Bahan Kuliah ke-6

IF5054 Kriptografi

Cipher yang Tidak Dapat Dipecahkan (*Unbreakable Cipher*)

Disusun oleh:

Ir. Rinaldi Munir, M.T.

Departemen Teknik Informatika
Institut Teknologi Bandung
2004

6. *Cipher* yang Tidak Dapat Dipecahkan (*Unbreakable Cipher*)

6.1 Pendahuluan

- *Unbreakable cipher* merupakan klaim yang dibuat oleh kriptografer terhadap algoritma kriptografi yang dirancangnya.

- *Cipher* substitusi (dengan segala varasinya) dan *cipher* transposisi sudah dibuktikan dapat dipecahkan. Kasus Queen Mary pada Abad 18 dan Enigma pada PD II adalah pelajaran betapa klaim *unbreakable cipher* mudah dipatahkan.

- Apakah *unbreakable cipher* memang ada dan dapat dirancang?
  Jawabannya: ada dan bisa dibuat. Untuk merancang *unbreakable cipher,* ada dua syarat yang harus dipenuhi:
  1. Kunci harus dipilih secara acak (yaitu, setiap kunci harus mempunyai peluang yang sama untuk terpilih).
  2. Panjang kunci harus sama dengan panjang plainteks yang akan dienkripsikan.

- Kedua syarat tersebut dapat menyebabkan *setiap* plainteks yang berbeda dan panjangnya sama akan sama-sama mempunyai kemungkinan menghasilkan cipherteks yang diberikan. Dengan kata lain, kriptanalis mendapatkan hasil bahwa cipherteks yang didekripsikannya menghasilkan beberapa plainteks yang mempunyai makna yang berbeda. Hal ini akan membingungkannya dalam menentukan plainteks yang benar.

- *Cipher* yang tidak dapat dipecahkan dikatakan memiliki tingkat kerahasiaan yang sempurna (*perfect secrecy*).

- Satu-satunya algoritma kriptografi sempurna sehingga tidak dapat dipecahkan adalah *one-time pad.*

6.2 *One-Time Pad* (*OTP*)

- *OTP* ditemukan pada tahun 1917 oleh Major Joseph Mauborgne. *Cipher* ini termasuk ke dalam kelompok algoritma kriptografi simetri.

- *One-time pad* (*pad* = kertas bloknot) berisi deretan karakter-karakter kunci yang dibangkitkan secara acak. Aslinya, satu buah *one-time pad* adalah sebuah pita (*tape*) yang berisi barisan karakter-karakter kunci.

- Satu *pad* hanya digunakan sekali (*one-time*) saja untuk mengenkripsi pesan, setelah itu *pad* yang telah digunakan dihancurkan supaya tidak dipakai kembali untuk mengenkripsi pesan yang lain.

- Aturan enkripsi yang digunakan persis sama seperti pada *Vigenere Cipher*. Pengirim pesan menggunakan setiap karakter kunci untuk mengenkripsikan satu karakter plainteks.

- Enkripsi dapat dinyatakan sebagai penjumlahan modulo 26 dari satu karakter plainteks dengan satu karakter kunci *one-time pad*:

$$c_i = (p_i + k_i) \bmod 26 \qquad (5.1)$$

yang dalam hal ini,

p_i : karakter plainteks
k_i : karakter kunci
c_i : karakter cipherteks

- Perhatikan bahwa panjang kunci sama dengan panjang plainteks, sehingga tidak ada kebutuhan mengulang penggunaan kunci selama proses enkripsi.

