บทที่ 4

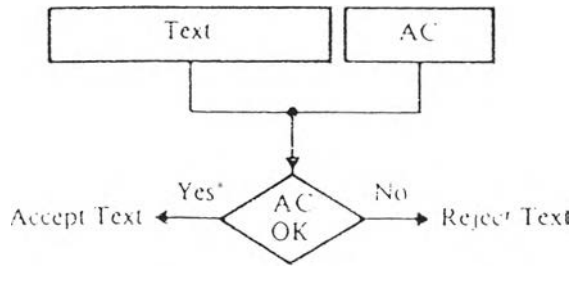
ออเทนทิเคชัน (Authentication)

คำนำบท

ออเทนทิเคชัน คือ กระบวนการที่ใช้สำหรับพิสูจน์ว่าข้อความหรือข้อมูลนั้นเป็นของจริงโดยสมบูรณ์ไม่ใช่ของที่ถูกทำเลียนแบบขึ้นมาหรือของจริงที่ถูกแก้ไขไปบางส่วนโดยปกติแล้วการทำออเทนทิเคชันจะมีหลักการคือ การสร้างรหัสรับรองข้อความขึ้นมาจากข้อความหรือข้อมูลนั้น เพื่อให้ได้เป็นข้อมูลอีกชุดหนึ่งสำหรับไว้ใช้เป็นตัวตรวจสอบ

การรับรองข้อความหรือเมสเสจออเทนทิเคชัน (Message Authentication)

คือการจัดการเกี่ยวกับข้อมูลเพื่อให้แน่ใจว่าข้อความที่ได้รับนั้นเป็นข้อความที่ผู้ส่งต้องการส่งให้เราจริงถ้าหากว่ามีการแก้ไขเปลี่ยนแปลงหรือความผิดพลาดของข้อความเนื่องจากมีผู้ตั้งใจจะเปลี่ยนข้อความสัญญาณรบกวนในสายนำสัญญาณหรือด้วยสาเหตุใดก็ตาม "รหัสรับรองข้อความ" (Message Authentication Code) หรือ MAC หรือ ACต่อท้ายมาด้วย ทางด้านผู้รับเมื่อได้รับข้อความข่าวสารก็จะสร้างรหัสรับรองข้อความนี้ขึ้นมาเปรียบเทียบกับรหัสรับรองข้อความที่ส่งมาถ้าหากว่ามีค่าเท่ากันก็จะถือได้ว่าข้อความข่าวสารนั้นเป็นข้อความที่มาจากแหล่งกำเนิดจริงถ้าหากว่าไม่เท่ากัน ก็แสดงว่าข่าวสารนั้นอาจจะถูกแก้ไขเปลี่ยนแปลงหรือถูกตัดตอนออกไป ดังแสดงในรูป 4.1



รูป 4.1 วิธีตรวจสอบข้อความโดยใช้รหัสรับรองข้อความ [Meyer and Matyas,1982]

รหัสรับรองข้อความที่ดีซึ่งเป็นส่วนสำคัญของการทำการรับรองข้อความควรจะมีลักษณะดังนี้ [Caelli et al.,1989]

1. ฝ่ายตรงข้ามไม่สามารถจะหาฟังก์ชันในการสร้างรหัสรับรองข้อความได้

2. ฝ่ายตรงข้ามไม่สามารถจะคำนวณหาข้อความใหม่ M' ในกรณีที่บังเอิญรหัสรับรองข้อความใหม่ AC' เหมือนกับรหัสรับรองข้อความเดิม AC ไม่เช่นนั้นแล้วฝ่ายตรงข้ามอาจจะแทนที่ข้อความเดิม M ด้วย M' ในขณะที่ยังคงทำให้ AC ไม่เปลี่ยนแปลง

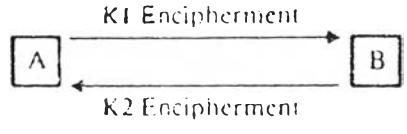
3. รหัสรับรองข้อความ AC ควรจะมีค่าแตกต่างกันในกรณีที่ M = M' โดยความน่าจะเป็น ของการแตกต่างกัน ของ AC คือ $1/2^C$ โดยที่ C คือจำนวนบิตใน AC

