Pemanfaatan Kombinatorial dan Kriptografi untuk Meningkatkan Keamanan Perangkat Elektronik IF2120 Matematika Diskrit

Alvin Limassa 13516039
Program Studi Teknik Informatika
Sekolah Teknik Elektro dan Informatika
Institut Teknologi Bandung, Jl. Ganesha 10 Bandung 40132, Indonesia
13516039@std.stei.itb.ac.id

***Abstrak* — Sistem keamanan perangkat elektronik atau yang biasanya disebut *cybersecurity* adalah suatu sistem yang dibuat agar para pengguna perangkat elektronik dapat menjaga keamanan dan kerahasiaan informasi yang dimilik. Dikarenakan pengguna perangkat elektronik yang semakin banyak dan terus bertambah setiap tahunnya, banyak oknum – oknum yang berusaha mencari celah pada sistem keamanan yang meningkatkan risiko informasi yang penting dicuri oleh pihak yang tidak bertanggung jawab. Namun, hal ini dapat di cegah dengan cara meningkatkan keamanan sandi memanfaatkan perhitungan kombinatorial dan pemanfaatan kriptografi dalam meningkatkan keamanan data dalam suatu perangkat elektronik.**

Kata kunci – kata sandi, kriptogarfi, sistem keamanan

I. PENDAHULUAN

Sistem keamanan perangkat elektronik atau yang lebih dikenal dengan istilah *cybersecurity* merupakan salah satu teknologi keamanan yang digunakan dalam sebagian besar perangkat elektronik. Sistem keamanan yang digunakan pada perangkat elektronik berbeda – beda. Beberapa contoh dari sistem keamanan perangkat elektronik maupun perangkat lunak berupa password (terdiri dari huruf dan angka) , pin (terdiri dari angka), pola ukir (*pattern)*, pemindai wajah, pemindai sidik jari, pemindai iris, kriptografi pada pesan, gambar, suara, dll. Sistem keamanan sampai sekarang terus berkembang dan terus digunakan oleh sebagian besar masyarakat yang menggunakan perangkat elektronik maupun perangkat lunak.

Celah keamanan pertama kali muncul pada tahun 1945 oleh *Murray Hopper* yang menemukan masalah pada komputer jaman dahulu yang dinamakan bug. Pada tahun 1964, AT&T salah satu operator seluler terkenal didunia melakukan pengamatan terhadap "*phreakers*" (orang yang memperoleh telepon gratis dengan memanfaatkan celah keamanan). Selanjutnya pada tahun 1979, program *worm* pertama diciptakan dengan tujuan membuat komputer lebih efisien, tetapi dimanfaatkan oleh *hacker* untuk menghapus atau menghancurkan data pengguna. Pada tahun 1983, istilah virus diperkenalkan pertama kali oleh *Fred Cohen* mahasiswa S3 *Southern California University*, yang kemudian berkembang menjadi virus komputer pertama yang dinamakan "the Brain". The brain pada awalnya tidak berbahaya, tetapi seiring perkembangan jaman pada tahun 1988 sebuah "*worm"* di unggah ke ARPANET (cikal bakal internet) yang menyebabkan masalah pada 6000 komputer yang terkoneksi. Pada tahun 1900-an virus yang dapat memodifikasi dirinya sendiri tercipta. Timbul beberapa masalah besar yang terjadi pada tahun-tahun tersebut seperti virus yang mulai menyebar melalui dokumen word, peretas yang mengambil alih 500 sistem komputer pemerintahan. Pada abad ke-21 ini perkembangan virus semakin pesat yang menyebabkan peretas mampu menumbangkan beberapa layanan besar seperti *Amazone, Yahoo, e-Bay, dll.* Selain itu, peretas mampu untuk mengendalikan komputer dari jarak jauh tanpa sepengetahuan pemiliknya, Virus menyebar melalui berbagai media seperti .doc, .xls, .ppt, .zip, dll, dan yang terbaru adalah virus *Ransoware* (2017) yang menyerang sebagian besar komputer di dunia, menyebabkan lumpuhnya beberapa rumah sakit, perkantoran, sistem-sistem pemerintahan yang terkoneksi dengan internet.

Permasalahan keamanan ini tidak hanya terjadi dinegara - negara maju saja tetapi juga terjadi di Indonesia. Indonesia dengan jumlah penduduk terbanyak ke-4 di dunia dengan jumlah penduduk sekitar 265.152.767 pada tahun 2017[1], serta pengguna internet terbesar ke-6 di dunia dengan jumlah pengguna sekitar 83,7 juta orang.[2] Dengan jumlah pengguna internet sebanyak itu sudah jelas bahwa ancaman virus dan celah keamanan pada sistem perangkat elektronik merupakan ancaman besar bagi bangsa Indonesia.

Sayangnya berbagai pengguna perangkat elektronik yang terkoneksi dengan internet masih kurang paham dan kurang peduli terhadap keamanan pada perangkat yang mereka miliki. Hal ini terbukti dengan banyaknya pengguna internet di dunia yang masih menggunakan kata sandi yang sangat sederhana yang mudah ditebak seperti 123456, qwerty, 11111, password, dll.[3] Penggunaan kata sandi yang sangat sering digunakan oleh orang menyebabkan mudahnya para peretas untuk mengakses berbagai data penting dan berharga yang terdapat pada

[1] http://www.worldometers.info/world-population/indonesia-population/
[2] https://kominfo.go.id/content/detail/4286/pengguna-internet-indonesia-nomor-enam-dunia/0/sorotan_media
[3] www.telegraph.co.uk/technology/2017/01/16/worlds-common-passwords-revealed-using/

perangkat elektronik.

