MATEMATIKA PERSANDIAN

Hendra Gunawan, Ph.D.

CBSED - ITB

Saya menerima pesan dari seorang teman berupa rangkaian bilangan sebagai berikut:

64, 43, 82, 55, 133, 95, 140, 97, 3, 2,
46, 31, 95, 65, 46, 31, 123, 85, 40, 27

Adakah yang bisa membantu saya mengartikan pesan tersebut?

Teman saya telah melakukan *pe-nyandian* atau *pengkodean* ter-hadap pesan yang ingin disampai-kannya kepada saya, dari rangkai-an huruf ke rangkaian bilangan seperti di atas, supaya pesan ter-sebut tidak dapat (dengan mudah) dimengerti oleh orang lain.

Penyandian atau pengkodean merupakan suatu bentuk penyimpanan dan/atau pengiriman data/ informasi secara rahasia.

Julius Caesar telah melakukan pengkodean untuk keperluan surat menyurat pada jamannya (lebih daripada 2000 tahun yang lalu).

Yang ia lakukan adalah menggeser setiap huruf dalam surat yang akan dikirimnya, misalnya 5 langkah ke depan:

A menjadi F,
B menjadi G,
. . . , dan
Z menjadi E.

Untuk mengirim pesan yang berkata

SAYA AKAN PULANG LUSA

Julius Caesar akan menulis

XFDF FPFS UZQFSL QZXF.

Untuk memahaminya, geser kembali setiap huruf 5 langkah ke belakang.

Untuk dapat memecahkan suatu pesan yang telah disandikan kita harus mengetahui sistem persandi-an yang dipakai. Jika sistemnya adalah mengggeser setiap huruf 5 langkah ke depan, maka untuk memahami pesan yang telah di-sandikan kita harus menggeser se-tiap huruf 5 langkah ke belakang.

Kembali ke pesan yang saya terima, saya dan teman saya telah menye-pakati sebelumnya bahwa kami akan menggunakan sebuah matriks untuk penyandian. Matriks yang kami pakai adalah

$$M = \begin{bmatrix} 3 & 7 \\ 2 & 5 \end{bmatrix}$$

Bagaimana teman saya melakukan penyandian dengan matriks ini?

Pertama ia ubah pesan yang ingin disampaikannya menjadi rangkaian bilangan dengan aturan:

spasi=0, A=1, B=2, C=3,. . ., Z=26.

Setelah itu ia menyusun rangkaian bilangan yang diperolehnya menjadi sebuah matriks dengan dua baris, dua bilangan pertama disimpan di kolom pertama, dan seterusnya. Sebutlah matriks yang diperolehnya X. Lalu, ia hitung hasil kali MX. Bilangan-bilangan dalam matriks MX ini diuraikan kembali menjadi rang-kaian bilangan yang ia kirimkan.

Intermezo: Perkalian dua Matriks

$$\begin{bmatrix} 3 & 7 \\ 2 & 5 \end{bmatrix} \cdot \begin{bmatrix} 1 & 3 & 5 \\ 2 & 4 & 6 \end{bmatrix} = \begin{bmatrix} 17 & 37 & 57 \\ 12 & 26 & 40 \end{bmatrix}$$

Hasil perkalian baris ke-1 pada matriks pertama dan kolom ke-1 pada matriks kedua sama dengan elemen pada baris ke-1 kolom ke-1 pada matriks di ruas kanan:

$$3(1) + 7(2) = 17.$$

Berbeda dengan perkalian dua bilangan, perkalian dua matriks tidak bersifat komutatif. Secara umum,

$$M.N \neq N.M.$$

Untuk meyakinkan diri, cobalah ambil dua matriks 2 x 2, sebut M dan N, lalu hitung M.N dan N.M.

Matriks bujursangkar, seperti M =

$$\begin{pmatrix} 3 & 7 \\ 2 & 5 \end{pmatrix}$$

mempunyai invers M^{-1} =

$$\begin{pmatrix} 5 & -7 \\ -2 & 3 \end{pmatrix}$$

yang bersifat: $M.M^{-1} = I = M^{-1}.M$,
di mana I adalah matriks identitas

$$\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$$

Lalu bagaimana saya dapat me-mecahkan pesan tadi? Mudah saja. Saya tinggal melakukan kebalikan dari apa yang telah teman saya lakukan, dari langkah terakhir sampai langkah pertama. Pertama, saya susun rangkaian bilangan di atas menjadi sebuah matriks (yang tdd 2 baris), sebutlah

$$Y = \begin{pmatrix} 64 & 82 & 133 & 140 & 3 & 46 & 95 & 46 & 123 & 40 \\ 43 & 55 & 95 & 97 & 2 & 31 & 65 & 31 & 85 & 27 \end{pmatrix}$$

Kemudian saya kalikan Y dengan M^{-1} dari kiri (jangan dari kanan karena perkalian matriks tidak komutatif):

$$\begin{pmatrix} 5 & -7 \\ -2 & 3 \end{pmatrix} \begin{pmatrix} 64 & 82 & 133 & 140 & 3 & 46 & 95 & 46 & 123 & 40 \\ 43 & 55 & 95 & 97 & 2 & 31 & 65 & 31 & 85 & 27 \end{pmatrix}$$

$$= \begin{pmatrix} 19 & 25 & 0 & 21 & 1 & 13 & 20 & 13 & 20 & 11 \\ 1 & 1 & 19 & 11 & 0 & 1 & 5 & 1 & 9 & 1 \end{pmatrix}$$

Lalu saya susun bilangan-bilangan dalam matriks di atas menjadi rangkaian bilangan di bawah ini

19, 1, 25, 1, 0, 19, 21, 11, 1, 0, 13, 1, 20, 5, 13, 1, 20, 9, 11, 1.

