บทที่ 3

รหัสแทนข้อมูล

รหัสหมายถึงสัญลักษณ์ที่ใช้แทนข้อมูล ขณะเมื่อต้องการสื่อสารกันระหว่างผู้รับสารกับผู้ส่งสารทั้งนี้เพื่อความปลอดภัยของข่าวสาร ที่ต้องมีการป้องกันมิให้ผู้อื่นรับรู้ข่าวสารนั้น ได้ สำหรับในเครื่องคอมพิวเตอร์ จะหมายถึง การเปลี่ยน ฐานของ ตัวเลขฐ านสิบให้เป็นกลุ่มของเลขฐานสอง เนื่องจากคอมพิวเตอร์ต้องสื่อสารกับผู้ใช้ซึ่งเป็นมนุษย์ โดยคอมพิวเตอร์จะป ฏิบัติตามคำสั่งได้ดีและรวดเร็ว ได้นั้น คำสั่งต้องมีลักษณะเป็นตัวเลขฐานสองคือมี 0 และ 1 เรียงต่อกันเป็นชุด ๆ ต่อ 1 คำสั่ง สำหรับมนุษย์ก็จะคุ้นเคยกับเลขฐานสิบ ถ้าต้องการสื่อสารให้เข้าใจซึ่งกันและกัน จำเป็นต้องมีการเปลี่ยนฐานของตัวเลขสลับกันไปมา ซึ่งมีวิธีการเปลี่ยนฐานตัวเลขอยู่หลายดังต่อไปนี้

รหัส BCD – 8421

รหัส BCD – 8421 (Binary Code Decimal) เป็นรหัสที่ใช้กันบ่อย มีตัวเลขทั้งสิ้น 10 ตัวเริ่มตั้งแต่ 0000 - 1001 สังเกตว่าเลขแต่ละตัว จะประกอบด้วยเลขฐาน สองจำนวน 4 ตัว เรียกว่า 4 บิต เริ่มตั้งแต่บิต 0 จนถึงบิต 3 แต่ละบิตมีลักษณะไม่เหมือนกันดังแสดงในตารางที่ 3.1

ตารางที่ 3.1 รหัส BCD – 8421 เปรียบเทียบกับเลขฐานสิบ

เลขฐานสิบ	BCD – 8421
0	0000
1	0001
2	0010
3	0011
4	0100
5	0101
6	0110
7	0111
8	1000
9	1001

รหัสเลขฐานแปดและเลขฐานสิบหก

รหัสนี้ถูกพัฒนามาจากรหัส BCD–8421 เพราะว่าในกรณีที่มีการนำเอาเลขมาบวกกัน เช่น 7+5 = 12 หรือ 0111+0101 =1100 ผลลัพธ์ 1100 นี้ไม่มีในรหัส BCD – 8421 จึงได้มีการคิดหารหัสเลขฐานแปดและเลขฐานสิบหกนี้มาใช้แทน ซึ่งถ้ามีการพิจารณาทีละ 3 บิตจะหมายถึงรหัสเลขฐานแปดและถ้าพิจารณาทีละ 4 บิตจะเป็นรหัสเลขฐานสิบหกตัวอย่างเช่นถ้าหากต้องการเปลี่ยนเลข $(1010010100100 11010)_2$ ให้เป็นเลขฐานแปดและฐานสิบหกให้ดำเนินการดังนี้

การเข้ารหัส $(1010010100100 11010)_2$ ให้เป็นรหัสเลขฐานแปด

101	001	010	010	011	010		
↓	↓	↓	↓	↓	↓		
5	1	2	2	3	2	=	$(512232)_8$

$\therefore$ $(1010010100100 11010)_2$ เมื่อเข้ารหัสแล้วจะมีค่า = $(512232)_8$

ตอบ $(512232)_8$

การเข้ารหัส $(1010010100100 11010)_2$ ให้เป็นรหัสเลขฐานสิบหก

1010	1001	0100	1001	1010		
↓	↓	↓	↓	↓		
A	9	4	9	A	=	$(A949A)_{16}$

$\therefore$ $(1010010100100 11010)_2$ เมื่อเข้ารหัสแล้วจะมีค่า = $(A949A)_{16}$

ตอบ $(A949A)_{16}$

การใช้พาริตี้ในรหัส

ในการส่งข่าวสาร จากต้นทางไปยังปลายทางในระบบ สัญญาณดิจิตอล (Digital) นั้น ผู้ให้บริการ สามารถตรวจสอบความถูกต้องของข่าวสารที่ส่งออกไปได้ ว่าผู้รับสามารถรับสารได้ถูกต้องหรือไม่ ซึ่งวิธีที่นิยมใช้กันมากที่สุดก็คือการใช้พาริตี้บิต (Parity bit)

