รายละเอียดของรายวิชา

ชื่อสถาบันอุดมศึกษา มหาวิทยาลัยราชภัฏอุบลราชธานี

วิทยาเขต/คณะ/ภาควิชา คณะเทคโนโลยีอุตสาหกรรม กลุ่มวิชาเทคโนโลยีคอมพิวเตอร์

หมวดที่ 1 ลักษณะและข้อมูลโดยทั่วไปของรายวิชา

1. รหัสและชื่อรายวิชา

5694404 วิทยาการเข้ารหัสลับ

Cryptography

2. จำนวนหน่วยกิต

3 หน่วยกิต (2 – 2 – 5)

3. หลักสูตรและประเภทรายวิชา

วิทยาศาสตรบัณฑิต สาขาวิชาเทคโนโลยีคอมพิวเตอร์ รายวิชาเอกบังคับ

4. อาจารย์ผู้รับผิดชอบรายวิชา

อาจารย์บริบูรณ์ 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 ตุลาคม 2562

หมวดที่ 2 จุดมุ่งหมายและวัตถุประสงค์

1. จุดมุ่งหมายของรายวิชา

เพื่อให้นักศึกษามีความรู้ ความเข้าใจเกี่ยวกับหลักการทั่วไปเกี่ยวกับวิทยาการรหัสลับ ด้วยการใช้โปรแกรมช่วยในการทดสอบขบวนการ รวมทั้งแนวทางวิธีการเข้ารหัสลับแบบต่าง ๆ การเปรียบเทียบข้อดี ข้อเสียของวิทยาการรหัสลับแบบต่าง ๆ และสามารถนำไประยุกต์ใช้ในชีวิตประจำวันได้

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 การใช้งานโปรแกรม ตัวอย่างในการวิเคราะห์ สังเคราะห์ - อภิปรายกลุ่ม - กำหนดให้นักศึกษาจัดทำโครงงานย่อยพร้อมจัดทำรายงานประกอบ - ตั้งปัญหาและออกแบบวิธีการของวิทยาการรหัสลับแบบใหม่	- พฤติกรรมการเข้าเรียน และส่งงานที่ได้รับมอบหมายตามขอบเขตที่ให้และตรงเวลา - มีการอ้างอิงเอกสารที่ได้นำมาทำรายงาน อย่างถูกต้องและเหมาะสม - การออกแบบวิธีการของวิทยาการรหัสลับและผลที่ได้ - ประเมินผลการวิเคราะห์โครงงานย่อย - ประเมินผลการนำเสนอรายงานในการจัดทำโครงการย่อยที่มอบหมาย

มาตรฐานการเรียนรู้ และเนื้อหาหรือทักษะรายวิชา	วิธีการสอนที่จะใช้พัฒนาการเรียนรู้	วิธีการวัดและประเมินผล
2. ความรู้ - มีความรู้และความเข้าใจเกี่ยวกับหลักการและทฤษฎีที่สำคัญในเนื้อหาที่ศึกษา - สามารถวิเคราะห์ปัญหา เข้าใจและอธิบายความต้องการของวิทยาการรหัสลับ รวมทั้งประยุกต์ความรู้ ทักษะ และการใช้เครื่องมือที่เหมาะสมกับการแก้ไขปัญหา - สามารถวิเคราะห์ ออกแบบวิธีการวิทยาการรหัสลับให้ตรงตามข้อกำหนด - รู้ เข้าใจและสนใจพัฒนาความรู้ความชำนาญในการออกแบบวิธีการวิทยาการรหัสลับ	- บรรยาย ฝึกปฏิบัติในห้องปฏิบัติการ แก้ปัญหาโจทย์ของวิทยาการรหัสลับ - การทำงานกลุ่ม การนำเสนอวิธีการของวิทยาการรหัสลับแบบใหม่ - มอบหมายให้ค้นคว้าหาบทความข้อมูลที่เกี่ยวข้อง โดยนำมาสรุปและนำเสนอ	- ทดสอบย่อย สอบกลางภาค สอบปลายภาค ด้วยข้อสอบข้อเขียน - นำเสนอสรุปการอ่านจากการค้นคว้าข้อมูลที่เกี่ยวข้อง - วิเคราะห์ และออกแบบวิธีการของวิทยาการรหัสลับอย่างน้อย 1 วิธีการ
3. ทักษะทางปัญญา - คิดอย่างมีวิจารณญาณและอย่างเป็นระบบ - สามารถรวบรวม ศึกษา วิเคราะห์ และสรุปประเด็นปัญหาและความต้องการ - สามารถออกแบบวงจรตามความต้องการจากปัญหาที่วิเคราะห์ได้	- วิเคราะห์จากกรณีศึกษาหรือจากปัญหาที่เกิดขึ้นจริง	- ทดสอบย่อย - สอบกลางภาคและปลายภาค โดยเน้นข้อสอบที่มีการวิเคราะห์โจทย์ในด้านการออกแบบวิธีการวิทยาการรหัสลับจนถึงระดับที่สูง - ทดสอบในเชิงปฏิบัติในการออกแบบวิธีการวิทยาการรหัสลับ