- Setelah pengirim mengenkripsikan pesan dengan kunci, ia menghancurkan kunci tersebut (makanya disebut satu kali pakai atau *one-time*)

- Penerima pesan menggunakan kunci yang sama untuk mendekripsikan karakter-karakter cipherteks menjadi karakter-karakter plainteks dengan persamaan:

$$p_i = (c_i - k_i) \bmod 26 \qquad (5.2)$$

Contoh 6.1: Misalkan plainteks dan kunci *one-time pad* adalah

plainteks: ONETIMEPAD
kunci: TBFRGFARFM

Nyatakan A = 0, B = 1, …, Z = 25, maka cipherteksnya adalah:

cipherteks: HOJKOREGHP

yang mana diperoleh sebagai berikut:
(O + T) mod 26 = H
(N + B) mod 26 = O
(E + F) mod 26 = J, dst

- Sistem *OTP* ini tidak dapat dipecahkan karena:
  1. Barisan kunci acak yang ditambahkan ke pesan plainteks yang tidak acak menghasilkan cipherteks yang seluruhnya acak.

  2. Beberapa barisan kunci yang digunakan untuk mendekripsi cipherteks mungkin menghasilkan pesan-pesan plainteks yang mempunyai makna, sehingga kriptanalis tidak punya cara untuk menentukan plainteks mana yang benar.

Contoh 6.2: Misalkan kriptanalis mencoba barisan kunci

```
LMCCAWAAZD
```

untuk mendekripsi cipherteks dari Contoh 5.1,

```
HOJKOREGHP
```

Plainteks yang dihasilkan (dengan menggunakan persamaan 5.2):

```
SALMONEGGS
```

Bila ia mencoba barisan kunci

```
ZDVUZOEYEO
```

maka plainteks yang dihasilkan adalah

```
GREENFIELD
```

Dua plainteks yang mempunyai makna ini membingungkan kriptanalis untuk memilih mana yang benar.

6.3 Kelemahan *OTP*

- Meskipun *OTP* merupakan *cipher* yang sempurna aman, namun faktanya ia tidak digunakan secara universal dalam aplikasi kriptografi sebagai satu-satunya sistem *cipher* yang tidak dapat dipecahkan (hanya sedikit sistem komunikasi yang menggunakan *OTP*). Malahan orang masih tetap menggunakan sistem *cipher* yang dapat dipecahkan.

  Alasannya adalah dari segi kepraktisan, yaitu:
  1. Karena panjang kunci harus sama dengan panjang pesan, maka *OTP* hanya cocok untuk pesan berukuran kecil. Semakin besar ukuran pesan, semakin besar pula ukuran kunci. Pada aplikasi kriptografi untuk mengenkripsikan data tersimpan, timbul masalah dalam penyimpanan kunci. Pada aplikasi kriptografi untuk komunikasi pesan, timbul masalah dalam pendistribusian kunci.

  2. Karena kunci dibangkitkan secara acak, maka 'tidak mungkin' pengirim dan penerima membangkitkan kunci yang sama secara simultan. Jadi, salah seorang dari mereka harus membangkitkan kunci lalu mengirimkannya ke pihak lain.

- Karena kerahasiaan kunci harus dijamin, maka perlu ada perlindungan selama pengiriman kunci. Jika hanya ada satu saluran komunikasi, maka pengirim dan penerima pesan perlu barisan kunci lain untuk melindungi kunci pertama, kunci ketiga untuk melindungi kunci kedua, dan seterusnya. Hal ini menghasilkan kumpulan barisan kunci yang tidak berhingga banyaknya.

- Mengirimkan barisan kunci melalui saluran komunikasi yang digunakan untuk pengiriman pesan juga tidak praktis karena pertimbangan lalu lintas (*traffic*) pesan yang padat.

- Oleh karena itu, *OTP* hanya dapat digunakan jika tersedia saluran komunikasi kedua yang cukup aman untuk mengirim kunci. Saluran kedua ini umumnya lambat dan mahal. Misalnya pada perang dingin antara AS dan Uni Soviet (dahulu), kunci dibangkitkan, disimpan, lalu dikirim dengan menggunakan jasa kurir yang aman.

  Penting diingat bahwa saluran kedua yang aman tersebut umumnya lambat dan mahal.