แนวข้อสอบ รุ่น 7 (2554)

1. ถอดรหัสนี้ FINUXMZPUEFTQKMZPAREYUXQ

   Ans THAILANDISTHELANDOFSMILE

2. ถอดรหัสนี้ TICIMCNEKSUJEMCNEQFTOIMGAOFTICIQGOQNEEQSNKLFOLPI

   Ans THAILANDISTHELANDOFSMILEANDTHAIPEAPLEDOSMILEALO

3. สำหรับ polynomial $x^8 + x^4 + x^3 + x^2 + 1$ ให้วาด LFSR ที่สร้าง...

   - ให้หา period ของ LFSR นี้

4. 577 (p) & 587 (q) เป็นจำนวนเฉพาะหรือไม่ ถ้าเป็นให้ใช้จำนวนทั้งสองสร้าง RSA keys (การ gen public และ Private key) โดยเลือก e และ d ขึ้นมา Encrypt & Decrypt ข้อความ 137

5. (1 ,3 ,10 ,20 ,70, 105, 210) เป็น simple knapsack หรือไม่ถ้าเป็นให้เลือกค่า u, w หา w^{-1} แล้วเข้ารหัส และถอดรหัสข้อความ 103

6. Security policy คืออะไร มีประโยชน์อย่างไร?

7. อธิบายความหมายของคำต่อไปนี้

   a. Smurf attack

   b. TCP Syn Flooding

   c. TCP Session Hijacking

8. ในห้องอาจารย์ขิมมี่ com กับ file ต่างๆรวมทั้งคะแนนสองของนักศึกษา

   a. อาจารย์ขิมตั้ง password เครื่องว่า panda และจด pwd ไว้ในเศษกระดาษ วางไว้ข้างโต๊ะ

   b. อาจารย์ขิมชอบเปิดห้องทิ้งไว้ระหว่างไปห้องน้ำ ทานอาหารกลางวัน ระหว่างที่... ไปชมภาพยนตร์

   c. แม่บ้านทำความสะอาดที่กุญแจห้องอาจารย์ขิม และมักเปิดห้องทำความสะอาดทุกวันบางครั้งเปิดทิ้งไว้

   d. กมล ภครุจน์ และอิงควิต ได้คะแนน 0 จากการสอบกลางภาค... อะไรคือ asset ,vulnerability ,threat ?

แนวข้อสอบ รุ่น 8 (2555)

ข้อ 1

หลังจากพระนางซูสีไทเฮาปลดฮ่องเต้องค์ที่ 20 ออกจากตำแหน่งก็มีความเบื่อหน่ายที่บุตรหลานของตนเองบริหารประเทศไม่ได้ดังใจ และในเวลานั้นเจ้าคุณทะนง คุณหญิงใจพรและบุตรีทั้งสองก็กำลังพักผ่อนตากอากาศอยู่ในกรุงปักกิ่ง ซูสีไทเฮาจึงตัดสินใจแต่งตั้งเจ้าคุณทะนงและคุณหญิงใจพรขึ้นเป็นฮ่องเต้และฮองเฮาแห่งราชวงศ์ชิง

ฮ่องเต้ทะนง ฮองเฮาใจพร องค์หญิงชัญญา และองค์หญิงอรพินท์จึงได้ย้ายที่พำนักจากตำหนักหลินฮุ่ย มาอยู่ที่ตำหนักใหญ่ในพระราชวังต้องห้ามกลางกรุงปักกิ่ง

ที่พระราชวังต้องห้ามมีเอกสารลับที่ส่งผลต่อความมั่นคงของราชสำนักอยู่ฉบับหนึ่ง ชื่อว่าเอกสารช่วงช่วง ซึ่งฮ่องเต้ทะนงจะต้องระมัดระวังไม่ให้รั่วไหลออกสู่ภายนอก โดยเฉพาะกับผู้ที่เป็นศัตรูกับราชวงศ์ชิง