การรับรองข้อความคือวิธีการที่เมื่อมีการติดต่อส่งข้อมูลระหว่างฝ่ายรับและฝ่ายส่งจะเป็นตัวแสดงว่าข้อมูลที่ฝ่ายรับได้รับเป็นข้อมูลที่แท้จริงที่ผู้ส่งต้องการส่งให้หน้าที่ของการทำการรับรองข้อความ คือ การทำให้ผู้รับข้อมูลได้ทราบถึง สภาวะต่อไปนี้

1. ข้อมูลหรือข้อความนั้นถูกสร้างขึ้นมาและส่งโดยผู้ใด
2. เนื้อหาของข้อความนั้น ไม่ถูกเปลี่ยนแปลงไปไม่ว่าจะด้วยความตั้งใจหรือบังเอิญ
3. ข้อความถูกส่งไปยังผู้รับที่ผู้ส่งตั้งใจจะส่งไปให้

<u>การแสดงการรับรองการเป็นผู้สร้างข้อความ</u> (Authentication of a Message's origin)

วิธีการที่จะแสดงว่าผู้ใดเป็นผู้สร้างข้อความ (ผู้ส่งข้อความ) 2 วิธี คือ วิธีแรกใช้คีย์ที่แตกต่างกันในการรับและส่งข้อความระหว่างผู้รับและผู้ส่ง ดังรูป 4.2

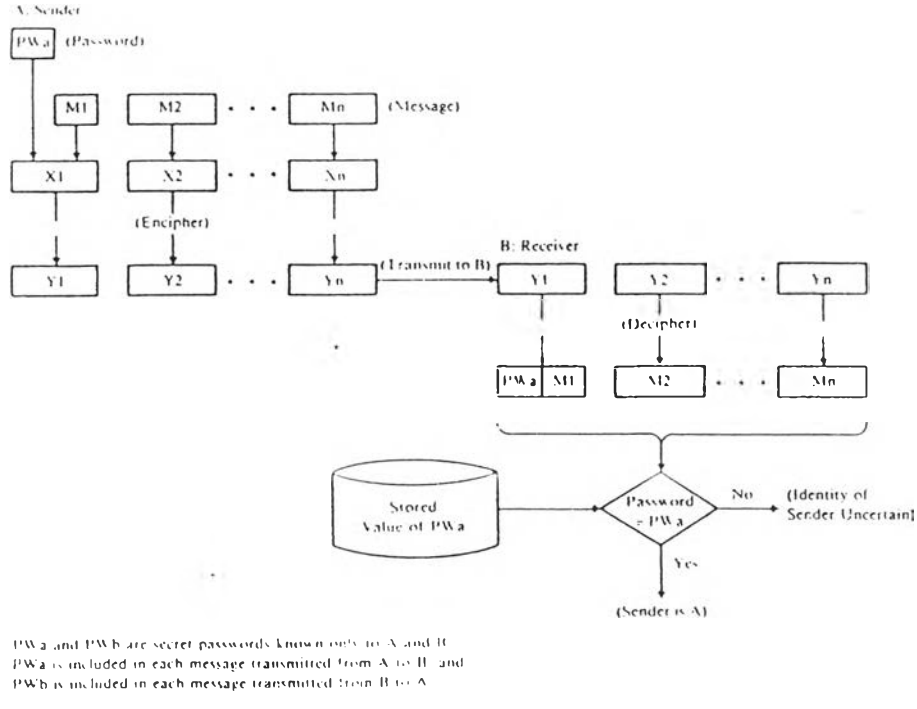


รูป 4.2 การเข้ารหัสโดยใช้คีย์ที่ต่างกัน [Meyer and Matyas,1982]

สมมติว่า A และ B ใช้คีย์ K1 และ K2 โดยที่ K1 ใช้สำหรับส่งจาก A ไป B เท่านั้น และ K2 ใช้สำหรับส่งจาก B ไป A เท่านั้น B จะรู้ว่าข้อความถูกส่งมาจาก A ก็ต่อเมื่อใช้คีย์ K1

ในการถอดรหัสแล้วสามารถอ่านข้อความได้ในทำนองเดียวกันจะสรุปได้ว่าข้อความถูกส่งมาจาก B ถ้าหากว่า A สามารถใช้คีย์ K2 ในการถอดรหัสและอ่าน ข้อความได้

