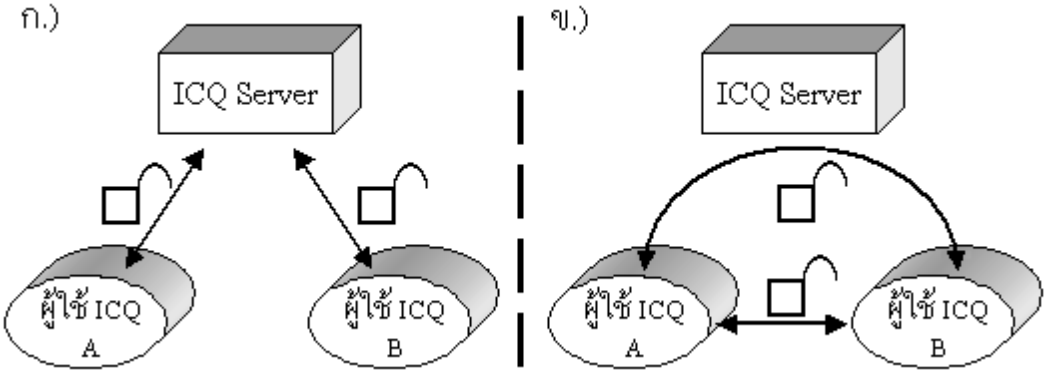
บทที่ 6
การออกแบบและพัฒนาโครงงาน

6.1 แนวคิดและการออกแบบความสามารถของโปรแกรม

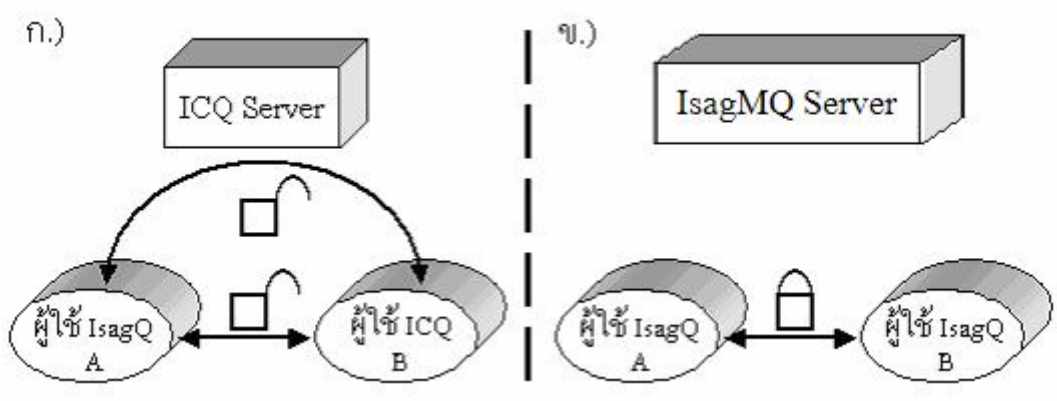
โครงงานนี้จะมุ่งเน้นถึงการปรับปรุงโปรแกรมรับส่งสารด่วนให้มีความปลอดภัยมากขึ้น โดยใช้การเข้าและถอดรหัสข้อมูลสารที่ต้องการรับส่ง

ในโปรแกรม ICQ จะมีขั้นตอนในการใช้งานคือ โปรแกรมฝั่งไคลเอ็นต์จะทำการติดต่อไปยังเซิร์ฟเวอร์ของ ICQ เพื่อขอใช้บริการตามรูปที่ 6.1 ก.) ซึ่งเซิร์ฟเวอร์ของ ICQ จะให้บริการโดยส่งค่ารายการของผู้ใช้ที่มีการติดต่อระหว่างกันกลับมาให้ผู้ใช้ที่ร้องขอไป จากนั้นจะเข้าสู่ขั้นตอนในรูป 6.1 ข.) ซึ่งเป็นการทำงานของผู้ใช้ที่มีการติดต่อกัน ซึ่งสามารถทำได้ 2 รูปแบบคือ การทำงานผ่านทางเซิร์ฟเวอร์ของ ICQ และการทำงานระหว่างกันโดยตรง



รูปที่ 6.1 รูปแบบการติดต่อในโปรแกรม ICQ

จากการทำงานในโปรแกรมไคลเอ็นต์ของ ICQ จะพบว่าการสื่อสารระหว่างกันโดยตรงในรูปที่ 6.1 ข.) จะไม่มีการเข้า-ถอดรหัสข้อมูลสารที่ทำการรับส่ง ทำให้การรับส่งสารระหว่างผู้ใช้งานโดยตรงไม่ปลอดภัย ดังนั้นในการรับส่งสารระหว่างผู้ใช้งานโดยตรงในโปรแกรม IsagQ จะมี 2 รูปแบบคือการรับส่งสารโดยไม่มีการเข้าและถอดรหัสข้อมูลซึ่งจะใช้งานเมื่อผู้รับใช้งานโปรแกรม ICQ ดังรูปที่ 6.2 ก.) และการรับส่งสารโดยมีการเข้าและถอดรหัสข้อมูลซึ่งใช้เมื่อผู้รับใช้งานโปรแกรม IsagQ ดังรูปที่ 6.2 ข.)

