ANALISIS MENGENAI TINGKAT PENGETAHUAN PENGGUNA JARINGAN KOMUNIKASI ELEKTRONIK TENTANG KRIPTOGRAFI KHUSUSNYA MANAJEMEN KUNCI

Diana Rosida – NIM : 13502050

Program Studi Teknik Informatika, Institut Teknologi Bandung
Jl. Ganesha 10, Bandung
E-mail : if12050@students.if.itb.ac.id

Abstrak

Dalam kehidupan sehari-hari sebenarnya manusia telah banyak berhubungan dengan kriptografi. Umumnya manusia menjadi konsumen dari produk-produk yang menjalankan proses enkripsi dan dekripsi baik dengan maupun tanpa mereka sadari.

Kriptografi saat ini lebih banyak diaplikasikan pada produk-produk untuk melakukan komunikasi data yang aman melalui jaringan komunikasi elektronik yang biasa juga disebut sebagai dunia maya. Contoh yang paling sering ditemui adalah transaksi melalui ATM, komunikasi melalui telepon selular, serta pengiriman dan penerimaan surat elektronik.

Dalam beberapa aplikasi layanan untuk melakukan komunikasi data di dunia maya, konsumen harus memiliki *PIN* (nomor identifikasi personal) atau *password* (sandi lewat) untuk keperluan keamanan. *PIN* atau *password* ini sebagian besar digunakan untuk otentikasi pengguna atau menjadi kunci untuk proses enkripsi/dekripsi yang perlu dijalankan oleh aplikasi terhadap data yang akan/sedang dikomunikasikan.

Sayangnya karena mengetahui pentingnya *PIN* dan *password* tersebut, banyak pihak yang tidak bertanggung jawab kemudian melakukan berbagai cara untuk mencuri *PIN* dan *password* dari pihak lain. Setelah itu, *PIN* dan *password* tersebut digunakan untuk melakukan tindakan kejahatan dunia maya.

Tindakan kejahatan dunia maya atau lebih dikenal dengan *cybercrime* telah banyak terjadi di Indonesia. Berhubungan dengan *PIN* dan *password* yang menjadi alat untuk melakukan kejahatan dunia maya, penulis mencoba mencari tahu tingkat kepedulian masyarakat pengguna jaringan komunikasi elektronik untuk menjalankan manajemen kunci yang setidaknya dapat mengurangi kemungkinan terjadinya pencurian terhadap *PIN* atau *password* yang mereka miliki.

Dengan hasil yang diperoleh, penulis akan menganalisis penyebabnya untuk kemudian merumuskan solusi apabila ternyata tingkat kepedulian masyarakat untuk menjalankan manajemen kunci tergolong bermasalah. Analisis dan solusi yang disampaikan penulis diharapkan akan dapat berguna bagi pembaca, khususnya masyarakat pengguna jaringan komunikasi elektronik.

Kata kunci: Manajemen kunci, kejahatan dunia maya, kriptogafi.

1. Pendahuluan

Teknologi informasi sebenarnya sangat dibutuhkan. Dengan teknologi informasi, dunia menjadi tanpa batas. Berbagai informasi dapat diakses dengan mudah. Transaksi perbankan menjadi lebih cepat dan mudah. Sekarang ini setidaknya transfer dana dengan memanfaatkan teknologi informasi di Indonesia mencapai kisaran Rp 200 triliun setiap hari. Apalagi dengan sistem elektronik diyakini akan terjadi efisiensi biaya sekitar 30%.

Sebagaimana lazimnya pembaharuan teknologi, internet selain memberi manfaat juga menimbulkan ekses negatif dengan terbukanya peluang penyalahgunaan teknologi tersebut. Penyalahgunaan tersebut bisa juga disebut sebagai kejahatan dunia maya

Kejahatan dunia maya merupakan jenis kejahatan yang berkaitan dengan pemanfaatan sebuah teknologi informasi tanpa batas dan memiliki karateristik yang kuat dengan sebuah rekayasa teknologi yang mengandalkan tingkat kemanan yang tinggi dan kredibilitas dari sebuah informasi yang disampaikan dan diakses oleh pelanggan internet.

Data-data yang ditemukan penulis menunjukkan bahwa di Indonesia, penggunaan jaringan komunikasi elektronik sangat rawan tindak kejahatan. Siapapun yang menggunakan internet mungkin saja terkecoh dan menjadi korban tindak kejahatan dunia maya.

Untuk itu, masyarakat pengguna jaringan komunikasi elektronik harus lebih waspada. Berbagai langkah pencegahan perlu dijalankan.

Sampai sejauh ini, langkah utama untuk mencegah terjadinya kejahatan dunia maya adalah dengan mengaplikasikan ilmu kriptografi. Berbagai teknik enkripsi digunakan dalam mnyembunyikan data-data penting.

2. Kejahatan dunia maya

2.1. Definisi Kejahatan dunia maya

Kejahatan dunia maya atau *cybercrime* pada dasarnya adalah suatu tindak pidana yang mempunyai hubungan dengan ruang dunia maya, baik yang menyerang fasilitas umum di dalam ruang dunia maya ataupun kepemilikan pribadi.

Encyclopedia of crime and justice, New York: Free Press, 1983, (volume 4 hlm. 218-222) mendefinisikan *cybercrime* atau kejahatan dunia maya sebagai: Setiap perbuatan melawan hukum yang memerlukan pengetahuan tentang teknologi komputer yang bertujuan untuk dapat melakukan kejahatan yang dapat dikategorikan dalam dua bentuk, yaitu: penggunaan komputer sebagai alat untuk melakukan suatu kejahatan, seperti pemilikan uang secara ilegal, pencurian properti; atau untuk merencanakan suatu kejahatan; mengunakan komputer sebagai obyek dari suatu kejahatan, seperti sabotase, pencurian atau perubahan data-data milik pihak lain.

Kejahatan dunia maya sudah pasti membutuhkan kemampuan *crytanalysis* yang relatif sulit karena untuk menembus keamanan komputer-komputer dan aplikasi-aplikasi di dalam dunia maya, seorang penyerang pasti menemukan kode-kode hasil enkripsi yang harus dipecahkan untuk bisa melanjutkan aksinya. Apalagi saat ini teknik-teknik enkripsi yang digunakan oleh penyedia layanan pada jaringan komunikasi elektronik sebagian besar hampir tidak mungkin untuk dipecahkan.

Salah satu versi membagi kejahatan dunia maya menjadi tiga bagian yaitu pelanggaran akses, pencurian data, dan penyebaran informasi untuk tujuan kejahatan.

Versi yang lain membagi tipe-tipe kejahatan dunia maya menjadi tujuh, seperti dikemukakan Philip Renata dalam suplemen BisTek Warta Ekonomi No. 24 edisi Juli 2000, h.52 yaitu:

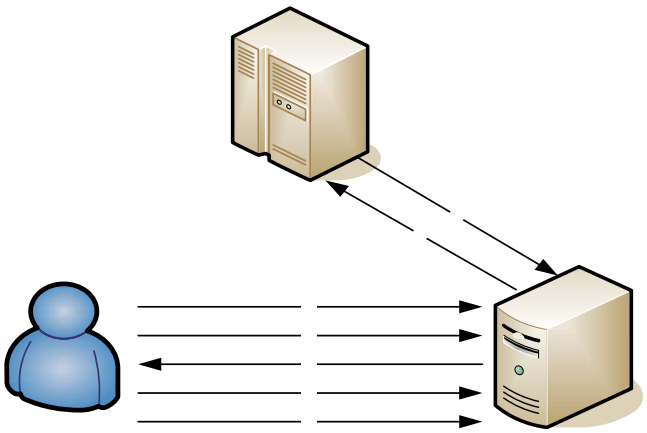
a. *Joy computing*, yaitu pemakaian komputer orang lain tanpa izin. Hal ini termasuk pencurian waktu operasi komputer. Penggunaan waktu operasi komputer lain banyak digunakan untuk mengirimkan *spam e-mail* agar tidak terlacak. Saat ini terdapat sekitar 3 sampai 4 juta *bot* yang aktif di Internet. *Botnet* telah menjadi pasukan penggerak di balik organisasi kejahatan *online* karena mereka memiliki risiko yang rendah dengan potensi keuntungan yang tinggi,

b. *Hacking*, yaitu mengakses secara tidak sah atau tanpa izin dengan alat suatu terminal. Menurut sebuah penelitian di Inggris, *hacker* biasanya melakukan serangan ke sistem komputer rumahan sebanyak 50 kali per malam. Serangan tersebut bisa berupa pembajakan sistem komputer seutuhnya atau hanya menjadikan komputer korban menjadi PC "zombie". Selama satu bulan penelitian, salah satu PC rumahan dibiarkan terkoneksi terus dengan internet. Ternyata para *hacker* berupaya memperoleh data di dalam PC dengan

menggunakan virus dan malware untuk menjumput informasi penting pemiliknya.