มาตรฐานการเรียนรู้ และเนื้อหาหรือทักษะรายวิชา	**วิธีการสอนที่จะใช้พัฒนาการเรียนรู้**	**วิธีการวัดและประเมินผล**
4. ทักษะความสัมพันธ์ระหว่างบุคคลและความรับผิดชอบ - สามารถให้ความช่วยเหลือและอำนวยความสะดวกแก่การแก้ปัญหาสถานการณ์ต่าง ๆในกลุ่มทั้งในบทบาทของผู้นำ หรือในบทบาทของผู้ร่วมทีมทำงาน - มีความรับผิดชอบในการกระทำของตนเองและรับผิดชอบงานในกลุ่ม - มีความรับผิดชอบการพัฒนาการเรียนรู้ทั้งของตนเองและทางวิชาชีพอย่างต่อเนื่อง	- จัดกิจกรรมกลุ่มในการวิเคราะห์โจทย์กรณีศึกษา และการนำเสนอวิธีแก้ปัญหา - การปฏิบัติในห้องปฏิบัติการ - มอบหมายงานรายกลุ่ม และรายบุคคล - การนำเสนอโครงงานย่อย	- ประเมินตนเอง และเพื่อน ด้วยแบบฟอร์มที่กำหนด - รายงานที่นำเสนอ พฤติกรรมการทำงานเป็นทีม - รายงานการศึกษาโครงงานย่อย
5. ทักษะการวิเคราะห์เชิงตัวเลข การสื่อสาร และการใช้เทคโนโลยีสารสนเทศ - มีความคิดอย่างมีวิจารณญาณและอย่างเป็นระบบ - มีความสามารถในการสืบค้น ตีความ และประเมินสารสนเทศเพื่อใช้ในการแก้ปัญหาอย่างสร้างสรรค์ - สามารถรวบรวม ศึกษาวิเคราะห์และสรุปประเด็นปัญหาและความต้องการ - สามารถประยุกต์ความรู้และ	- มอบหมายงานให้ศึกษาค้นคว้าด้วยตนเอง จากเว็บไซต์ สื่อการสอน e-Learning และทำรายงาน โดยเน้นแหล่งที่มาของข้อมูลที่น่าเชื่อถือ - นำเสนอโดยใช้รูปแบบและเทคโนโลยีที่เหมาะสม	- การจัดทำรายงาน และนำเสนอด้วยสื่อเทคโนโลยี - การมีส่วนร่วมในการอภิปรายและวิธีการอภิปราย

ทักษะกับการแก้ไขปัญหาทางคอมพิวเตอร์ได้อย่างเหมาะสม		

หมวดที่ 5 แผนการสอนและการประเมินผล

1. แผนการสอน

สัปดาห์ที่	หัวข้อ/รายละเอียด	จำนวน (ชม.)	กิจกรรมการเรียนการสอน สื่อที่ใช้	ผู้สอน
1	Introduction to Cryptography - Overview of Cryptology - Symmetric Cryptography - Cryptanalysis - Modular Arithmetic and More Historical Ciphers	4	- บรรยาย ยกตัวอย่าง ฝึกทำโจทย์ มอบหมายแบบฝึกหัด - เครื่องคอมพิวเตอร์โปรเจคเตอร์	บริบูรณ์
2	Stream Ciphers - Introduction - Random Numbers and an Unbreakable Stream Cipher - Shift Register-Based Stream Ciphers	4	- บรรยาย ยกตัวอย่าง ฝึกทำโจทย์ มอบหมายแบบฝึกหัด - เครื่องคอมพิวเตอร์โปรเจคเตอร์	บริบูรณ์
3	The Data Encryption Standard (DES) - Introduction to DES - Overview of the DES Algorithm - Internal Structure of DES - Decryption - Security of DES - Implementation in Software and Hardware - DES Alternatives	4	- บรรยาย ยกตัวอย่างโปรแกรม ทดลองเขียนและใช้งานโปรแกรม - เครื่องคอมพิวเตอร์โปรเจคเตอร์	บริบูรณ์
4	The Advanced Encryption Standard (AES) - Introduction	4	- บรรยาย ยกตัวอย่างโปรแกรม ทดลองเขียนและใช้งานโปรแกรม	บริบูรณ์