อาจารย์สุพัณณดามีความโกรธแค้นพระนางซูสีไทเฮา ที่พระนางได้ตัดสินใจจับตัวอาจารย์สุพัณณดาส่งมาอยู่ที่เชียงใหม่ ภายใต้การดูแลของรัฐบาลไทย อาจารย์สุพัณณดาจึงประกาศตนเป็นศัตรูกับซูสีไทเฮาและราชวงศ์ชิงโดยเปิดเผย

อาจารย์สุพัณณดามีสายสอดแนมอยู่ในพระราชวังต้องห้าม โดยทำหน้าที่เป็นหัวหน้าคนรับใช้ผู้มีอิทธิพลภายในพระราชวัง มีชื่อว่า จามิ-กงกง โดยที่ซูสีไทเฮาและฮ่องเต้ทะนงก็ทราบว่า จามิกงกงเป็นสายลับให้กับศัตรูแต่ยังไม่มีหลักฐานผูกมัดเอาผิดได้

จามิกงกงมีข้อจำกัดในการทำงานคือ จามิกงกงไม่สามารถติดต่อสื่อสารกับอาจารย์สุพัณณดาได้

ในพระราชวังต้องห้ามจะมีเอกสารอีกฉบับคือ วิธีการติดต่อสื่อสารกับต่างประเทศ ซึ่งหากใครได้อ่านเอกสารนี้ก็จะสามารถติดต่อสื่อสารกับผู้ที่อยู่ในต่างประเทศได้ หากจามิกงกงได้อ่านเอกสารนี้ก็จะสามารถติดต่อสื่อสารกับอาจารย์สุพัณณดาได้

ฮองเฮาใจพรไม่ต้องการเกี่ยวข้องกับเรื่องความลับ และพระนางซูสีไทเฮาก็เสด็จออกไปพำนักที่พระราชวังฤดูร้อน ทำให้ผู้ที่เกี่ยวข้องคือ

อยู่ในวัง: ฮ่องเต้ทะนง องค์หญิงชัญญา องค์หญิงอรพินท์ และจามิกงกง

ต่างประเทศ: อาจารย์สุพัณณดา

องค์หญิงชัญญาสนิทสนมกับจามิกงกง และไม่มีความลับต่อกัน องค์หญิงอรพินท์ไม่ชอบจามิกงกง และจะไม่บอกข้อมูลใดๆ แก่จามิกงกง เป็นอันขาด นอกจากนี้องค์หญิงอรพินท์จะไม่บอกข้อมูลใดๆ แก่องค์หญิงชัญญา เพราะองค์หญิงอรพินท์เห็นว่าองค์หญิงชัญญาเป็นองค์หญิงที่ปากโป้งเก็บความลับไว้ไม่อยู่

ให้ระบุ state ทั้งหมดที่เป็นไปได้ของระบบนี้ (SxOxA) ของผู้ที่เกี่ยวข้องทั้ง 5 และเอกสารที่เกี่ยวข้องมีสองเอกสารคือ เอกสารช่วงช่วง และเอกสารวิธีการติดต่อสื่อสารกับต่างประเทศ และสิทธิการเข้าถึงมีเพียงอย่างเดียวคือการอ่านหรือรับทราบข้อความในเอกสาร

เป้าหมายของฮ่องเต้ทะนงคือ ป้องกันไม่ให้อาจารย์สุพัณณดาทราบข้อมูลใน เอกสารช่วงช่วง

ให้ระบุด้วยว่า state ใดเป็น safe state และ state ใดเป็น unsafe state (7 คะแนน)

- หากระบบอยู่ใน safe state และจามิกงกงไม่ทราบข้อมูลในเอกสารวิธีการติดต่อสื่อสารกับต่างประเทศ การที่ฮ่องเต้ทะนงบอกข้อมูลเอกสารช่วงช่วงแก่จามิกงกงจะทำให้ระบบเปลี่ยนไปอยู่ใน unsafe state หรือไม่ (1 คะแนน)