c. *The Trojan Horse*, yaitu manipulasi data atau program dengan jalan mengubah data atau instruksi pada sebuah program, menghapus, menambah, menjadikan tidak terjangkau dengan tujuan untuk kepentingan pribadi atau orang lain.
Salah satu kasus terbaru dengan trojan terjadi pada pengguna *Voice over Internet Protocol* (*VoIP*) *Skype*. Trojan tersebut menyebar melalui *software* komunikasi *VoIP Skype* dan berupaya mencuri *password* aplikasi tersebut. Trojan mengirim sebuah pesan melalui *tool Skype Chat* dan meminta penerimanya untuk menjumput *file* **sp.exe**. Virus di dalam *file* tersebut akan menyebar jika program dijalankan dan akan men-*download* kode pemrograman *Skype*, menggandakan diri, dan mengambil alih *password*. Situs web yang diserang oleh trojan ini telah ditutup untuk menghindari kerugian lebih lanjut.

d. *Data Leakage*, yaitu menyangkut bocornya data ke luar terutama mengenai data yang harus dirahasiakan. Pembocoran data komputer itu bisa berupa berupa rahasia negara, perusahaan, data yang dipercayakan kepada seseorang dan data dalam situasi tertentu.
Ilustrasi salah satu contoh tindakan kejahatan dunia maya oleh seorang penyusup (*intruder*) melalui komputernya untuk mencuri data yang sedang dipertukarkan antara dua komputer lain dengan cara memperlambat respon server dapat dilihat pada gambar berikut:



Keterangan gambar:
1. *Look up* foobar.the-intruder.com untuk dipaksakan masuk ke ISP's cache
2. *Look up* www.the-intruder.com untuk mendapatkan nomor sekuensial selanjutnya dari ISP
3. Permintaan kepada www.the-intruder.com (membawa nomor sekuensial selanjutnya dari ISP, sebut saja n
4. Dengan sigap dan cepat look up user2.com (untuk memaksa ISP untuk memasukkan com server ke dalam antrian pada langkah 5)
5. Antrian yang sah untuk user2 dengan sekuensial = n+1
6. Intruder memberikan jawaban palsu
7. Jawaban asli datang (ditolak karena sudah terlambat

e. *Data Diddling*, yaitu suatu perbuatan yang mengubah data valid atau sah dengan cara tidak sah, mengubah *input* data atau *output* data. Perbuatan penyusup yang memasuki ruang komunikasi antara para pengguna yang sah bisa berlanjut kepada *data didling*.

f. *To frustate data communication* atau penyia-nyiaan data komputer.

g. *Software piracy* yaitu pembajakan perangkat lunak terhadap hak cipta yang dilindungi HAKI.

Salah satu jenis kejahatan lain pada dunia maya yang termasuk baru tetapi telah cukup banyak merugikan konsumen internet adalah "*phishing*".

Phishing adalah suatu tindak kejahatan yang menggunakan cara sosial. Pelakunya mencoba untuk mendapatkan informasi sensitif seperti *password* dan informasi detil kartu kredit dengan cara yang curang seperti dengan menyamar menjadi seseorang

atau perusahaan pada suatu jaringan komunikasi elektronik, baik melalui surat elektronik, pesan instan, dengan membuat *website* yang seakan-akan dari perusahaan dagang elektronik yang menawarkan berbagai barang, ataupun sejenisnya. *Phishing* sebelumnya telah banyak dilakukan melalui telepon.

2.2. Kejahatan Dunia Maya di Indonesia

Berdasarkan survei AC Nielsen 2001, Indonesia ternyata menempati posisi ke enam terbesar di dunia atau ke empat di Asia dalam tindak kejahatan di internet, meski tidak disebutkan secara rinci kejahatan macam apa saja yang terjadi di Indonesia maupun WNI yang terlibat dalam kejahatan tersebut.

Sepanjang 2003 Indonesia berada di urutan teratas sebagai negara asal pelaku kejahatan kartu kredit via Internet (c*yberfraud/carding*) secara presentase, dan secara volume berada di urutan ketiga.

Di tahun 2005 Indonesia masih membawahi negara lain seperti Nigeria, Pakistan, Ghana dan Israel. Banyak warga Indonesia yang kedapatan melakukan penipuan, penyadapan, pencurian dan kejahatan lainnya. Di Indonesia sendiri, daerah yang menjadi tempat terjadinya kriminalitas dunia maya yang terbanyak yakni Yogyakarta dan menyusul Jawa Tengah, Jawa Barat, Jakarta, dan Medan. Selain kejahatan lewat internet, juga banyak terjadi kejahatan di bidang perbankan. Sudah banyak juga terungkap adanya pembobolan kartu ATM.

Kasus-kasus kejahatan dunia maya yang banyak terjadi di Indonesia setidaknya ada empat jenis berdasarkan modusnya, yaitu:

1. Pencurian Nomor Kartu Kredit.

   Penyalahgunaan kartu kredit milik orang lain di internet atau *carding* merupakan kasus kejahatan dunia maya terbesar yang berkaitan dengan dunia bisnis internet di Indonesia. *Carding* menimbulkan kerugian dalam jumlah puluhan miliar rupiah setiap tahunnya.

   Penyalahgunaan kartu kredit milik orang lain memang tidak rumit dan bisa dilakukan secara fisik atau *on-line*. Nama dan kartu kredit orang lain yang diperoleh di berbagai tempat (restaurant, hotel atau segala tempat yang melakukan transaksi pembayaran dengan kartu kredit) dimasukkan di aplikasi pembelian barang di *internet.*

2. Memasuki, memodifikasi atau merusak homepage (hacking)

   Salah satu kegiatan yang sering dilakukan oleh *cracker* adalah mengubah halaman web, yang dikenal dengan istilah *deface*. Pembajakan dapat dilakukan dengan mengeksploitasi lubang keamanan. Selama caturwulan terakhir tahun 2006, statistik di Indonesia menunjukkan bahwa terdapat 1 (satu) situs web dibajak setiap harinya.

   Menurut seorang ahli pada umumnya tindakan *hacker* Indonesia belum separah aksi di luar negeri. Perilaku *hacker* Indonesia baru sebatas masuk ke suatu situs komputer orang lain yang ternyata rentan penyusupan dan memberitahukan kepada pemiliknya untuk berhati-hati. Di luar negeri *hacker* sudah memasuki sistem perbankan dan merusak data base bank.

3. Pencurian dan penggunaan account Internet milik orang lain.

   Pola umum yang digunakan untuk menyerang jaringan komputer adalah memperoleh akses terhadap *account user* dan kemudian menggunakan sistem milik korban sebagai *platform* untuk menyerang situs lain. Hal ini dapat diselesaikan hanya dalam waktu 45 detik dan mengotomatisasi akan sangat mengurangi waktu yang diperlukan.