วิธีที่ 2 คือ A และ B ใช้คีย์เดียวกัน ในการรับและส่งข้อความในส่วนต้นของข้อความจะมีรหัสผ่าน (Password)อยู่โดยที่ A และ B จะรู้รหัสผ่านของกันและกันโดยสมมติว่า PW_a และ PW_b เป็นรหัสผ่านของ A และ B ตามลำดับ A จะส่ง PW_a ไปกับข้อความที่จะส่งไป B ทุกครั้ง เมื่อ B ได้รับข้อมูลก็จะตรวจสอบว่ารหัสผ่านที่มากับข้อมูลนั้นตรงกับรหัสผ่านของ A ที่มีอยู่ในฐานข้อมูลหรือไม่ ถ้าตรงกันก็แสดงว่าข้อมูลนั้นถูกส่งมาจาก A ดังแสดงในรูป 4.3



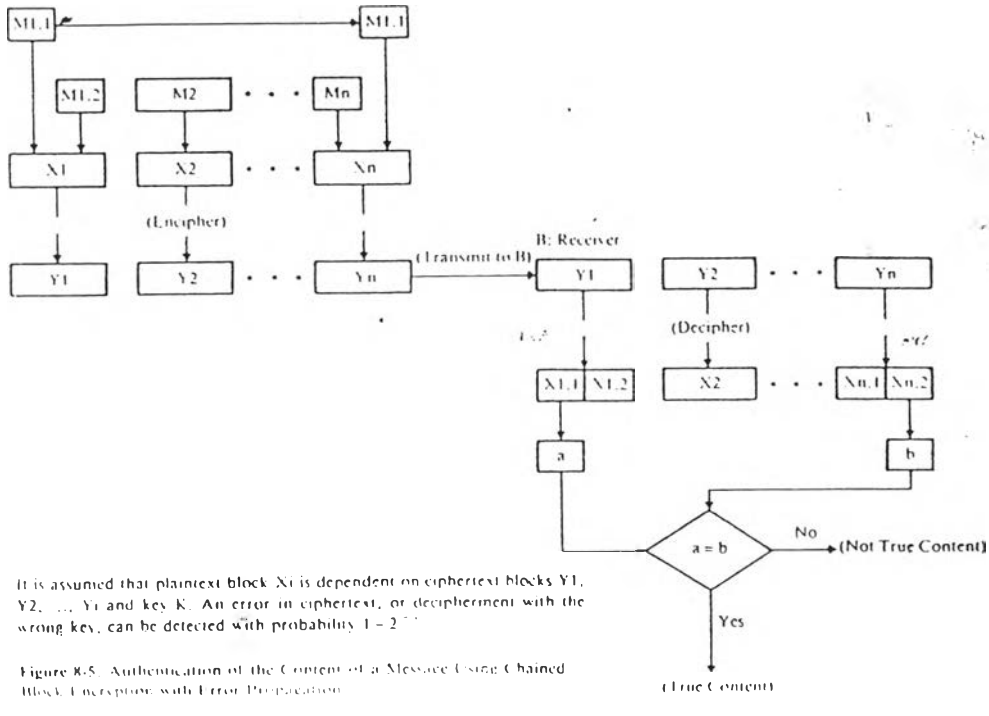
รูป 4.3 แสดงการรับรองการเป็นผู้สร้างข้อความ [Meyer and Matyas,1982]

<u>การแสดงการรับรองความถูกต้องของเนื้อหาของข้อความ</u>(Authentication of Message's Content)

เนื้อหาของข้อความจะถูกพิสูจน์ว่าถูกต้องหรือไม่จากสิ่งที่เราเรียกว่า รหัสรับรองข้อความหรือ MAC ซึ่งถูกสร้างขึ้นมาจากผู้ส่งและต่อท้ายเข้าไปยังข้อความก่อนที่จะส่งมาให้ผู้รับ ซึ่งมี 2 วิธีคือ

1. รับรองความถูกต้องของเนื้อหาของข้อความโดยวิธีการเข้ารหัสที่มีคุณสมบัติของการแพร่กระจายความผิดพลาด

