ชื่อ..... รหัส.....

PRINCE OF SONGKLA UNIVERSITY

FACULTY OF ENGINEERING

Midterm Examination: 2nd Semester Academic Year: 2009

Date: 24 December 2009 Time: 9:00-12:00

Subject: 241-427 Computer Security Room: R201

ทุจริตในการสอบ โทษขั้นต่ำคือ ปรับตกในรายวิชาที่ทุจริต และพักการเรียน 1 ภาคการศึกษา

คำสั่ง

- อนุญาตให้นำกระดาษ A4 ที่เขียนด้วยลายมือเข้าห้องสอบได้ คนละ 1 แผ่นและให้นักศึกษาส่งกระดาษที่ตนเองนำเข้ามาพร้อมข้อสอบ
- กรุณาเขียนชื่อและรหัสนักศึกษาบนข้อสอบทุกหน้า ข้อสอบมีทั้งหมด 11 หน้า
- ข้อสอบมี 10 ข้อ กรุณาตอบทุกข้อ
- ข้อสอบแต่ละข้อมีคะแนนเท่ากันคือ ข้อละ 10 คะแนน รวม 100 คะแนน

อาจารย์จะสามารถตรวจได้เฉพาะคำตอบที่อาจารย์อ่านออกเท่านั้น

หากอาจารย์อ่านคำตอบคุณไม่ออก คุณจะไม่ได้คะแนน

ข้อ	คะแนน
1	
2	
3	
4	
5	

ข้อ	คะแนน
6	
7	
8	
9	
10	

รวม_____

ชื่อ..... รหัส.....

1. ในกรณีต่อไปนี้ จงบอกว่าเป็นการใช้วิธีการใด (cryptography หรือ steganography) ในการรักษาความลับ พร้อมให้คำอธิบาย

ก. นักเรียนเขียนคำตอบลงในกระดาษชิ้นเล็กๆ แล้วม้วนใส่ในปากกาแล้วส่งปากกาด้ามนั้นไปให้เพื่อนที่สอบอยู่ข้างๆ

ข. สายลับคนหนึ่งส่งข้อมูลไปให้หัวหน้าของตนเองโดยการแทนตัวอักขระแต่ละตัวด้วยสัญลักษณ์ที่ตนเองและหัวหน้าได้มีการตกลงกันไว้ล่วงหน้า

ค. บริษัทแห่งหนึ่งใช้น้ำหมึกพิเศษในการพิมพ์เช็คของตนเองเพื่อป้องกันการปลอมเช็ค

ง. นักศึกษาปริญญาเอกคนหนึ่งทำ water mark บนเอกสารวิทยานิพนธ์ของตนเองที่เธอแขวนไว้บนเว็บ

ชื่อ..... รหัส.....

2. ในแต่ละกรณีต่อไปนี้ จงตอบคำถามว่าเป็นการคุกคามความปลอดภัยด้านใด ในสามด้านต่อไปนี้ confidentiality, integrity, availability พร้อมให้คำอธิบาย

ก. นักศึกษารายหนึ่งเข้าไปในห้องพักอาจารย์เพื่อแอบดูข้อสอบที่อาจารย์จะใช้ทดสอบตนเองในวันรุ่งขึ้น

ข. แม่บ้านรายหนึ่งเขียนเช็คให้พ่อค้าเป็นจำนวน 1,000 บาท เพื่อซื้อตู้เย็นเก่าเครื่องหนึ่ง แต่ภายหลังพบว่าเช็คที่ตนเองจ่ายไปนั้น พ่อค้านำไปขึ้นเงินเป็นจำนวน 10,000 บาท

ค. พนักงานร้านคอมพิวเตอร์รายหนึ่งส่งอีเมล์ไปให้เพื่อนตนเองที่มหาวิทยาลัยเป็นจำนวนร้อยๆอีเมล์ต่อวัน โดยใช้อีเมล์ที่ตนเองปลอมขึ้นมา

