkan rumus :

$$PBB(m, n) = PBB(n, r)$$

Dengan memanfaatkan fakta bahwa $PBB(m, 0) = m$, maka pencarian PBB untuk m, n dapat dilakukan dengan sistematis dan dapat dikomputasi.

Contoh, akan dicari $PBB(80{,}12)$, maka karena $80 \geq 12$, proses pencarian PBB adalah sebagai berikut :

$$80 = 6\ x\ 12 + 8$$
$$12 = 1\ x\ 8 + 4$$
$$8 = 2\ x\ 4 + 0$$

$PBB(80{,}12) = PBB(12{,}8) = PBB(8{,}4) = PBB(4{,}0) = 4$

Kombinasi Linier

Misal terdapat a dan b bilangan bulat positif, maka terdapat bilangan bulat x dan y sehingga

$$PBB(a, b) = xa + yb$$

Relatif Prima

Dua bilangan bulat misal x, y dikatakan relatif prima jika dan hanya jika

$$PBB(x, y) = 1$$

Aritmatika Modulo

Jika terdapat bilangan bulat a dan m, dengan $m > 0$ maka

$$a\ mod\ m = r$$

sedemikian sehingga

$$a = mq + r$$

dengan

$$0 \leq r < m$$

Di sini, m disebut juga modulo atau modulus di mana hasilnya selalu di antara 0 dan $m - 1$.

Kongruen

Jika terdapat a dan x di mana $a\ mod\ x = y$ dan b di mana $b\ mod\ x = y$, maka dapat dikatakan bahwa a kongruen dengan b dalam modulus x, atau ditulis :

$$a \equiv b\ (mod\ x)$$

Untuk $x > 0$, maka juga berlaku :

$$x \mid (a - b)$$

Teorema Kongruen :

a) Jika $a \equiv b\ (mod\ m)$ dan c sembarang bilangan bulat, maka berlaku :

$$(a + c) \equiv (b + c)(mod\ m)$$

$$ac \equiv bc \ (mod\ m)$$
$$a^p \equiv b^p \ (mod\ m)$$

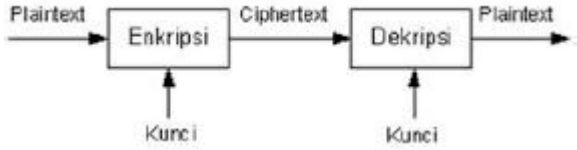
b) Jika $a \equiv b \ (mod\ m)$ dan $c \equiv d \ (mod\ m)$, maka
$$(a + c) \equiv (b + d)(mod\ m)$$
$$ac \equiv bd \ (mod\ m)$$

2. Kriptografi

Definisi dan Istilah Kriptografi

Kriptografi adalah ilmu untuk menjaga keamanan suatu pesan dalam bentuk lain yang tidak memiliki makna dengan tujuan agar pesan tersebut hanya dapat dimengerti oleh pihak pengirim dan pihak yang dituju. Berikut adalah istilah-istilah di dalam kriptografi :

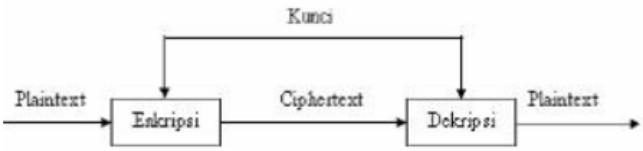
a) *Teks Biasa / Plaintext* : Istilah lain untuk pesan yang hendak dikirim oleh pengirim dengan tujuan agar dimengerti oleh penerima yang ditujukan.
b) *CipherTeks / Ciphertext* : Pesan yang telah disandikan dengan pola atau metode tertentu sehingga tidak dapat dimengerti maknanya.
c) *Enkripsi* : Proses mengubah Teks Biasa menjadi CipherTeks. Dilakukan saat pesan akan dikirim.
d) *Dekripsi* : Proses mengubah CipherTeks menjadi Teks Biasa. Dilakukan saat pesan akan diterima.
e) *Kunci* : Rumus/pola untuk mengubah *Plaintext* menjadi *Ciphertext* ataupun sebaliknya



Gambar 2.1 Prinsip Kriptografi
Sumber : http://mutiasulisetyani.blogspot.com/2015/03/algoritma-kriptografi.html

Kriptografi Simetrik

Kriptografi simetrik atau disebut juga kriptografi konvensional adalah kriptografi di mana kunci untuk melakukan enkripsi dan kunci untuk melakukan dekripsi adalah sama. Algoritma kriptografi simetrik terbagi atas 2 kategori besar, yaitu algoritma aliran (Stream Ciphers) di mana penyandian dilakukan per bit atau per byte dan algoritma blok (Block Ciphers), di mana penyandian dilakukan pada sekumpulan bit atau byte sekaligus. Contoh dari algoritma ini adalah Caesar Cipher, DES, dan Blowfish



Gambar 2.2 Prinsip Kriptografi Simetrik
Sumber : https://dimasandree.wordpress.com/2013/11/13/kriptografi-simetri-dan-asimetri/

Kriptografi Asimetrik

Kriptografi asimetrik adalah kriptografi di mana kunci untuk melakukan enkripsi berbeda dengan kunci untuk melakukan dekripsi. Kelebihan dari kriptografi asimetrik ini adalah antara lain :

a) Keamanan lebih terjamin dengan adanya kunci yang berbeda untuk enkripsi dan deskripsi
b) Manajemen kunci lebih baik karena jumlah kunci lebih sedikit
c) Hanya satu kunci saja yang harus dirahasiakan
d) Pasangan kunci tidak harus diubah-ubah dalam waktu yang sering (keamanan tetap akan terjaga)

Sementara itu kelemahan dari kriptografi asimetrik adalah :

a) Proses enkripsi dan dekripsi memerlukan waktu yang lebih lama dari kriptografi simetrik karena prosesnya menggunakan kunci yang memerlukan bilangan dan operasi perpangkatan yang besar.
b) Ukuran *Ciphertext* yang jauh lebih besar dari *Plaintext.*
c) Kunci publik diberikan secara luas dan tidak dirahasiakan, maka tidak bisa dipergunakan untuk autentifikasi pengirim.
d) Masih tidak menjamin keamanan 100% karena prinsipnya hanya mempersulit peretas dan pihak yang tidak bertanggung jawab dengan persoalan aritmatika yang kompleks dan bilangan yang sangat besar.

Gambar 2.3 Prinsip Kriptografi Asimetrik
Sumber : https://dimasandree.wordpress.com/2013/11/13/kriptografi-simetri-dan-asimetri/

Algoritma RSA (Rivest-Shamir-Adleman)

Sebuah algoritma kriptografi yang dibuat oleh tiga orang peneliti dari MIT (*Massachussets Institute of Technology*), yaitu Ron Rivest, Adi Shamir, dan Leonard Adleman. Algoritma RSA termasuk ke dalam kriptografi asimetri karena memiliki kunci yang berbeda untuk enkripsi dan dekripsi. Kunci untuk enkripsi disebut kunci publik dan kunci untuk dekripsi disebut kunci privat.