   Salah satu kesulitan dari sebuah ISP (Internet Service Provider) adalah adanya account pelanggan mereka yang dicuri dan digunakan secara tidak sah. Berbeda dengan pencurian yang dilakukan secara fisik, pencurian account cukup menangkap userid dan *password* saja. Hanya informasi yang dicuri. Sementara itu orang yang kecurian tidak merasakan hilangnya benda yang dicuri. Pencurian baru terasa efeknya jika informasi ini digunakan oleh yang tidak berhak. Akibat

dari pencurian ini, penggunaan dibebani biaya penggunaan acocunt tersebut. Kasus ini banyak terjadi di ISP. Namun yang pernah diangkat adalah penggunaan account curian oleh dua Warnet di Bandung.

4. Penyerangan situs atau *surat elektronik* melalui virus atau *spamming*.

   Modus yang paling sering terjadi adalah mengirim virus melalui surat elektronik. Lebih dari 90 persen surat elektronik yang dikirim pada bulan Juli dan Oktober tahun 2006 merupakan *junk mail*. Volume spam sering dianggap sebagai barometer yang menunjukkan tingkat keamanan komunitas Internet secara luas. Ini dikarenakan kebanyakan spam disebarkan melalui *bot*, yaitu komputer yang telah terserang virus atau *worm*. Saat ini terdapat sekitar 3 sampai 4 juta *bot* yang aktif di Internet. Para pelaku kriminal juga menyiapkan *bot* dengan program yang dapat menyimpan dan mencuri *username* dan *password* dari komputer yang telah terjangkiti.Di luar negeri kejahatan seperti ini sudah diberi hukuman yang cukup berat. Berbeda dengan di Indonesia yang sulit diatasi karena peraturan yang ada belum menjangkaunya.

Selain keempat modus di atas masih terdapat beberapa modus lain seperti penyadapan pesan, pencurian dan/atau pengrusakan data-data pada basis data milik pihak lain, dan sebagainya.

Pengamat telematika bahkan menilai kejahatan dunia maya atau *cybercrime* melalui telepon seluler akan mengalami peningkatan yang signifikan tahun depan seiring bertambahnya layanan Internet pada kartu prabayar dan pascabayar oleh beberapa operator seluler. Sebelumnya, kejahatan dunia maya memang lebih dikenal lewat akses Internet melalui komputer desktop maupun *notebook* yang biasanya dilakukan di warung internet dan perkantoran. Dari total kejahatan dunia maya yang akan terjadi di Indonesia pada tahun depan, diprediksikan kejahatan dunia maya melalui ponsel akan mencapai 30%.

3. Manajemen Kunci

Kriptografi memang sangat membantu para pengguna layanan pada jaringan komunikasi elektronik dalam melindungi privasinya. Namun, semakin canggih teknik kriptografi yang digunakan, semakin hebat pula teknik *crtanalysis* yang digunakan oleh para *hacker*. Apalagi dengan adanya pembatasan teknik kriptografi yang boleh diterapkan oleh konsumen dan penyedia layanan di dunia maya di beberapa negara dengan alasan mencegah terorisme.

Dari semua informasi yang telah penulis sampaikan sebelumnya, sebenarnya hal utama yang diincar oleh *hacker* ataupun pelaku kejahatan dunia maya lainnya adalah *user id* dan *password* para konsumen di dunia maya. Selain dengan menginstal dan mengaktifkan *antivirus* dan *firewall* terkini, mewaspadai adanya pesan atau surat elektronik yang datang dari pengirim yang tidak dikenal, kita juga perlu menjaga kerahasiaan user id beserta *PIN* atau *password* yang kita miliki.

PIN atau *password* tersebut merupakan kunci yang digunakan untuk otentikasi pengguna. Jika kunci tersebut telah dikuasai oleh suatu pihak, secara otomatis keseluruhan aplikasi bisa dikuasai oleh pihak tersebut.

Untuk menjaga kerahasiaan kunci, tidak cukup dengan hanya tidak memberitahukannya kepada pihak lain. Banyak perilaku kita yang tanpa kita sadari telah memudahkan pihak lain untuk mengetahui kunci berupa *PIN* atau *password* kita. Contohnya ketika kita dengan sengaja mengetikkan semua *user id* beserta *PIN* atau *password* yang kita miliki untuk beberapa aplikasi pada sebuah file di media penyimpanan elektronik yang kita miliki dan jarang bahkan tidak pernah mengganti *PIN* atau *password* yang kita miliki.

3.1. Manajemen Kunci Publik

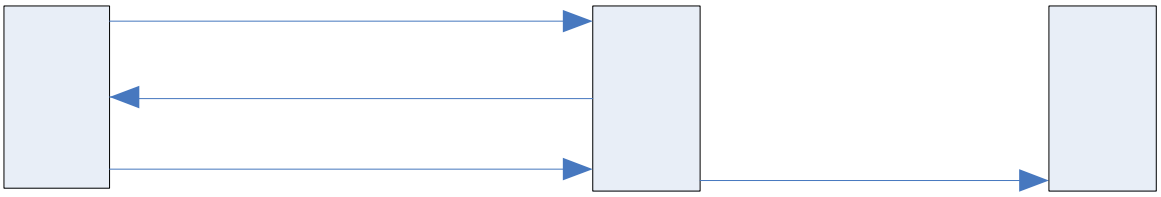
Kriptografi kunci publik memungkinkan komunikasi yang aman bagi pihak-pihak yang tidak memberitahukan kunci secara langsung. Kriptografi kunci publik juga tidak membutuhkan peran dari pihak ketigaa yang bisa dipercaya. Untuk mengecek keaslian dan kesatuan dari pesan yang diterima, dilakukan

penandaan dengan *message digests* yang metodenya telah disepakati sebelumnya.

Walaupun tampaknya begitu mudah untuk melakukan komunikasi yang aman dengan kunci publik, masih terdapat satu masalah yang harus diatasi sebelumnya. Ketika satu pihak, sebut saja A ingin mengirimkan pesan kepada satu pihak lain, sebut saja B; A perlu mengetahui kunci publik yang dimiliki oleh B. Untuk mengetahuinya, A cukup mengetikkan pada *URL* (*Uniform Resource Locater*) yang dimiliki B untuk mendapatkan alamat DNS (*Domain Name System*) dari *home page* milik B, baru kemudian A mengirimkan permintaan GET ke alamat DNS tersebut.

Masalah akan timbul apabila pihak ketiga, sebut saja C, yang mempunyai maksud negatif menengahi pengiriman permintaan dari A dan bertindak sebagai home page B kemudian menjawab permintaan kunci publik B dengan kunci publik yang dimiliknya. Ketika bermaksud mengirimkan pesan kepada B, A akan menggunakan kunci publik palsu tersebut dan pesan yang telah terenkripsi akan diterima oleh C. C bisa mendekripsinya untuk mengetahui isi pesan yang sebenarnya kemudian mengenkripsinya kembali dengan kunci publik yang asli dari B. Kemudian C akan mengirimkannya kepada B seolah-olah C adalah A. Ketika C mendekripsi pesan dari A untuk B dengan kunci publik yang diberikannya kepada A, sangatlah memungkinkan bagi C untuk mengubah pesan aslinya. Selanjutnya, banyak hal yang bisa terjadi.

Ilustrasinya sebagai berikut:



Untuk mencegah terjadinya penyadapan dan pengubahan pesan yang dikirimkan, beberapa mekanisme bisa dilakukan. Penjelasan lebih lanjut mengenai hal ini telah dibahas pada kuliah IF5054 Kriptografi dalam topik *Public Key Infrastucture* (*PKI*)

3.2. Manajemen Kunci Simetri

PIN dan *password* yang biasanya kita gunakan ketika *login* pada suatu layanan di dalam jaringan komunikasi elektronik seperti pada *ATM* dan surat elektronik hanyalah untuk otentikasi pengguna. Kunci semacam ini termasuk jenis kunci simetri. Manajemen kunci simetri telah dibahas pada kuliah IF5054 Kriptografi dalam topik Manajemen Kunci.