Dengan mudah saya dapat membaca rangkaian bilangan ini sebagai

SAYA SUKA MATEMATIKA.

Mungkin ada yang bertanya, bagai-mana kalau kita menerima sebuah pesan yang telah disandikan tetapi kita tidak tahu sistem persandian yang digunakan oleh si pengirim?

Mungkin kita dapat mengutak-atik dan memecahkan sandi tersebut. Seandainya kita tidak tahu apa yang telah dilakukan oleh Julius Caesar sebelum ia mengirim pesan tadi, tidak terlalu sulit bagi kita (yang hidup di era komputer) untuk me-mecahkan maksud pesan tersebut.

Sistem persandian yang kita pakai tentunya harus sedemikian rupa sehingga jika informasi yang kita simpan atau kirim jatuh ke tangan orang lain, maka sulit bagi orang tersebut untuk memahaminya. Untuk sistem persandian menggunakan matriks, semakin besar ukuran matriks yang digunakan, semakin sulit sandi untuk dipecahkan.

Selain menggunakan matriks, masih banyak perangkat lain yang dapat digunakan untuk persandian.

Persandian yang cukup canggih dan banyak dipakai di kalangan agen rahasia sekarang ini biasanya me-manfaatkan bilangan-bilangan *prima* yang besar sekali.

Gagasannya sederhana: Jika kita punya dua buah bilangan prima, maka mudah bagi kita untuk meng-hitung hasil kalinya. Tetapi sebalik-nya, jika kita punya sebuah bilangan komposit (yang merupakan hasil kali dari sejumlah bilangan prima), maka sulit bagi kita untuk memfaktorkan-nya, apalagi jika bilangan tersebut besar sekali.

Sebagai contoh, dengan mudah kita dapat menghitung

$$257 \times 65.537 = 16.843.009.$$

Tetapi coba faktorkan bilangan di bawah ini:

$$4.294.967.297.$$

Jawab: $4.294.967.297 = 641 \times 6.700.417$.

Jadi, dengan menggunakan fakta ttg bilangan prima tsb, mudah bagi kita untuk membuat sandi, namun sulit bagi orang untuk memecahkan sandi kita, kecuali bila mereka tahu sistem persandian yang kita pakai. Gagasan ini dicetuskan oleh Ron **Rivest**, Adi **Shamir**, dan Len **Adleman**. Sistem persandian mereka dikenal sebagai *teknik RSA*.

Teknik RSA menggunakan sebuah bilangan komposit N (besar) dan bilangan *kunci penyandi* r. Pasangan bilangan N dan r dikenal sebagai *public key*.

Selain kedua bilangan tersebut, terdapat bilangan *kunci pemecah* s untuk memecahkan sandi. Bilangan ini tergantung pada r.

Sebagai ilustrasi, kita gunakan N = 33 (= 3 x 11) dan r = 7. [Bilangan r dipilih di antara 1, ..., 20. Di sini 20 = (3 – 1) x (11 – 1).]

Untuk menyandikan huruf B (= 2), kita hitung 2^7 mod(33) = 29.
Jadi sandi untuk huruf B adalah bilangan 29.

Bila kita menerima sandi 29, maka pesan aslinya adalah 2 (= B). Tetapi bagaimana kita bisa mendapatkan bilangan 2 dari 29, dengan meng-gunakan bilangan N = 33 dan r = 7? (N dan r diketahui sbg *public key*.) Dalam hal ini, kita harus mengetahui bilangan kunci pemecah s.

Bilangan kunci pemecah s di sini adalah bilangan yang memenuhi

$$rs = 1 \bmod (20).$$

Untuk r = 7, kita dapatkan s = 3. Sandi 29 kita terjemahkan sebagai

$$29^3 \bmod(33) = 2.$$

Dengan menggunakan N = 33 dan r = 7 (dan, tentu saja, s = 3), coba pecahkan sandi berikut:

7, 1, 26, 2, 0, 15, 13, 0, 30, 21, 20.

Rangkaian bilangan ini harus diter-jemahkan sbg rangkaian bilangan di {0, 1, ... , 32}. Di sini 0 = spasi, 1 = A, dst (27 s/d 32 tidak terpakai).

Sekadar informasi, cabang ilmu matematika yang mempelajari persandian adalah **kriptografi** (*to encript* = membuat sandi).

Di negara kita, terdapat **Lembaga Sandi Negara** yang menangani persandian untuk keperluan negara. Lembaga ini bernaung di bawah Departemen Pertahanan.

28, 1, 19, 4, 1, 3, 0,
11, 26, 14, 26, 19, 21, 0,
12, 1, 13, 3, 0,
14, 1, 17, 21, 5, 0,
31, 26, 4, 1, 5.