Pembangkitan pasangan kunci publik-privat :

1) Pilih dua bilangan prima misalkan p dan q. Kedua bilangan ini dirahasiakan
2) Hitung $n = pq$. n tidak perlu dirahasiakan
3) Hitung $m = (p - 1)(q - 1)$. Bilangan m dirahasiakan
4) Pilih sebuah bilangan bulat untuk kunci publik, misal e, yang relatif prima terhadap m, yaitu $PBB(e, m) = 1$
5) Hitung kunci privat, d, melalui kekongruenan $ed \equiv 1 \ (mod\ m)$.

Setelah didapatkan e sebagai kunci publik dan d sebagai kunci privat, maka proses enkripsi dan dekripsi dapat dilakukan dengan rumus :

$p^e \equiv c \ (mod\ n)$ atau $c = p^e \ (mod\ n)$ **(Enkripsi)**
$c^d \equiv p \ (mod\ n)$ atau $p = c^d \ (mod\ n)$ **(Dekripsi)**

Algoritma ini dinilai lebih aman dalam menjaga kerahasiaan suatu pesan karena tidak mudah (bahkan hampir tidak

mungkin) untuk memfaktorkan bilangan yang sangat besar (>200 digit) menjadi faktor-faktor prima yang dibutuhkan untuk mendapatkan kunci privat yang dirahasiakan. Menurut pencetus algoritma RSA, dibutuhkan waktu 4 milyar tahun untuk mencari faktor bilangan dengan >200 digit menggunakan algoritma mutakhir tercepat dan komputer dengan kecepatan 1 milidetik.

3. *Protocol S/MIME*

S/MIME (Secure/Multipurpose Internet Mail Extensions) merupakan metode atau protokol pengamanan yang sudah umum digunakan untuk mengamankan suatu surat elektronik (*email*). S/MIME memungkinkan pengguna untuk mengenkripsi pesan dan juga menandai pesan tersebut. Dengan menggunakan S/MIME, maka penerima pesan juga dapat yakin bahwa pesan yang berada pada *inbox*-nya telah sesuai dengan pesan yang dimaksudkan oleh pengirim. Penerima pun juga dapat yakin bahwa pengirim dengan alamat *email* itu merupakan pengirim sesungguhnya dan bukan orang lain yang tidak bertanggungjawab dan menggunakan alamat *email* tersebut. Secara umum pengamanan S/MIME dibagi atas dua bagian, yaitu *Digital Signatures* dan *Message Encryption* yang akan dibahas lebih lanjut pada beberapa segmen berikut.

Sejarah S/MIME dan Perkembangan Kriptografi Surat Elektronik

Sebelum S/MIME umum digunakan sebagai protokol pengamanan surat elektronik, para penyedia layanan surat elektronik menggunakan protokol yang umum pula digunakan pada saat itu, yaitu protokol Simple Mail Transfer Protocol (SMTP). Meskipun demikian, protokol SMTP ternyata tidak mampu memberikan keamanan yang cukup bagi pesan yang dikirimkan. Terdapat pula admin-admin surat elektronik yang lantas menggunakan protokol pengamanan perusahaannya sendiri, namun hal ini ternyata juga menjadi kendala karena meskipun dapat bekerja dengan baik untuk menghubungkan antar *staff* dalam perusahaan secara lokal, namun ternyata konektivitas dengan pengguna surat elektronik dari luar perusahaan pun terganggu karena pihak luar tidak menggunakan protokol serupa. Hal ini menyebabkan sulitnya perusahaan untuk berkomunikasi dengan *client*, perusahaan, atau pihak lain di luar perusahaan tersebut.

Menjawab persoalan tersebut, pada 1995 muncullah protokol S/MIME pertama yang kemudian dipakai oleh beberapa vendor sekuritas. Berikut adalah sejarah versi-versi protokol S/MIME yang pernah digunakan oleh para penyedia surat elektronik dan agen sekuritas :

1) S/MIME version 1
   Muncul sebagai S/MIME pertama yang dipakai oleh berbagai agen sekuritas. Pada masanya, S/MIME belum memiliki satu standar umum yang dipakai oleh semua pengguna, namun hanya berupa sejumlah standar yang berkompetisi satu sama lain di dalam pasar
2) S/MIME version 2
   Muncul pertama kali pada tahun 1998. Berbeda dengan version 1, version 2 diajukan ke Internet Engineering Task Force (IETF) sebagai salah satu alternatif standar protokol pengamanan surat elektronik. S/MIME versi kedua ini lantas disetujui menjadi standar protokol pengamanan surat elektronik secara umum. Terdapat dua Request for Comments (RFC) yang diajukan oleh IETF untuk S/MIME versi kedua ini, yaitu RFC 2311 mengenai standar pengamanan pesan dan RFC 2312 mengenai *certificate handling*.
3) S/MIME version 3
   Tidak lama setelah munculnya versi 2, pada tahun 1999 muncul pula S/MIME versi 3 yang kemudian hadir pula dengan beberapa RFC yang mengembangkan kemampuan pengamanan S/MIME secara keseluruhan. S/MIME versi ini telah menjadi protokol pengamanan surat elektronik yang dipakai di berbagai produk Microsoft seperti Microsoft Outlook dan juga pada produk *email* google, yaitu gmail.

III. Penerapan Protokol S/MIME Dengan Prinsip Algoritma RSA Dalam Enkripsi Surat Elektronik

1. *Sekilas Mengenai Pengamanan S/MIME Melalui Digital Signatures (Sumber : https://docs.microsoft.com/en-us/previous-versions/tn-archive/aa995740(v=exchg.65)*

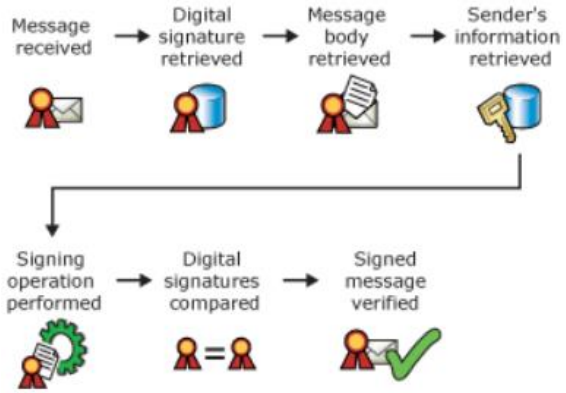
Gambar 3.1 Prinsip Digital Signatures
Sumber : https://docs.microsoft.com/en-us/previous-versions/tn-archive/aa995740(v=exchg.65)

Seperti tertulis pada namanya, *Digital Signatures* merupakan metode penandaan pesan secara *digital*. Beberapa kemampuan *Digital Signatures* adalah sebagai berikut :

1) Authentication
   Sebelum S/MIME, protokol SMTP tidak memiliki kemampuan untuk melakukan autentikasi pengirim pesan elektronik. Dengan demikian, penerima pesan tidak memiliki kepastian bahwa pemilik alamat email tersebutlah yang benar-benar mengirim pesan dan bukan pihak lain. Melalui S/MIME, autentikasi tersebut dapat dilakukan sehingga penerima surat memiliki kepastian mengenai pihak pengirim.
2) Nonrepudiation
   Nonrepudiation adalah kondisi di mana *Signatures* yang diberikan pada masing-masing pesan yang terkirim dapat disahkan dan tidak bisa dibantah. Melalui authentication yang telah dilakukan, maka *signature* yang ada dapat dipastikan benar dan tidak dapat diperdebatkan.
3) Data Integrity
   Melalui authentication dan nonrepudiation, pengiriman surat elektronik bahkan menjadi lebih aman daripada surat biasa. Hal ini karena apabila pesan diubah oleh pihak yang tidak bertanggung jawab, maka *signature* akan langsung tidak tervalidasi, sehingga penerima mempunyai kepastian akan keamanan pesan yang terkirim.