- หากระบบอยู่ใน safe state และจามิกงกงทราบข้อมูลในเอกสารช่วงช่วง การที่ฮ่องเต้ทะนงบอกข้อมูลเอกสารวิธีการติดต่อสื่อสารกับต่างประเทศแก่องค์หญิงชัญญาจะทำให้ระบบเปลี่ยนไปอยู่ใน unsafe state หรือไม่ (1 คะแนน)

ข้อ 2

ฮ่องเต้ทะนงพยายามเพิ่มความมั่นคงให้กับราชสำนักจีนด้วยการผูกสัมพันธไมตรีกับอาณาจักรหมีแพนด้าที่อยู่ใกล้เคียง โดยจัดให้มีการอภิเษกองค์หญิงทั้งสองกับองค์ชายหมีแพนด้าสององค์ด้วยกัน องค์หญิงชัญญาอภิเษกกับ องค์ชายหมี นราทร และองค์หญิงอรพินท์อภิเษกกับองค์ชายหมีศุภโชค

ในงานพิธีดังกล่าว มีงานสามอย่าง คือการทำอาหาร การล้างจาน และการยกของ เพื่อป้องกันความผิดพลาดในการทำงาน ทางราชสำนักจีนจึงได้ออกเอกสารหลายฉบับว่าด้วยการทำงานทั้งสามอย่างในพิธีอภิเษก รายชื่อเอกสารต่างๆ และ category และระดับความสำคัญมีดังนี้

เอกสารรูปแบบการจัดเลี้ยง ({การทำอาหาร, การล้างจาน}, สำคัญมาก)
เอกสารการล้างจานให้แวววับด้วยซันไลท์ผสมมะนาวดอง ({การล้างจาน}, สำคัญน้อย)
เอกสารวิธีการยกของให้ถูกหลักสุขภาพ ({การยกของ}, สำคัญมาก)

- ตามหลักการของ Biba Static Integrity Model ให้ระบุว่าใครสามารถอ่านเอกสารใดได้บ้าง (1 คะแนน)

- ตามหลักการของ Biba Static Integrity Model ให้ระบุว่าใครสามารถเขียนเอกสารใดได้บ้าง

(1 คะแนน)

- ตามหลักการของ Biba Dynamic Integrity Model ให้ระบุ security label ที่เปลี่ยนไปหากฮ่องเต้ทะนงอ่านเอกสารเอกสารรูปแบบการจัดเลี้ยง (0.5 คะแนน)

- ตามหลักการของ Biba Dynamic Integrity Model ให้ระบุ security label ที่เปลี่ยนไปหากฮ่องเต้ทะนงอ่านเอกสารการล้างจานให้แวววับด้วยซันไลท์ผสมมะนาวดอง (0.5 คะแนน)

- ตามหลักการของ Biba Dynamic Integrity Model ให้ระบุ security label ที่เปลี่ยนไปหากฮ่องเต้ทะนงอ่านเอกสารวิธีการยกของให้ถูกหลักสุขภาพ (0.5 คะแนน)

- ตามหลักการของ Biba Dynamic Integrity Model ให้ระบุ security label ที่เปลี่ยนไปหากฮองเฮาใจพรอ่านเอกสารเอกสารรูปแบบการจัดเลี้ยง (0.5 คะแนน)

- ตามหลักการของ Biba Dynamic Integrity Model ให้ระบุ security label ที่เปลี่ยนไปหากฮองเฮาใจพรอ่านเอกสารการล้างจานให้แวววับด้วยซันไลท์ผสมมะนาวดอง (0.5 คะแนน)

- ตามหลักการของ Biba Dynamic Integrity Model ให้ระบุ security label ที่เปลี่ยนไป หากฮองเฮาใจพรอ่านเอกสารวิธีการยกของให้ถูกหลักสุขภาพ (0.5 คะแนน)

- ตามหลักการของ Biba Dynamic Integrity Model ให้ระบุ security label ที่เปลี่ยนไป หากซูสีไทเฮาอ่านเอกสารเอกสารรูปแบบการจัดเลี้ยง (0.5 คะแนน)