3. กลุ่มผู้รักช้างในจังหวัดสงขลามีจำนวน 200 คน ซึ่งสมาชิกของกลุ่มนี้จะส่งข้อความเป็นความลับถึงสมาชิกอื่นเพื่อส่งข่าวเรื่องการนำช้างมาใช้งานอย่างไม่ถูกกฎหมาย หากสมาชิกในกลุ่มใช้วิธีการเข้ารหัสแบบ symmetric key cryptography ถามว่า

ก. จะมีจำนวน key ทั้งหมดเท่าไร เพื่อให้สมาชิกสามารถติดต่อสื่อสารกันได้ แสดงวิธีการคิดพร้อมอธิบาย

ข. หากสมาชิกในกลุ่มเชื่อใจหัวหน้ากลุ่มของตนเอง โดยในการส่งข้อความแต่ละครั้งจะทำการส่งผ่านหัวหน้าของตนเองทุกครั้ง นั่นคือ หากนายเอ จะส่งข้อความถึงนายบี นายเอจะส่งข้อความของตนไปให้หัวหน้า แล้วหัวหน้าก็จะส่งข้อความต่อไปให้นายบี ถามว่าจำนวน key ทั้งหมดจะเป็นเท่าไร เพื่อให้สมาชิกสามารถติดต่อสื่อสารกันได้ แสดงวิธีการคิดพร้อมอธิบาย

ชื่อ..... รหัส.....

4. กำหนดให้ S-Box ใน DES เป็นดังตาราง

	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
0	10	00	09	14	06	03	15	05	01	13	12	07	11	04	02	08
1	13	07	00	09	03	04	06	10	02	08	05	14	12	11	15	01
2	13	06	04	09	08	15	03	00	11	01	02	12	05	10	14	07
3	01	10	13	00	06	09	08	07	04	15	14	03	11	05	02	12

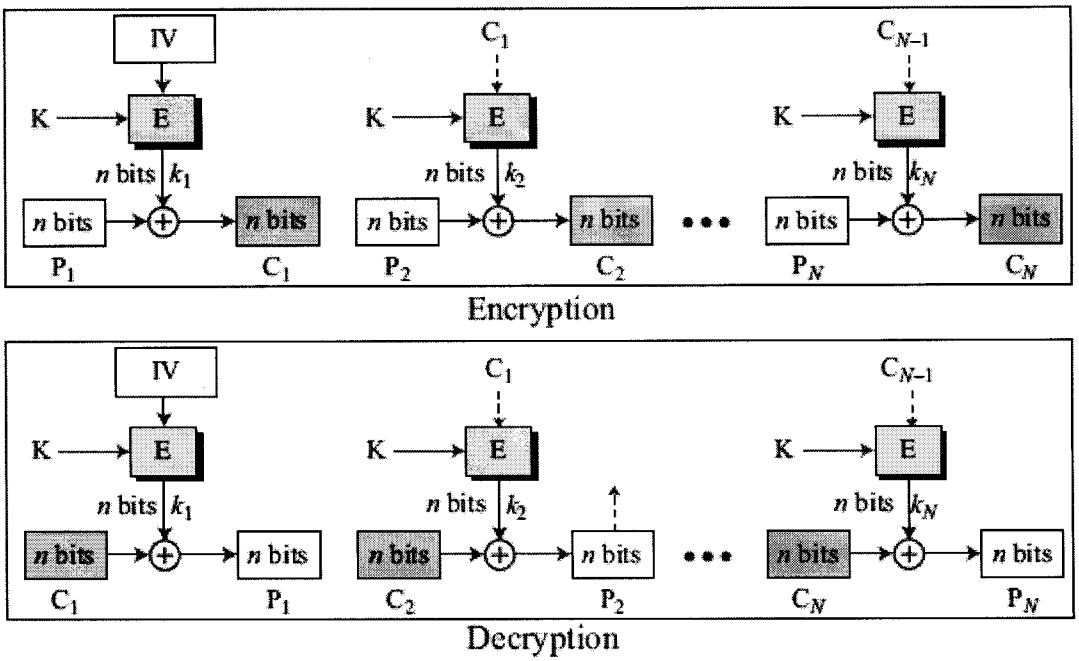
จงหาผลลัพธ์ของ input ต่อไปนี้ แสดงวิธีการคิด

