

วิทยาการรหัสลับ และ การทำลายน้ำดิจิทัล

Cryptography & Digital Watermarking





วิทยาการรหัสลับและ การทำลายน้ำดิจิทัล

Cryptography & Digital Watermarking



รศ. ดร. อัครรัตน์ อมรรักษา

ภาควิชาวิศวกรรมคอมพิวเตอร์

คณะวิศวกรรมศาสตร์

มหาวิทยาลัยเทคโนโลยีพระจอมเกล้าธนบุรี

สารบัญ

คำนำ	iv	บทที่ 3 อัลกอริทึมกุญแจสมมาตร	
บทที่ 1 วิทยาการรหัสลับ		3.1 บทนำ	85
1.1 บทนำ	1	3.2 ทฤษฎีจำนวน	86
1.2 ศัพท์เฉพาะด้านวิทยาการรหัสลับ	4	3.2.1 เลขคณิตมอดุลาร์	86
1.3 พื้นฐานอัลกอริทึมด้านวิทยาการรหัสลับ	6	3.2.2 ตัวหารร่วมมาก	89
1.4 ข้อกำหนดทั่วไปของระบบการเข้ารหัสลับ	9	3.2.3 ตัวผกผันทวีคูณในมอดุโล k	90
1.5 ความแข็งแกร่งของระบบและการวิเคราะห์รหัสลับ	11	3.2.4 ทฤษฎีเศษเหลือของชาวจีน	93
1.6 การประเมินระบบความปลอดภัย	14	3.3 ความซับซ้อนในการแก้ปัญหาเชิงคณิตศาสตร์	95
1.7 โพรโทคอลด้านวิทยาการรหัสลับ	16	3.4 ข้อตกลงกุญแจของ Diffie-Hellman	96
1.7.1 การโจมตีโพรโทคอล	18	3.5 อัลกอริทึม El Gamal	100
1.7.2 การโจมตีแบบคนที่อยู่ตรงกลาง	23	3.6 อัลกอริทึม RSA	101
1.8 บทสรุป	26	3.7 ระบบการเข้ารหัสลับเส้นโค้งเชิงวงรี	106
1.9 คำตามท้ายบท	27	3.8 บทสรุป	108
		3.9 คำตามท้ายบท	109
บทที่ 2 อัลกอริทึมกุญแจสมมาตร		บทที่ 4 ฟังก์ชันแฮชและลายเซ็นดิจิทัล	
2.1 บทนำ	28	4.1 บทนำ	110
2.2 ตัวแปลงรหัสลับแบบบล็อกดั้งเดิม	28	4.2 ฟังก์ชันแฮชทางเดียว	110
2.2.1 ตัวแปลงรหัสลับแบบแทนที่	29	4.2.1 อัลกอริทึม MD5	113
2.2.2 ตัวแปลงรหัสลับแบบสลับตำแหน่ง	36	4.2.2 อัลกอริทึม SHA-1	118
2.3 ตัวแปลงรหัสลับแบบบล็อกยุคใหม่	41	4.2.3 การโจมตีแบบวันเกิด	120
2.3.1 ตัวแปลงรหัสลับผลคูณ	41	4.3 รหัสพิสูจน์ตัวตนจริงข้อความ	123
2.3.2 ตัวแปลงรหัสลับไฟร์เทล	43	4.3.1 อัลกอริทึม HMAC	125
2.3.3 ตัวแปลงรหัสลับ DES	46	4.4 ลายเซ็นดิจิทัล	127
2.3.4 ตัวแปลงรหัสลับ DESX	54	4.4.1 การนำอัลกอริทึม RSA มาใช้ ในการสร้างลายเซ็นดิจิทัล	129
2.3.5 ตัวแปลงรหัสลับ IDEA	54	4.4.2 การนำอัลกอริทึม El Gamal มาใช้ในการสร้างลายเซ็นดิจิทัล	131
2.3.6 ตัวแปลงรหัสลับ AES	59	4.4.3 การสร้างลายเซ็นดิจิทัลพร้อม ตราเวลา	133
2.4 ตัวแปลงรหัสลับแบบสตรีม	71	4.5 บทสรุป	134
2.4.1 เรจิสเตอร์แบบเลื่อนป้อนกลับ เชิงเส้น	73	4.6 คำตามท้ายบท	135
2.4.2 ตัวแปลงรหัสลับแบบสตรีมโดยใช้ LFSR	78		
2.4.3 ตัวแปลงรหัสลับ One-time Pad	80		
2.5 บทสรุป	83		
2.6 คำตามท้ายบท	84		