การรับรองความถูกต้องของเนื้อหาของข้อความจะไม่ยุ่งยากมากนักถ้าหากว่าเราใช้วิธีการเข้ารหัสที่มีคุณสมบัติของการแพร่กระจายความผิดพลาดเช่นการใช้วิธีการเข้ารหัสที่เป็นแบบบล็อคเชนนิ่งเพลนเท็กซ์ ไซเฟอร์เท็กซ์ฟีดแบ็ค (ดังรูป 3.12) เป็นตัวอย่างหนึ่งที่ใช้สำหรับงานนี้วิธีการคือการต่อท้ายข้อความที่จะส่งด้วยข้อความชุดหนึ่งที่รู้กันทั้งผู้ส่งและผู้รับ (เช่น เวกเตอร์เริ่มต้นหรือบล็อกแรกของข้อความนั้น X(i) ก่อนจะทำการเข้ารหัส หลังจากถอดรหัสแล้วเราจะตรวจสอบความถูกต้องของข้อความได้โดยการเปรียบเทียบส่วนที่ต่อท้ายเข้าไปนี้ระหว่าง ด้านรับและด้านส่งถ้าหากว่ามีค่าเท่ากันแสดงว่าข้อความถูกต้องแต่ถ้าไม่ตรงกันแสดงว่ามีข้อผิดพลาดขึ้นในข้อความนั้นสมมติว่าข้อความที่นำมาต่อท้ายมีขนาด C บิต โอกาสในการที่จะพิสูจน์ได้ว่าข้อความนั้นถูกต้องหรือไม่มีถึง $(2^c-1)/2^c = 1-2^{c-1}$ รูป 4.4 แสดงให้เห็นว่าข้อความ C บิตแรกถูกต่อเข้าข้างท้ายของข้อความนั้นเมื่อผ่านการเข้ารหัสข้อความCบิตนี้จะเป็นรหัสรับรองข้อความถ้าหากว่าเกิดความผิดพลาดขึ้นกับไซเฟอร์เท็กซ์ เพลนเท็กซ์ที่ถอดรหัสออกมาได้ (หลังจากจุดที่เกิดความผิดพลาด) ก็จะมีความผิดพลาดด้วยในกรณีนี้ C บิตแรกของข้อความเพลนเท็กซ์ที่ถูกถอดรหัสกลับมาจะมีค่าแตกต่างจากCบิทสุดท้ายโดยมีความน่าจะเป็นของการแตกต่างกันเท่ากับ$1-2^{c-1}$



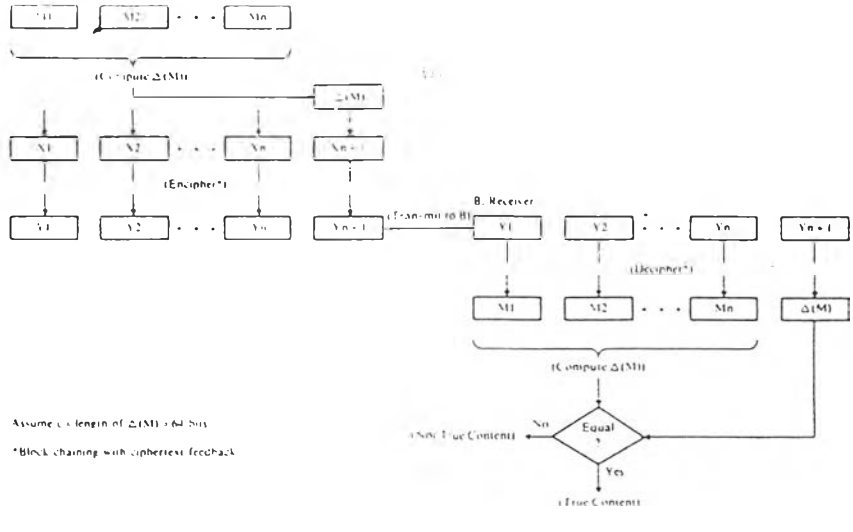
It is assumed that plaintext block Xi is dependent on ciphertext blocks Y1, Y2, ..., Yi and key K. An error in ciphertext, or decipherment with the wrong key, can be detected with probability $1 - 2^{-c}$.

