What is RSA?

4 วินาที 32 MB

RSA (Rivest-Sharmir-Adleman) เป็นหนึ่งในการเข้ารหัสที่มีการใช้งานอย่างแพร่หลายมาอย่างยาวนานที่ใช้หลักการทางคณิตศาสตร์ *Congruence Modulo* ช่วยในการเข้ารหัสเพื่อให้การเดาเป็นไปได้ยากลำบาก

ดร. บ๋าวผู้ศึกษาคณิตศาสตร์มามากกว่า 2 ชั่วโมงและได้ไปเจอกับบทความนึงเกี่ยวกับการเข้ารหัส RSA ที่เขียนโดยคุณเนิร์ดพีร่วมกับคุณแอนดี้

1. เลือกจำนวนเฉพาะสองตัวที่ต่างกัน p และ q
2. คำนวณค่า $n = p \times q$ เพื่อเป็น $Public\ Key$
3. หาค่า $\Phi(n) = (p-1)(q-1)$
4. เลือกค่า e ที่ $1 < e < \Phi(n)$ และ $gcd(e, \Phi(n)) = 1$
5. หาค่า $Private\ Key\ d$ ที่ $e \times d \equiv 1\ mod\ \phi(n)$
6. เข้ารหัสข้อความ M โดย $C = M^e \mod n$ จะได้ C เป็นข้อความลับ
7. ถอดรหัสข้อความ C โดย $M = C^d \mod n$ จะได้ M เป็นข้อความต้นฉบับ

หลังจากอ่านบทความนี่เสร็จดร. บ่าวมอบหมายงานเด็กโอคอมที่ไฟแรงโดยจะถาม t ครั้ง ว่าถ้าให้ *Encrypt* (เข้ารหัส) ข้อความ M เมื่อให้ p, q และ e เมื่อเช็คกับขั้นตอนแล้วถ้าถูกต้องให้ส่งค่า C *ที่เป็นฐาน 16* กลับมาแต่ถ้าไม่ถูกต้องให้ส่ง *Error* และถ้าให้ *Decrypt* (ถอดรหัส) ข้อความ C เมื่อให้ p, q และ e ให้ส่งค่า M *ที่เป็นฐาน 16* กลับมา แต่ถ้าเช็คกับขั้นตอนไม่ถูกให้ส่ง *Error* ออกมา

ข้อมูลนำเข้า

แต่ละชุดทดสอบมีหลายเทสเคส บรรทัดแรกรับค่าจำนวนเต็ม t แทนจำนวนเทสเคส

บรรทัดแรกของแต่ละเทสเคส ข้อความ K (Encrypt หรือ Decrypt)

บรรทัดที่สองของแต่ละเทสเคส M หรือ C $(1 < M, C < 10^5)$ ตามด้วย p $(1 < p < 10^5)$, q $(1 < q < 10^5)$ และ e $(1 < e < 10^4)$

ข้อมูลส่งออก

แต่ละชุดทดสอบส่งค่าข้อความออก: ข้อความ M หรือ C ที่เป็นฐาน 16 และถ้าค่าที่ได้ไม่เป็นไปตามขั้นตอนให้ตอบ *Error*

*** รับประกันว่า p, q จะเป็นจำนวนเฉพาะ**

ตัวอย่างข้อมูลนำเข้าและข้อมูลส่งออก

ข้อมูลนำเข้า	ข้อมูลส่งออก
1 Encrypt 70919 677 251 3	13E19
1 Decrypt 689 599 929 3	2D437

3 Encrypt 76070 821 127 4 Encrypt 27537 307 919 5 Decrypt 233 701 577 17	Error 16B71 26983