Ketika seorang pengguna layanan memasukkan *PIN* atau *password* mereka, PIN atau *password* itu akan ditranformasi ke dalam bentuk kompresi dengan fungsi *hash* satu arah untuk disesuaikan dengan data di basis data pada komputer *host*.

Cryptanalyst yang menyerang *PIN* atau *password* seperti ini biasanya telah menyiapkan basis data sendiri yang berisi hasil kompresi sejumlah rangkaian kata dan angka yang mungkin digunakan seseorang sebagai *PIN* atau *password*-nya. Hal ini memang telah dibahas pada kuliah IF5054 Kriptografi di dalam topik Protokol Kriptografi, tetapi berhubungan dengan judul makalah yang diangkat oleh penulis, maka hal ini perlu disampaikan kembali pada makalah ini.

Tingkat penggunaan jaringan komunikasi elektronik di Indonesia masih tergolong sedikit berdasarkan persentasenya terhadap jumlah penduduk (sekitar 0,5%) dan penggunaannya juga relatif baru dibandingkan di negara-negara lain yang lebih maju. Penggunaan jaringan komunikasi elektronik di Indonesia juga masih tergolong sederhana. Sebagian besar masyarakat menggunakannya untuk sekedar mencari informasi, berkirim surat, dan mengobrol dengan kenalannya.

Pengguna jaringan komunikasi elektronik di Indonesia masih banyak yang belum

mengetahui benar proses enkripsi/dekripsi yang terjadi pada produk yang mereka gunakan. Karena itu, langkah awal yang penulis anjurkan untuk para pengguna jaringan komunikasi elektronik adalah dengan melakukan manajemen kunci yang sederhana dan mudah.

4. Kuesioner

Karena banyaknya kejahatan di dunia maya yang terjadi di Indonesia dan pentingnya kerahasiaan *PIN* dan *password*, penulis mencoba mencari tahu mengenai tingkat pengetahuan pengguna jaringan komunikasi elektronik untuk menjalankan manajemen kunci.

Manajemen kunci yang dimaksud penulis adalah rangkaian langkah sederhana (seperti yang telah disebutkan pada bagian 3. Manajemen Kunci) yang bertujuan untuk melindungi kerahasiaan kunci berupa *PIN* atau *password* yang dimiliki.

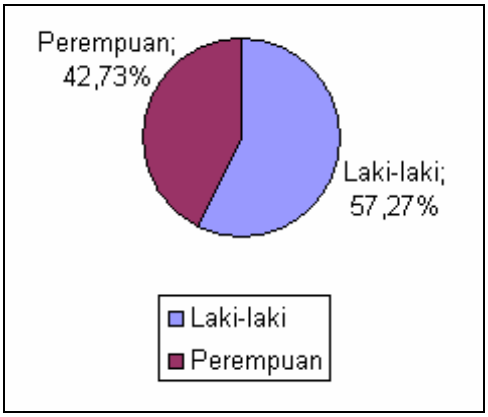
Kuesioner berisi sembilan pertanyaan inti dengan pertanyaan pertama memiliki dua anak pertanyaan, pertanyaan kedua memiliki empat anak pertanyaan, pertanyaan ketiga memiliki dua anak pertanyaan, sedangkan keenam pertanyaan selanjutnya tidak memiliki anak pertanyaan.

4.1. Sebaran Responden

Penulis menyebarkan kuesioner kepada 150 (seraus lima puluh) orang responden di kota Bandung. Karena sejumlah lembaran kuesioner tidak diisi dengan lengkap, maka penulis hanya mengambil jawaban dari lembaran kuesioner yang lengkap dari 110 (seratus sepuluh) orang responden saja dengan sebaran jenis kelamin dan usia sebagai berikut:

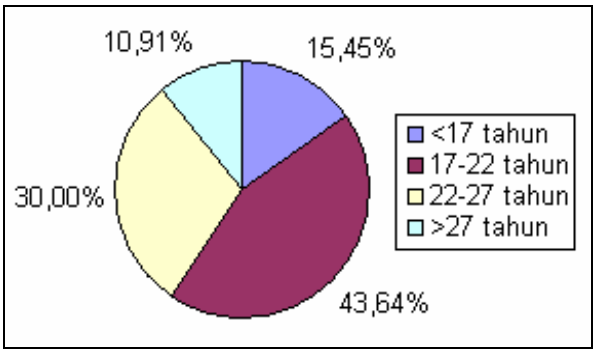
Jenis kelamin:

- Sebanyak 63 orang atau 57,27% dari seluruh responden berjenis kelamin laki-laki dan
- Sisanya sebanyak 47 orang atau 42,73% dari seluruh responden berjenis kelamin perempuan.



Usia responden:

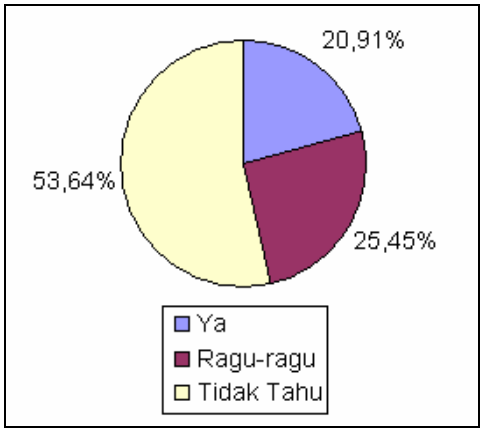
- Sebanyak 17 orang atau 15,45% responden berusia di bawah 17 tahun,
- Sebanyak 48 orang atau 43,64% responden berusia di antara 17 sampai 22 tahun,
- Sebanyak 33 orang atau 30,00% responden berusia di antara 22 sampai 27 tahun, dan
- Sebanyak 12 orang atau 10,91% responden berusia di atas 27 tahun.



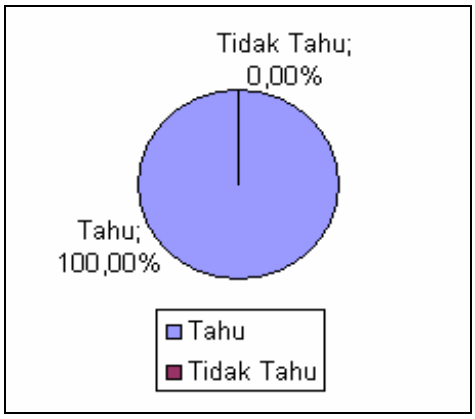
4.2. Jawaban Responden

Pertanyaan pertama menanyakan apakah responden mengetahui pengertian kriptografi atau enkripsi. Hasilnyayang diperoleh sebagai berikut:

- Sebanyak 23 orang atau 20,91% dari responden menjawab ya,
- Sebanyak 28 orang atau 25,45% dari responden menjawab ragu-ragu, sedangkan
- 59 orang sisanya atau 53,64% dari responden menjawab tidak tahu.

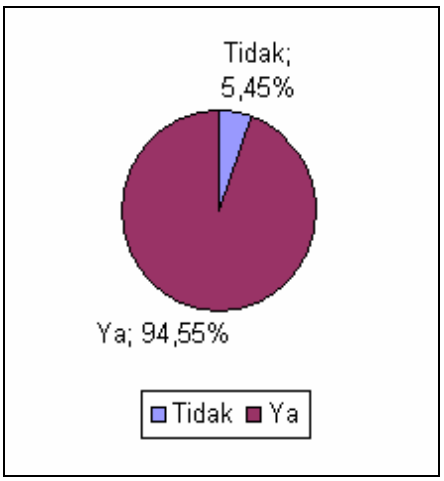


Di antara 18 orang yang menjawab ya, semuanya mengetahui penggunaan kriptografi atau enkripsi dalam kehidupan sehari-hari. Sebagian besar responden mencontohkan penggunaannya pada layanan surat elektronik.