ก. 110111

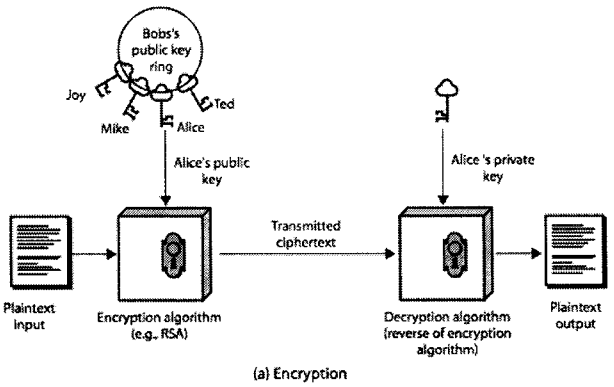
ข. 001100

ค. 000000

5. นักคณิตศาสตร์รายหนึ่งได้คิดค้นวิธีการเข้ารหัสแบบใหม่ขึ้นมาเพื่อใช้งาน โดยวิธีการเข้ารหัสและถอดรหัสแสดงไว้ในรูป จงวิเคราะห์วิธีการดังกล่าว และแจกแจงข้อดีข้อเสียของระบบดังกล่าว



6. ภายใต้ RSA cryptosystem จงอธิบายว่า



ก. อะไรคือ one-way function ของระบบ

ข. อะไรคือ trapdoor ของระบบ

ค. public-key คืออะไร

ง. private-key คืออะไร

จ. ความปลอดภัยของระบบนี้ ขึ้นอยู่กับอะไรบ้าง

ฉ. ทำไมจึงไม่สามารถใช้เลข 1 เป็น public-key ภายใต้ RSA

7. นักศึกษาคนหนึ่งนั่งคิดวิธีการทำ Message digest ซึ่งมีรายละเอียดดังนี้

```
Simple_digest(message)
    MD = 0
    For each byte i of the message
        MD =  (message(i) + MD) mod 26
```

กำหนดตารางการเทียบค่าอักขระเป็นตัวเลขดังตาราง

A	B	C	D	E	F	G	H	I	J	K	L	M
0	1	2	3	4	5	6	7	8	9	10	11	12

N	O	P	Q	R	S	T	U	V	W	X	Y	Z
13	14	15	16	17	18	19	20	21	22	23	24	25

จงตอบคำถามต่อไปนี้

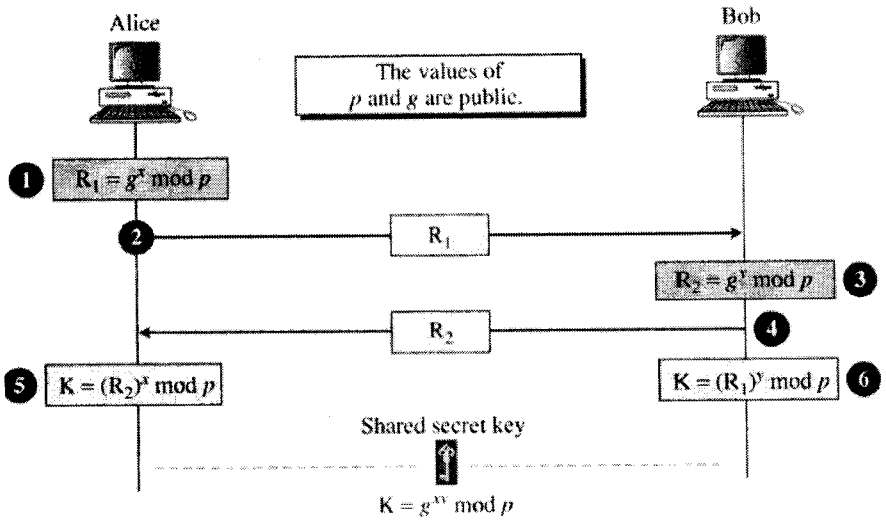
ก. ค่า digest ของข้อความ HELLO เป็นเท่าไร พร้อมแสดงวิธีคิด