Berikut ini merupakan tahapan umum dalam *Digital Signatures*, namun tidak akan dibahas secara lebih lanjut pada makalah ini.

Gambar 3.2 Alur *Digital Signing* Suatu Pesan Elektronik
Sumber : https://docs.microsoft.com/en-us/previous-versions/tn-archive/aa995740(v=exchg.65)



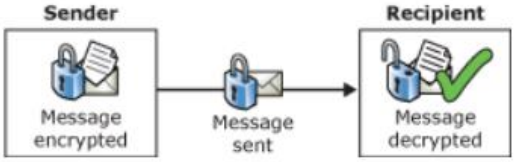
Gambar 3.3 Alur Verifikasi *Digital Signature* Suatu Pesan Elektronik
Sumber : https://docs.microsoft.com/en-us/previous-versions/tn-archive/aa995740(v=exchg.65)

2. *Implementasi Kriptografi dengan Algoritma RSA Pada Protocol S/MIME*

Berdasarkan Microsoft, dijelaskan keunggulan S/MIME sebagai berikut : Berbeda dengan SMTP, protokol S/MIME menyediakan fitur keamanan ekstra dengan cara melakukan enkripsi pada pesan yang hendak dikirim. Terdapat dua kemampuan besar yang dimiliki oleh protokol S/MIME dalam melakukan enkripsi :

1) Confidentiality
   Enkripsi pesan pada protokol S/MIME memastikan bahwa hanya penerima yang dimaksudkan saja yang dapat membaca dan mengerti makna dari pesan yang dikirim.
2) Data Integrity
   Bersama dengan *Digital Signatures* protokol S/MIME memastikan bahwa pesan yang dibaca oleh penerima adalah pesan yang dituliskan oleh pengirim.

Apabila dianalisis lebih lanjut secara garis besar, proses kriptografi pada protocol S/MIME terdiri atas enkripsi pesan yang ditulis ke dalam bentuk bahasa yang tidak dapat dipahami (CipherText) , kemudian didekripsi kembali menjadi PlainText ketika penerima yang dimaksud membuka dan membaca pesan tersebut.



Gambar 3.4 Prinsip Kriptografi Dalam Pengiriman Surat Elektronik

Sumber : https://docs.microsoft.com/en-us/previous-versions/tn-archive/aa995740(v=exchg.65)

Berikut ini adalah proses enkripsi suatu surat elektronik menggunakan protokol S/MIME :

1) Pesan telah selesai ditulis kemudian *body* dari surat elektronik dibaca oleh sistem
2) Informasi unik yang mengidentifikasi penerima surat (recipient) diterima dan disimpan
3) Proses enkripsi menggunakan algoritma RSA
   Pada saat enkripsi, kunci publik sudah jadi dan siap untuk dipakai. Contoh public key yang terbentuk adalah sebagai berikut :

Public key length k=|n|=1024 bits
r=0000481DD2EEB162F18BE26BF64BB980FF99134C39F1
443823811D837370F8FAE4364C3171CEE355082118BC9E
F97779B9DEB6FBAC33E2DCB4F7B6AB5299B1661AD5C
DEF8C76B72A1F0D85A1079B96F7C293C029AFD2442FB
65AFB370FE7A971A235C3BDD866C8242C15BB4B82369
6FF51681C012905101F1D643A4AC057DECE
CEK=6670B591275D5B9946741A1BFA3755068831A4B69
6AF7DA39FBAF208D99ADF8C
c=0BF2770071E690C2327729978037F9BE5513A594A6F9C
D25C4834CF51C4277414991EC3871B0183FB183636A28B
4294D48766E6AC69061A84B4D5E192143CFBEC3ABFEE
56501F7D1A2C544A84077DD3C8AC8B390A34214FDBFC
8964CC10252E4EA6936F8430BCC0355A67C33C0307F1D
3E4A9459A323745DB64B541A61CB9977
m=
48656C6C6F2C20776F726C6421205468697320697320612O
736563726574206D6573736167652E20466F7220426F62277
32065796573206F6E6C792E
PT=48656C6C6F2C20776F726C642120546869732069732061
207365632657420 6D6573736167652E20466F7220426F62
27732065796573206F6E6C792E04040404
IV=84D8A4C56B5EA779A42D358081F940A2
CT=8487F05119052DA340612DA5F70E5CD590854A5C56
8405DB14EF7FB09939D5E64CC2180BD8923E6785079040
D815709FCF9DB188BBB71FCA3D5943EB10B25C78

Gambar 3.6 Contoh Public Key yang digunakan dalam protokol S/MIME
Sumber : https://www.cryptosys.net/pki/rsa_ferguson_schneier.html

Pada saat yang bersamaan dengan enkripsi, dilakukan pula generasi private key yang dibentuk berdasarkan informasi unik penerima. Berikut adalah contoh private key yang di-*generate* oleh protokol S/MIME :

```
-----BEGIN RSA PRIVATE KEY-----
MIIEpQIBAAKCAQEAxR9nz41hKHqHfrNBxcGjkHp+JwBwEnV/dovHI3xBcHzde4/x
oNFZD24m8mlCRZUfjPH3r8T/MjS3SUMxi1k2qtrXqH6DFscmCiralHBEI6LJi7+n
a/O+9nV20VMxz+YiKCMD/veSiS6LraPUQXL/981UiKGRVLesDB6r58jyokdIyF1z
Zphr3A4/R4Z78dOINiBPgvh/YdMYwYbBCCPW+5vSClHhgeY2qvQbIQDreYdRBRmm
eY3UUSX6dUUDk227i4X76p/+2ROOLz395dgF0pfbJR1N5MgqgIjrkgsRfF7ONNzx
oWN//wTRpYZVlH8O0KyNY6H+z+ZXuf9g/Jvj4QIDAQABAoIBAQC6LWFU7IkZPDEA
/7ldV/huGuNPXuB67rLGelpJL7B219gwPdHPPCrLohPy3GuVYLT94AM55evJtXRv
I6GFpWs2j58kKukQ+GL7M2Ji1G3m4ndNIGS2Vu7DxEnGhrcDTq5wDjJV++pQ2r9d
7uAoOL99glcW/NJQm3FJuSZPssFHdjfzFrirRUwLPq9RoYsvst/EECxoq5WOZbeM
OsyGJ0ARsJpvBhIMFq/6eo/dFfTR4qba3BP0RksbETRNUk7ld2iQJ9huZkThNz11
lxMpvpYRCHkmM8CIVzvb0IsCBmio/5YpShP3PVB39Zw5XDs/A9Yn5b46hjEX45mn
HTqaAz/JAoGBAN7ayderxL4C0jm8aif3wWMazXetuU8dU0jeYAmYCNl+R6dxtBSI
KAv770caDfDD7wxmjBDqEIBqIHYUPo3ouXiGt6r3WWNEzvRp3VbOS9TfR0MQys1K
WAgroB7mSJUG14I/JTpuFqwqN+VBXNTND2zb7ULj9UYOedIgxBqNCkbbAoGBAOJw
3r2tQNGBaT2VKlp5Jflvy09OOFaypdqMujSkbLi/gfU2WulYw8hti9yjsJdeAhv7
jk8LBIfiXyByXk/qc+IcEov79Uq5x44lV/KiP4FcZ3kGVMYmr2ldTa+JJ0gtIkDh
ZKVzw6SaXnqxbygCtNY+DRxCTBGcCpZQCkZhjIbzAoGBAJPjd1zjRU2fC6l66quZ
U8GT0NRh+f6RhGpwACV9uimzDpQE9a9GZ+UEDFcP6D5lmCaPitXSrp65Ts9tQdHk
pehg5lPTj4M772btNhBcGKCsh1rvMtYnRuItKTY4NeSHxM5PX0I2Ol+IKM2/oX4q
ktj33aytIGCcTKVwTxMbk71PAoGACVtImOXTy9RhGN5VBbAD1a684+YDhfGT0NgH
ya0RoQCoyg0Y7JNyY5HDOba50UddJvLaCoIWCddcvuZ65yp0517plUcv94p9qG36
mFgD78B1thaA4j8u+FeWoi40pVLYG340vnFuIBsQ1FkIksqp1kByIjzLD982wMdF
5Wqad+kCgYEAjqXkzyFiD71D6g205kwwPzoIV8unmNMsvNn3UFF50/MS/f/ubTTy
FoHYUt5E/YiHbPRyr8zTzSGWUGhV286jRPq4iCwhd2ZQDRw1DuqNooQAqQeY93nS
YDg6U+BjPWQx0lN4LucF+BKwXWQ8ZNdwxjs8SSf6XQMVco4LiUZBOyo=
-----END RSA PRIVATE KEY-----
```