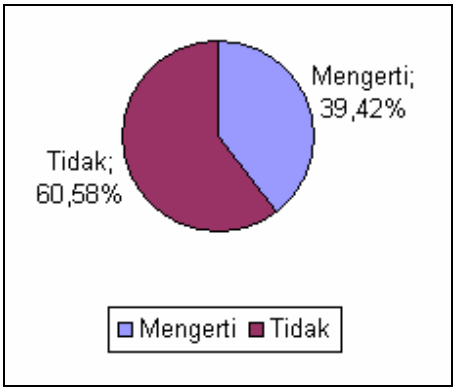
Pertanyaan kedua menanyakan apakah responden pernah menggunakan surat elektronik. Hasilnya yang diperoleh sebagai berikut:

- Hanya terdapat 6 orang atau 5,45% dari keseluruhan responden yang menjawab tidak pernah sedangkan
- sisanya sebanyak 104 orang atau 94,55% dari keseluruhan responden menjawab mereka pernah menggunakan layanan surat elektronik.



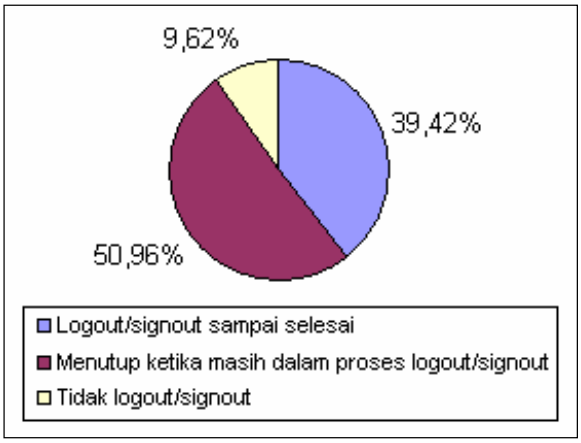
Di antara responden-responden yang pernah menggunakan surat elektronik tersebut, penulis menanyakan lagi apakah mereka menekan tombol yes/no untuk semua pertanyaan yang muncul ketika login dan mengerti/tidak mengerti tentang maksud pertanyaannya. Hasil yang diperoleh:

- Sebanyak 41 orang menekan 39,42% tombol yes/no untuk semua pertanyaan yang muncul ketika login dan mengerti maksud pertanyaannya dan
- Sisanya sebanyak 63 orang atau 60,58% menekan tombol yes/no untuk semua pertanyaan yang muncul ketika login tanpa mengerti maksud pertanyaannya.



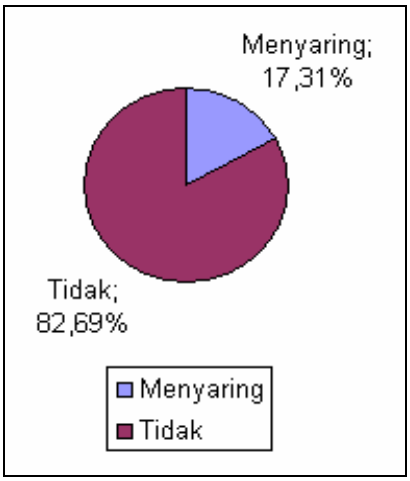
Jawaban responden atas pertanyaan mengenai cara *logout* atau *sign out* yang mereka lakukan setelah selesai menggunakan layanan surat elektronik tersebut menunjukkan hasil sebagai berikut:

- Sebanyak 41 orang atau 39,42%menutup aplikasi setelah proses *logout* atau *sign out* benar-benar selesai,
- 53 orang atau 50,96% menutup aplikasi ketika proses *logout* atau *sign out* masih berlangsung,
- 10 orang atau 9,62% langsung menutup aplikasi tanpa *logout* atau *sign out*.



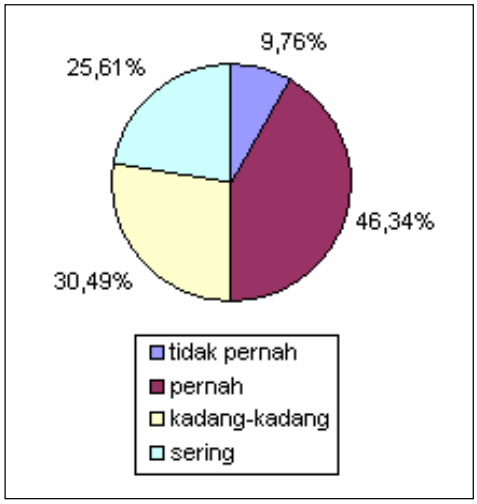
Juga di antara yang pernah menggunakan surat elektronik tersebut, penulis menanyakan lagi apakah mereka melakukan penyaringan terhadap surat-surat yang masuk. Diperoleh hasil:

- Hanya 18 orang atau 17,31% di antaranya yang menyaring atau memisahkan surat-surat yang masuk dan
- 82 orang sisanya atau 82,69% tidak memisahkan atau menyaring surat-surat yang masuk.



Di antara responden yang tidak memisahkan atau menyaring surat-surat yang masuk, ditanyakan kembali mengenai respon mereka terhadap surat-surat yang masuk dengan nama pengirim yang tidak mereka kenal. Hasil yang diperoleh yaitu:

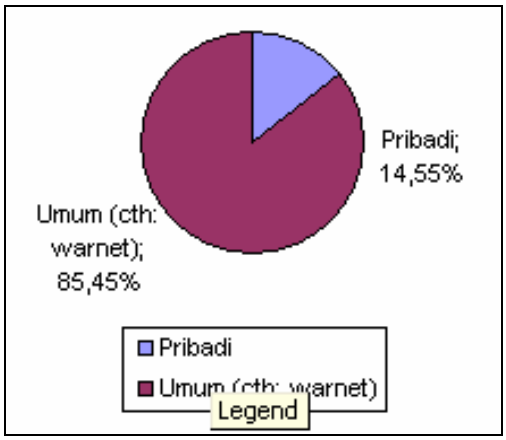
- Sebanyak 8 orang atau 9,76% tidak pernah membuka surat masuk yang berasal dari pengirim yang tidak dikenal olehnya,
- Sebanyak 35 orang atau 46,34% pernah membuka surat masuk yang berasal dari pengirim yang tidak dikenal,
- Sebanyak 18 orang 30,49% kadang-kadang membuka surat masuk yang berasal dari pengirim yang tidak dikenal olehnya,
- Sebanyak 21 orang atau 25,61% sering membuka surat masuk yang berasal dari pengirim yang tidak dikenal,
- Tidak ada yang selalu membuka surat yang berasal dari pengirim yang tidak dikenal.



Pertanyaan ketiga menanyakan apakah responden lebih sering terhubung dengan internet melalui komputer/*notebook*/telepon seluler pribadi ataukah melalui warung internet/tempat umum lainnya. Hasil yang diperoleh:

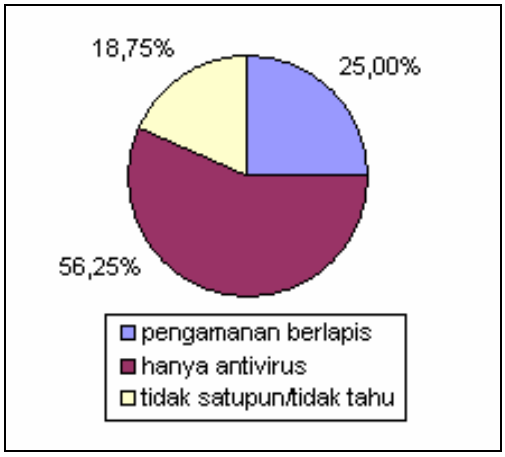
- Sebanyak 16 orang atau 14,55% menjawab lebih sering sering terhubung dengan internet melalui komputer/ *notebook*/telepon seluler pribadi dan
- sisanya 94 orang atau 85,45% menjawab lebih sering terhubung dengan internet

melalui warung internet atau tempat umum lainnya.