พาริตี้บิตคือบิต (เลข 0 หรือ 1) ที่เติมเข้าไปใน Code word ใด ๆ ก็ตามแล้วทำให้ Code word นั้น ๆ มีจำนวนของเลข 1 เป็นจำนวนคู่ (Even) หรือคี่ (Odd) ก็ได้ตามต้องการ การใช้พาริตี้ในรหัสจึงแบ่งออกเป็น 2 แบบดังนี้

1) พาริตี้เลขจำนวนคู่ (Even Parity) เช่น เลขจำนวนคู่ = 0111 **1**

2) พาริตี้เลขจำนวนคี่ (Odd Parity) เช่น เลขจำนวนคี่ = 0101 **1**

ตารางที่ 3.2 พาริตี้บิตในรหัส BCD – 8421

เลขฐานสิบ	รหัส BCD – 8421	BCD with Odd Parity	BCD with Even Parity
0	0000	0000 1 หรือ 00001	0000 0 หรือ 00000
1	0001	0001 0 หรือ 00010	0001 1 หรือ 00011
2	0010	0010 0 หรือ 00100	0010 1 หรือ 00101
3	0011	0011 1 หรือ 00111	0011 0 หรือ 00110
4	0100	01000 หรือ 01000	01001 หรือ 01001
5	0101	0101 1 หรือ 01011	0101 0 หรือ 01001
6	0110	0110 1 หรือ 01101	0110 0 หรือ 01100
7	0111	0111 0 หรือ 01110	0111 0 หรือ 01111
8	1000	1000 0 หรือ 10000	1000 1 หรือ 10001
9	1001	1001 1 หรือ 10011	1001 0 หรือ 10010

รหัสเกิน 3

รหัสเกิน 3 ดัดแปลงมาจากรหัส BCD – 8421 เมื่อเปรียบเทียบรหัสเกิน 3 กับรหัส BCD – 8421 ตามตาราง ที่ 3.3 จะเห็นได้ว่ารหัสเกิน 3 จะมีค่ามากกว่ารหัส BCD – 8421 อยู่ 3

ตารางที่ 3.3 การเปรียบเทียบระหว่างรหัส BCD – 8421 กับรหัสเกิน 3

เลขฐานสิบ	รหัส BCD – 8421	รหัสเกิน 3
0	0000	0011
1	0001	0100
2	0010	0101
3	0011	0110
4	0100	0111

5	0101	1000
6	0110	1001
7	0111	1010
8	1000	1011
9	1001	1100

ตัวอย่างที่ 2.1 การหารหัสเกิน 3 ของ $(0110)_2$

<u>วิธีทำ</u> รหัส BCD – 8421 = 0110

$$\begin{array}{r} 0011 \\ + \\ \hline 1001 \end{array}$$

$\therefore$ รหัสเกิน 3 ของ 0110 = 1001

<u>ตอบ</u> $(1001)_2$

รหัสเกรย์

รหัสเกรย์ (Gray Code) ใช้กันมากในระบบการตร วจจับสัญญาณด้วยแสง หรือระบบ ที่ทำด้วยแกนหมุนทางกล ไกล เพื่อบอกตำแหน่งของเพลาหมุน รหัสแบบนี้เป็นแบบ Non Weighted ในระหว่างกลุ่มรหัส (Code Group) ที่เรียงลำดับกันไปจะมีการเปลี่ยนแปลงของรหัสครั้งละ 1 บิต เท่านั้น ทำให้โอกาสความผิดพลาดในการรับรหัสเป็นไปได้น้อยมาก

การเปลี่ยนรหัสเลขฐานสองให้เป็นรหัสเกรย์ สามารถทำได้โดยนำบิตที่ 2 ดึงลงมาเป็นคำตอบต่อจากนั้นนำเอ าบิตที่ 2 และบิตที่ 1 มาเปรียบเทียบกัน ถ้าบิตทั้งสอง ต่างกันผลลัพธ์ที่ได้จะเป็น “1” เสมอ แต้ถ้าเปรียบเทียบกันแล้ว บิตทั้งสองเหมือนกัน ผลลัพธ์ที่ได้จะเป็น “0” จากนั้นทำเช่นนี้ไปเรื่อย ๆ จนถึงบิตสุดท้าย