Gambar 3.6 Contoh Private Key yang Di-*generate* untuk pesan dengan title AlicePrivDSSign
Sumber : https://tools.ietf.org/html/rfc4134#section-2.2

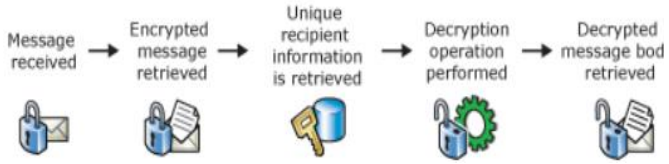
Kunci privat yang di-*generate* tersebut dibentuk berdasarkan algoritma RSA di mana $ed \equiv 1 \ (mod \ m)$ dengan e sebagai kunci publik dan d sebagai kunci privat.

4) Pesan dikirimkan kepada penerima beserta kunci privat yang dibuat pada nomor 3.

Gambar 3.7 Alur Enkripsi Suatu Pesan Elektronik
Sumber : https://docs.microsoft.com/en-us/previous-versions/tn-archive/aa995740(v=exchg.65)

Sementara itu, berikut ini adalah proses dekripsi suatu surat elektronik menggunakan protokol S/MIME :

1) Pesan diterima oleh penerima yang dimaksud dalam bentuk *Ciphertext.* Informasi unik mengenai penerima surat (recipient) diterima.
2) *Ciphertext* didekripsi kembali menjadi *Plaintext* dengan menggunakan informasi unik *recipient* yang diterima.
3) Pesan yang telah didekripsi dikembalikan kepada penerima surat elektronik.



Gambar 3.8 Alur Dekripsi Suatu Pesan Elektronik
Sumber : https://docs.microsoft.com/en-us/previous-versions/tn-archive/aa995740(v=exchg.65)

3. *Kombinasi Antara Kedua Fungsi Pengamanan Surat Elektronik Menggunakan Protokol S/MIME*

Secara garis besar, kedua fungsi pengamanan, baik itu *Digital Signature* maupun Kriptografi pesan memegang peran masing-masing dan saling melengkapi di dalam menjamin keamanan surat elektronik. *Digital Signature* berperan besar dari sisi penerima di mana fungsi tersebut memberikan jaminan keamanan bahwa pesan yang diterima adalah pesan yang benar-benar dikirim oleh alamat surat elektronik yang tercantum dan dengan isi pesan yang sama. Sementara itu Kriptografi surat elektronik berperan besar dari sisi pengirim di mana pengirim mendapat jaminan bahwa pesan yang dikirim hanya akan dapat dimengerti oleh pihak yang dimaksud dan bukan oleh pihak-pihak lain yang tidak bertanggung jawab.

4. *Simulasi 1 : Kriptografi Pesan Dengan Protokol S/MIME Version 1 dengan Algoritma Hashing SHA-1 dan Algoritma Signature RSASSA-PKCS1-v1_5*

BASE-64 encoded certificate
Pertama-tama, protokol S/MIME akan men-*generate* suatu *certificate* yang tidak lain merupakan aplikasi dari fitur *Digital Signature* yang sudah dijelaskan pada bagian sebelumnya. *Signature* ini bersifat unik untuk pesan ini saja.

```
-----BEGIN CERTIFICATE-----
MIIC0zCCAb2gAwIBAgIBATALBgkqhkiG9w0BAQUwHjEcMAkGA1UEBhMCUlUwDwYD
VQQDHggAVABlAHMAdDAeFw0xNjAxMzExNzAwMDBaFw0xOTAxMzExNzAwMDBaMB4x
HDAJBgNVBAYTAlJVMA8GA1UEAx4IAFQAZQBzAHQwggEiMA0GCSqGSIb3DQEBAQUA
A4IBDwAwggEKAoIBAQDqNlf1Eh8zsAR481IcDoYNTgCrhTnNEgigCaAW5l+Pz/Ml
oceXBkzWnD8U94DSWEFeOpIPnLjhKflOPL048MjsUcmb6Ohgc6nvSOIKvo7s+95T
YyG/+h5sb53vvrvkRfD924XkKxLPfoendGFEhGR3aQ3yEWy5iydIDvMnEZCQA7Tu
7Tf+XVXA29ErROpEfbX8IjUJZqH1uz0b3BKVnZb3mMSZDrKFNAngKnAvyZ3Nu3aK
41ZAV7pFkPFI4owpPh6V+Rkj0X51/2b3dsG7ha/xt0Bgd+tDqg64WnUzZFDZrn3h
TPhh0RJWfxuaFHG1EBvCTnJb7Vkd+sQ/+KYGMa8BAgMBAAGjIDAeMA8GA1UdEwQI
MAYBAf8CAQMwCwYDVR0PBAQDAgAGMAsGCSqGSIb3DQEBBQOCAQEAUUsGxklsTeNc
euUu/O7p0d4MQVkUg++P7te26O1ZNmjR11kaz3i1ltp2M8wc8gPKEfOqW1oz6gaY
SfDgAtAiMzUQMm3KyLx1TDEdPYqN0XKy+/bSHb5HSjEbEXv8Tjk9t7MfFKiyZFVe
2V8iHp64vBAH3IBrUuQkp8kVPeNIBemo5rUMeiXyzGblmemLHBkAO+l6X3OMHD+u
v7jf3/JADuLMULHvye3QxIM21adLziwhOTRbdBgvdPqB7uuOZQ1mX3RLjB2VeF5S
bSpwGbYue0jHxjLRPiHeo9sp1W+3ZyKgCUzGVGZm8stR4/UPy6ESk7CBf0guLf/c
voXbR5G2JA==
-----END CERTIFICATE-----
```