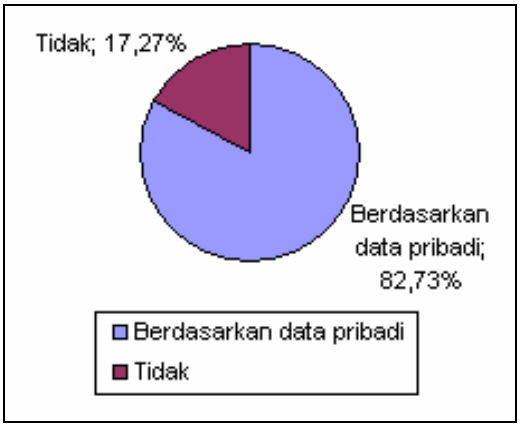
Untuk responden yang menjawab bahwa mereka lebih sering terhubung dengan internet melalui komputer *desktop*/*notebook*/telepon seluler pribadi, penulis menanyakan lagi apakah mereka menggunakan pengaman berlapis seperti *firewall*, antivirus, dan sebagainya. Hasilnya sebagai berikut:

- Sebanyak 4 orang atau 25,00% menjawab bahwa mereka telah menggunakan pengaman berlapis seperti *firewall* dan antivirus,
- Sebanyak 9 orang atau 56,25% menjawab bahwa mereka hanya menggunakan antivirus,
- Sisanya sebanyak 3 orang atau 18,75% menjawab bahwa mereka tidak menggunakan pengaman sama sekali atau tidak tahu bahwa mereka menggunakan pengaman.



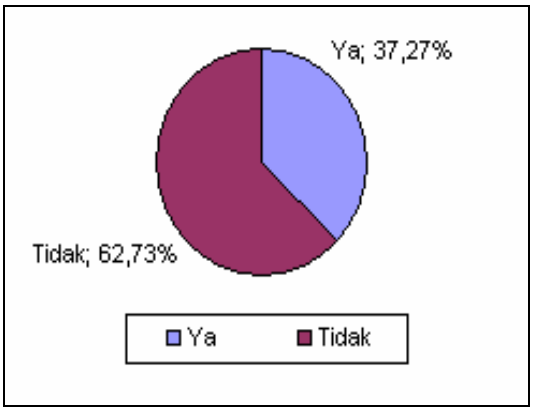
Pertanyaan keempat menanyakan apakah responden membuat *PIN* atau *password* berdasarkan data pribadinya (nama, tanggal lahir, no telepon, dan sebagainya). Jawaban responden:

- Sebanyak 91 orang atau 82,73% menjawab ya,
- sisanya sebanyak 19 orang atau 17,27% menjawab tidak.



Pertanyaan kelima menanyakan apakah *PIN* atau *password* responden ada yang diketahui juga oleh orang lain (seperti keluarga, sahabat, dan sebagainya). Diperoleh hasil sebagai berikut:

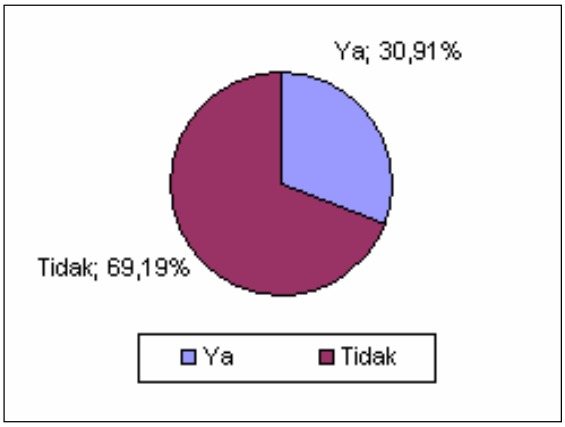
- Sebanyak 41 orang atau 37,27% menjawab ya dan
- Sebanyak 69 orang atau 62,73% menjawab tidak.



Pertanyaan keenam menanyakan apakah responden menyimpan *PIN* atau *password*

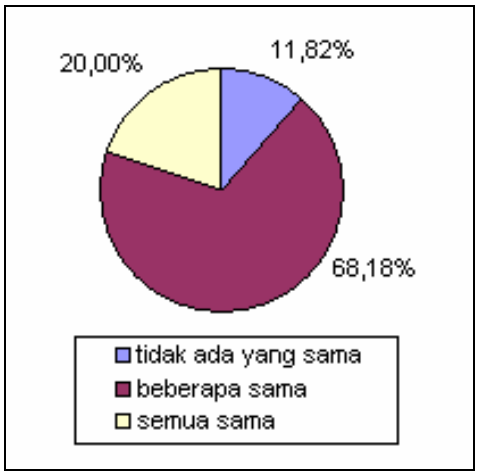
yang dimilikinya pada suatu media penyimpanan (seperti memori HP, komputer, kartu ATM, buku catatan, dan sebagainya). Diperoleh hasil sebagai berikut:

- sebanyak 34 orang atau 30,91% menjawab ya dan
- sisanya sebanyak 76 orang atau 69,19% menjawab tidak.



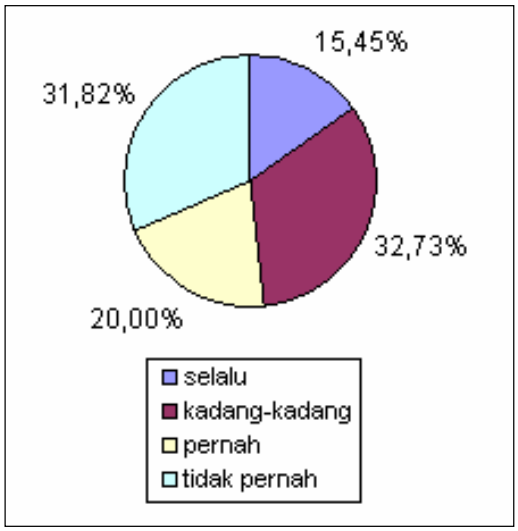
Pertanyaan ketujuh menanyakan apakah responden menggunakan *PIN* atau *password* yang sama untuk aplikasi-aplikasi yang responden gunakan. Hasil yang diperoleh menunjukkan:

- 13 orang atau 11,82% menjawab ya, semuanya sama,
- 75 orang atau 68,18% menjawab ya, beberapa sama,
- 22 orang atau 20,00% menjawab tidak, semuanya berbeda.

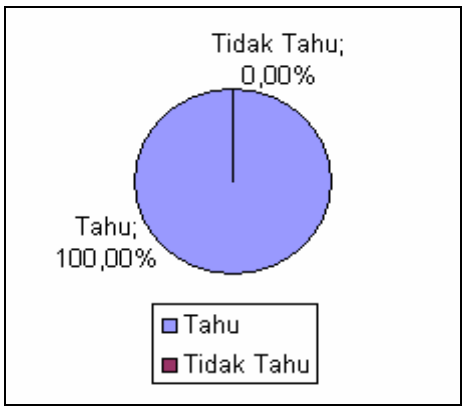


Pertanyaan kedelapan menanyakan apakah responden mengganti *PIN* atau *password*-nya secara rutin. Hasil yang diperoleh penulis sebagai berikut:

- Sebanyak 17 orang atau 15,45% dari keseluruhan responden menjawab bahwa mereka selalu menggantinya secara rutin,
- Sebanyak 36 orang atau 32,73% dari keseluruhan responden menjawab bahwa mereka kadang-kadang menggantinya,
- Sebanyak 22 orang atau 20,00% dari keseluruhan responden menjawab bahwa mereka pernah mengganti *PIN* atau *password* mereka, dan
- Sisanya sebanyak 35 orang atau 31,82% dari keseluruhan responden menjawab bahwa mereka tidak pernah mengganti *PIN* atau *password* mereka.