ข. ทำไมระบบเช่นนี้จึงไม่มีความปลอดภัย

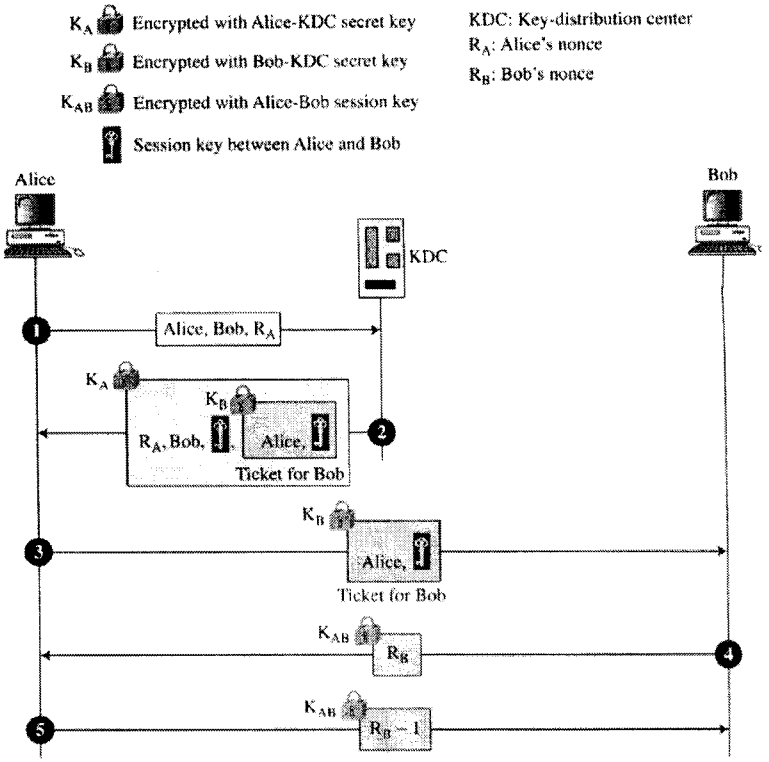
ค. หากเปลี่ยนสมการ จากเดิม ใช้ mod 26 เป็น mod 27 จะมีผลอย่างไรต่อระบบ

ง. หากเปลี่ยนสมการ จากเดิม ใช้ mod 26 เป็น mod 25 จะมีผลอย่างไรต่อระบบ

8. จากรูปแสดงวิธีการ Diffie-Hellman ในการสร้างคีย์โดยไม่ผ่านคนกลาง จงอธิบายว่าผู้ไม่ประสงค์ดีสามารถทำลายระบบนี้ได้อย่างไร



9. จากรูปเป็นวิธีการ Needhan-Schroeder ซึ่งเป็นการสร้างคีย์ผ่านคนกลาง จงอธิบายว่าหากตัดขั้นตอนที่ 4 และ 5 ออกไปจากระบบจะสร้างปัญหาอะไรได้บ้าง



10. บริษัทขายอาหารแช่แข็งส่งออกรายหนึ่งได้มาว่าจ้างให้คุณ เป็นคนดูแลระบบฐานข้อมูลของบริษัท โดยลูกค้าสามารถ log-in เข้ามาสั่งสินค้า และดูรายละเอียดของ order ผ่านทาง web ของบริษัทได้ จงอธิบายวิธีการจัดเก็บฐานข้อมูล login name และ password ของลูกค้า ให้คำนึงถึง dictionary attack ด้วย