BASE-64 encoded PKCS#8 private key
Berikutnya, protokol S/MIME akan men-*generate* suatu kunci privat yang di dalamnya mengandung informasi unik penerima yang dimaksud. Kunci privat ini disimpan dalam bentuk *encoded* dan hanya bisa dipakai untuk dekripsi apabila informasi penerima berkesesuaian dengan penerima pesan nanti

```
-----BEGIN PRIVATE KEY-----
MIIEvQIBADANBgkqhkiG9w0BAQEFAASCBKcwggSjAgEAAoIBAQDqNlf1Eh8zsAR4
81IcDoYNTgCrhTnNEgigCaAW5l+Pz/MloceXBkzWnD8U94DSWEFeOpIPnLjhKflO
PL048MjsUcmb6Ohgc6nvSOIKvo7s+95TYyG/+h5sb53vvrvkRfD924XkKxLPfoen
dGFEhGR3aQ3yEWy5iydIDvMnEZCQA7Tu7Tf+XVXA29ErROpEfbX8IjUJZqH1uz0b
3BKVnZb3mMSZDrKFNAngKnAvyZ3Nu3aK41ZAV7pFkPFI4owpPh6V+Rkj0X51/2b3
dsG7ha/xt0Bgd+tDqg64WnUzZFDZrn3hTPhh0RJWfxuaFHG1EBvCTnJb7Vkd+sQ/
+KYGMa8BAgMBAAECggEAAejBHyw8ylWCrCf7HQ46Vg7NsyLmvN2bFIS5kWrjCpOC
JqtmwAFZvwoxZTLL4fhnqYHfmDkcRHPHXor2FaoNpZKt2puQ891+LCc8tk7VpaLG
DgmAhZ2qHHMNOfkPfpRk9akhwnbeVugf6SvPTGvqG/3/LSr1UdP2Sohaf5tiptrd
41afZ15mwAenGsFBkEsMumYxQ1UtPtsxzRBg8DnGP+BD+lpdAFelxFBwavDHPJsZ
hJnQQqlD3kNA+ug39+V/hyB/x5l55mlyG+KMCdtqb5Ah3spwECfYHisJFhmgMsFx
saFKqUPhtVWwmOaeuWIoLwD5LBDp6S0N4GEIR+3V8QKBgQD38YjvPLiY3O5X2boO
p9REf+BBB1LOIvoq/0jV/NN20wKIYlp7Sr1uDyhW6gOeZ6zvIFojmarYeYc5I4I7
lOJIrKvoDyrpOHlW5LZBy0ObPMkah8QMgA+EN2Ej1+vp2bS9IHP4o9sy5CK4xDEU
13UwdE2HQu1E8TrbPAJYOshnMQKBgQDx0panQwUMjK5JGAajFVCXosVk/wqdh1Rj
R/xorsU+45lKSH2EfWjPNV7pVz//ZO/pNKS3cK8LVXqA2gR1dlru9Y7YpFEL7p0G
M3tsKvEGxTXRyNyDFU+YfAI18sEggVcHzvDhC9vov0phA9i9124aLcW7unKq28/3
0plLFnBw0QKBgCDfbC1T4qGZwRvyqQFibPk7/w6AGxFrf8GNoSmF4L+DUHWmnJp2
GVFrPwzu79XjpwD5SBoqOIWE71G7DHw7zBiYlB4rTKQpMaU8o5FrkqYVVBBpaavC
mswLz5xB92xEyfq9P8L6boh7yMK4eE1sF4R6FwFU9UJLvWLtvN3XxVQxAoGATXND
KSL/9PsBvwtg5M6o10gcrLI6tiVn07x0jRqctf2zVOVOviZkcSkI0vdM2gF8DVb9
AnumtJyV9brd/rj/etVPAPfvtUChLiFDAGvocmCrUhtg9OLYcWAWXSz4ye5i729K
GunvbuYFbnkK6/4aF2xdjjizDSIFw7vBuRjgvmECgYEA1LJzxZ5fR15UkKXuR8uB
6c9TaWTuYk6FypEJ+GFn5GcsytZu9Nj3laCBLoBkXVnOUeGWaY8382I9eIvGdIIq
HECzL4/5Ie0NRAH1CbdSr912quowIWPtAH1v0c8o2sHHXWCjm3++GYOMgZq2Sm3m
R+zhYQdORD+Hp54RUcNu4f4=
-----END PRIVATE KEY-----
```

Plaintext (Isi Surat Email) yang hendak di Enkripsi
Pada percobaan ini pengirim dengan alamat email sender@example.com akan mengirimkan pesan kepada teman jauhnya dengan alamat *email* recipient@example.com. Berikut ini adalah *Body* dari *email* yang hendak dikirim :

```
Selamat Malam, Salam Hangat dari Ibukota.

Ujian Mata Kuliah Matematika Diskrit Hari Ini Keren Sekali, ya! Semoga
ujian berikutnya bisa lebih seru lagi.

Semoga kita dapat bertemu lagi di semester depan, di saat pandemi COVID-19
ini telah usai. Pasti akan lebih seru lagi, ya!

Salam, temanmu
Gregorius Dimas Baskara
AD MAIOREM DEI GLORIAM
```

CipherText (Hasil Enkripsi Isi Surat Email)