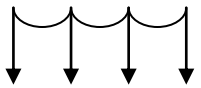
ตารางที่ 3.4 การเปรียบเทียบระหว่างเลขฐานสองกับรหัสเกรย์ 0 – 15

เลขฐานสิบ	เลขฐานสอง	รหัสเกรย์
0	0000	0000
1	0001	0001
2	0010	0011
3	0011	0010

4	0100	0110
5	0101	0111
6	0110	0101
7	0111	0100
8	1000	1100
9	1001	1101
10	1010	1111
11	1011	1110
12	1100	1010
13	1101	1011
14	1110	1001
15	1111	1000

ตัวอย่างที่ 2.2 การเปลี่ยนรหัสเลขฐานสองจาก $(1011)_2$ ให้เป็นรหัสเกรย์

<u>วิธีทำ</u> รหัสเลขฐานสอง 1 0 1 1



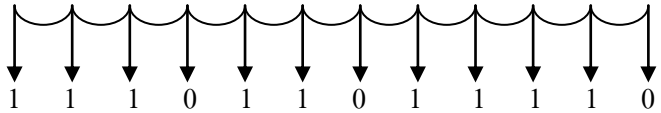
รหัสเกรย์ 1 1 1 0

∴ รหัสเกรย์ ของ 1011 = 1110

<u>ตอบ</u> $(1110)_2$

ตัวอย่างที่ 2.3 การแปลงเลขฐานสอง $(101101101011)_2$ ให้เป็นรหัสเกรย์

<u>วิธีทำ</u> เลขฐานสอง → 1 0 1 1 0 1 1 0 1 0 1 1



รหัสเกรย์ → 1 1 1 0 1 1 0 1 1 1 1 0

∴ รหัสเกรย์ ของ 101101101011 = 111011011110

<u>ตอบ</u> $(111011011110)_2$

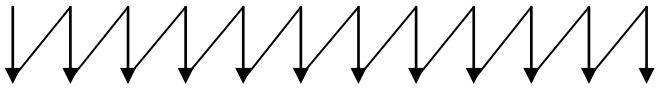
การแปลงรหัสเกรย์ให้เป็นรหัสเลขฐานสองสามารถดำเนินการได้ดังนี้

1) ดึงบิตแรกลงมา เป็นผลลัพธ์

2) นำผลลัพธ์ไปเปรียบเทียบกับบิตถัดไป ถ้าต่างกันผลลัพธ์จะมีค่าเป็น "1" ถ้าเหมือนกันผลลัพธ์จะมีค่าเป็น "0" ดังตัวอย่างต่อไปนี้

ตัวอย่างที่ 2.4 การแปลงรหัสเกรย์ให้เป็นเลขฐานสอง

วิธีทำ รหัสเกรย์ → 1 1 1 0 1 1 0 1 1 1 1 0



เลขฐานสอง → 1 0 1 1 0 1 1 0 1 0 1 1

∴ รหัสเกรย์ ของ 111011011110 = 101101101011

ตอบ $(101101101011)_2$

รหัสแทนข้อมูลในคอมพิวเตอร์

คอมพิวเตอร์ทำงานด้วยหลักการทางอิเล็กทรอนิกส์ ที่แทนสัญญาณทางไฟฟ้าด้วยตัวเลขศูนย์ และหนึ่ง (0 และ1)ซึ่งเป็นตัวเลขในระบบเลขฐานสองแต่ละหลักเรียกว่า บิต (BinaryDigit:Bit)และเมื่อนำตัวเลขหลายๆบิตมาเรียงกันจะหมายถึงการสร้างรหัสแทนความหมายของเลขจำนวน
หรือตัวอักษร หรือสัญลักษณ์ ทั้งภาษาอังกฤษและภาษาไทย และเพื่อให้การสื่อสารสามารถแลกเปลี่ยนข้อความระหว่างมนุษย์กับคอมพิวเตอร์เป็นไปในแนวทางเดียวกันจึงมีการกำหนดมาตรฐานรหัสตัวเลข ในระบบฐานสองสำหรับแทนสัญลักษณ์เหล่านี้ รหัสมาตรฐานที่นิยมใช้กันอยู่มากมีสองกลุ่ม ได้แก่ รหัสแอสกี รหัสเอ็บซีดิก