Pemanfaatan kombinatorial dan Kriptografi dapat meningkatkan sistem keamanan suatu perangkat elektronik. Kombinatorial dapat digunakan untuk mengukur keamanan kata sandi yang digunakan. Kriptografi dapat digunakan untuk mengamkan data-data penting yang dimiliki. Ketika suatu data akan dikirim, dengan kriptografi data dapat dienkripsi sehingga hanya orang yang memiliki kunci yang dapat membaca isi data tersebut.

II. LANDASAN TEORI

A. Kombinatorial

Kombinatorial adalah salah satu cabang ilmu matematika yang mendalami tentang pengaturan objek – objek. Solusi yang diharapkan didapatkan dari kombinatorial adalah banyaknya cara untuk mengatur obyek – obyek tertentu dalam suatu himpunan.

Kaidah dasar menghitung kombinatorial terdiri dari dua kaidah dasar yaitu kaidah perkalian (*rule of product)* dan kaidah penjumlahan (*rule of sum).* Kaidah perkalian digunakan apabila percobaan pertama mempunyai n kemungkinan hasil yang dapat dicapai dan percobaan kedua mempunyai m kali kemungkinan hasil yang dapat dicapai, maka total kemungkinan yang akan terjadi apabila percobaan pertama dan kedua dilakukan adalah m × n kemungkinan. Sedangkan kaidah penjumlahan adalah ketika dari percobaan pertama dan percobaan kedua, hanya salah satu dilakukan maka total kemungkinan yang akan diperoleh adalah n + m kemungkinan. Kaidah penjumlahan dan perkalian dapat digunakan untuk lebih dari dua kasus percobaan sehingga dinamakan perluasan kaidah menghitung.

Prinsip Inklusi-Eksklusi untuk menghitung kombinatorial :

Misalkan

A = himpunan bilangan diawali angka 1

B = himpunan bilangan diakhiri angka 1

A ∩ B = himpunan bilangan diawali angka 1 dan diakhiri angka 1

A ∪ B = himpunan bilangan diawali angka 1 atau diakhiri angka 1

Maka :

$$|A \cup B| = |A| + |B| - |A \cap B|$$

Permutasi adalah jumlah berbagai urutan berbeda yang dapat disusun dari objek – objek. Permutasi merupakan pengembangan dari aturan perkalian. Permutasi dapat digunakan untuk menyelesaikan beberapa masalah seperti menghitung cara untuk memasukkan bola yang berbeda warna ke dalam kotak yang jumlahnya kurang dari jumlah bola, mengurutkan nama mahsiswa, dll. Permutasi dapat dihitung menggunakan rumus berikut : $P(n,r) = n(n-1)(n-2)\ldots\big(n-(r-1)\big) = \frac{n!}{(n-r)!}$

r adalah jumlah obyek yang akan dipilih, n nadalah jumlah obyek yang dapat dipilih, dan tidak ada obyek yang sama pada proses pengurutan.

Permutasi melingkar adalah permutasi dari n buah obyek yang proses penyusunan obyek dilakukan secara melingkar membentuk suatu bentuk lingkaran. Permutasi melingkar ini biasanya digunakan pada saat akan menghitung berapa banyak cara yang dapat dilakukan untuk mendudukkan orang pada suatu meja melingkar. Rumus dari permutasi melingkar adalah $(n-1)!$.

Kombinasi merupakan bentuk khusus dari permutasi, pada kombinasi urutan kemunculan tidak diperhitungkan sedangkan pada permutasi urutan kemunculan diperhitungkan. Sebagai contoh pada permutasi AAB dan ABA merupakan dua hal yang berbeda, sedangkan pada kombinasi AAB dan ABA dianggap sama karena terdiri dari dua buah A dan satu buah B. Beberapa contoh permasalahan yang dapat diselesaikan dengan kombinasi adalah pemilihan panitia, penyusunan menu makan, dll. Rumus dari kombinasi merupakan perkembangan dari rumus permutasi yaitu : $C(n,r) = \frac{n!}{r!(n-r)!}$. C(n,r) merupakan Kombinasi pemilihan r elemen dari n elemen yang tidak memperhatikan urutan pemilihannya.

Permutasi bentuk umum adalah permutasi yang digunakan untuk menghitung pengurutan n buah objek dari suatu himpunan ganda yang memiliki n buah objek, objek pada himpunan tersebut tidak harus berbeda semuanya. Permutasi bentuk umum memiliki rumus $P(n; n_1, n_2, \ldots, n_k) = \frac{n!}{n_1!n_2!\ldots n_k!}$

Kombinasi bentuk umum adalah kombinasi yang digunakan untuk mengurutkan n buah objek yang terdapat pada himpunan ganda. Kombinasi bentuk umum ini tidak memiliki perbedaan dengan permutasi bentuk umum sehingga memiliki rumus yang sama juga yaitu $P(n; n_1, n_2, \ldots, n_k) = C(n; n_1, n_2, \ldots, n_k) = \frac{n!}{n_1!n_2!\ldots n_k!}$ beberapa contoh kasus yang dapat diselesaikan menggunakan permutasi atau kombinasi bentuk umum adalah penyusunan himpunan ganda huruf tertentu, pengurutan objek dari himpunan ganda objek, dll.