Pertanyaan terakhir menanyakan kepada responden apakah mereka mengetahui pentingnya kerahasiaan *PIN* atau *password* yang dimiliki oleh responden. Ternyata diperoleh hasil bahwa 100,00% atau seluruh responden menjawab ya, mereka mengetahuinya. Sebagian besar menjelaskan bahwa kerahasiaan tersebut harus dijaga untuk menghindari terjadinya tindak kejahatan seperti pencurian data, pengrusakan data, pencurian uang, serta penyalahgunaan kartu kredit.



Ringkasan hasil kuesioner adalah sebagai berikut:

- Sebagian besar responden (53,64%) tidak mengetahui tentang kriptografi atau enkripsi,
- Hampir seluruh responden (94,55%) pernah menggunakan layanan surat elektronik,
- Sebagian (60,58%) responden yang pernah menjadi pengguna layanan surat elektronik tidak mengerti maksud dari tulisan-tulisan yang muncul ketika mengakses layanan surat elektronik,
- Kurang dari setengah (39,42%) responden yang pernah menjadi pengguna layanan surat elektronik melakukan *logout/signout* dengan benar,
- Sebagian besar responden (82,69%) yang pernah menjadi pengguna layanan surat elektronik tidak melakukan penyaringan terhadap surat-surat elektronik yang mereka terima,
- Sebagian besar (46,34%) responden yang pernah menggunakan layanan surat elektronik pernah membuka surat yang datang dari pengirim yang tidak dikenal.
- Sebagian besar responden (85,45%) mengaku terhubung dengan internet melalui warung internet atau tempat umum lainnya,
- Lebih dari setengah (56,25%) responden yang terhubung dengan internet melalui komputer *desktop* / *notebook* / telepon seluler pribadi hanya menggunakan antivirus sebagai pengaman dan masih terdapat responden yang tidak mengetahui apakah komputer *desktop* / *notebook* / telepon seluler pribadi mereka telah dilengkapi dengan pengamanan atau belum (18,75%).
- Sebagian besar (82,73%) responden membuat *PIN* atau *password* berdasarkan data pribadinya,
- Sebagian besar (68,18%) responden memiliki *PIN* atau *password* yang sama untuk beberapa aplikasi yang mereka gunakan,
- Sebagian besar (69,19%) responden tidak menyimpan *PIN* atau *password* yang dimilikinya pada suatu media penyimpanan,
- Masih terdapat cukup banyak (37,27%) responden yang *PIN* atau *password* mereka diketahui oleh orang lain,
- Hanya sebagian kecil (15,45%) responden yang mengganti *PIN* atau *password* yang mereka miliki secara rutin,
- Seluruh responden mengaku mengetahui pentingnya kerahasiaan *PIN* atau *password* yang dimiliki

4.3. Analisis Hasil Kuesioner

Berdasarkan hasil kuesioner, diketahui bahwa pengetahuan masyarakat pengguna jaringan komunikasi elektronik di kota Bandung tentang kriptografi, khususnya manajemen kunci masih rendah.

Penyebabnya bisa datang dari berbagai pihak. Pihak utama yang paling berpengaruh adalah pengguna itu sendiri. Sebagai seorang yang banyak berhubungan dengan jaringan komunikasi elektronik, seorang pengguna perlu menggali informasi yang memadai mengenai apapun yang berhunbungan dengan jaringan komunikasi elektronik tersebut.

Salah satu pihak lain yang juga sangat berpengaruh adalah penyedia layanan pada jaringan komunikasi elektronik. Konsumen layanan pada jaringan komunikasi elektronik lebih memperhatikan tampilan pada layanan

yang mereka akses. Apabila pihak penyedia layanan pada jaringan komunikasi elektronik tidak memberikan penekanan yang cukup pada pentingnya menjaga kemanan kunci yang mereka miliki.

Pihak lain yang seharusnya juga banyak berperan adalah pemerintah. Pemerintah harus membantu masyarakatnya dalam menjaga keamanan data dan sistem elektronik yang beroperasi di negara Indonesia.

Pengetahuan mengenai kriptografi, khususnya enkripsi dan dekripsi data harus lebih diperhatikan dan perlu diperbaiki mengingat inti penjagaan keamanan di dunia maya adalah mengerti cara kerja alat yang digunakan untuk menjaga keamanan itu. Sejalan dengan itu, pengetahuan dan penerapan manajemen kunci yang sesuai juga ditingkatkan karena hal utama yang diperlukan untuk proses enkripsi/dekripsi data adalah kuncinya.

5. Solusi

5.1 Solusi terhadap Rendahnya Pengetahuan Pengguna Jaringan Komunikasi Elektronik mengenai Kriptografi Khususnya Manajemen Kunci

Beberapa solusi yang diajukan penulis terhadap rendahnya pengetahuan masyarakat tentang kriptografi, khususnya dalam menjaga *PIN* atau *password* yang mereka miliki antara lain:

- Pemberitahuan dan himbauan dari penyedia layanan pada jaringan komunikasi elektronik kepada para konsumennya untuk menjaga kunci yang dimilikinya dengan baik. Contohnya himbauan untuk mengganti *PIN* atau *password* secara rutin.

- Sosialisasi oleh pemerintah melalui Departemen Komunikasi dan Informasi mengenai kriminalitas di dunia maya dan langkah-langkah pencegahannya.

- Konsumen layanan di dunia maya perlu mencari informasi yang banyak mengenai dunia maya, khususnya mengenai keamanan di dunia maya serta memperhatikan lebih teliti layanan yang mereka akses.

- Tidak ada salahnya apabila warnet turut berpartisipasi membuat papan informasi yang diisi dengan berita-beriita dan pengetahuan-pengetahuan yang penting bagi para konsumen layanan di dunia maya, mengingat banyaknya konsumen yang mengakses layanan-layanan di dunia maya melalui warung internet.

5.2 Solusi untuk Mengurangi Tingkat Kejahatan Dunia Maya yang Relatif Sangat Tinggi

Berhubungan dengan tingkat pengetahuan masyarakat yang masih rendah mengenai kriptografi, maka manajemen kunci yang perlu disosialisasikan dan diterapkan harus dimulai dari langkah-langkah yang mudah dimengerti dan mudah pula untuk dilakukan.

Beberapa langkah yang manajemen kunci direkomendasikan oleh penulis kepada masyarakat pengguna jaringan komunikasi elektronik di Indonesia, khususnya di kota Bandung, untuk bisa mempertahankan kerahasiaan *PIN* atau *password* dalam tujuan mengurangi kemungkinan terjadinya kejahatan dunia maya adalah sebagai berikut:

1. Jangan membuat *PIN* atau *password* berdasarkan data pribadi yang akan relatif mudah untuk ditebak, seperti tanggal-tanggal, nama bulan, nama jalan, dan sebagainya. Gunakan bilangan/data acak dengan cakupan yang luas supaya tidak mudah ditebak. Usahakan untuk membuat *PIN* atau *password* yang panjang jika memungkinkan. Setidaknya hal ini bisa mempersulit penyerang. Karena kemampuan komputer yang masih terbatas untuk memproses data, maka semakin panjang *PIN* atau *password* yang digunakan, semakin banyak pula kemungkinan rangkaian *PIN* atau *password* yang harus diperiksa oleh komputer penyerang. Berarti akan semakin lama juga waktu yang diperlukan untuk mengetahui rangkaian *PIN* atau *password* yang tepat

2. Jangan menggunakan PIN atau password yang sama untuk beberapa aplikasi. Jika *PIN* atau *password* yang sama digunakan untuk beberapa aplikasi, kemungkinan besar akan banyak *account* yang dicuri sekaligus apabila sistem keamanan

komputer yang kita gunakan telah berhasil ditembus oleh penyerang.

3. Jangan pernah menuliskan *PIN* atau *password* pada sembarang tempat. Usahakan untuk mengingatnya dan tidak menuliskannya. Jika terpaksa menuliskannya, tempatnya harus diyakini relatif aman dari kemungkinan pencurian. Akan lebih baik jika dituliskan terpisah-pisah dan dienkripsi.