รหัสแอสกี

รหัสแอสกี (ASCII) เป็นมาตรฐานที่นิยมใช้กันมากในระบบคอมพิวเตอร์ส่วนใหญ่คำว่า ASSCII ย่อมาจาก American Standard Code for Information Interchange เป็นหัส 8 บิต แทนสัญลักษณ์ต่าง ๆ ได้ 256 ตัวเมื่อใช้แทนตัวอักษรภาษาอังกฤษ สำนักงานมาตรฐานผลิตภัณฑ์อุตสาหกรรม หรือสมอ.ได้กำหนดรหัสภาษาไทยเพิ่มลงไปเพื่อให้ใช้งานร่วมกันได้ ตามตารางดังนี้

ตารางที่ 3.5 แสดงรหัส ASCII แทนตัวอักษรภาษาอังกฤษและภาษาไทย

	b7	0	0	0	0	0	0	0	0	1	1	1	1	1	1	1	1
	b6	0	0	0	0	1	1	1	1	0	0	0	0	1	1	1	1
	b5	0	0	1	1	0	0	1	1	0	0	1	1	0	0	1	1
	b4	0	1	0	1	0	1	0	1	0	1	0	1	0	1	0	1
b3	b2	b1	b0														
0	0	0	0				□	0	@	P	²	p				ฐ	ภ	ะ	เ	๐
0	0	0	1				!	1	A	Q	a	q			ก	ฑ	ม	ั	แ	๑
0	0	1	0				"	2	B	R	b	r			ข	ฒ	ย	ำ	โ	๒
0	0	1	1				£	3	C	S	c	s			ฃ	ณ	ร	ิ	ใ	๓
0	1	0	0				$	4	D	T	d	t			ค	ด	ฤ	ี	ไ	๔
0	1	0	1				%	5	E	U	e	u			ฅ	ต	ล	ึ	ๅ	๕
0	1	1	0				&	6	F	V	f	v			ฆ	ถ	ฦ	ื	ๆ	๖
0	1	1	1				'	7	G	W	g	w			ง	ท	ว	ุ	็	๗
1	0	0	0				(	8	H	X	h	x			จ	ธ	ศ	ู	่	๘
1	0	0	1				)	9	I	Y	i	y			ฉ	น	ษ	ฺ	้	๙
1	0	1	0				*	:	J	Z	j	z			ช	บ	ส		๊	๚
1	0	1	1				+	;	K	[	k	¼			ซ	ป	ห		๋	๛
1	1	0	0				,	<	L		l	:			ฌ	ผ	ฬ		์	
1	1	0	1				-	=	M	]	m				ญ	ฝ	อ		๎	
1	1	1	0				.	>	N	¾	n	³			ฎ	พ	ฮ			
1	1	1	1				/	?	O	-	o				ฏ	ฟ	ฯ	฿	๏	

รหัสเอ็บซีดิก

รหัสเอ็บซีดิก(EBCDIC)ย่อมาจาก (Extended Binary Coded Decimal Interchange Code) มีการกำหนดรหัสที่ใช้แทนข้อมูลขนาด 8 บิต เหมือนกันกับรหัสแอสกี รูปแบบของรหัสจะมีความแตกต่างกัน ทั้งรหัสแอสกีและเอ็บซีดิกจะใช้เลขฐาน 2 (0 หรือ 1) จำนวน 8 หลักแทนข้อมูลหนึ่งตัวหรือ 1 Byte ดังนั้นรหัสแทนข้อมูลทั้งแอสกีและเอ็บซีดิกจะสามารถแทนข้อมูลที่แตกต่างกันได้ทั้งหมด 256 ตัว