Kombinasi dengan pengulangan adalah kombinasi yang memperbolehkan adanya pengulangan elemen, artinya n buah objek yang ada dapat diambil r buah objek dengan pengulangan diperbolehkan. Rumus dari kombinasi dengan pengulangan adalah $C(n+r-1,r) = C(n+r-1,n-1)$. Beberapa contoh penerapan kombinasi dengan pengulangan adalah mencari kemungkinan solusi untuk persamaan linear yang memiliki batasan-batasan tertentu untuk setiap variabelnya, pembagian suatu objek ke beberapa orang dalam hal ini satu orang bisa mendapatkan lebih dari satu objek, dll.

Kombinasi juga dapat digunakan untuk menentukan

koefisien dari binomial. Koefisien binomial sebenarnya dapat diperoleh dari segitiga pascal, selain itu untuk menentukan suatu koefisien dari binomial tertentu dapat menggunakan rumus $x^{n-k}y^k = C(n,k)$. Serta untuk menjabarkan persamaan

$$(x+y)^n = \sum_{k=0}^{n} C(n,k)x^{n-k}y^k$$

Prinsip sarang merpati adalah prinsip yang menjelaskan apabila terdapat n+1 objek yang ditempatkan pada n buah kotak, maka paling sedikit terdapat satu buah kotak yang memiliki isi lebih dari satu obyek. Contoh penerapan dari prinsip sarang merpati adalah menghitung jumlah minimal agar dapat memastikan pengambilan suatu objek dari suatu himpunan didapatkan dua buah objek yang sama, dll.

Kombinatorial juga dekat hubungannya dengan peluang. Teori peluang banyak memanfaatkan teori kombinatorial untuk menentukan titik sampel maupun hasil dari perhitungan peluang tersebut. Peluang adalah kemungkinan suatu titik sampel pada suatu ruang percobaan terjadi. Peluang diskrit memiliki beberapa sifat meliputi peluang diskrit memiliki rentang hasil nol sampai 1 tidak mungkin lebih maupun kurang dari rentang tersebut dan jumlah peluang diskrit dari semua titik contoh pada suatu ruang contoh adalah 1. Sebagian besar persoalan kombinatorial dapat dijadikan permasalahan peluang karena peluang diskrit adalah hasil dari perhitungan kombinatorial dibagi dengan total semua kemungkinan yang dapat terjadi pada suatu ruang contoh. Termasuk sebagian besar prinsip – prinsip pada kombinatorial dapat digunakan pada peluang diskrit, misalkan prinsip inklusi dan eksklusi.

B. Kriptografi

Kriptografi bukanlah ilmu yang muncul ketika virus mulai menyerang sistem keamanan perangkat elektronik, melainkan merupakan ilmu lama yang telah ditemukan oleh tentara Sparta di Yunani pada pemulaan tahun 400 SM. Para tentara Sparta memanfaatkan suatu alah yang dikenal dengan scytale. Scytale merupakan suatu alat yang terdiri dari pipa silinder dan daun. Pesan akan ditulis pada daun tersebut pada saat dililitkan pada pipa silinder, kemudian akan dikirim tanpa pipa silinder tersebut. Untuk membaca tulisan tersebut maka penerima harus menggunakan pipa silinder dengan ukuran dan diameter yang sama agar tulisan yang telah tertulis dapat terurut dengan benar. Sehingga hanya orang yang mengetahui ukuran diameter yang tepat yang dapat membacanya. Teknik yang digunakan ini dikenal dengan nama transposisi cipher. Transposisi ciper merupakan salah satu teknik enkripsi tertua yang pernah diketahui.

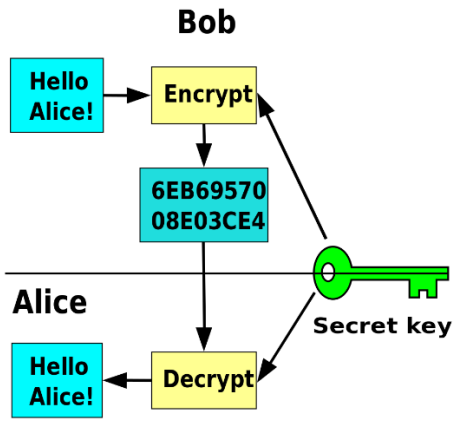
Kriptanalisis adalah ilmu yang mempelajari berbagai cara untuk memecahkan cipherteks tanpa harus mengetahui kunci yang tepat. Ia mempelajari dan berusaha mencari tahu metode enkripsi sehingga diperoleh pesan asli yang terdapat pada cipherteks. Kriptografer adalah orang yang membuat enkripsi untuk merahasiakan data ataupun pesan seseorang sehingga hanya orang yang memiliki kode deskripsinya yang dapat membaca pesan tersebut.

Notasi matematis dari kriptografi dilambangkan dengan E(P) = C dengan C adalah cipherteks, P adalah plainteks dan E merupakan fungsi yang melakukan enkripsi dari E menjadi C. Proses sebaliknya yaitu melakukan dekripsi dilambangkan dengan D(C) = P dengan D adalah fungsi yang digunakan untuk mengubah cipherteks menjadi plain teks. Contoh plainteks STRUKTUR DISKRIT , cipherteksnya TSURTKRU IDKSIRT.