Figure 8-5. Authentication of the Content of a Message Using Chained Block Encryption with Error Propagation

รูป 4.4 แสดงวิธีการรับรองความถูกต้องของเนื้อหาข้อความ
[Meyer and Matyas,1982]

2. การรับรองความถูกต้องของเนื้อหาของข้อความโดยวิธีการเข้ารหัสที่ไม่มีคุณสมบัติของการกระจายความผิดพลาด

ถ้าวิธีการเข้ารหัสที่เราใช้ไม่มีคุณสมบัติของการกระจายความผิดพลาด(ตัวอย่างเช่น ไซเฟอร์บล็อคเชนนิ่งCBCในรูปที่3.13)แล้ว การเปลี่ยนแปลงของไซเฟอร์เท็กซ์อาจจะไม่ทำให้บล็อคสุดท้ายของเพลนเท็กซ์ที่ถูกถอดรหัสกลับมาเปลี่ยนแปลงไปก็ได้ในกรณีเช่นนี้การพิสูจน์ความถูกต้องของเนื้อหาของข้อความจะแตกต่างไปหัวข้อก่อนหน้านี้เล็กน้อยเนื่องจากความผิดพลาดในไซเฟอร์เท็กซ์บล็อคใด ๆ ไม่ทำให้เกิดการแพร่กระจายความผิดพลาดในเพลนเท็กซ์ที่ถูกรหัสกลับมาแต่จะเกิดความผิดพลาดเฉพาะบล็อคนั้นแทนดังนั้นรูปแบบของของบิตที่จะนำไปต่อท้ายข้อความ จะต้องขึ้นอยู่กับข้อความทั้งหมดหรือเป็นฟังก์ชัน Δของข้อความทั้งหมด (ไม่ใช่เฉพาะส่วนใดส่วนหนึ่งของข้อความ) จะทำการแปลงข้อความ M ที่มีความยาว ขนาดเท่าไรก็แล้วแต่เป็นข้อความที่มีขนาดเล็กมีจำนวนบิตที่แน่นอนและโอกาสที่ข้อความ M และ M′ ที่ต่างกันซึ่งมีบิตที่จะทำให้เกิดบิตที่จะต่อท้ายข้อความ Δ(M) และ Δ(M)′ ที่ต่างกันมีความน่าจะเป็นสูงการเข้ารหัส Δ(M) นี้จะทำให้เกิดเป็นรหัสรับรองข้อความขึ้น วิธีการแสดงการรับรองความถูกต้องของเนื้อหาของข้อความนี้แสดงดังในรูปที่ 4.5



รูป 4.5 แสดงวิธีการรับรองความถูกต้องของเนื้อหาข้อความที่รหัสรับรองความถูกต้องถูกสร้างภายใต้คีย์ที่รู้เฉพาะผู้ส่งและผู้รับ [Meyer and Matyas,1982]

การแสดงการรับรองผู้รับข้อความ(Authentication of Message's Receiver)

การที่จะระบุว่าผู้รับรายใดคือผู้ที่ส่งตั้งใจจะส่งข้อความไปให้นั้นจะมีวิธีการคล้ายกับการรับรองว่าผู้ใดเป็นผู้สร้างข้อมูลดังได้กล่าวถึงแล้วในหัวข้อก่อนหน้านี้ซึ่งก็จะขอกล่าวโดยสรุปเป็นข้อๆได้ดังนี้ สมมติว่า A และ B คือผู้ส่งและผู้รับข้อความตามลำดับB จะสามารถรู้ว่าข้อความดังกล่าวถูกส่งมาให้ตัวเองจริงถ้าใช้วิธีการข้อใดข้อหนึ่งดังต่อไปนี้

1. A และ B ใช้คีย์ 2 คีย์โดยที่ทั้ง A และ B รู้คีย์ทั้งคู่โดยคีย์หนึ่งใช้สำหรับเข้ารหัสข้อมูลและส่งจาก A ไป B อีกคีย์หนึ่ง B ใช้เข้ารหัสข้อมูลแล้วส่งไปให้ A

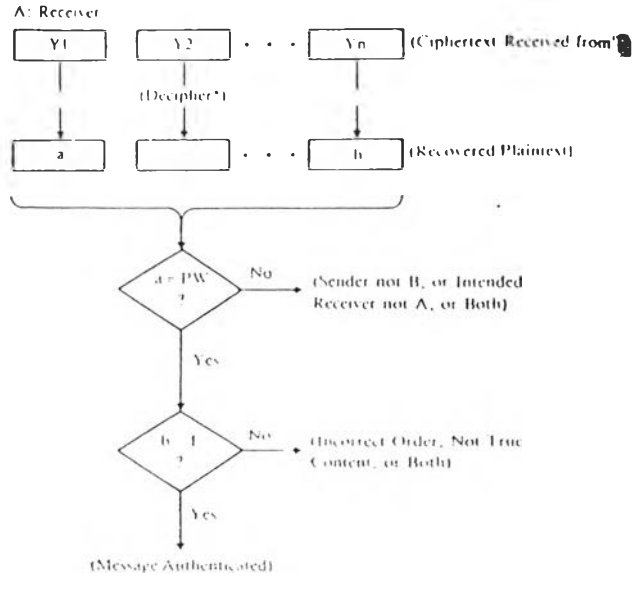
2. Aและ B ใช้คีย์เดียวกันในการเข้ารหัสและส่งข้อมูลสู่กันและกัน แต่ส่งรหัสประจำตัว ของผู้รับลงไปในข้อความด้วย