ตารางที่ 3.6 เปรียบเทียบรหัสเอ็บซีดิกและรหัสแอสกี ที่ใช้แทนตัวอักษรภาษาอังกฤษ

Symbol	ASCII	EBCDIC	Symbol	ASCII	EBCDIC
A	0100 0001	1100 0001	!	0010 0001	0101 1010
B	0100 0010	1100 0010	"	0010 0010	0111 1111
C	0100 0011	1100 0011	#	0010 0011	0111 1011
D	0100 0100	1100 0100	$	0010 0100	0101 1011
E	0100 0101	1100 0101	%	0010 0101	0110 1100
F	0100 0110	1100 0110	&	0010 0110	0101 0000
G	0100 0111	1100 0111	(	0010 1000	0100 1101
H	0100 1000	1100 1000	)	0010 1001	0101 1101
I	0100 1001	1100 1001	*	0010 1010	0101 1100
J	0100 1010	1101 0001	+	0010 1011	0100 1110
K	0100 1011	1101 0010			
L	0100 1100	1101 0011	0	0011 0000	1111 0000
M	0100 1101	1101 0100	1	0011 0001	1111 0001
N	0100 1110	1101 0101	2	0011 0010	1111 0010
O	0100 1111	1101 0110	3	0011 0011	1111 0011
P	0101 0000	1101 0111	4	0011 0100	1111 0100
Q	0101 0001	1101 1000	5	0011 0101	1111 0101
R	0101 0010	1101 1001	6	0011 0110	1111 0110
S	0101 0011	1110 0010	7	0011 0111	1111 0111
T	0101 0100	1110 0011	8	0011 1000	1111 1000
U	0101 0101	1110 0100	9	0011 1001	1111 1001
V	0101 0110	1110 0101			
W	0101 0111	1110 0110			
X	0101 1000	1110 0111			
Y	0101 1001	1110 1000			
Z	0101 1010	1110 1001			

เทคโนโลยีในการรักษาความปลอดภัยของข้อมูล

การรักษาความปลอดภัยของข้อมูลในการทำธุรกรรมอิเล็กทรอนิกส์ ต้องครอ บคลุมในเรื่องของการระบุตัวบุคคล การควบคุมการเข้าถึงการรักษาความลับ ความถูกต้องครบถ้วนของข้อมูล และการป้องกันการปฏิเสธความรับผิด นั้น จำเป็นต้องอาศัยเทคโนโลยีเข้ามาช่วยในการ

รักษาความปลอดภัย ซึ่งเทคโนโลยีที่นิยมในปัจจุบัน ได้แก่ เทคโนโลยีการใช้รหัส และเทคโนโลยีลายมือชื่อดิจิตอล

1. เทคโนโลยีการใช้รหัส

เทคโนโลยีการใช้รหัส (Cryptography) หมายถึง การทำให้ข้อมูลที่จะนำส่งผ่านไปทางเครือข่ายอยู่ในรูปแบบที่ไม่สามารถอ่านออกได้ด้วย การเข้ารหัส ซึ่งผู้มีสิทธิ์จริงเท่านั้นจะสามารถอ่านข้อมูลได้ด้วยการถอดรหัส ซึ่งการเข้าและถอดรหัสนั้นจะอาศัยสมการทางคณิตศาสตร์ ที่ซับซ้อน และต้องอาศัยกุญแจซึ่งอยู่ในรูปของพารามิเตอร์ที่กำหนดไว้ ในการเข้าและถอดรหัสสามารถแบ่งเป็น 2 ประเภท ดังนี้

1.1. การใช้รหัสแบบกุญแจสมมาตร เป็นการเข้าและถอดรหัสโดย ใช้กุญแจส่วนตัวที่เหมือนกันซึ่งจะต้องเป็นที่รู้กันเพียงผู้ส่งและผู้รับเท่านั้น

1.2. การใช้รหัสแบบกุญแจอสมมาตร เป็นการเข้าและถอดรหัสด้วยกุญแจต่างกัน โดยจะเน้นที่ผู้รับเป็นหลัก คือ จะใช้กุญแจสาธารณะของผู้รับซึ่งเป็นที่เปิดเผยในการเข้ารหัส และจะใช้กุญแจส่วนตัวของผู้รับในการถอดรหัส การใช้รหัสแบบกุญแจสมมาตร และกุญแจอสมมาตร มีข้อดี/ข้อเสียที่แตกต่างกันดังนี้

ตารางที่ 3.7 การเปรียบเทียบข้อดี-ข้อเสียของการใช้กุญแจสมมาตร

ข้อดี	ข้อเสีย
1. มีความรวดเร็วเพราะใช้การคำนวณที่ น้อยกว่า	การบริหารจัดการกุญแจทำได้ยาก เพราะกุญแจในการเข้ารหัสและถอดรหัสเหมือนกัน
2. สามารถสร้างได้ง่ายโดยใช้ฮาร์ดแวร์	

