รายละเอียดของรายวิชา

ชื่อสถาบันอุดมศึกษา มหาวิทยาลัยราชภัฏอุบลราชธานี

วิทยาเขต/คณะ/ภาควิชา คณะเทคโนโลยีอุตสาหกรรม กลุ่มวิชาเทคโนโลยีคอมพิวเตอร์

หมวดที่ 1 ลักษณะและข้อมูลโดยทั่วไปของรายวิชา

1. รหัสและชื่อรายวิชา

7024403 วิทยาการเข้ารหัสลับยุคใหม่ (Modern Cryptography)

2. จำนวนหน่วยกิต

3 หน่วยกิต (2 – 2 – 5)

3. หลักสูตรและประเภทรายวิชา

วิทยาศาสตรบัณฑิต สาขาวิชาวิศวกรรมเครือข่ายคอมพิวเตอร์ รายวิชาเอกบังคับ

4. อาจารย์ผู้รับผิดชอบรายวิชา

ผู้ช่วยศาสตราจารย์บริบูรณ์ ดีกา อาจารย์ผู้สอน

5. ภาคการศึกษา / ชั้นปีที่เรียน

ภาคการศึกษาที่ 1 / ชั้นปีที่ 4

6. รายวิชาที่ต้องเรียนมาก่อน (Pre-requisite) (ถ้ามี)

ไม่มี

7. รายวิชาที่ต้องเรียนพร้อมกัน (Co-requisites) (ถ้ามี)

ไม่มี

8. สถานที่เรียน

คณะเทคโนโลยีอุตสาหกรรม มหาวิทยาลัยราชภัฏอุบลราชธานี

9. วันที่จัดทำหรือปรับปรุงรายละเอียดของรายวิชาครั้งล่าสุด

15 มิถุนายน 2566

หมวดที่ 2 จุดมุ่งหมายและวัตถุประสงค์

1. จุดมุ่งหมายของรายวิชา

เพื่อให้นักศึกษามีความรู้ ความเข้าใจเกี่ยวกับหลักการทั่วไปเกี่ยวกับวิทยาการรหัสลับ ด้วยการใช้โปรแกรมช่วยในการทดสอบขบวนการ รวมทั้งแนวทางวิธีการเข้ารหัสลับแบบต่าง ๆ การเปรียบเทียบข้อดี ข้อเสียของวิทยาการรหัสลับแบบต่าง ๆ และสามารถนำไปประยุกต์ใช้ในชีวิตประจำวันได้

2. วัตถุประสงค์ในการพัฒนา/ปรับปรุงรายวิชา

เพื่อให้นักศึกษาเข้าใจและอธิบายหลักการของวิทยาการรหัสลับ สามารถออกแบบขั้นตอนในการเข้าและถอดรหัสลับได้ เขียนโปรแกรมเพื่อทดสอบขั้นตอนของวิทยาการรหัสลับได้ และสามารถนำความรู้ที่ได้นำไปออกแบบและประยุกต์ใช้ในงานทางด้านความปลอดภัยได้

หมวดที่ 3 ส่วนประกอบของรายวิชา

1. คำอธิบายรายวิชา

แนวคิดและหลักการ การเข้ารหัสลับ การถอดรหัสลับ แบบจำลองเบื้องต้นของการเข้ารหัสลับ กรรมวิธีรหัสลับแบบดั้งเดิม กรรมวิธีการแทนที่ กรรมวิธีการเปลี่ยนตำแหน่ง กระบวนการรหัสแบบกุญแจสมมาตร มาตรฐานการเข้ารหัสลับข้อมูล มาตรฐานการเข้ารหัสลับขั้นสูง รูปแบบของข้อความรหัสลับ กระบวนการรหัสลับแบบกุญแจสาธารณะ กรรมวิธีรหัสลับแบบอาร์เอสเอ ลายเซ็นดิจิทัล ลายเซ็นต์สมมาตร ลายเซ็นต์สาธารณะ และเมสเซสไดเจสต์

2. จำนวนชั่วโมงที่ใช้ต่อภาคการศึกษา

จำนวนชั่วโมงบรรยายต่อสัปดาห์	30	ชั่วโมง
จำนวนชั่วโมงฝึกปฏิบัติการต่อสัปดาห์	30	ชั่วโมง
จำนวนชั่วโมงการศึกษาด้วยตนเอง	75	ชั่วโมง
จำนวนชั่วโมงที่สอนเสริมในรายวิชา	สอนเสริมตามความต้องการของนักศึกษาเป็นกลุ่มและเฉพาะราย	