วิธีการสำหรับการทำการรับรองข้อความ

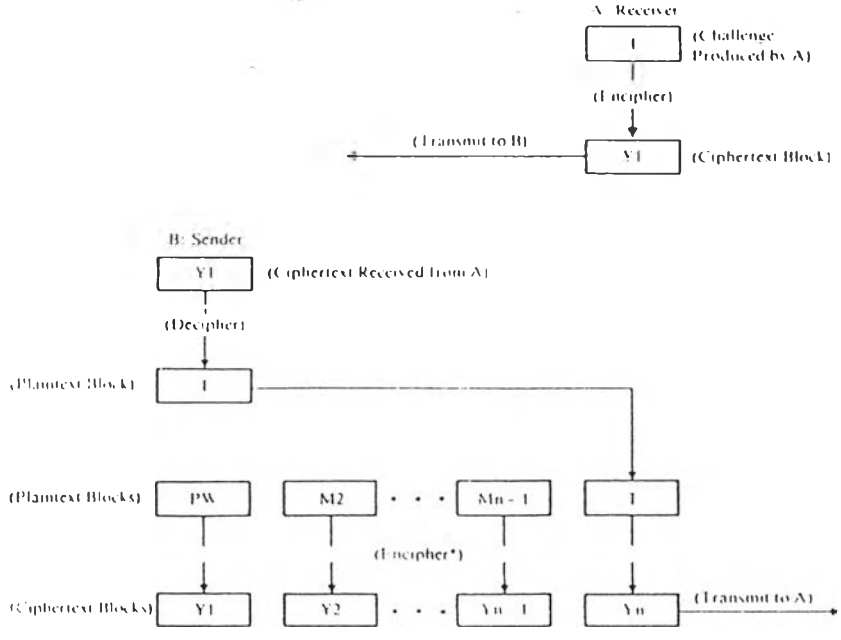
จากการแสดงการรับรองของส่วนต่างๆของข้อความตามที่ได้กล่าวมาแล้วนั้นจะนำทั้งหมดมารวมเป็นวิธีหรือขั้นตอนที่ใช้ในการรับรองข้อความตามรูปที่ 4.6 ซึ่งมีคุณลักษณะดังนี้

1.ใช้วิธีการเข้ารหัสที่มีคุณสมบัติของการกระจายของความผิดพลาดในการรับรองเนื้อหาของข้อความ

2. ใช้รหัสผ่านเพื่อแสดงว่าผู้ใดเป็นผู้รับหรือผู้ส่ง



รูป 4.6 วิธีการสำหรับการทำการรับรองข้อความ [Meyer and Matyas,1982]



รูป 4.6 (ต่อ) วิธีการสำหรับการทำการรับรองข้อความ
[Meyer and Matyas,1982]

จากวิธีการตามรูป 4.6ที่กล่าวมานี้เป็นตัวอย่างหนึ่งของวิธีการรับรองข้อความที่มีคุณสมบัติครบทั้ง 3 ข้อ (ผู้ส่ง ,เนื้อหา , ผู้รับ) แต่อย่างไรก็ตามในการประยุกต์ใช้งานบางงานเราไม่จำเป็นต้องสร้างวิธีรับรองข้อความให้มีคุณสมบัติครบทั้ง3ข้อดังกล่าวก็ได้เพียงแต่ให้มีคุณสมบัติข้อใดข้อหนึ่งเหมาะสมกับงานนั้นๆ ก็เพียงพอซึ่งก็จะได้กล่าวถึงวิธีการที่ใช้ในการรับรองข้อความที่ใช้ในวิทยานิพนธ์ฉบับนี้ในบทต่อไป