- ตามหลักการของ Biba Dynamic Integrity Model ให้ระบุ security label ที่เปลี่ยนไป หากซูสีไทเฮาอ่านเอกสารการล้างจานให้แวววับด้วยซันไลท์ผสมมะนาวดอง (0.5 คะแนน)

- ตามหลักการของ Biba Dynamic Integrity Model ให้ระบุ security label ที่เปลี่ยนไป หากซูสีไทเฮาอ่านเอกสารวิธีการยกของให้ถูกหลักสุขภาพ (0.5 คะแนน)

- ตามหลักการของ Biba Dynamic Integrity Model ให้ระบุ security label ที่เปลี่ยนไป หากจามิกงกงอ่านเอกสารเอกสารรูปแบบการจัดเลี้ยง (0.5 คะแนน)

- ตามหลักการของ Biba Dynamic Integrity Model ให้ระบุ security label ที่เปลี่ยนไป หากจามิกงกงอ่านเอกสารการล้างจานให้แวววับด้วยซันไลท์ผสมมะนาวดอง (0.5 คะแนน)

- ตามหลักการของ Biba Dynamic Integrity Model ให้ระบุ security label ที่เปลี่ยนไป หากจามิกงกงอ่านเอกสารวิธีการยกของให้ถูกหลักสุขภาพ (0.5 คะแนน)

ข้อ 3

ข้อความข้างล่างสองข้อความนี้ถูกเข้ารหัสด้วยวิธีการของ shift cipher หรือ transposition cipher ให้ถอดรหัสข้อความทั้งสอง

SFWDWHZSFLAKTAYYWJLZSFSZAHHG (3 คะแนน)

AOATNHHILHEAISLALNPSENETPMRAP (3 คะแนน)

ข้อ 4

ฮ่องเต้ทะนงแต่งตั้งบารมีเป็นแม่ทัพใหญ่ดูแลรอบนอกกรุงปักกิ่ง ฮ่องเต้ทะนงสื่อสารกับแม่ทัพบารมีผ่านเครือข่ายอินเตอร์เน็ท broad band ความเร็วสูงและมีการเข้ารหัสข้อความด้วย AES-256 ใน Electronic Code Book Mode

จามิกงกงต้องการสอดแนมข้อความที่ฮ่องเต้ส่งไปหาแม่ทัพเพื่อส่งข้อมูลไปให้อาจารย์สุพัณณดา จามิกงกงไม่สามารถถอดรหัสลับได้ แต่หากข้อความที่ทะนงส่งไปหาบารมีในแต่ละวันนั้นมีเพียงข้อความใดในสองข้อความต่อไปนี้คือ “วันนี้ช่วยพาหนีออกไปเที่ยวด้วย” กับ “วันนี้งานยุ่ง ไม่ต้องมารับ” เมื่อจามิกงกงดักฟังข้อความที่ฮ่องเต้ทะนงส่งหาแม่ทัพบารมีทุกวัน และสังเกต

พฤติกรรมของทั้งสอง ในวันถัดๆ ไปเมื่อจามิกงกงดักจับข้อความที่ทะนงส่งออกมาได้อีก จามิกงกงจะทราบได้ไหมว่าในวันนั้นจะเกิดอะไรขึ้น (1 คะแนน)

- ถ้าฮ่องเต้เปลี่ยนการเข้ารหัสจาก Electronic Code Book Mode เป็น Cipher Block Chaining Mode แต่ยังใช้ IV ตัวเดิมในการ Encrypt ทุกครั้ง จะทำให้จามิกงกงทราบเหตุการณ์ล่วงหน้าจากข้อความที่เข้ารหัสได้หรือไม่ (1 คะแนน)

- ถ้าฮ่องเต้เปลี่ยนการเข้ารหัสจาก Electronic Code Book Mode เป็น Cipher Block Chaining Mode แต่ใช้ IV ที่ต่างกันในการ Encrypt ข้อความที่ต่างกัน โดยจะใช้ IV สองตัวสลับกันไปมาตามข้อความตั้งต้นทั้งสอง จะทำให้จามิกงกงทราบเหตุการณ์ล่วงหน้าจากข้อความที่เข้ารหัสได้หรือไม่ (1 คะแนน)