3. จำนวนชั่วโมงต่อสัปดาห์ที่อาจารย์ให้คำปรึกษาและแนะนำทางวิชาการแก่นักศึกษาเป็นรายบุคคล

อาจารย์จัดเวลาให้คำปรึกษาเป็นรายบุคคล หรือ รายกลุ่มตามความต้องการ 1 ชั่วโมงต่อสัปดาห์ (เฉพาะรายที่ต้องการ) โดยการประกาศเวลาให้คำปรึกษาผ่านเว็บไซต์ของทางกลุ่มวิชา ฯ หรือตามตารางเวลาเข้าพบที่กำหนด

หมวดที่ 4 การพัฒนาการเรียนรู้ของนักศึกษา

มาตรฐานการเรียนรู้ และเนื้อหาหรือทักษะรายวิชา	วิธีการสอนที่จะใช้พัฒนาการเรียนรู้	วิธีการวัดและประเมินผล
1. คุณธรรม จริยธรรม - ตระหนักในคุณค่าและคุณธรรม จริยธรรม เสียสละ และซื่อสัตย์สุจริต - มีวินัย ตรงต่อเวลา และความรับผิดชอบต่อตนเองและสังคม - มีภาวะความเป็นผู้นำและผู้ตาม สามารถทำงานเป็นทีมและสามารถแก้ไขข้อขัดแย้งและลำดับความสำคัญ - เคารพสิทธิและรับฟังความคิดเห็นของผู้อื่น รวมทั้งเคารพในคุณค่าและศักดิ์ศรีของความเป็นมนุษย์ - เคารพกฎระเบียบและข้อบังคับต่าง ๆ ขององค์กรและสังคม - สามารถวิเคราะห์ผลกระทบจากการใช้คอมพิวเตอร์ต่อบุคคลองค์กรและสังคม - มีจรรยาบรรณทางวิชาการและวิชาชีพ	- บรรยายพร้อมยกตัวอย่างกรณีศึกษาที่เกี่ยวข้องกับวิทยาการรหัสลับ ตัวอย่างในการวิเคราะห์ สังเคราะห์ - อภิปรายกลุ่ม	- พฤติกรรมการเข้าเรียน และส่งงานที่ได้รับมอบหมายตามขอบเขตที่ให้และตรงเวลา - มีการอ้างอิงเอกสารที่ได้นำมาทำรายงาน อย่างถูกต้องและเหมาะสม - การออกแบบวิธีการของวิทยาการรหัสลับและผลที่ได้ - ประเมินผลการวิเคราะห์ - ประเมินผลการนำเสนอ
2. ความรู้ - มีความรู้และความเข้าใจเกี่ยวกับหลักการและทฤษฎีที่สำคัญในเนื้อหาที่ศึกษา - สามารถวิเคราะห์ปัญหา เข้าใจและอธิบายความต้องการของวิทยาการรหัสลับ รวมทั้งประยุกต์ความรู้ ทักษะ และการใช้เครื่องมือที่เหมาะสมกับการแก้ไขปัญหา - สามารถวิเคราะห์ ออกแบบ วิธีการวิทยาการรหัสลับให้ตรงตามข้อกำหนด	- บรรยาย ฝึกปฏิบัติในห้องปฏิบัติการ แก้ปัญหาโจทย์ของวิทยาการรหัสลับ - การทำงานกลุ่ม การนำเสนอวิธีการของวิทยาการรหัสลับแบบใหม่	- ทดสอบย่อย สอบกลางภาค สอบปลายภาค ด้วยข้อสอบข้อเขียน - นำเสนอสรุปการอ่านจากการค้นคว้าข้อมูลที่เกี่ยวข้อง - วิเคราะห์ และออกแบบวิธีการของวิทยาการรหัสลับอย่างน้อย 1 วิธีการ