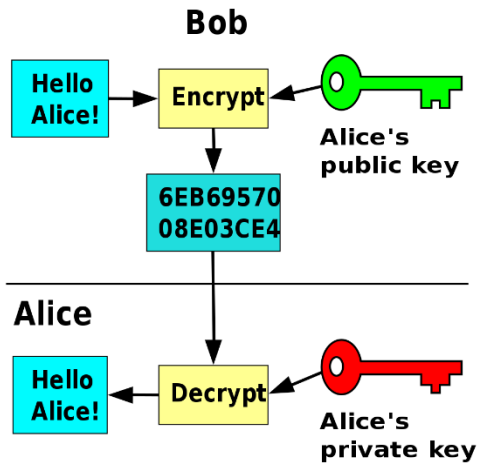
Kekuatan kriptografi yang ditentukan oleh kerahasiaan algoritma kriptografi disebut alogritma *restricted.* Sehingga jika seseorang telah mengetahui algoritma tersebut maka orang tersebut dapat membaca atau mendekripsi cipherteks, akan tetapi penggunaan alogritma *restricted* sudah jarang digunakan pada zaman sekarang, hal ini dikarenakan apabila seseorang dalam perusahaan yang membuat program kriptografi keluar dari perusahaan tersebut maka kerahasiaan dari algoritma tersebut tidak dapat diandalkan lagi sehingga harus membuat algoritma baru agar kerahasiaan data dapat tetap terjamin..

Kekuatan kriptografi zaman sekarang lebih difokuskan pada kunci yang untuk membuka enkripsi, sehingga walaupun seseorang telah mengetahui algoritma untuk melakukan enkripsi tetap saja orang tersebut belum dapat mengetahui isi data/ pesan kecuali orang tersebut telah memiliki kuncinya. Kunci pada kriptografi zaman sekarang mirip dengan kata sandi untuk masuk ke perangkat komputer, pin, dll. Salah satu contoh dari enkripsi adalah *Caesar cipher* yaitu teknik kriptografi pada zaman Kaisar Romawi, teknik ini yaitu memanfaatkan proses penggeseran huruf sebanyak 3 kata, sehingga untuk membaca arti dari kata yang telah di enkripsi hanya perlu menggeser kata-kata tersebut kebelakang sebanyak 3.

Kriptografi zaman sekarang yang menggunakan kunci dibedakan menjadi dua bagian besar yaitu algoritma simetri dan algoritma nirsimetri. Algoritma simetri adalah algoritma yang memiliki kunci yang sana untuk melakukan enkripsi dan dekripsi sehingga untuk dapat membaca isi enkripsi penerima harus memiliki kunci yang sama dengan pengirim agar dapat membaca isi pesan tersebut. Sedangkan, Algoritma nirsimetri adalah algoritma yang memiliki kunci yang berbeda antara pengirim dan penerima, sehingga pada saat proses enkripsi terdapat suatu kunci yang dimasukkan tetapi ketika ingin di dekripsi kunci yang dimasukkan berbeda. Kriptografi simetri lebih sering disebut dengan istilah kriptografi kunci pribadi karena kunci harus dirahasiakan karena untuk mengunci dan membuka kunci menggunakan kode yang sama, kelemahan dari metode ini adalah pengguna harus mencari cara lain untuk memberitahu kepada penerima kunci yang digunakan. Kriptografi nirsimetri atau yang lebih sering disebut dengan kriptografi kunci-publik karena untuk melakukan enkripsi kunci yang digunakan adalah kunci publik yang boleh diketahui banyak orang, tetapi untuk membuka kunci tersebut penerima memiliki kunci lain dan hanya penerimalah yang dapat membukanya. Untuk tingkat keamanannya dan kepraktisannya kunci nirsimetri lebih baik dan efisien apabila digunakan untuk keperluan bersama, tetapi jika untuk keperluan pribadi algoritma simetri masih dapat diandalkan.



Gambar 1 Penerapan algoritma kunci simetri (sumber:https://id.wikipedia.org/wiki/Berkas:Symmetric_key_encryption.svg diakses pada tanggal 1/12/2017 jam 10.00)



Gambar 2 Penerapan algoritma kunci nirsimetri (sumber:https://id.wikipedia.org/wiki/Berkas:Public_key_encryption.svg diakses pada tanggal 1/12/2017 jam 10.00)

DES (*Data Encryption Standard)* merupakan salah satu contoh dari penerapan algoritma kriptografi kunci pribadi yang sangat kuat. Algoritma DES adalah algoritma yang memadukan beberapa teknik-tenik seperti permutasi, kompaksi, ekspansi, subsitutsi sebanyak 16 kali perulangan. Kunci yang digunakan pada algoritma DES sepanjang 8 karakter yang setara dengan 64 bit, akan tetapi tidak semua bit digunakan untuk proses enkripsi melainkan hanya 56 bit yang digunakan. Tingkat keamanan yang dapat dicapai oleh sistem keamanan DES ini dapat dihitung menggunakan metode kombinatorial yaitu $2^{56} = 72.057.594.037.927.936$ kemungkinan. Sehingga untuk seseorang yang tidak memiliki kunci untuk membuka enkripsi DES memerlukan waktu yang sangat lama untuk membukanya, asumsikan bahwa seribu prosesor hanya dapat menguji satu juta kemungkinan setiap detik, maka diperlukan waktu sekitar 2284 tahun untuk memecahkan kode tersebut. Algoritma DES ini terus berkembang dengan meningkatnya jumlah bit yang digunakan untuk mengenkripsi agar data yang dienkripsi lebih aman. 3DES diperkenalkan pada tahun 2005 untuk mengamankan berbagai informasi penting yang dimiliki suatu negara. Algoritma 3DES merupakan 3 kali iterasi dari algoritma DES sehingga memiliki tingkat keamanan yang jauh lebih tinggi.