บทที่ 5 เทคนิคทางวิทยาการรหัสลับ			
5.1 บทนำ	136	5.7 การกระจายกุญแจ	164
5.2 การเลือกใช้ตัวแปรรหัสลับ	136	5.7.1 ระบบการกระจายกุญแจสมมาตร	164
5.2.1 การเลือกใช้ตัวแปรรหัสลับแบบ สตรีมและแบบบล็อก	138	5.7.2 ระบบการกระจายกุญแจอสมมาตร	167
5.2.2 การเลือกใช้ตัวแปรรหัสลับแบบ ซอฟต์แวร์และฮาร์ดแวร์	139	5.8 การพิสูจน์ตัวตนดิจิทัล	169
5.3 การเข้ารหัสลับในระบบสื่อสารข้อมูล	141	5.7 บทสรุป	171
5.3.1 การเข้ารหัสลับแบบจุดเชื่อมโยง ถึงจุดเชื่อมโยง	142	5.8 คำถามท้ายบท	173
5.3.2 การเข้ารหัสลับแบบจุดปลาย ถึงจุดปลาย	143		
5.3.3 การประยุกต์ใช้งานสองระบบ ร่วมกัน	144	บทที่ 6 วิทยาการรหัสลับประยุกต์	
5.4 การเข้ารหัสลับในหน่วยเก็บข้อมูล	145	6.1 บทนำ	174
5.4.1 กุญแจอ้างอิงลับ (Dereferencing Key)	145	6.2 ซูลโพรโทคอล IPSec	175
5.5 โหมดการทำงานของตัวแปรรหัสลับ แบบบล็อก	148	6.2.1 โหมดการทำงานใน IPSec	176
5.5.1 การทำงานในโหมด ECB (Electronic Code Book)	148	6.2.2 โพรโทคอลย่อยใน IPSec	178
5.5.2 การทำงานในโหมด CBC (Cipher Block Chaining)	150	6.3 ซูลโพรโทคอล SSL/TLS	181
5.5.3 การทำงานในโหมด CFB (Cipher Feed Back)	151	6.3.1 โพรโทคอลย่อยใน SSL	182
5.5.4 การทำงานในโหมด OFB (Output Feed Back)	153	6.3.2 โพรโทคอล TLS	185
5.5.5 จุดอ่อนในการใช้งานตัวแปร รหัสลับแบบบล็อก	154	6.4 โพรโทคอล PGP	185
5.6 การเพิ่มความแข็งแกร่งของตัวแปร รหัสลับแบบบล็อก	157	6.5 โพรโทคอลเคอร์เนล	188
5.6.1 การเข้ารหัสลับสองครั้ง (Double Encryption)	157	6.5.1 ความแตกต่างระหว่างเทอร์โบลอส รุ่นที่ 4 และ 5	191
5.6.2 การโจมตีแบบพบกันตรงกลาง (Meet-in-the-middle Attack)	158	6.6 การตรวจสอบบูรณาภาพข้อมูลในระบบ กล้องวงจรปิด	191
5.6.3 การเข้ารหัสลับสามครั้ง (Triple Encryption)	159	6.6.1 โพรโทคอลเพื่อใช้ตรวจสอบบูรณาภาพ ข้อมูลในระบบกล้องวงจรปิด	191
5.6.4 การเข้ารหัสลับแบบต่อเนื่อง	162	6.6.2 การวิเคราะห์ความปลอดภัย	194
		6.7 การพิสูจน์ตัวตนในระบบแพร่ภาพทางเดียว	
		6.7.1 โพรโทคอลการกระจายกุญแจในระบบ แพร่ภาพทางเดียว	196
		6.7.2 การวิเคราะห์ความปลอดภัย	200
		6.8 การรักษาความลับเมื่อมีการขโมยจาก ผู้ไม่ประสงค์ดี	201
		6.8.1 วิธีการปกปิดข้อความรหัสต่าง	202
		6.8.2 การปกปิดข้อความรหัสโดยใช้ การเข้ารหัสลับแบบต่อเนื่อง	203
		6.8.3 การวิเคราะห์ความปลอดภัย	205
		6.9 บทสรุป	207
		6.10 คำถามท้ายบท	207