มาตรฐานการเรียนรู้ และเนื้อหาหรือทักษะรายวิชา	วิธีการสอนที่จะใช้พัฒนาการเรียนรู้	วิธีการวัดและประเมินผล
- รู้ เข้าใจและสนใจพัฒนาความรู้ ความชำนาญในการออกแบบวิธีการวิทยาการรหัสลับ	- มอบหมายให้ค้นคว้าหาบทความ ข้อมูลที่เกี่ยวข้อง โดยนำมาสรุปและนำเสนอ	
3. ทักษะความสัมพันธ์ระหว่างบุคคลและความรับผิดชอบ - สามารถให้ความช่วยเหลือและอำนวยความสะดวกแก่การแก้ปัญหาสถานการณ์ต่าง ๆ ในกลุ่มทั้งในบทบาทของผู้นำ หรือในบทบาทของผู้ร่วมทีมทำงาน - มีความรับผิดชอบในการกระทำของตนเองและรับผิดชอบงานในกลุ่ม - มีความรับผิดชอบการพัฒนาการเรียนรู้ทั้งของตนเองและทางวิชาชีพอย่างต่อเนื่อง	- จัดกิจกรรมกลุ่มในการวิเคราะห์โจทย์กรณีศึกษา และการนำเสนอวิธีแก้ปัญหา - การปฏิบัติในห้องปฏิบัติการ - มอบหมายงานรายกลุ่ม และรายบุคคล - การนำเสนอโครงงานย่อย	- ประเมินตนเอง และเพื่อนด้วยแบบฟอร์มที่กำหนด - รายงานที่นำเสนอพฤติกรรมการทำงานเป็นทีม - รายงานการศึกษาโครงงานย่อย
4. ทักษะการวิเคราะห์เชิงตัวเลข การสื่อสาร และการใช้เทคโนโลยีสารสนเทศ - มีความคิดอย่างมีวิจารณญาณและอย่างเป็นระบบ - มีความสามารถในการสืบค้น ตีความ และประเมินสารสนเทศเพื่อใช้ในการแก้ปัญหาอย่างสร้างสรรค์ - สามารถรวบรวม ศึกษา วิเคราะห์และสรุปประเด็นปัญหาและความต้องการ - สามารถประยุกต์ความรู้และทักษะกับการแก้ไขปัญหาทางคอมพิวเตอร์ได้อย่างเหมาะสม	- มอบหมายงานให้ศึกษาค้นคว้าด้วยตนเอง จากเว็บไซต์ สื่อการสอน e-Learning และทำรายงาน โดยเน้นแหล่งที่มาของข้อมูลที่น่าเชื่อถือ - นำเสนอโดยใช้รูปแบบและเทคโนโลยีที่เหมาะสม	- การจัดทำรายงาน และนำเสนอด้วยสื่อเทคโนโลยี - การมีส่วนร่วมในการอภิปรายและวิธีการอภิปราย

หมวดที่ 5 แผนการสอนและการประเมินผล

1. แผนการสอน

สัปดาห์ที่	หัวข้อ/รายละเอียด	จำนวน (ชม.)	กิจกรรมการเรียนการสอน สื่อที่ใช้	ผู้สอน
1	Introduction Recommendations for Cryptographic Algorithms	4	- บรรยาย ยกตัวอย่าง ฝึกทำโจทย์ มอบหมายแบบฝึกหัด - เครื่องคอมพิวเตอร์โปรเจคเตอร์	ผศ. บริบูรณ์
2	Introduction to Cryptography	4	- บรรยาย ยกตัวอย่าง ฝึกทำโจทย์ มอบหมายแบบฝึกหัด - เครื่องคอมพิวเตอร์โปรเจคเตอร์	ผศ. บริบูรณ์
3	Next Generation Encryption NGE Background Information Categories of Cryptographic Algorithms Symmetric Key • DES	4	- บรรยาย ยกตัวอย่างโปรแกรม ทดลองเขียนและใช้งานโปรแกรม - เครื่องคอมพิวเตอร์โปรเจคเตอร์	ผศ. บริบูรณ์
4	Categories of Cryptographic Algorithms Symmetric Key • AES	4	- บรรยาย ยกตัวอย่างโปรแกรม ทดลองเขียนและใช้งานโปรแกรม - เครื่องคอมพิวเตอร์โปรเจคเตอร์	ผศ. บริบูรณ์
5	Categories of Cryptographic Algorithms Public Key • RSA	4	- บรรยาย ยกตัวอย่างโปรแกรม ทดลองเขียนและใช้งานโปรแกรม - เครื่องคอมพิวเตอร์โปรเจคเตอร์	ผศ. บริบูรณ์
6	Categories of Cryptographic Algorithms Public Key • Diffie–Hellman key exchange	4	- บรรยาย ยกตัวอย่างโปรแกรม ทดลองเขียนและใช้งานโปรแกรม - เครื่องคอมพิวเตอร์โปรเจคเตอร์	ผศ. บริบูรณ์
7	Categories of Cryptographic Algorithms Public Key • Digital Signature Algorithm (DSA)	4	- บรรยาย ยกตัวอย่างโปรแกรม ทดลองเขียนและใช้งานโปรแกรม	ผศ. บริบูรณ์