RSA (*Rivest-Shamir-Adleman)* merupakan algoritma yang dicetus oleh tiga orang yang berasal dari *Massachussets Institute of Technology* atau yang lebih dikenal dengan singkatan MIT pada tahun 1976. Algoritma ini didasarkan pada teorima bilangan prima dan modulo. Algoritma ini merupakan salah satu algoritma yang menerapkan sistem enkripsi nirsimetri sehingga untuk mengenkripsi dan mendekripsi memiliki kunci yang berbeda. Untuk memecahkan kunci dekripsi seseorang harus melakukan pemfaktoran terhadap bilangan – bilangan prima menjadi faktor – faktor nonprimanya, hal ini dimanfaatkan oleh penemu algoritma RSA karena sampai saat ini belum ditemukan algoritma program yang mangkus untuk menyelesaikan permasalahan tersebut. Sehingga kode tersebut dapat digunakan sebagai kunci. Algoritma RSA sendiri terdiri atas tiga bagian penting yaitu bagian pembangkit pasangan kunci, bagian enkripsi, dan bagian dekripsi.

III. Menghitung Tingkat Keamanan Perangkat Elektronik

Kebanyakan perangkat elektronik jaman sekarang memanfaatkan berbagai metode dan cara untuk melindungi data – data pengguna, akan tetapi masih banyak pengguna terutama di Indonesia yang kurang dapat memanfaatkan dan mengoptimalkan sistem keamanan yang sudah ada. Misalkan para pengguna yang menggunakan kata sandi yang mudah ditebak seperti qwert, password, 123456, dll. para pengguna masih belum mengetahui tentang seberapa mudah suatu kata sandi untuk ditebak. Berikut adalah beberapa hal yang dapat dilakukan untuk memperhitungkan seberapa cepat seseorang dapat mengetahui kata sandi Anda.

Perhitungan untuk tingkat keamanan kata sandi dapat dilakukan dengan menggunakan teknik kombinatorial yaitu kaidah perkalian dengan mengalikan kemungkinan karakter – karakter yang dapat digunakan sebagai kata sandi sebanyak panjang kata sandi yang dibuat.

Beberapa contoh kata sandi dan tingkat keamanan kata sandi tersebut :

a. Kata sandi yang memiliki 4 karakter hanya menggunakan huruf a-z tanpa kombinasi huruf besar kecil memiliki kemungkinan $26^4 = 456.976$
b. Kata sandi yang memiliki 5 karakter hanya menggunakan huruf a-z tanpa kombinasi huruf besar kecil memiliki kemungkinan $26^5 = 11.881.376$
c. Kata sandi yang memiliki 6 karakter hanya menggunakan huruf a-z tanpa kombinasi huruf besar kecil memiliki kemungkinan $26^6 = 308.915.776$
d. Kata sandi yang memiliki 4 karakter hanya menggunakan huruf a-z dengan kombinasi huruf besar kecil memiliki kemungkinan $52^4 = 7.311.616$
e. Kata sandi yang memiliki 5 karakter hanya menggunakan huruf a-z dengan kombinasi huruf besar kecil memiliki kemungkinan $52^5 = 380.204.032$
f. Kata sandi yang memiliki 6 karakter hanya menggunakan huruf a-z dengan kombinasi huruf besar kecil memiliki kemungkinan $52^6 = 19.770.609.664$
g. Kata sandi yang memiliki 4 karakter hanya menggunakan

huruf dan kombinasi dengan karakter khusus yang yang dapat digunakan sebagai kata sandi kemungkinan $93^4 = 74.805.201$

h. Kata sandi yang memiliki 5 karakter hanya menggunakan huruf dan kombinasi dengan karakter khusus yang yang dapat digunakan sebagai kata sandi kemungkinan $93^5 = 6.956.883.693$

i. Kata sandi yang memiliki 6 karakter hanya menggunakan huruf dan kombinasi dengan karakter khusus yang yang dapat digunakan sebagai kata sandi kemungkinan $93^6 = 646.990.183.449$

j. Kata sandi yang memiliki 8 karakter hanya menggunakan huruf dan kombinasi dengan karakter khusus yang yang dapat digunakan sebagai kata sandi kemungkinan $93^8 = 5.595.818.096.650.401$

