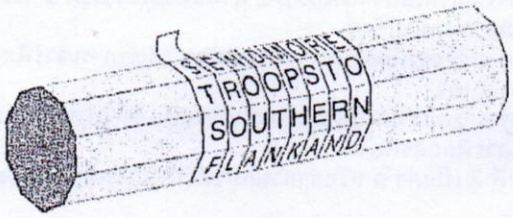
การเข้ารหัสแบบ Spartan Scytale

โจทย์ปัญหา

การเข้ารหัสข้อมูลโดยการสลับตำแหน่งตัวอักษรวิธีหนึ่งสำหรับใช้เข้ารหัสข่าวสารที่ใช้การสงคราม เรียกว่า"Spartan scytale" ซึ่งเริ่มใช้งานในช่วง 5 ศตวรรษก่อนคริสตกาล คำว่า Spartan เป็นชื่อนักรบจากเมือง Sparta ซึ่งเป็นเมืองในสมัยกรีกโบราณ ส่วนคำว่า Scytale เป็นแท่งไม้เป็นแท่งไม้รูปหลายเหลี่ยม สำหรับพันแถบหนังหรือกระดาษชุบไขไปตลอดความยาวของแท่งไม้ ผู้ส่งสารจะเขียนข่าวสารไปตามความยาวของแท่งไม้ทีละแถว เมื่อคลายออกจะได้แถบหนังหรือกระดาษชุบไขที่มีตัวอักษรที่ดูเหมือนจะไม่มีความหมายใด ในกรณีที่เขียนลงบนแถบหนังจะมีการนำแถบหนังนั้นมาทำเป็นเข็มขัดสำหรับผู้ส่งสาร โดยกลับด้านที่มีข้อความไว้ด้านในเพื่อเป็นการตบตาศัตรูอีกชั้นหนึ่ง



สมมุติให้ข่าวสารที่ต้องการส่ง (เรียกว่า Plain text) เป็นดังนี้

HELP ME I AM UNDER ATTACK.

ขั้นแรกให้ทำการกำจัดเครื่องหมายวรรคตอนออกทั้งหมด จะได้ข่าวสารซึ่งมีเฉพาะตัวอักษรตัวใหญ่ (Uppercase) ดังนี้

HELPMEIAMUNDERATTACK

จากนั้นจึงทำการคำนวณหาจำนวนตัวอักษรต่อบรรทัดที่จะเขียนลงใน Scytale แต่ละด้าน โดยคำนวณจากความยาวของสายอักขระที่กำจัดเครื่องหมายวรรคตอนแล้ว หารด้วยจำนวนเหลี่ยม เศษที่เหลือของการหารปัดให้เป็น 1 ในตัวอย่างนี้คือ 20/4 = 5 ซึ่งหากใช้หากกำหนดให้ Scytale สี่เหลี่ยมจตุรัส สามารถเขียนตัวอักษรแต่ละด้านได้ 1 แถว แถวละ 5 ตัว เมื่อนำกระดาษหรือแผ่นหนังพันรอบแล้ว เขียนข่าวสารในแต่ละด้านได้ดังนี้

H	E	L	P	M
E	I	A	M	U
N	D	E	R	A
T	T	A	C	K

เมื่อเขียนเสร็จ ทำการคลี่แถบกระดาษหรือแถบหนังออกจะปรากฏข้อความที่เข้ารหัสแล้ว (เรียกว่า Cipher text) บนแถบกระดาษหรือแถบหนังดังนี้

HENTEIDTLAEAPMRCMUAK

สำหรับการถอดรหัส สามารถทำได้โดยใช้วิธีการกลับกันกับการเข้ารหัส

จงเขียนโปรแกรมรับข้อความจากผู้ใช้ ในกรณีที่เป็นข่าวสารธรรมดา (Plain text) ให้ทำการเข้ารหัสและแสดงข่าวสารที่เข้ารหัสแล้ว หากเป็นข่าวสารที่เข้ารหัสแล้ว (Cipher text) ให้ทำการถอดรหัส และแสดงข้อความที่ถอดรหัสแล้ว

ข้อมูลเข้า

ข้อมูลเข้าแต่ละชุดประกอบด้วยข้อมูล 2 บรรทัด บรรทัดแรกเป็นจำนวนเต็มสองจำนวนได้แก่ n และ m เมื่อ n เป็นจำนวนเหลี่ยมของแท่งไม้ Scytale และ $3 \le n \le 6$, ส่วน m เป็นรหัสดำเนินการซึ่งมีค่าเพียง 2 ค่าคือ 1 และ 2 เมื่อ 1 ใช้แทนการเข้ารหัส (Encryption) และ 2 ใช้แทนถอดรหัส (Decryption)

ข้อมูลเข้าบรรทัดที่สองเป็นสายอักขระภาษาอังกฤษที่มีจำนวนตัวอักขระ s ตัวรวมทั้งเครื่องหมายวรรคตอนด้วยเมื่อ $16 \le s \le 128$ (ในกรณีที่ m = 1 สายอักขระจะเป็นข่าวสารธรรมดา (Plain text) ซึ่งต้องเปลี่ยนให้เป็นข่าวสารที่เข้ารหัสแล้ว และหาก m = 2 สายอักขระจะเป็นข่าวสารที่เข้ารหัสแล้ว (Cipher text) ซึ่งต้องเปลี่ยนให้เป็นข่าวสารธรรมดา (Plain text)

การแสดงผล

สำหรับข้อมูลเข้าแต่ละชุด กำหนดให้มีข้อมูลออกเพียงชุดเดียว เป็นสายอักขระที่ทำการเข้ารหัสแล้ว (Cipher text) ในกรณีที่ m = 1, และข้อมูลออกเป็นสายอักขระที่ทำการถอดรหัสแล้ว (Plain text) ในกรณีที่ m = 2

ตัวอย่างข้อมูลเข้าและการแสดงผล

ตัวอย่างที่ 1

<u>ข้อมูลเข้า</u>

4 1

HELP ME I AM UNDER ATTACK

<u>ผลลัพธ์</u>

HENTEIDTLAEAPMRCMUAK

ตัวอย่างที่ 2

<u>ข้อมูลเข้า</u>

6 2

TSETRRHTRIETYHITAOSYFGPIEPTORTCRHTIRIOHSESUOOTOLUNINEAE

<u>ผลลัพธ์</u>

THYSECRETISTHYPRISONERIFTHOULETITGOTHOUAREAPRISONERTOIT