Hint: Dani Sedang Bingung

Keanu Fortuna Taufan

Naskah Soal:

Tidak terasa Dani sudah setengah jalan dalam mempelajari Kecerdasan Buatan. Selanjutnya ia harus mulai mempelajari matematika dasar yang mana merupakan kelemahannya. Kemarin ia diberikan soal matematika yang harus dikerjakan dalam waktu yang singkat, soal seperti dibawah:

$$A = \left(X^{Y^Z} \bmod N\right) + 1$$

Bantulah Dani untuk menyelesaikan soal tersebut!

Perhatikan bahwa tidak ada *constraint* tertentu terhadap masing-masing dari X, Y, Z dan N pada persamaan tersebut selain dari fakta bahwa masing-masing nilai tersebut muat di dalam bilangan integer 32-bit. Sehingga teorema Fermat:

$$a^{p-1} \equiv 1 \pmod{p}$$

(1)

Tidak berlaku karena N tidak selalu prima. Kita dapat menggunakan generalisasi dari teorema tersebut, yaitu dengan menggunakan teorema Euler totient:

$$a^{\varphi(n)} \equiv 1 \pmod{n} \;\forall\; \gcd(a, n) = 1$$

(2)

Dengan $\varphi(n)$ adalah fungsi Euler totient dari n. Terdapat beberapa cara untuk melakukan komputasi fungsi $\varphi(n)$. Salah satu cara yang umum adalah dengan secara manual mengecek seluruh bilangan dari 2 hingga n yang koprima dengan n. Untuk nilai n yang besar, kompleksitas fungsi dapat mencapai $O(N \log N)$ dengan asumsi implementasi fungsi gcd (a, b) menggunakan algoritma Euclid. Untuk menyelesaikan masalah ini, dimanfaatkan fungsi multiplikatif $\varphi(n)$ untuk mendapatkan formula produk Euler:

$$\varphi(n) = n \prod_{p|n} \left(1 - \frac{1}{p}\right)$$

(3)

Secara algoritmik, nilai p dapat diperoleh dengan membuat implementasi dari fungsi faktorisasi dengan kompleksitas $O\left(\sqrt{N}\right)$. Implikasi dari persamaan (1) adalah soal dapat disederhanakan menjadi bentuk:

$$X^{Y^Z} \equiv X^{Y^Z \bmod \varphi(N)} \pmod{N} \;\forall\; \gcd(X, N) = 1$$

(4)

Perhatikan bahwa teorema tersebut hanya berlaku ketika X dan N saling prima, sedangkan tidak ada jaminan bahwa kondisi tersebut pasti akan selalu terpenuhi untuk setiap *test case*. Untuk mengatasi hal tersebut, pertama perhatikan salah satu sifat *modular arithmetic* berikut:

$$a \equiv b \pmod{n} \Leftrightarrow ka \equiv kb \pmod{n}$$

(5)

Berdasarkan sifat tersebut, maka basis pada persamaan (4) dapat dipecah menjadi beberapa operasi. Pertanyaannya adalah, apakah ada aturan yang dapat secara efektif memecah basis sedemikian sehingga setiap basis yang dipecah saling prima dengan N? Tanpa memerhatikan kesalingprimaan basis dengan N, dapat dipastikan bahwa basis X dapat dipecah berdasarkan faktorisasi prima dari X.

$$X = x_1^{p_1} \times x_2^{p_2} \times \ldots \times x_n^{p_n}$$

(6)

Untuk x_i adalah suatu faktor prima dan p_i adalah pangkat dari faktor prima x_i. Menggunakan cara ini, kita dapat memecah persamaan (4) menjadi seperti berikut:

$$X^{Y^Z} \equiv \left(\prod_{x|X} x_i^{p_i} \right)^{Y^Z \bmod \varphi(N)} \pmod{N}$$

(7)

Masalah lain yang muncul adalah, bahkan ketika X dipecah berdasarkan faktor prima, masih tidak ada jaminan bahwa setiap x_i dan N saling prima. Namun, pemecahan ini akan membantu kita untuk merekayasa angka menjadi saling prima. Perhatikan bahwa selain basis, modulo juga dapat dipecah berdasarkan sifat berikut:

$$a \equiv b \pmod{n} \Leftrightarrow ka \equiv kb \pmod{kn}$$

(8)

Sifat tersebut adalah kunci penyelesaian masalah ini. Manfaatkan persamaan-persamaan yang telah diberikan dan gabungkan sifat-sifat yang relevan terhadap algoritma Anda untuk menemukan solusi dari soal ini!