สัปดาห์ที่	หัวข้อ/รายละเอียด	จำนวน (ชม.)	กิจกรรมการเรียนการสอน สื่อที่ใช้	ผู้สอน
	- Overview of the AES Algorithm - Some Mathematics: A Brief Introduction to Galois Fields - Internal Structure of AES - Decryption - Implementation in Software and Hardware		- เครื่องคอมพิวเตอร์โปรเจคเตอร์	
5	More About Block Ciphers - Encryption with Block Ciphers: Modes of Operation - Exhaustive Key Search Revisited - Increasing the Security of Block Ciphers	4	- บรรยาย ยกตัวอย่างโปรแกรม ทดลองเขียนและใช้งานโปรแกรม - เครื่องคอมพิวเตอร์โปรเจคเตอร์	บริบูรณ์
6	Introduction to Public-Key Cryptography - Symmetric vs. Asymmetric Cryptography - Practical Aspects of Public-Key Cryptography - Essential Number Theory for Public-Key Algorithms	4	- บรรยาย ยกตัวอย่างโปรแกรม ทดลองเขียนและใช้งานโปรแกรม - เครื่องคอมพิวเตอร์โปรเจคเตอร์	บริบูรณ์
7	The RSA Cryptosystem - Introduction - Encryption and Decryption - Key Generation and Proof of Correctness - Encryption and Decryption: Fast Exponentiation - Speed-up Techniques for RSA - Finding Large Primes	4	- บรรยาย ยกตัวอย่างโปรแกรม ทดลองเขียนและใช้งานโปรแกรม - เครื่องคอมพิวเตอร์โปรเจคเตอร์	บริบูรณ์

สัปดาห์ที่	หัวข้อ/รายละเอียด	จำนวน (ชม.)	กิจกรรมการเรียนการสอน สื่อที่ใช้	ผู้สอน
	- RSA in Practice: Padding - Attacks - Implementation in Software and Hardware			
8	สอบกลางภาคเรียน	2 ชม.		
9	Public-Key Cryptosystems Based on the Discrete Logarithm Problem - Diffie–Hellman Key Exchange - Some Algebra - The Discrete Logarithm Problem - Security of the Diffie–Hellman Key Exchange - The Elgamal Encryption Scheme	4	- บรรยาย ยกตัวอย่าง โปรแกรม ทดลองเขียนและใช้งานโปรแกรม - เครื่องคอมพิวเตอร์โปรเจคเตอร์	บริบูรณ์
10	Elliptic Curve Cryptography - How to Compute with Elliptic Curves - Building a Discrete Logarithm Problem with Elliptic Curves - Diffie–Hellman Key Exchange with Elliptic Curves - Security - Implementation in Software and Hardware	4	- บรรยาย ยกตัวอย่าง โปรแกรม ทดลองเขียนและใช้งานโปรแกรม - เครื่องคอมพิวเตอร์โปรเจคเตอร์	บริบูรณ์
11	Digital Signatures - Introduction - The RSA Signature Scheme - The Elgamal Digital Signature Scheme - The Digital Signature Algorithm (DSA) - The Elliptic Curve Digital Signature Algorithm (ECDSA)	4	- บรรยาย ยกตัวอย่าง โปรแกรม ทดลองเขียนและใช้งานโปรแกรม - เครื่องคอมพิวเตอร์โปรเจคเตอร์	บริบูรณ์

สัปดาห์ที่	หัวข้อ/รายละเอียด	จำนวน (ชม.)	กิจกรรมการเรียนการสอน สื่อที่ใช้	ผู้สอน
12	Hash Functions - Motivation: Signing Long Messages - Security Requirements of Hash Functions - Overview of Hash Algorithms - The Secure Hash Algorithm SHA-1	4	- บรรยาย ยกตัวอย่างโปรแกรม ทดลองเขียนและใช้งานโปรแกรม - เครื่องคอมพิวเตอร์โปรเจคเตอร์	บริบูรณ์
13	Message Authentication Codes (MACs) - Principles of Message Authentication Codes - MACs from Hash Functions: HMAC - MACs from Block Ciphers: CBC-MAC - Galois Counter Message Authentication Code (GMAC)	4	- บรรยาย ยกตัวอย่างโปรแกรม ทดลองเขียนและใช้งานโปรแกรม - เครื่องคอมพิวเตอร์โปรเจคเตอร์	บริบูรณ์
14	Key Establishment - Introduction - Key Establishment Using Symmetric-Key Techniques - Key Establishment Using Asymmetric Techniques	4	- บรรยาย ยกตัวอย่างโปรแกรม ทดลองเขียนและใช้งานโปรแกรม - เครื่องคอมพิวเตอร์โปรเจคเตอร์	บริบูรณ์
15	Presentation Project	4	- สรุปและอภิปรายโครงงานย่อยที่นำเสนอ - เครื่องคอมพิวเตอร์โปรเจคเตอร์	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% 15% 30%
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