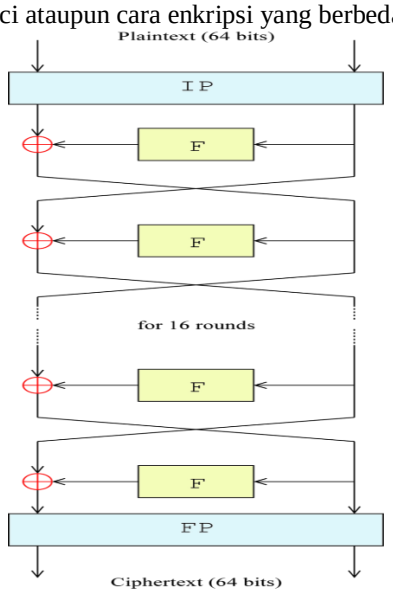
Berdasarkan beberapa contoh kemungkinan kata sandi yang dapat dibuat dengan karakter a-z, kombinasi semua karakter, dan pajang kata-kata yang terdapat pada sebuah kata sandi. Bagian ini akan menjelaskan tentang seberapa cepat seseorang dapat menebak kata sandi Anda dengan mencoba seluruh kemungkinan yang ada. Komputer standar pada tahun 2011 dengan menggunakan kartu grafis yang tingkat tinggi (yang biasa digunakan para gamer) memiliki kemampuan untuk mencoba 10.000.000 kemungkinan setiap detiknya.[4] Berdasarkan pada data kecepatan komputer pada tahun 2011 berikut ini adalah data waktu yang diperlukan untuk memecahkan kata sandi dengan beberapa spesifikasi tertentu (urutan spesifikasi sama dengan poin sebelumnya)

a. Waktu : $\pm 4.57 \times 10^{-2}\ detik$
b. Waktu : $\pm 1.18\ detik$
c. Waktu : $\pm 30.9\ detik$
d. Waktu : $\pm 0.731\ detik$
e. Waktu : $\pm 38\ detik$
f. Waktu : $\pm 32.9\ menit$
g. Waktu : $\pm\ 7.48\ detik$
h. Waktu : $\pm\ 11.59\ menit$
i. Waktu : $\pm\ 18\ jam$
j. Waktu : $\pm\ 18\ tahun$

Metode enkripsi yang ada pada jaman sekarang sudah sangat canggih, misalkan saja teknologi enkripsi DES yang memiliki $2^{56} = 72.057.594.037.927.936$ untuk satu kali perulangan , jadi untuk menghitung semua kemungkinan diperlukan waktu untuk 3600 tahun untuk memecahkan kode tersebut. Sedangkan hanya untuk menguji satu kali pengulangan kode DES memerlukan waktu kurang lebih 228 tahun. Enkripsi DES ini sangat cocok digunakan untuk keperluan pribadi karena DES menggunakan sistem algoritma enkripsi kunci simetri yang artinya untuk mengunci dan membuka kunci memerlukan kunci yang sama. Apabila data yang akan di enkripsi merupakan keperluan umum maka akan lebih baik jika enkripsi menggunakan metode RSA yang menggunakan kunci publik sehingga pengguna tidak perlu mencari cara lain untuk menyampaikan kunci kepada penerima (penerima telah memiliki kunci pribadi sendiri).

[4] https://www.betterbuys.com/estimating-password-cracking-times/

Cara Kerja DES adalah memanfaatkan fungsi enkripsi yang diulang – ulang sebanyak 16 kali sehingga hasil enkripsi merupakan hasil dari enkripsi 16 kali fungsi – fungsi yang memiliki kunci ataupun cara enkripsi yang berbeda – beda



Gambar 3 Gambar tahapan Enkripsi DES (sumber:https://en.wikipedia.org/wiki/Data_Encryption_Standard#The_Feistel_.28F.29_function diakses pada tanggal 1/12/2017 jam 12.00)

Walaupun sistem keamanan yang diberikan oleh enkripsi DES sudah sangat mumpuni, teknologi enkripsi masih terus berkembang dan apabila teknologi DES masih dianggap kurang aman karena perkembangan teknologi perangkat keras yang terus berkembang. Teknologi *Tripel DES* dapat menjadi solusinya yaitu teknologi DES yang memiliki panjang karakter kunci 112 bit yang jika dihitung kemungkinan satu kali pengulangannya memiliki $2^{112} = 5.19\ x\ 10^{33}$ kemungkinan. Teknologi ini membuat enkripsi berkali – kali lipat jauh lebih aman dari teknologi DES murni dan hampir tidak mungkin komputer jaman sekarang dapat melakukan pengujian semua kemungkinannya.

Cara kerja algoritma RSA adalah enkripsi yang dilakukan dengan menggunakan dua faktor prima dengan tahapan – tahapan sebagai berikut :

1. Pilih dua bilangan prima secara acan misalkan a dan b
2. Hitunglah $n = a\ b$
3. Hitunglah $m = (a-1)(b-1)$
4. Pilih bilangan e secara acak dengan syarat e relatif prima terhadap m (digunakan sebagai kunci publik)
5. Pilih kunci pribadi (untuk dekripsi ‘d’) dengan syarat $ed\ \equiv (mod\ m)$.
6. Untuk melakukan enkripsi digunakan rumus $c_i = p_i^e mod\ n$
7. Untuk melakukan dekripsi digunakan rumus $p_i = c_i^d mod\ n$
8.

