# Ramai-ramai Memecahkan Enkripsi

Salah satu cara untuk mengamankan data dari penyadapan adalah dengan menggunakan enkripsi (*encryption*). Data diacak dengan menggunakan sebuah algoritma dan sebuah kunci. Contoh algoritma yang terkenal antara lain DES, IDEA, RSA, ECC, dan masih banyak lainnya.

Salah satu cara untuk memecahkan penyandian ini adalah dengan melakukan serangan yang disebut "*brute force attack*", yaitu dengan mencoba segala kombinasi kunci. Misalnya, kita diberi sebuah pesan yang sudah disandikan (disebut *ciphertext*) dengan sebuah algoritma dan sebuah kunci. Kemudian kita ingin mengetahui pesan awal tersebut akan tetapi kita tidak tahu kunci yang digunakan, meskipun kita diberitahu algoritma yang digunakan. Maka, yang dapat kita lakukan adalah mencoba semua kombinasi kunci. Kita coba menggunakan kunci "1" untuk membuka ciphertext tersebut. Jika gagal kita coba dengan "2", "3", ..., "a", "b", ..., "z" dan seterusnya. Kalau masih gagal juga, kita coba dengan dua kombinasi "11", "12", "13", ..., "1a", "1b", ..., "zz". Masih gagal juga, kita coba dengan tiga kombinasi dan seterusnya. Anda sudah bisa membayangkan, *kan*? Tentunya kunci yang dicoba tidak hanya sekadar huruf dan angka saja, akan tetap semua kombinasi yang diperkenankan oleh algoritma yang digunakan.

**Semakin panjang kunci yang dipergunakan, semakin banyak permutasi kombinasi karakter...**

Cara coba-coba di atas itu tentunya membutuhkan waktu yang sangat lama karena kombinasi yang ada bisa bermacam-macam. Meskipun memakai komputer masih dibutuhkan waktu yang lama. Semakin panjang kunci yang dipergunakan, semakin banyak permutasi kombinasi karakter, semakin lama untuk memecahkan enkripsi tersebut. Itulah sebabnya semakin panjang *password* yang digunakan, semakin aman.

Timbul ide dari sekelompok orang. Bagaimana kalau serangan coba-coba tadi dilakukan secara bersama-sama dan terdistribusi? Misalnya, saya mencoba satu kunci. Anda mencoba satu kunci. Kawan kita mencoba satu kunci, dan seterusnya. Kunci mana yang harus dicoba diorganisasi oleh sebuah komputer sentral yang memiliki database tentang kunci-kunci yang sudah dicoba. Lebih bagus lagi kalau semuanya ini bisa dilakukan lewat Internet secara otomatis. Inilah yang dilakukan oleh kelompok "distributed.net". Lihat situs *http://www.distributed.net.*

Distributed.net menjalankan proyek untuk memecahkan beberapa algoritma (enkripsi). Saat ini algoritma yang sedang dicoba dipecahkan adalah RC5-72. Anda dapat mengambil program "client" untuk ikut memecahkan algoritma enkripsi dari situs distributed.net tersebut. Di sana tersedia client untuk berbagai sistem operasi, termasuk untuk Linux tentunya. Setelah program client tersebut dipasang, Anda harus melakukan konfigurasi dahulu. Minimal konfigurasi yang harus Anda lakukan adalah dengan mengisi alamat e-mail Anda yang akan dijadikan *userid* Anda di distributed.net. Setelah itu jika Anda terhubung ke Internet, program *client* ini akan mengambil beberapa kunci yang harus dicoba, kemudian mulai melakukan *cracking* secara *off-line* (tidak perlu *online* ke Internet terus). Ini tidak melanggar hukum *lho*.

Program client yang jalan di komputer Anda ini tidak mengganggu *resources* komputer anda. Dia akan aktif mengambil siklus CPU ketika komputer tidak aktif (misalnya ketika kita membaca e-mail, mengetik surat). Jadi, komputer Anda tidak terasa lambat. Saya pasang client distributed.net ini di hampir semua komputer yang saya miliki, termasuk di *notebook*.

Jika sudah ada satu blok (atau lebih) yang diselesaikan oleh komputer Anda, maka Anda bisa mengirimkan blok tersebut ke distributed.net ketika anda terhubung ke Internet. Satu hari kemudian Anda akan masuk ke statistik dari distributed.net yang bisa dilihat di *http://stats.distributed.net.* Ini menariknya karena Anda bisa melihat ranking Anda. Seberapa hebat *computing cycle* yang Anda miliki?

Selain statistik individual, ada juga statistik kelompok. Jika tertarik, Anda bisa bergabung dengan kami di tim "*Indonesia Raya (aka GBT)*" atau tim nomor 6362 dan menggabungkan statistik individu anda bersama kami. Bagi saya ini yang menarik karena bisa jadi suatu ukuran kemampuan komputasi orang-orang Indonesia. Ayo, saya tunggu keikutsertaan Anda di tim Indonesia Raya!