

การบ้านวิชา วพ.208 ครั้งที่ 12 (Bonus Points)

กำหนดส่ง 19 ก.พ. 2552

ในการสื่อสารข้อมูล ดังเช่น ประวัติด่วน เลขบัญชี หรืออื่นๆ ถ้าหากต้องการป้องกันไม่ให้ผู้อื่นสามารถล่วงรู้ถึงข้อมูลที่ส่งได้ จำเป็นต้องทำการเข้ารหัสข้อมูล วิธีพื้นฐานที่ใช้กันสำหรับข้อมูลที่เป็นตัวอักษร ได้แก่

1. การแทนที่ตัวอักษร (Substitution) ที่มีวิธีการง่ายๆคือ สร้างตาราง Substitution เช่น

a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z
Q	W	E	R	T	Y	U	I	O	P	A	S	D	F	G	H	J	K	L	Z	X	C	V	B	N	M

และทำการแทนที่ตัวอักษรโดยใช้ตารางนี้เป็นหลัก เช่น attack -> QZZQEA เป็นต้น

2. การใช้ keyword เป็นการเข้ารหัสโดยนำตัวอักษรในข้อมูล EXCLUSIVE OR กับ keyword ที่กำหนดขึ้น ยกตัวอย่าง เช่น ถ้าข้อมูลเท่ากับ application และ keyword ที่ใช้คือ music ข้อมูลที่ผ่านการเข้ารหัสจะเท่ากับ

a^m p^u p^s l^i i^c c^m a^u t^s i^i o^c n^m

จงเขียนโปรแกรมที่ทำการเข้ารหัสและถอดรหัสข้อมูลตัวอักษร โดยให้อ่านข้อมูลจากไฟล์ และเก็บข้อมูลลงในไฟล์