บทที่ 7 การทำลายน้ำดิจิทัล		บทที่ 8 การประยุกต์ใช้วิทยาการรหัสลับ ร่วมกับการทำลายน้ำภาพดิจิทัล	
7.1 บทนำ	209	8.1 บทนำ	265
7.2 การซ่อนสารสนเทศในเครือข่าย สื่อสารข้อมูล	211	8.2 ความจำเป็นและหลักการบีบอัดข้อมูล	266
7.3 ข้อจำกัดและประเภทของการทำ ลายน้ำดิจิทัล	215	8.3 การบีบอัดข้อมูลด้วยการเข้ารหัสเอนโทรปี	267
7.4 งานประยุกต์ที่ใช้การทำลายน้ำดิจิทัล	218	8.3.1 การลดรูปข้อมูลที่ซ้ำกัน	267
7.5 การโจมตีลายน้ำดิจิทัล	221	8.3.2 การเข้ารหัสเชิงสถิติ	268
7.5.1 การโจมตีแบบลบออก (Removal Attack)	223	8.4 การบีบอัดข้อมูลด้วยการเข้ารหัสต้นทาง	271
7.5.2 การโจมตีเชิงเรขาคณิต (Geometry Attack)	224	8.4.1 การเข้ารหัสแบบให้ค่าความสว่าง	271
7.5.3 การโจมตีด้านวิทยาการรหัสลับ (Cryptographic Attack)	225	8.4.2 การเข้ารหัสแบบการแปลงโดเมน	273
7.5.4 การโจมตีโพรโทคอล (Protocol Attack)	226	8.5 การบีบอัดภาพตามมาตรฐาน JPEG	274
7.5.5 การทดสอบความทนทานของลายน้ำ ที่ฝังโดยใช้สเตอริโอภาพ	227	8.5.1 ขั้นตอนการจับเตรียมภาพ	276
7.6 การประเมินประสิทธิภาพการทำลายน้ำดิจิทัล		8.5.2 ขั้นตอนการเข้ารหัสต้นทาง	277
7.6.1 การประเมินคุณภาพเชิงจิตวิสัย	230	8.5.3 ขั้นตอนการเข้ารหัสเอนโทรปี	279
7.6.2 การประเมินคุณภาพเชิงวัตถุวิสัย	232	8.6 หลักการบีบอัดวีดิทัศน์	281
7.7 การทำลายน้ำภาพด้วยวิธีที่ล้ำความแรง สัญญาณ	236	8.6.1 การลดขนาดการเคลื่อนไหว	284
7.7.1 การเพิ่มประสิทธิภาพของระบบ	240	8.6.2 การเข้ารหัสเฟรมภาพในวีดิทัศน์	285
7.7.2 ผลกระทบจากสามเหลี่ยมที่ใช้	245	8.7 การจัดการหน่วยวีดิทัศน์อย่างปลอดภัยผ่าน เครือข่ายสาธารณะ	230 288
7.7.3 การประเมินประสิทธิภาพที่เพิ่มขึ้น	249	8.7.1 การเข้ารหัสลับแบบเลือกได้	290
7.8 การทำลายน้ำภาพสำหรับเครือข่ายสังคม	254	8.7.2 การฝังลายน้ำดิจิทัลลงในวีดิทัศน์ ที่เข้ารหัสลับมาแล้ว	292
7.8.1 การแปลงเวฟเล็ตแบบไม่ต่อเนื่อง	255	8.7.3 โพรโทคอลการจัดการหน่วยวีดิทัศน์ อย่างปลอดภัย	296
7.8.2 การทำลายน้ำภาพด้วยวิธีรับค่า สัมประสิทธิ์เวฟเล็ต	257	8.8 บทสรุป	300
7.8.3 การประเมินประสิทธิภาพของระบบ ที่นำเสนอ	260	8.9 คำถามท้ายบท	301
7.9 บทสรุป	262	เอกสารอ้างอิง	302
7.10 คำถามท้ายบท	263	ดัชนี	306
		ประวัติผู้เขียน	310