ตารางที่ 3.8 การเปรียบเทียบข้อดี-ข้อเสียของการใช้กุญแจอสมมาตร

ข้อดี	ข้อเสีย
1. การบริหารจัดการกุญแจทำได้ง่ายกว่า เพราะ ใช้กุญแจในการเข้ารหัส และถอดรหัสต่างกัน	ใช้เวลาในการเข้าและถอดรหัสค่อนข้างนาน เพราะต้องใช้การคำนวณอย่างมาก
2. สามารถระบุผู้ใช้โดยการใช้ร่วมกับลายมือชื่ออิเล็กทรอนิกส์	

ในการส่งข้อมูลผ่านเครือข่ายนั้น นอกจากจะทำให้ข้อมูลที่ส่งมาเป็นความลับสำหรับผู้ไม่มีสิทธิ์โดยการใช้เทคโนโลยีการใช้รหัสแล้ว สำหรับการทำนิติกรรมสัญญาโดยทั่ วไป ลายมือชื่อจะเป็นสิ่งที่ใช้ในการระบุตัวบุคคล และยังมีการแสดงถึงเจตนาในการยอมรับสาระในสัญญานั้นๆ ซึ่งสัมพันธ์กับการป้องกันการปฏิเสธความรับผิดสำหรับในธุรกรรมอิเล็กทรอนิกส์จะใช้ ลายมือชื่ออิเล็กทรอนิกส์ ซึ่งมีรูปแบบต่างๆ แต่ที่ได้รับการยอมรับกันมากที่สุด คือ ลายมือชื่อดิจิตอล ซึ่งเป็นองค์ประกอบหนึ่งในโครงสร้างพื้นฐานกุญแจสาธารณะ

2. ลายมือชื่อ ดิจิตอล เป็นลายมือชื่ออิเล็กทรอนิกส์ ที่สร้างจากเทคโนโลยีเข้ารหัสด้วยกุญแจสาธารณะ ในการลงลายมือชื่อ ดิจิตอลกำกับข้อความที่ต้องการ ส่งผ่านเครือข่าย ผู้ส่งข้อความจะใช้กุญแจส่วนตัวของตนในการลงลายมือชื่อโดยผ่านกระบวนการทางคณิตศาสตร์ ผู้รับจะสามารถตรวจสอบความถูกต้องของลายมือชื่อดังกล่าวโดยใช้กุญแจสาธารณะของผู้ส่ง ซึ่งลายมือชื่อของผู้ส่งจะถูกรับรองด้วยองค์กรออกใบรับรอง โดยแสดงอยู่ในรูปของ "ใบรับรองดิจิตอล " ประโยชน์ของลายมือชื่อดิจิตอลนั้น นอกจากจะช่วยระบุตัวผู้ส่งข้อมูลแล้ว ยังช่วยป้องกันข้อมูลให้มีความถูกต้องไม่ได้ผ่านการแก้ไข หรือหากมีการแก้ไขมาก่อนก็สามารถตรวจสอบได้

กระบวนการสร้างและลงลายมือชื่อดิจิตอล

การสร้างและลงลายมือชื่อดิจิตอล มี 3 ขั้นตอนดังนี้

ขั้นตอนที่ 1 : นำข้อมูลอิเล็กทรอนิกส์ต้นฉบับที่จะส่งไปนั้นมาผ่านกระบวนการทางคณิตศาสตร์ที่ เรียกว่า ฟังก์ชันย่อยข้อมูล เพื่อให้ได้ข้อมูลที่สั้น ๆ ที่เรียกว่า ข้อมูลที่ย่อยแล้ว ก่อนที่จะทำการเข้ารหัส

ขั้นตอนที่ 2 : ทำการเข้ารหัสด้วยกุญแจส่วนตัวของผู้ส่งเอง ซึ่ งเปรียบเสมือนการลงลายมือชื่อของผู้ส่ง เพราะผู้ส่งเท่านั้นที่มีกุญแจส่วนตัวของผู้ส่งเอง และจะได้ข้อมูลที่เข้ารหัสแล้ว เรียกว่า ลายมือชื่อดิจิตอล