สัปดาห์ที่	หัวข้อ/รายละเอียด	จำนวน (ชม.)	กิจกรรมการเรียนการสอน สื่อที่ใช้	ผู้สอน
			- เครื่องคอมพิวเตอร์โปรเจคเตอร์	
8	สอบกลางภาคเรียน	2 ชม.		
9	Categories of Cryptographic Algorithms Elliptic Curve and Elliptic-curve Diffie–Hellman ● How to Compute with Elliptic Curves ● Building a Discrete Logarithm Problem with Elliptic Curves ● Diffie–Hellman Key Exchange with Elliptic Curves ● Security ● Implementation using software and hardware	4	- บรรยาย ยกตัวอย่างโปรแกรม ทดลองเขียนและใช้งานโปรแกรม - เครื่องคอมพิวเตอร์โปรเจคเตอร์	ผศ. บริบูรณ์
10	Categories of Cryptographic Algorithms Hash and Secure Hash Algorithms ● Motivation: Signing Long Messages ● Security Requirements of Hash Functions ● Overview of Hash Algorithms ● The Secure Hash Algorithm SHA-1	4	- บรรยาย ยกตัวอย่างโปรแกรม ทดลองเขียนและใช้งานโปรแกรม - เครื่องคอมพิวเตอร์โปรเจคเตอร์	ผศ. บริบูรณ์
11	Security Levels Cryptographic Algorithm Configuration Guidelines	4	- บรรยาย ยกตัวอย่างโปรแกรม ทดลองเขียนและใช้งานโปรแกรม - เครื่องคอมพิวเตอร์โปรเจคเตอร์	ผศ. บริบูรณ์
12	IPsec VPN with Encapsulating Security Payload	4	- บรรยาย ยกตัวอย่างโปรแกรม ทดลองเขียนและใช้งานโปรแกรม - เครื่องคอมพิวเตอร์โปรเจคเตอร์	ผศ. บริบูรณ์

สัปดาห์ที่	หัวข้อ/รายละเอียด	จำนวน (ชม.)	กิจกรรมการเรียนการสอน สื่อที่ใช้	ผู้สอน
13	Internet Key Exchange in VPN Technologies • Avoid IKE Groups 1, 2, and 5. • Use IKE Group 15 or 16 and employ 3072-bit and 4096-bit DH, respectively. • When possible, use IKE Group 19 or 20. They are the 256-bit and 384-bit ECDH groups, respectively. • Use AES for encryption.	4	- บรรยาย ยกตัวอย่าง โปรแกรม ทดลองเขียนและใช้งานโปรแกรม - เครื่องคอมพิวเตอร์โปรเจคเตอร์	ผศ. บริบูรณ์
14	Transport Layer Security and Cipher Suites	4	- บรรยาย ยกตัวอย่าง โปรแกรม ทดลองเขียนและใช้งานโปรแกรม - เครื่องคอมพิวเตอร์โปรเจคเตอร์	ผศ. บริบูรณ์
15	Other Popular Symmetric Ciphers	4	- สรุปและอภิปรายโครงงานย่อยที่นำเสนอ - เครื่องคอมพิวเตอร์โปรเจคเตอร์	ผศ. บริบูรณ์
16	สอบปลายภาค	2 ชม.		

2. แผนการประเมินผลการเรียนรู้

ผลการเรียนรู้ (Learning Outcome)	วิธีการประเมิน	กำหนดเวลาการประเมิน (สัปดาห์ที่)	สัดส่วนของการประเมินผล
1.1, 1.3, 1.5, 1.7, 2.1-2.5, 2.7-2.8, 3.1-3.4, 5.1	สอบกลางภาค นำเสนอโครงงานย่อย สอบปลายภาค	8 15 16	20% 5% 30%
1.1, 1.3, 1.5, 1.7, 2.1-2.5, 2.7-2.8, 3.1-3.4, 5.1	การเข้าห้องเรียนและกิจกรรมพิเศษ	ตลอดภาคการศึกษา	10%

1.1, 1.3, 1.5, 1.7, 2.1-2.5, 2.7-2.8, 3.1-3.4, 4.1,4.6, 5.1-5.4	การส่งงานตามที่มอบหมายรายบุคคลและรายกลุ่ม	ตลอดภาคการศึกษา	35%

หมวดที่ 6 ทรัพยากรประกอบการเรียนการสอน

1. เอกสารและตำราหลัก

Christof Paar and Jan Pelzl. 2010. **Understanding Cryptography**. Springer Heidelberg Dordrecht London New York.