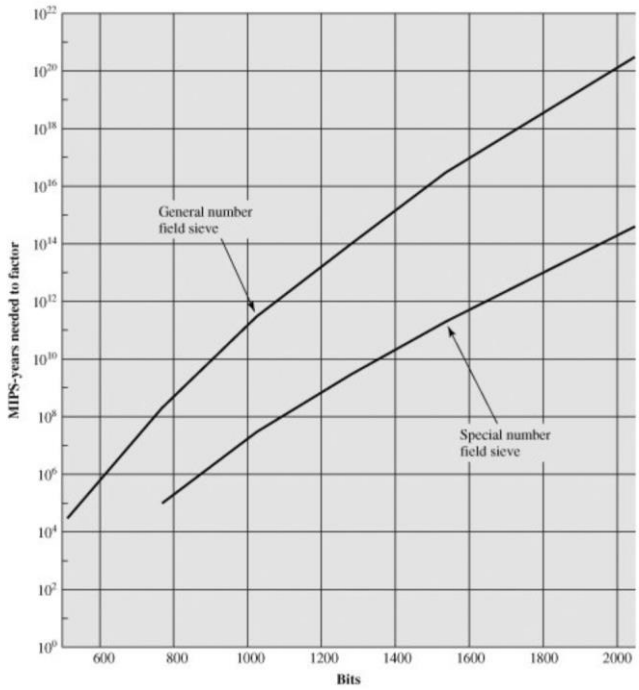
Untuk memecahkan algoritma RSA yang merupakan enkripsi berdasarkan faktor prima maka diperlukan waktu yang cukup lama, hal ini dikarenakan untuk mencari suatu bilangan yang

merupakan kunci harus dilakukan dengan cara pemfaktoran. Sampai saat ini belum ada algoritma pemfaktoran yang mangkus, hal ini yang menyebabkan enkripsi RSA masih dapat digunakan hingga sekarang. Apabila sudah ditemukan algoritma pemfaktoran yang mangkus maka algoritma enkripsi RSA menjadi tidak relevan lagi karena sudah tidak aman.

Tingkat keamanan algoritma RSA dapat dilihat dari tabel berikut, beberapa algoritma yang dirancang untuk mencoba menyelesaikan/ memecahkan kata sandi dari suatu kunci RSA memerlukan waktu bertahun-tahun untuk diselesaikan karena belum adanya algoritma pemfaktoran yang tidak efisien. Untuk saat ini dan beberapa tahun ke depan kunci RSA dengan panjang 1024 – 2048 bit masih sangat relevan untuk digunakan karena belum dapat diselesaikan dalam waktu yang cepat.

Number of Decimal Digits	Approximate Number of Bits	Date Achieved	MIPS-years	Algorithm
100	332	April 1991	7	Quadratic sieve
110	365	April 1992	75	Quadratic sieve
120	398	June 1993	830	Quadratic sieve
129	428	April 1994	5000	Quadratic sieve
130	431	April 1996	1000	Generalized number field sieve
140	465	February 1999	2000	Generalized number field sieve
155	512	August 1999	8000	Generalized number field sieve
160	530	April 2003		Lattice sieve
174	576	December 2003		Lattice sieve
200	663	May 2005		Lattice sieve

Gambar 4 Gambar kecepatan pemfaktoran oleh komputer (sumber: Buku Cryptography and Network Security Principles and Practices, Fourth Edition. Halaman 276)



Gambar 4 Gambar waktu yang diperlukan untuk memecahkan kode RSA dengan panjang tertentu MIPS adalah satuan berapa juta instruksi per-tahun yang dikerjakan (sumber: Buku Cryptography and Network Security Principles and Practices, Fourth Edition. Halaman 277)

IV. CARA MENINGKATKAN KEAMANAN PERANGKAT ELEKTRONIK

Dari data yang telah diperoleh terlihat bahwa untuk kata sandi yang memiliki panjang karakter yang kurang dari 6 kata sangat tidak aman, apabila sistem memperbolehkan pengguna untuk menebak terus kata sandi maka hanya kurang dari satu jam menggunakan komputer biasa dengan kartu grafis yang baik sudah dapat membobol akun Anda. Dilihat dari data dan perhitungan matematis sebaiknya kata sandi yang aman adalah kata sandi yang memiliki panjang lebih dari 6 karakter dan berisi kombinasi dari angka, huruf besar, huruf kecil, dan karakter khusus. Kata sandi dengan kombinasi tersebut dapat meningkatkan keamanan data, akun, perangkat elektronik agar tidak diakses oleh orang yang tidak berkepentingan. Berdasarkan data yang diperoleh dari beberapa situs di internet, 17% kata sandi didunia merupakan "123456".[5] Hal ini membuktikan bahwa masih kurang sadarnya orang akan bahaya yang dapat ditimbulkan apabila data – data pribadi yang terdapat dalam perangkat elektronik jatuh ke tangan orang yang tidak bertanggung jawab.

Peningkatan keamanan perangkat elektronik dapat diperoleh melalui beberapa cara. Seperti yang telah diperlihatkan dalam bab sebelumnya bahwa angka kemungkinan kata sandi untuk ditebak berdasarkan beberapa kriteria tersebut. Untuk kata sandi yang memiliki panjang kata kurang dari 6 sangat mudah untuk dilakukan *cracking* terhadap sandi tersebut walaupun telah digunakan kombinasi huruf besar, huruf kecil, angka, dan karakter khusus. Kata sandi yang hanya menggunakan salah satu dari kombinasi yang telah disebutkan memiliki daya tahan terhadap serangan *bruteforce* yang lebih rendah ketimbang menggunakan kombinasi tersebut (dengan panjang kata sandi yang sama). Sehingga disarankan kata sandi yang baik untuk digunakan adalah kata sandi yang memiliki lebih dari 6 karakter dan memiliki kombinasi huruf kapital, huruf kecil, angka, dan karakter khusus, selain itu beberapa saran yang penulis dapat berikan untuk meningkatkan keamanan kata sandi yaitu lebih sering untuk mengganti kata sandi, tidak menggunakan kata sandi yang sama untuk semua akun maupun perangkat yang dimiliki, dan gunakan sistem pengecekan dua kali (sudah tersedia pada beberapa situs besar).