Setelah pengirim menekan tombol untuk mengirim pesan, maka *engine* dari penyedia layanan *email* yang menggunakan protokol S/MIME akan mengubahnya ke dalam bentuk *CipherText* sebagai berikut :

```
Content-Type: application/pkcs7-mime; name=smime.p7m;
 smime-type=enveloped-data; charset=binary
Content-Description: Enveloped Data
Content-Disposition: attachment; filename=smime.p7m
Content-Transfer-Encoding: base64
From: sender@example.com
To: recipient@example.com
Subject: Example S/MIME encrypted message
Date: Fri, 11 Dec 2020 12:35:01 +0000
Message-Id: <1607690101869-89a877a7-1dd7ea1b-004ad928@example.com>
MIME-Version: 1.0

MIIC7wYJKoZIhvcNAQcDoIIC4DCCAtwCAQIxggE/MIIBOwIBADAjMB4xHDAJBgNVBAYTAlJVM
A8G
A1UEAx4IAFQAZQBzAHQCAQEwDQYJKoZIhvcNAQEHMAAEggEA0Z2kF7vU6Yzl+4Ws7J4QEOZnm
bWN
93HD5B+0ekeUAzjfiwTRNpneee5tc7Qax94QDHN2qksaoFjuCTm4TAIOIUnR8a1MRKhI9EDI8
gK4
JpHfrenm6lND4mwmYDhnp7JuJUMJGa2ojU2FrPEqrbe+7//1v4mybjK/3iAc8ghyiWRn6Zv/r
tLy
+ArBPl5nN8jQJ+Zr/ROh1tIVIbutyLsN7jmEZUM6xPBa5c3WRKa3aJ+ugai9WgnL3yfHcAKnt
ggJ
JFqRV0buc3ApsHGvl4fAywf9cgvb+595aXyzoABgALCsn8Aer9cN/Yg0n38guT6dLxItN5aEB
nFL
rg96yTakJDCABgkqhkiG9w0BBwEwHQYJYIZIAWUDBAECBBAKpck57jV4Km+1GvVvTqC1oIAEg
gFg
ONLYWgdfABmbgZCacGOUDFuC6ZPAjiPw52d55FM6UgpZ1/b+kWiaXKeM7CuvqnK1w9VhaGaA0
UB9
CCGKNdtHe4Qd5nBj5N8t+F0wm+YCk4IoLVgIIUTCzN55dDOtIYZWt/XO3akU4gTn5YYe4A0dL
RnQ
SOnk3CMYae2eVGkFh44vVMltemS/nA7cDvzlxl/zCZ43qfVoJIKZC3UFdJl9Ing6bq2y3QAIY
lgw
9Ffm9d4CCF8ZiuMz5brYPANO8cv17067wd/qvPSJGsoheDn1i+HVZduaH3R4zmZx3Jv8s6a9f
xCW
PEpiAyxGaSYqIKSA+fCFR8c7zZIVtUaLUeYuu/fNr3sxktOFbK3PYRS+TgAlY8O5zE/ahYq1Y
ubQ
8ZTDRDgm7OjBscJu3XnMJHEuCRvqf2/hG8De5l9IMM4oabhLcVN/H5p9CyUKK2bNoucvOTq2U
6Ef
/w9XZCUxS8DrvQAAAAA=
```

Hasil Dekripsi Kembali (Dibaca oleh Penerima)

Setelah diterima oleh alamat *email* recipient@example.com, maka hasil enkripsi akan didekripsikan kembali apabila identitas penerima yang tercantum pada *CipherText* sesuai dengan pembuka *email.* Seperti pada sisi pengirim, berikutlah yang akan terbaca pada sisi penerima :

```
Selamat Malam, Salam Hangat dari Ibukota.

Ujian Mata Kuliah Matematika Diskrit Hari Ini Keren Sekali, ya! Semoga
ujian berikutnya bisa lebih seru lagi.

Semoga kita dapat bertemu lagi di semester depan, di saat pandemi COVID-19
ini telah usai. Pasti akan lebih seru lagi, ya!

Salam, temanmu
Gregorius Dimas Baskara
AD MAIOREM DEI GLORIAM
```

5. *Simulasi 2 : Kriptografi Pesan Dengan Protokol S/MIME Version 1 dengan Algoritma Hashing SHA-384 dan Algoritma Signature RSA-PSS*

BASE-64 encoded certificate

Seperti percobaan sebelumnya protokol S/MIME akan men-*generate* suatu *certificate* yang tidak lain merupakan aplikasi dari fitur *Digital Signature* yang bersifat unik untuk pesan ini saja.

```
-----BEGIN CERTIFICATE-----
MIIDPzCCAfOgAwIBAgIBATBBBgkqhkiG9w0BAQowNKAPMA0GCWCGSAFlAwQCAgUA
oRwwGgYJKoZIhvcNAQEIMA0GCWCGSAFlAwQCAgUAogMCATAwHjEcMAkGA1UEBhMC
UlUwDwYDVQQDHggAVABlAHMAdDAeFw0xNjAxMzExNzAwMDBaFw0xOTAxMzExNzAw
MDBaMB4xHDAJBgNVBAYTAlJVMA8GA1UEAx4IAFQAZQBzAHQwggEiMA0GCSqGSIb3
DQEBAQUAA4IBDwAwggEKAoIBAQDJGJDgLqWH94OC9f5SBAuNi286EjEq4H6CvTwF
KEPWESRSD7melpeALy4WOOY4qFwYq3yQAoOZgo/L6DO84r/TOM1szSGiAXwU6gR9
pN2erpPJEMu4pNOpSG+MS08ZG+f5ezMZ2X6Nzd9TfOQSsJA7BOnOZyN2mxyPiLVf
ywqYkqrtL8q1xQuYrZhCpXT5KtvPKn63PPdaJ1Umj1gOxACBPgc87js2vXIBFCtc
5s+FvZA6tIjTxjXIaC/G8AFv6WZerJUEqkd8VcGJ/J34ek7NBMfclQy1tL7y7nXs
fV/O3lEsg7YMOtZ6KL2XwxIs2SR0saxnDljPWkCsbyB3gKSrAgMBAAGjIDAeMA8G
A1UdEwQIMAYBAf8CAQMwCwYDVR0PBAQDAgAGMEEGCSqGSIb3DQEBCjA0oA8wDQYJ
YIZIAWUDBAICBQChHDAaBgkqhkiG9w0BAQgwDQYJYIZIAWUDBAICBQCiAwIBMAOC
AQEAmLGFjs79BjHaMloM9nQmWMeRuiDrGsejmK0oxY5PZEaoqj1YdLAve3EmfOHS
3lGDkBDzW8c3ICc5iRvNR+orNmHVI+nClyvcP3nRQGrtgw8LTySaXP74mow3XQkE
0n8BBxS02STbgS5sR86IkpojegXWZtAzVjfV1eQdbNAjiuYGizTNBnbsihApkUtp
x4ISUNCX7bU4ley31r/m7z6VXKiXQaUkKUwxEyK+QteVGyVfhUbWV7Wd8FnhAZAx
MP80812Z4X6Sbqj2aZk/aoW9T2Qj/vQxdB3OEAiRhf2+Bu+ri006r8Otkebc6fy+
aTtBr0VZFsrkFRO/W7cO5Rf7FA==
-----END CERTIFICATE-----
```

