
วิชา 344-484 วิทยาการเข้ารหัสลับ (Introduction to Cryptography)

วัตถุประสงค์ 1. เพื่อให้เรียนรู้และเข้าใจหลักการของวิทยาการเข้ารหัสลับ
2. เข้าใจถึงประโยชน์ของวิทยาการเข้ารหัสลับซึ่งถูกนำมาใช้อย่างแพร่หลายในเครือข่ายอินเตอร์เน็ตเพื่อความปลอดภัยของข้อมูลและสารสนเทศต่างๆ
3. สามารถนำความรู้ที่ได้รับไปประยุกต์ใช้ต่อไป

เนื้อหาวิชา หลักการความปลอดภัยในคอมพิวเตอร์และความจำเป็น ภัยที่เกิดกับคอมพิวเตอร์ ความหมายของวิทยาการเข้ารหัสลับ การประยุกต์ใช้วิทยาการเข้ารหัสลับในปัจจุบัน ระบบรหัสลับ การวิเคราะห์รหัสลับและ การโจมตีแบบตะลุย เทคนิคการเข้ารหัสลับ วิทยาการรหัสลับแบบสมมาตร เช่น มาตรฐานรหัสลับ DES วิทยาการรหัสลับแบบไม่สมมาตร เช่น มาตรฐานรหัสลับ RSA ลายมือชื่อดิจิตอล รหัสลับกุญแจสาธารณะและ ฟังก์ชันแฮช

วิธีการเรียนการสอน บรรยาย 3 ชั่วโมงต่อสัปดาห์
ฝึกปฏิบัติการด้วยตนเอง

การวัดผล
- การบ้าน 20%
- สอบกลางภาคการศึกษา 40%
- สอบปลายภาคการศึกษา 40%

วิธีการตัดเกรด อิงเกณฑ์และกลุ่ม

ระดับขั้น	A	B+	B	C+	C	D+	D	E
ช่วงคะแนน	85-100	80-84	75-79	65-74	55-64	48-54	41-47	0-40

อาจารย์ผู้สอน ผู้ช่วยศาสตราจารย์ ดร. ลัดดา ปรีชาวีรกุล **ห้องทำงาน** CS303
E-mail: ladda.p@psu.ac.th **โทรศัพท์** 074-288581

เอกสารประกอบการสอน

1. ลัดดา ปรีชาวีรกุล. วิทยาการเข้ารหัสลับเบื้องต้น. โรงพิมพ์ดิจิตอล คณะวิทยาศาสตร์ มหาวิทยาลัยสงขลานครินทร์ 2552.
2. ลัญฉกร วุฒิสิทธิกุลกิจ ธงชัย โรจน์กังสดาล วรากร ศรีเชวงทรัพย์ และนภดล พรมภักษร. วิทยาการรหัสลับเบื้องต้น . สำนักพิมพ์จุฬาลงกรณ์ มหาวิทยาลัย 2548.
3. Kahate, A . Cryptography and Network Security. McGraw-Hill Publishing Company Limited, 2003.
4. Stallings, W. Cryptography and Network Security: Principles and Practice. 2 nd Ed. Prentice Hall International, Inc., 2003.