ขั้นตอนที่ 3 : ขั้นตอนของการส่งลายมือชื่อไปพร้อมกับข้อมูลต้นฉบับ ไปยังผู้รับ ผู้รับก็จะทำการตรวจสอบว่าข้อมูลที่ได้รับถูกแก้ไขระหว่างทางหรือไม่ โดยการนำข้อมูลต้นฉบับที่ได้รับมาอ่านกระบวนการย่อย ฟังก์ชั่นย่อยข้อมูล ก็จะได้ข้อมูลที่ย่อยแล้ว และ นำลายมือชื่อดิจิตอลมาทำการถอด รหัสด้วย กุญแจสาธารณะของผู้ส่ง ก็จะได้ข้อมูลที่ย่อยแล้วอีกอันหนึ่ง แล้วทำการเปรียบเทียบข้อมูลที่ย่อยแล้วทั้ง 2 อัน ถ้าหากว่าเหมือนกัน แสดงว่า ข้อมูลที่ได้รับนั้นไม่ได้ถูกแก้ไข แต่ถ้าข้อมูลที่ย่อยแล้วแตกต่างกัน แสดงว่า ข้อมูลที่ได้รับถูกเปลี่ยนแปลงระหว่างทาง

ใบรับรองดิจิตอล

การเข้ารหัส และ ลายมือชื่อดิจิตอล ในการทำธุรกรรม ทำให้สาม ารถรักษาความลับของข้อมูล สามารถรักษาความถูกต้องของข้อมูล และสามารถระบุตัวบุคคลได้ระดับหนึ่ง เพื่อเพิ่มระดับความปลอดภัยในการระบุตัวบุคคล โดยสร้างความเชื่อถือมากขึ้นด้วย ใบรับรองดิจิตอล ซึ่งออกโดยองค์กรกลางที่เป็นที่เชื่อถือ เรียกว่า องค์กรรับรองความถูกต้อง จะถูกนำมาใช้สำหรับยืนยันในการทำธุรกรรมว่า เป็นบุคคลนั้นๆจริงตามที่ได้อ้างไว้ ใบรับรองดิจิตอลที่ออกตามมาตรฐาน X.509 Version 3 ซึ่งเป็นมาตรฐานที่ได้รับความนิยมอย่าง แพร่หลายที่สุด จะประกอบด้วยข้อมูลดังต่อไปนี้

1. หมายเลขของใบรับรอง
2. วิธีการที่ใช้ในการเข้ารหัสข้อมูล
3. หน่วยงานที่ออกใบรับรอง
4. เวลาเริ่มใช้ใบรับรอง
5. เวลาที่ใบรับรองหมดอายุ
6. ผู้ได้รับการรับรอง (
7. กุญแจสาธารณะของผู้ได้รับการรับรอง
8. ลายมือชื่อดิจิตอลของหน่วยงานที่ออกใบรับรอง

องค์กรออกใบรับรอง

เป็นองค์กรที่ น่าเชื่อถือ ที่ทำหน้าที่เป็นบุคคลที่ดำเนิ นการออกใบรับรองดิจิตอล ให้กับผู้ทำธุรกรรมอิเล็กทรอนิกส์ ที่ขอใช้บริการ โดยบริการต่างๆขององค์กรออกใบรับรองนี้ ได้แก่

1. บริการเทคโนโลยีเข้ารหัส ซึ่งประกอบด้วยการผลิตกุญแจส่วนตัว การส่งมอบกุญแจส่วนตัว การผลิตกุญแจสาธารณะและกุญแจส่วนตัว การผลิตลายมือชื่อดิจิตอล และการรับรองลายมือชื่อดิจิตอล

2. บริการที่เกี่ยวข้องกับการออกใบรับรอง มีหลายบริการ ซึ่ง ประกอบไปด้วย การออกใบรับรอง การตีพิมพ์ใบรับรองเพื่อเผยแพร่แก่บุคคลทั่วไป การเก็บต้นฉบับใบรับรอง และการกำหนดนโยบายการออกและอนุมัติใบรับรอง

3. บริการเสริมต่าง ๆ ได้แก่ การลงทะเบียนการตรวจสอบสัญญาต่าง ๆ การกู้กุญแจ เป็นต้น