BASE-64 encoded PKCS#8 private key

Seperti percobaan sebelumnya, protokol S/MIME akan men-*generate* suatu kunci privat yang bersifat *encoded*

```
-----BEGIN PRIVATE KEY-----
MIIEvgIBADANBgkqhkiG9w0BAQEFAASCBKgwggSkAgEAAoIBAQDJGJDgLqWH94OC
9f5SBAuNi286EjEq4H6CvTwFKEPWESRSD7melpeALy4WOOY4qFwYq3yQAoOZgo/L
6DO84r/TOM1szSGiAXwU6gR9pN2erpPJEMu4pNOpSG+MS08ZG+f5ezMZ2X6Nzd9T
fOQSsJA7BOnOZyN2mxyPiLVfywqYkqrtL8q1xQuYrZhCpXT5KtvPKn63PPdaJ1Um
j1gOxACBPgc87js2vXIBFCtc5s+FvZA6tIjTxjXIaC/G8AFv6WZerJUEqkd8VcGJ
/J34ek7NBMfclQy1tL7y7nXsfV/O3lEsg7YMOtZ6KL2XwxIs2SR0saxnDljPWkCs
byB3gKSrAgMBAAECggEAEpo1qK9X+7RvU3mLDa43HWB1KSOOrc83lMOJnlaDs/VA
/WBcBOocWKzEoCSiU2JrppKSgsXgw54azDuOMa5uHU13X1W4g0KM5mhhgvfx0mCG
5kYp+koxFEtRmlJLHmEA/AikCQOgG+EMBC6c8Iepx/Pj5waOdsXRhguY76QaNlPM
0wm0Zsm8+3rpt2JjsD1q0/OuVfNO9uBN7Lp1OkGVAhcSt3bMHyGWNvc/1UMJPVVq
x4JK3PYZ/UfkTWwiSMbOmzOh79hYeSK6YqWw/vlEZTrZes9wawjnN93fEAgih/yC
BpV/pplAHShoEACuFI0cgV2NoUI6XCVTyNs/W+CloQKBgQD6PLx6FSVpRh00iUki
NE66rrqZeSZc2Hl0FCsfO8hYhgyiKp3gjlQpw96yK9N2PJ8mc9dd/KY0AB05CXsg
WydHgibthWHrgYYZEdUEZSUd92kVj0QD68+bko2B7T2l24PNXSLrStpQCe7A2xhB
CqKd6TrT/WeGyLF9ztM3YpCHoQKBgQDNuh6BReS0qSz1Tz1+ox2/OrkP+HNAtBYw
E6p311yONzGdNeOuCaaaHVmrlsNkavpjkpWI9AJ4rUs2s02/UxTI0u0wRVB+4Yep
Fj+kW4TZZ2gxKmtlM/9ZsJsaN2b5OOurRGM1y9UVUQ/w8DyvmIY/VIu6CdhTinvA
F5Bfm24YywKBgQCLpiWRBAgSzhwyW4NC4WomaKieSawNGIn/K9o83gIa1QRr49ij
nwp9HGBFkou6am5u6SsBuqOOVZn5YL8j+XrcP1g2Kb/RzEDn8LmucDvck1xDueY9
QfZkXc82+Qz0aKMPkrCQGv/mtwRVAHByq9rAwY4hDEQgRhQ3n5rkR89cwQKBgQCA
TrY71gWgD2s0y+kElGM3Iz7MkR4AmtDDx2AoQi89m3rcHAIWR3qa3/dPJ0ZR2M61
T3Tn55erABnK0eWJkB2Eatj3pCNiHvLnKDMlJNckaHP5RgWZJub5X0Y9AZS9lxyU
wqBFqw0IsHgKwyp2MeB4mxhSPVWoNNSdp5SprFzsJQKBgGGc5ejeT5Mo8ZB72FfU
wm9fx6ls3XLGcGzhNvlKEnLUNr3t+VnGpZrszWr3gzLN3SogcFaxukzzghVRH4CP
9NqDiKkC+vZNqy2zOfLzPQ6L5nEH/7OgVy9PLG9jn/C3GpAbRzpKhLnmd7+w5SbF
b2lEqNFLXLrlkRmsRcYQffnB
-----END PRIVATE KEY-----
```

Plaintext (Isi Surat Email) yang hendak di Enkripsi

Seperti pada percobaan sebelumnya, pengirim dengan alamat email sender@example.com akan mengirimkan aplikasi kegiatan magang (*internship*) kepada bagian *Human Resource* Perusahaan CodeMaster dengan alamat *email* recipient@example.com. Berikut ini adalah *Body* dari *email* yang hendak dikirim :

```
Salam Hormat,

Perkenalkan saya Gregorius Dimas Baskara, seorang mahasiswa tingkat II
program studi Teknik Informatika Sekolah Teknik Elektro dan Informatika
Institut Teknologi Bandung (ITB). Saya mendengar bahwa perusahaan
CodeMaster membuka lowongan magang dengan posisi sebagai Web Developer dan
saya berminat untuk mengisi posisi tersebut.

Saya memiliki pengalaman sebagai intern pada perusahaan startup lainnya
dengan posisi yang sama, secara spesifik sebagai Frontend Developer dan
UI/UX Researcher.

CV, Resume, dan Surat Motivasi telah saya lampirkan pada Attachment, Terima
Kasih.

Hormat Saya,
Gregorius Dimas Baskara
```

CipherText (Hasil Enkripsi Isi Surat Email)
Setelah pengirim menekan tombol untuk mengirim pesan, maka *engine* dari penyedia layanan *email* yang menggunakan protokol S/MIME akan mengubahnya ke dalam bentuk *CipherText* sebagai berikut :

```
Content-Type: application/pkcs7-mime; name=smime.p7m;
 smime-type=enveloped-data; charset=binary
Content-Description: Enveloped Data
Content-Disposition: attachment; filename=smime.p7m
Content-Transfer-Encoding: base64
From: sender@example.com
To: recipient@example.com
Subject: Example S/MIME encrypted message
Date: Fri, 11 Dec 2020 14:40:28 +0000
Message-Id: <1607697628713-22476a4e-0ef8218b-3015d439@example.com>
MIME-Version: 1.0

MIIEDwYJKoZIhvcNAQcDoIIEADCCA/wCAQIxggE/MIIBOwIBADAjMB4xHDAJBgNVBAYTAlJVM
A8G
A1UEAx4IAFQAZQBzAHQCAQEwDQYJKoZIhvcNAQEHMAAEggEASjQNmR+++y3PXhgBUlCeBpAAd
tm3
6YWomFCmfRhgVCY0XOl4vIsGAZ2B7a13YlobZIzOkpc7TCuMn9NHYGxTMrfi6yMjYBFw/+mEn
jgu
eIGOgvEyt3GsVFyPMsCqY4vHyRNxYJW35AIOwn0W1azPm0RB2DbFVe58S1oZvlfVY11HKwL1t
6sb
CmG0gRZbhZmtBdgIb5ZQDmVRX7imxGdCulrxkpNDqsnqajlMI+pIPbtjo5xhgk4H5GmCEsg8c
ztt
xGV4fvQg3a+O+PrL1/4Bzr3znz3KsaWUOTANkQo2BC8JtZWdjAwXTzRCCMqHdxzGM5e3OAxnX
JaH
A5EbHBvdmzCABgkqhkiG9w0BBwEwHQYJYIZIAWUDBAECBBCA1J54bVWmR+1bsTDSjOWuoIAEg
gKA
QIpz2O0riDXe/hPMdmSLK/KTqUnBYlC2U8ShrDMcXt78SmnNqSBbF1kdyIxuzxOjIe9W/uQ1Y
7KA
oVC8ncNq+c6oHWkPORgIEQMpDpjn2M3FmHT1q3j75NJcDFKfmsGW0of4eLIDyFDGadhvNxDLm
RCq
SyoA9QXYdWv46SbW8H++2qLvebhrohjfMIOoJRO+fay19bwC9HVwu9A4NhFVsdgH5H9P6OB5n
tE+
8TkyC+difobkGztG7abRaStKcKLJEKxWp47xFiC1e2ZZWraSG/Fto/z0mYIzOzR1DuahT3Qvo
CsG
ny5SM7euNT7wybN+nutxeBJpEmEk6P5GsN9vHAYV097tRGNyShBXGoNByb6ccPx71KrJA+NW4
5P1
et9r7e5871ekBWkIbHWVz30OnDuoxgKa5EUkbsaLn6RE0Xx5dgRrxU4D3vxwU1KA++HYJF0FL
/ni
3ZuDTgDgQz6f1Es2zfKqxcWBMZU1InLTLHjZheofyKoOSnOHkXYQdRPZg90YbjHqAFw5cUmfe
mLv
dI+Ssj18QOC9k8Gd6N0YubjuYjCtNAIUHOu+CAJf7BIHaQP6Fa4t/T4GmXotJgta4nCOXcYvE
WaY
3M3QonS7s3PHiSO0a60buERaPfw9Itg2uH154Nb/8BuBrcHyOM3OPokWvx2wSspx5LeFlSZpn
fF4
wpYl4TTwJIm2pdkEduIJJxEyQFzJuUJzr3P9mbrHzZlczUhOujF80N42pHJH4ax4Z3AOrOZkb
Fzo
7OaLelYYD9geXMOEsg7HQZd1o99Kt6l0KmLcc9Pbp+5/ZfCAHIScfO/D+V/EGOpfl0s8M8hDG
w4b
ibpOLo3iacVz8CPmWOAAAAA=
```