2. เอกสารและข้อมูลสำคัญ

- วรเศรษฐ สุวรรณิก. 2553. **วิทยาการรหัสลับ Cryptography.** กรุงเทพ ฯ : สำนักพิมพ์วรรณิก
- ลัญจกร วุฒิสิทธิกุลกิจและคณะ ฯ. 2548. **วิทยาการรหัสลับเบื้องต้น.** กรุงเทพ ฯ : สำนักพิมพ์แห่งจุฬาลงกรณ์มหาวิทยาลัย.

3. เอกสารและข้อมูลแนะนำ

- Rolf Oppliger. 2005. **Contemporary Cryptography.** ARTECH HOUSE, INC. BOSTON: LONDON.
- Hans Delfs and Helmut Knebl. 2007. **Introduction to Cryptography Principles and Applications**. 2nd ed. Springer Heidelberg Dordrecht London New York.
- David Bishop. 2003. **INTRODUCTION TO CRYPTOGRAPHY WITH JAVA™ APPLETS**. Jones and Bartlett Publishers, Inc.
- Wade Trappe and Lawrence C. Washington. 2006. **Introduction to Cryptography with Coding Theory.** 2nd ed. Prentice-Hall.

หมวดที่ 7 การประเมินรายวิชาและกระบวนการปรับปรุง

1. กลยุทธ์การประเมินประสิทธิผลของรายวิชาโดยนักศึกษา

การประเมินประสิทธิผลในรายวิชานี้ ที่จัดทำโดยนักศึกษา ได้จัดกิจกรรมในการนำแนวคิดและความเห็นจากนักศึกษาได้ดังนี้

- การสนทนากลุ่มระหว่างผู้สอนและผู้เรียน

- การสังเกตการณ์จากพฤติกรรมของผู้เรียน
- แบบประเมินผู้สอน และแบบประเมินรายวิชา
- ข้อเสนอแนะผ่านเวบบอร์ด ที่อาจารย์ผู้สอนได้จัดทำเป็นช่องทางการสื่อสารกับนักศึกษา

2. กลยุทธ์การประเมินการสอน

- ผลการสอบ
- การทวนสอบผลประเมินการเรียนรู้
- ผลที่ได้จากการทำโครงงานย่อย

3. การปรับปรุงการสอน

หลังจากผลการประเมินการสอนในข้อ 2 จึงมีการปรับปรุงการสอน โดยการจัดกิจกรรมในการระดมสมองและหาข้อมูลเพิ่มเติมในการปรับปรุงการสอน ดังนี้

- สัมมนาการจัดการเรียนการสอน
- การวิจัยในและนอกชั้นเรียน

4. การทวนสอบมาตรฐานผลสัมฤทธิ์รายวิชาของนักศึกษา

ในระหว่างกระบวนการสอนรายวิชา มีการทวนสอบผลสัมฤทธิ์ในรายหัวข้อ รวมถึงพิจารณาจากผลที่ได้จากการทำโครงงานย่อย และหลังการออกผลการเรียนรายวิชา มีการทวนสอบผลสัมฤทธิ์โดยรวมในวิชาดังนี้

- การทวนสอบการให้คะแนนจากการสุ่มตรวจผลงานของนักศึกษาโดยอาจารย์อื่น หรือผู้ทรงคุณวุฒิที่ไม่ใช่อาจารย์ประจำหลักสูตร
- มีการตั้งคณะกรรมการในกลุ่มวิชา ตรวจสอบผลการประเมินการเรียนรู้ของนักศึกษา โดยตรวจสอบข้อสอบ รายงาน วิธีการให้คะแนนสอบ และการให้คะแนนพฤติกรรม

5. การดำเนินการทบทวนและการวางแผนปรับปรุงประสิทธิผลของรายวิชา

จากผลการประเมิน และทวนสอบผลสัมฤทธิ์ประสิทธิผลรายวิชา ได้มีการวางแผนการปรับปรุงการสอนและรายละเอียดวิชา เพื่อให้เกิดคุณภาพมากขึ้น ดังนี้

- ปรับปรุงรายวิชาทุก 3 ปี หรือ ตามข้อเสนอแนะและผลการทวนสอบมาตรฐานผลสัมฤทธิ์ตามข้อ 4
- นำงานวิจัยในด้านวิทยาการรหัสลับที่ได้มีการประยุกต์ใช้ เพื่อให้นักศึกษามีมุมมองในเรื่องการประยุกต์ความรู้นี้กับปัญหาที่มาจากการใช้งานหรือแหล่งข้อมูลต่าง ๆ ที่เกี่ยวข้องกับในรายวิชา