- ถ้าฮ่องเต้เปลี่ยนการเข้ารหัสจาก Electronic Code Book Mode เป็น Cipher Block Chaining Mode แต่ใช้ IV ที่ต่างกันในการ Encrypt แต่ละครั้ง โดยจะใช้ IV สองตัวสลับกันไปแบบสุ่มโดยไม่ขึ้นกับข้อความตั้งต้นทั้งสอง จะทำให้จามิกงกงทราบเหตุการณ์ล่วงหน้าจากข้อความที่เข้ารหัสได้หรือไม่ (1 คะแนน)

- ถ้าฮ่องเต้เปลี่ยนการเข้ารหัสจาก Electronic Code Book Mode เป็น Cipher Block Chaining Mode แต่ใช้ IV ที่ต่างกันในการ Encrypt แต่ละครั้ง โดยจะเลือก IV ตัวใหม่ทุกครั้งที่มีการ Encrypt จะทำให้จามิกงกงทราบเหตุการณ์ล่วงหน้าจากข้อความที่เข้ารหัสได้หรือไม่ (1 คะแนน)

- ถ้าฮ่องเต้เปลี่ยนการเข้ารหัสจาก AES-256 เป็น Stream Cipher ที่มี seed เหมือนเดิมทุกครั้ง จะทำให้จามิกงกงทราบเหตุการณ์ล่วงหน้าจากข้อความที่เข้ารหัสได้หรือไม่ (1 คะแนน)

ข้อ 5

ในกรุงปักกิ่งมีประชากรสามสิบล้านชีวิต โดยแบ่งเป็นมนุษย์ผู้ชายห้าล้านคน มนุษย์ผู้หญิงห้าล้านคน หมีแพนด้าชายสิบห้าล้านตัว และหมีแพนด้าหญิงห้าล้านตัว

- มนุษย์ผู้ชายครึ่งหนึ่งพอใจการปกครองของฮ่องเต้ทะนง อีกครึ่งหนึ่งไม่พอใจ
- มนุษย์ผู้หญิงหนึ่งในสามพอใจการปกครองของฮ่องเต้ทะนง อีกสองในสามไม่พอใจ
- หมีแพนด้าชายหนึ่งในสามพอใจการปกครองของฮ่องเต้ทะนง อีกสองในสามไม่พอใจ
- หมีแพนด้าหญิงหนึ่งในห้าพอใจการปกครองของฮ่องเต้ทะนง อีกสี่ในห้าไม่พอใจ
- มนุษย์ผู้ชาย 90% เห็นว่าฮองเฮาใจพรอ้วนเกินไป อีก 10% เห็นว่าไม่อ้วน
- มนุษย์ผู้หญิง 40% เห็นว่าฮองเฮาใจพรอ้วนเกินไป อีก 60% เห็นว่าไม่อ้วน

- หมีแพนด้าชายทั้งหมดเห็นว่าใจพรฮองเฮาอ้วนเกินไป ไม่มีหมีแพนด้าชายเห็นว่าฮองเฮาใจพรไม่อ้วน

- หมีแพนด้าหญิง 80% เห็นว่าใจพรฮองเฮาอ้วนเกินไป 20% เห็นว่าฮองเฮาใจพรไม่อ้วน

ให้เรียงลำดับการรั่วไหลของข้อมูลทั้งสี่แบบต่อไปนี้ จากรั่วไหลน้อยไปรั่วไหลมาก

แบบ 1 ข้อมูลความพอใจกับการทำงานของฮ่องเต้แล้ว -> ข้อมูลว่าเป็นมนุษย์หรือหมีแพนด้า