Hasil Dekripsi Kembali (Dibaca oleh Penerima)
Setelah diterima oleh alamat *email* recipient@example.com, maka hasil enkripsi akan didekripsikan kembali sebagai berikut:

```
Salam Hormat,

Perkenalkan saya Gregorius Dimas Baskara, seorang mahasiswa tingkat II
program studi Teknik Informatika Sekolah Teknik Elektro dan Informatika
Institut Teknologi Bandung (ITB). Saya mendengar bahwa perusahaan
CodeMaster membuka lowongan magang dengan posisi sebagai Web Developer dan
saya berminat untuk mengisi posisi tersebut.

Saya memiliki pengalaman sebagai intern pada perusahaan startup lainnya
dengan posisi yang sama, secara spesifik sebagai Frontend Developer dan
UI/UX Researcher.

CV, Resume, dan Surat Motivasi telah saya lampirkan pada Attachment, Terima
Kasih.

Hormat Saya,
Gregorius Dimas Baskara
```

Simulasi yang dijalankan (baik simulasi 1 maupun 2) dilakukan menggunakan program yang telah dibuat pada https://pkijs.org/examples/SMIMEEncryptionExample.html

IV. KESIMPULAN

Teori bilangan merupakan cabang matematika murni yang mempelajari secara khusus mengenai bilangan bulat atau *integer*. Di dalam cabang tersebut dipelajari mengenai pembagian dan sisa pembagian, faktor pembagi bersama terbesar, relatif prima, aritmetika modulo, kombinasi linier, dan kongruensi.

Teori bilangan memiliki banyak aplikasi di dalam kehidupan nyata, salah satunya di dalam kriptografi. Kriptografi merupakan ilmu untuk mengubah bentuk pesan dari yang dapat dimengerti maknanya ke pesan yang tidak dapat dimengerti dan sebaliknya. Salah satu penggunaan kriptografi adalah pada sekuritas dan pengamanan pengiriman surat elektronik (*email*). Kriptografi pada pengamanan surat elektronik pada umumnya menggunakan algoritma RSA, yaitu salah satu jenis algoritma kriptografi asimetrik di mana terdapat kunci yang berbeda untuk enkripsi dan dekripsi.

Kriptografi pada pengamanan surat elektronik tertanam dan terintegrasi pada protokol sekuritas penyedia layanan surat elektronik. Salah satu protokol sekuritas yang masih dipakai hingga sekarang merupakan protokol S/MIME (Secure/Multipurpose Internet Mail Extensions) yang dipakai pada Microsoft Outlook dan Gmail. Proses kriptografi pada protokol S/MIME menggunakan algoritma RSA di mana dibutuhkan kunci publik untuk mengenkripsikan suatu pesan dan kunci privat untuk mendekripsikannya kembali. Bersama dengan sistem pengamanan dengan *Digital Signature*, kriptografi telah teruji sebagai protokol yang cukup terpercaya dalam pengiriman surat elektronik.

V. UCAPAN TERIMA KASIH

Penulis ingin mengucapkan terima kasih sebesar-besarnya kepada beberapa pihak yang telah berperan besar dalam penyelesaian makalah ini :

1. Tuhan Yang Maha Esa karena berkat dan rahmat-Nya, makalah ini dapat terselesaikan dengan baik tanpa kurang satu bagian pun.
2. Dra. Harlili, M.Sc. sebagai dosen kelas K2 karena telah membimbing penulis selama pembelajaran matematika diskrit.

3. Dr. Ir. Rinaldi, M.T. dan seluruh tim dosen matematika diskrit yang telah berperan juga dalam kegiatan perkuliahan secara daring.
4. Teman-teman seangkatan karena telah memberikan dukungan selama perkuliahan sehingga penulis dapat menulis makalah ini dengan baik.

DAFTAR PUSTAKA

[1] Badan Pusat Statistik Indonesia, "Statistik Telekomunikasi Indonesia 2019". Diakses pada 5 Desember 2020 pukul 17.18, dari https://www.bps.go.id/publication/2020/12/02/be999725b7aeee62d84c6660/statistik-telekomunikasi-indonesia-2019.html

[2] Hott, Allison, "40+ Email Marketing Statistics You Need to Know for 2021". Diakses pada 5 Desember 2020 pukul 17.39, dari https://optinmonster.com/email-marketing-statistics/#:~:text=The%20number%20of%20email%20users,with%20family%20and%20friends%20either.

[3] Virtru, "*Email Security: What You Need to Know and Best Practices*". Diakses pada 5 Desember 2020 pukul 18.12, dari https://www.virtru.com/blog/email-security-2/#:~:text=Data%20breaches%20exposed%204.1%20billion,phishing%20or%20social%20engineering%2C%20respectively.&text=43%25%20of%20breach%20victims%20were,on%20average%20after%20a%20breach.

[4] Rinaldi Munir, Diktat Kuliah IF2120 : Matematika Diskrit, Bandung : Program Studi Teknik Informatika Sekolah teknik Elektro dan informatika Institut Teknologi Bandung, 2006.

[5] Taufik, Ilfan, "Kriptografi Asimetris" . Diakses pada 6 Desember 2020 pukul 10.13, dari https://blogteknologiinformasi.wordpress.com/2011/11/01/kriptografi-asimetris/

[6] "ALGORITMA ASIMETRI". Diakses pada 6 Desember 2020 pukul 10.19, dari https://repository.dinus.ac.id/docs/ajar/Kriptografi_-_Week12_-_RSA.pdf

[7] Microsoft, "*S/MIME for message signing and encryption in Exchange Online*". Diakses pada 6 Desember 2020 pukul 12.47, dari https://docs.microsoft.com/en-us/microsoft-365/security/office-365-security/s-mime-for-message-signing-and-encryption?view=o365-worldwide#:~:text=S%2FMIME%20(Secure%2FMultipurpose,emails%20and%20digitally%20sign%20them.

[8] "*SMIMEEncryptionExample*". Diakses pada 10 Desember 2020 pukul 20.23, dari https://pkijs.org/examples/SMIMEEncryptionExample.html

PERNYATAAN

Dengan ini saya menyatakan bahwa makalah yang saya tulis ini adalah tulisan saya sendiri, bukan saduran, atau terjemahan dari makalah orang lain, dan bukan plagiasi.

Bandung, 3 Desember 2020

Gregorius Dimas Baskara – 13519190