Peningkatan sistem keamanan juga dapat dilakukan dengan cara melakukan enkripsi terhadap data – data penting di dalam perangkat elektronik, sehingga ketika suatu perangkat berhasil dibuka oleh orang yang tidak bertanggungjawab data – data penting dan pribadi tidak jauh ke-tangan orang tersebut. Selain itu akan lebih baik jika akan melakukan pengiriman data penting kepada orang lain, sebaiknya data tersebut dienkripsi terlebih dahulu sehingga jika terjadi perampasan data pada saat pengiriman data yang dikirim tidak dapat langsung dibaca oleh orang tersebut. Beberapa metode enkripsi yang dapat digunakan yaitu metode enkripsi DES dan RSA. Metode DES sangat cocok

[5] https://www.huffingtonpost.com/entry/2016-most-common-passwords_us_587f9663e4b0c147f0bc299d

untuk orang yang ingin melakukan enkripsi terhadap data – dat pribadi yang ia miliki (hanya untuk digunakan secara pribadi), sedangkan algoritma RSA lebih cocok untuk orang yang ingin melakukan pengiriman pesan / data kepada orang lain sehingga tidak perlu repot untuk mencari cara lain untuk mengirimkan kunci kepada penerima. Kedua algoritma enkripsi tersebut memiliki tingkat keamanan yang sangat tinggi apabila kunci yang digunakan sangat panjang. Semakin panjang kunci enkripsi maka akan semakin sulit bagi orang yang ingin melakukan *cracking/bruteforce* terhadap data yang terlah terenkripsi.

V. KESIMPULAN

Sistem keamanan perangkat elektronik dapat ditingkatkan oleh pengguna melalui beberapa cara yaitu dengan menggunakan kata sandi yang merupakan kombinasi antara huruf besar, kecil, angka, dan karakter khusus sehingga untuk melakukan *bruteforce* terhadap sandi Anda akan lebih sulit. Kata sandi yang Anda gunakan minimal memiliki panjang 6 atau untuk lebih aman disarankan minimal 8 karakter berdasarkan perhitungan yang telah dilakukan, lebih sering untuk mengganti kata sandi Anda, jangan gunakan kata sandi yang sama untuk beberapa akun dan gunakan enkripsi untuk data – data ataupun informasi penting yang ada dalam perangkat. Beberapa cara preventif ini dapat mengurangi pengguna perangkat elektronik terhadap kejahatan berbasis teknologi digital.

Peningkatan terhadap sistem keamanan elektronik harus menjadi perhatian pemerintah dan masyarakat Indonesia, karena pada era teknologi yang hampir semua lapisan masyarakat menggunakannya untuk berbagai keperluan. Sebagian besar aktivitas masyarakat zaman sekarang menggunakan teknologi sebagai salah satu medianya, misalkan belanja daring, taksi daring, ojek daring, sistem pelayanan masyarakat yang sudah mulai terkoneksi dengan internet, sistem pemerintahan dan masih banyak hal lainnya. Dengan ditingkatkannya sistem keamanan perangkat elektronik pemerintah dan masyarakat dapat mengurangi kehilangan data – data penting dan berharga.

VI. UCAPAN TERIMAKASIH

Penulis mengucap syukur kepada Tuhan yang Maha Esa, karena dengan rahmat karunia-Nya penulis dapat menyelesaikan makalah ini. Selain itu, ucapan terima kasih juga penulis sampaikan kepada Bapak Dr.Ir. Rinaldi Munir, MT , Dr. Judhi Santoso, M.Sc , dan Ibu Dra. Harlili S., M.Sc. selaku Dosem Matematika Diskrit (IF2120) yang telah memberikan ilmu dasar sehingga penulis dapat membuat dan menyelesaikan makalah ini dengan baik.

REFERENSI

[1] Munir, Rinaldi. 2005. Matematika Diskrit. Bandung : Penerbit Informatika.
[2] Rosen, Kenneth H. 2012. *Discrete Mathematics and Its Applications*. McGraw-Hill : New York.
[3] William, Starlings. 2005. Cryptography and Network Security Principles and Practices, Fourth Edition. Prentice Hall : New Jersey.
[4] https://blog.dell.com/en-us/computer-security-threats-a-brief-history/ diakses pada tanggal 1/12/2017 jam 08.00
[5] http://www.worldometers.info/world-population/indonesia-population/ diakses pada tanggal 1/12/2017 jam 08.15
[6] https://kominfo.go.id/content/detail/4286/pengguna-internet-indonesia-nomor-enam-dunia/0/sorotan_media diakses pada tanggal 1/12/2017 jam 09.00
[7] http://searchsecurity.techtarget.com/definition/Data-Encryption-Standard diakses pada tanggal 1/12/2017 jam 09.00
[8] https://www.betterbuys.com/estimating-password-cracking-times/ diakses pada tanggal 1/12/2017 jam 14.00

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 2017

Alvin Limassa
13516039