สรุป

รหัสที่ใช้แทนข้อมูลมีความสำคัญอย่างยิ่งในระบบการสื่อสารข้อมูล โดยเฉพาะข้อมูลที่ลับเฉพาะที่ไม่ต้องการให้คนอื่นล่วงรู้ จำเป็นอย่างยิ่งที่จะต้องทำการเข้ารหัสเพื่ อเปลี่ยนแปลงข้อมูลให้มีลักษณะข้อมูลที่ผู้อื่นไม่เข้าใจเสียก่อนจึงจะดำเนินการส่งข้อมูลนั้น ๆ ออกไป ส่วนผู้รับสารเมื่อต้องการที่จะอ่านข้อมูลที่รับเข้ามา ก็ จะต้องทำการถอดรหัสเสียก่อนถึงจะอ่านข้อมูลได้ถูกต้อง ซึ่งรูปแบบของการเข้ารหัสและถอดรหัสมีอยู่หลายวิธี เช่น การเข้ารหัสและถอดรหัส จากรหัสเลขฐานสองเป็นรหัส BCD-8421 การเข้ารหัสและถอดรหัสฐานแปดและฐานสิบหก การเข้ารหัสและถอดรหัสเกิน 3 และการเข้ารหัสและถอดรหัสเกรย์เป็นต้น

แบบฝึกหัดท้ายบท

1. จงถอดรหัส BCD – 8421 ให้อยู่ในรูปเลขฐานสิบ
   ก. 0110
   ข. 0101, 0010, 1001
   ค. 0011, 1001, 0000, 1000
2. จงเข้ารหัสเลขฐานสิบต่อไปนี้ให้อยู่ในรูปของรหัส BCD – 8421
   ก. 5, 7
   ข. 4, 5, 6
3. จงเข้ารหัสเลขฐานสองต่อไปนี้ให้อยู่ในรูปของรหัสเลขฐานแปด
   ก. 1100100011
   ข. 10110110110110101
4. จงเข้ารหัสเลขฐานสองต่อไปนี้ให้อยู่ในรูปของรหัสเลขฐานสิบหก
   ก. 11001100011011010101
   ข. 10111001100011011010101
5. จงเข้ารหัสเลขฐานสิบไปนี้ให้อยู่ในรูปของรหัส BCD – 8421 ที่มีพาริตี้บิตเลขคู่ต่อเลขฐานสิบ 1 หลัก
   ก. 2
   ข. 9 , 1
   ค. 8,0,2

6. จงเข้ารหัสเลขฐานสิบต่อไปนี้ให้อยู่ในรูปของรหัสเกิน 3

   ก. 7

   ข. 3,8

   ค. 4,9,3

7. จงเข้ารหัสเลขฐานสองต่อไปนี้ให้อยู่ในรูปของรหัสเกรย์

   ก. 111100110101011

   ข. 01100100101101101101

8. การแปลงรหัสเกรย์ให้เป็นเลขฐานสอง

   ก. 100110101100101101

   ข. 011110101111000011

9. จงเข้ารหัสเลขฐานสิบต่อไปนี้ให้อยู่ในรูปของรหัสเกรย์

   ก. 7

   ข. 3,8

   ค. 4,9,3

10. จงเข้ารหัสเลขเกรย์ต่อไปนี้ให้อยู่ในรูปของเลขฐานสิบ

    ก. 1100

    ข. 1101,0110

    ค. 0001,0011,0111

เอกสารอ้างอิง

กุลยา นิ่มสกุล. 2540. **ความรู้พื้นฐานทาง คอมพิวเตอร์.** กรุงเทพมหานคร : ฟิสิกส์เซ็นเตอร์.

ธนัท ชัยยุทธ และกณพ แก้วพิชัย. 2546. **ดิจิตอลพื้นฐาน.** กรุงเทพมหานคร : ซีเอ็ดยูเคชั่น จำกัด.

ธวัชชัย เลื่อนฉวี และคณะ. 2546. **วงจรดิจิตอล ภาคปฏิบัติ.** กรุงเทพมหานคร : หจก.ภาพพิมพ์.

ธวัชชัย เลื่อนฉวี และอนุรักษ์ เถื่อนศิริ. 2546. **ดิจิตอลเทคนิค.** กรุงเทพมหานคร : มิตรนราการพิมพ์.

ธีรวัฒน์ ประกอบผล. 2545. **ดิจิตอลลอจิก.** กรุงเทพมหานคร : ซีเอ็ดยูเคชั่น จำกัด.

นภัทร วัจนเทพินทร์. 2545. **วงจรดิจิตอล ภาคปฏิบัติ.** กรุงเทพมหานคร : สยามสปอร์ต ซินดิเคท.

บัณฑิต บัวบูชา. 2545. **ทฤษฎีและการออกแบบวงจรดิจิตอล.** กรุงเทพมหานคร : ฟิสิกส์เซ็นเตอร์.