แบบ 2 ข้อมูลความพอใจกับการทำงานของฮ่องเต้แล้ว -> ข้อมูลว่าเป็นชายหรือหญิง

แบบ 3 ข้อมูลความเห็นว่าฮองเฮาอ้วนหรือไม่ -> ข้อมูลว่าเป็นมนุษย์หรือหมีแพนด้า

แบบ 4 ข้อมูลความเห็นว่าฮองเฮาอ้วนหรือไม่ -> ข้อมูลว่าเป็นชายหรือหญิง

(5 คะแนน)

ข้อ 6

ในกรุงปักกิ่งมีพ่อค้าสองคนชื่อโอ๊ตศรัญและโอ๊ตสุรศักดิ์ร่วมหุ้นกันเปิดร้านขายข้าวโอ๊ต ข้าวโอ๊ตที่ทั้งคู่ขายเป็นอาหารชั้นดีสำหรับหมีแพนด้าที่เลี้ยงไว้ในพระราชวังจึงต้องการการดูแลเป็นพิเศษ โดยข้าวโอ๊ตที่ยังไม่ส่งมอบให้กับพระราชวังจะถูกเก็บไว้ที่ธนาคารแห่งกรุงปักกิ่ง ธนาคารแห่งนี้มีตู้นิรภัยสำหรับเก็บข้าวโอ๊ตจำนวน 5 ตู้ แต่ละตู้มีรหัสเข้าใช้งานจำนวน 5 หลัก เป็นเลขฐาน 8 (แต่ละหลักมีเลขได้ 0 - 7) โดยรหัสแต่ละหลักของตู้เดียวกันจะไม่ซ้ำกัน โอ๊ตศรัญและโอ๊ตสุรศักดิ์จำรหัสพวกนี้ไม่ได้ จึงตกลงกันเข้ารหัสพวกนี้ทั้งหมดด้วยการบวกเลขฐานสิบ 4 3 7 9 5 เข้าไปในแต่ละหลัก เช่นตู้ 0 1 2 3 4 จะกลายเป็น 4 4 9 2 9

จามิกงกงต้องการขโมยข้าวโอ๊ตของโอ๊ตศรัญและโอ๊ตสุรศักดิ์ เพื่อส่งไปให้อาจารย์สุพัณณดารับประทาน จึงต้องหาวิธีถอดรหัสดังกล่าว หากรหัสที่บวกด้วย 4 3 7 9 5 เป็นรหัสข้างล่างนี้ ให้ถอดรหัสทั้งหมด

4 4 4 1 0

6 6 1 9 2

8 0 7 5 6

0 8 8 6 5

1 9 0 3 8

(5 คะแนน)

ข้อ 7

เมื่อพบว่าการแบ่งความลับในข้อ 6 ถูกจามิกงกงถอดรหัสได้โดยง่าย โอ๊ตศรัญและโอ๊ตสุรศักดิ์จึงเปลี่ยนวิธีการใหม่โดยทำการแบ่งความลับของรหัสตู้นิรภัยออกเป็นสองส่วน ส่วนหนึ่งให้โอ๊ตศรัญจดไว้ อีกส่วนให้โอ๊ตสุรศักดิ์จดได้ และต้องนำทั้งสองส่วนมาประกอบกันจึงจะสามารถเปิดตู้นิรภัยเพื่อนำข้าวโอ๊ตออกมาได้ การแบ่งความลับ 0 5 7 4 1 ออกเป็นสองส่วน โดยส่วนแรกคือ 1 3 4 7 1 ส่วนที่สองคืออะไร (ใช้คณิตศาสตร์เลขฐาน 8) (3 คะแนน)

ข้อ 8 (โจทย์ผิด)

อาจารย์สุพัณณดาได้หลบหนีออกจากประเทศไทยไปพำนักอยู่ที่ประเทศออสเตรเลียและอาจารย์ต้องการติดต่อกับจามิกงกงที่กรุงปักกิ่งโดยการเข้ารหัสข้อความด้วย RSA ให้แสดงการเข้ารหัสและถอดรหัสเลข 483 ด้วย RSA เมื่อ p และ q คือ 487 และ 491 และให้ e = 25 แสดงวิธีการหาค่า d ด้วย (8 คะแนน)