4. Jangan menerima tawaran untuk menyimpan user id dan *password* pada perangkat lunak pengingat yang biasanya ditawarkan ketika mengakses layanan surat elektronik. Bacalah dulu setiap tulisan yang muncul sebelum memilih ya atau tidaknya.

5. Gantilah *PIN* atau *password* secara rutin dalam jangka waktu yang relatif tidak terlalu lama, misalnya satu minggu satu kali atau dua minggu satu kali. Mengganti *PIN* atau *password* secara rutin akan sangat membantu apabila *PIN* atau *password* yang kita miliki ternyata hampir atau telah diketahui oleh pihak lain.

6. Jangan mudah terpengaruh untuk memberitahukan *PIN* atau *password* kepada pihak manapun yang memintanya, walaupun pihak tersebut mengatasnamakan seseorang atau perusahaan yang mempunyai hubungan baik dengan kita.

Selain langkah-langkah yang telah disebutkan penulis, tidak menutup kemungkinan bahwa terdapat langkah-langkah lain yang terpikirkan oleh dalam meningkatkan keamanan PIN dan password yang dimiliki.

Bagi para pengguna layanan surat elektronik harus melakukan prosedur keamanan yang memadai yaitu minimal:

- Tidak menyimpan *username* dan *password* pada media pengingat, terutama ketika mengakses layanan tersebut di tempat umum,
- Jangan pernah membuka surat masuk dari pengirim yang tidak dikenal. Apabila terdapat subjek surat yang mencurigakan, sebaiknya bertanya kepada rekan yang mengerti.
- Melakukan *signout/logout* ketika telah selesai menggunakan layanan dan menunggu sampai prosesnya benar-benar selesai. Dengan tidak melakukan *signout/logout* yang sempurna, pengguna layanan telah memberi celah bagi penyusup untuk memasuki dan menggunakan *account* yang dimiliki pengguna tersebut.

Salah satu langkah dari pemerintah yang sangat baik menurut penulis adalah peraturan yang menyebutkan bahwa pemilik warung internet diwajibkan mendata Kartu Tanda Penduduk setiap pengunjungnya. Peraturan ini baru direncanakan akan diterapkan. Data tersebut harus dilaporkan kepada tim *Indonesia Security Incident Response Team on Information Infrastructure* (*ID SIRTII*) setiap bulan. Pertimbangannya, banyaknya kejahatan di dunia maya, seperti pencurian lewat kartu kredit (*carding),* pembobolan situs internet *(deface),* dan terorisme melalui warung internet.

Selain itu masyarakat konsumen di dunia maya juga harus waspada. Manajemen kunci yang efektif perlu diterapkan. Konsumen juga tidak boleh mudah terpengaruh oleh suatu tawaran atau pemberitahuan hadiah dari pihak lain di dunia maya.

7. Penutup

7.1. Kesimpulan

Tingkat kejahatan dunia maya di Indonesia tergolong tinggi di dunia internasional. Daerah Jawa Barat merupakan salah satu daerah yang menjadi tempat terjadinya sejumlah besar kejahatan dunia maya. Tindak kejahatan dunia maya di Indonesia sebagian besar dilakukan di warung internet.

Pengguna jaringan komunikasi elektronik di Indonesia masih banyak yang belum mengetahui benar mengenai metode dan proses enkripsi/dekripsi yang dijalankan pada aplikasi-aplikasi yang mereka gunakan.

Pengetahuan masyarakat pengguna jaringan komunikasi elektronik di kota Bandung tentang kriptografi, khususnya mengenai manajemen kunci masih rendah.

Teknik dalam kriptografi telah berkembang menjadi semakin canggih. Namun, teknik kriptografi secanggih apapun tidak akan berguna apabila masyarakat yang menjadi calon penggunanya tidak mengerti mengenai penggunaannya.

Penyebabnya bisa datang dari berbagai pihak seperti masyarakat pengguna itu sendiri, penyedia layanan di dunia maya, serta pemerintah. Oleh karena itu, untuk memperbaikinya diperlukan peran dari berbagai pihak pula.

Para pengguna layanan pada jaringan komunikasi elektronik harus melakukan prosedur keamanan yang memadai. Beberapa langkah minimal yang direkomendasikan pada makalah ini adalah sebagai berikut:

1. Tidak membuat *PIN* atau *password* berdasarkan data yang akan relatif mudah untuk ditebak. Usahakan untuk membuat *PIN* atau *password* yang panjang jika memungkinkan.

2. Tidak menggunakan PIN atau password yang sama untuk beberapa aplikasi.

3. Tidak menuliskan *PIN* atau *password* pada sembarang tempat.

4. Tidak menyimpan user id dan *password* pada perangkat lunak pengingat.

5. Mengganti *PIN* atau *password* secara rutin dalam jangka waktu yang relatif tidak terlalu lama.

6. Tidak mudah terpengaruh untuk memberitahukan *PIN* atau *password* kepada pihak manapun yang memintanya.

7. Tidak membuka surat masuk dari pengirim yang tidak dikenal apabila tidak dengan pengamanan.

8. Melakukan *signout/logout* ketika telah selesai menggunakan layanan dan menunggu sampai prosesnya benar-benar selesai.

Kriptografi memang banyak membantu dalam menjaga privasi para konsumen di dunia maya, tetapi perlu diingat bahwa inti dari kriptografi adalah kunci yang digunakan, baru kemudian tekniknya.

7.2. Saran

Saran-saran dari penulis berhubungan dengan makalah yang dibuat oleh penulis adalah sebagai berikut:

- Penyedia layanan pada jaringan komunikasi elektronik harus menerapkan teknik kriptografi yang efektif untuk menjamin keamanan data para konsumennya.

- Perlu lebih banyak aspek sosial yang diperhatikan oleh semua pihak mengenai keamanan di dunia maya. Karena walaupun teknik kriptografi telah dikembangkan sampai secanggih-canggihnya tetapi ternyata sebagian masyarakat tidak mengerti tentang penggunaannya, maka hasilnya tidak akan optimal.

- Perlu diadakan penelitian terhadap responden yang lebih banyak dan lebih luas agar bisa menilai dengan lebih baik tingkat pengetahuan masyarakat Indonesia dan daerah-daerahnya mengenai kriptografi dengan topik-topik yang lebih khusus lagi dengan hasil yang lebih bisa dipercaya, analisis yang lebih detail, beserta solusinya.

- Perlu adanya tindak lanjut dari pihak-pihak yang berkepentingan untuk memperbaiki masalah rendahnya pengetahuan masyarakat pengguna layanan pada jaringan komunikasi elektronik.

- Perlu adanya tindakan tegas dari pemerintah terhadap para pelaku pelanggaran-pelanggaran hak konsumen di dunia maya.

Daftar Pustaka

[1] Muddin, Andhy. *Cybercrime Mencapai Puncaknya di 2006?*. www.detikinet.com. 2006.

[2] Safitri, Indra. *Tindak Pidana di Dunia* Cyber. Pasar Modal dan Investasi Indonesia. 2004.

[3] Tanenbaum, Andrew S. Computer Networks, Fourth Edition. Prentice Hall. 2003

[4] Mursito, Danan dkk. *Pendekatan Hukum Untuk Keamanan Dunia* Cyber*Serta Urgensl* Cyber Law *Bagi Indonesia*. Program Studi Teknologi Informasi Program Magister Fakultas Ilmu Komputer Universitas Indonesia. 2005.
[5] Nopiansyah, Eko. *Warung Internet Harus Mendata Identitas Pengunjungnya*. http://www.tempointeraktif.com. 2006
[6] http://komputeraktif.web.id
[7] http://id.wikipedia.org
[8] http://depkominfo.go.id
[9] http://gerbang.jabar.go.id