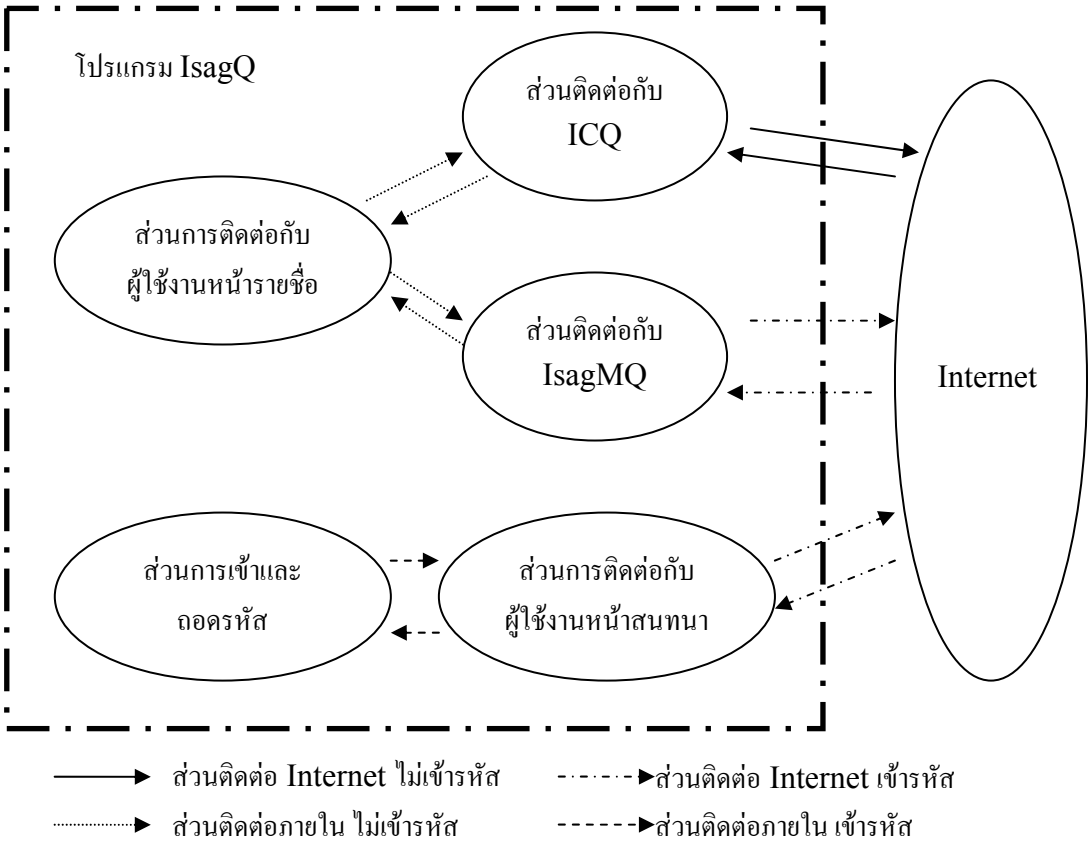


รูปที่ 6.2 รูปแบบการสื่อสารโดยตรงในโปรแกรม IsagQ

6.2 ส่วนประกอบของโปรแกรม

ในโครงงานนี้ได้แบ่งส่วนประกอบของโปรแกรม IsagQ ออกเป็น 3 ส่วนหลักๆ คือ

1. ส่วนการติดต่อกับผู้ใช้งานหน้ารายชื่อ
2. ส่วนการติดต่อกับผู้ใช้งานหน้าสนทนา
3. ส่วนการติดต่อกับICQ
4. ส่วนการติดต่อกับIsagMQ
5. ส่วนการเข้า-ถอดรหัสข้อมูล



รูปที่ 6.3 ส่วนประกอบในการทำงานของโปรแกรม IsagQ

6.2.1 ส่วนการติดต่อกับผู้ใช้งานหน้ารายชื่อ

ส่วนการติดต่อกับผู้ใช้งานเป็นส่วนที่ใช้รับคำสั่งและข้อมูลจากผู้ใช้งาน ซึ่งหากเราต้องการส่งสารโดยการเข้ารหัสข้อมูลไปยังผู้ใช้งานโปรแกรม IsagQ ส่วนการติดต่อกับผู้ใช้งานหน้ารายชื่อจะสร้างส่วนการติดต่อกับผู้ใช้งานหน้าสนทนาขึ้นมาแล้วจึงส่งข้อความผ่านหน้านั้น แต่หากต้องการส่งข้อมูลไปยังผู้ใช้งานโปรแกรม ICQ ส่วนการติดต่อกับผู้ใช้งานจะทำการส่งสารไปยังส่วนการติดต่อกับICQได้ทันที

6.2.2 ส่วนการติดต่อกับผู้ใช้งานหน้าสนทนา

หลังจากส่วนการติดต่อกับผู้ใช้งานหน้าสนทนาขึ้นมา ระบบจะติดต่อกับคู่สนทนาที่เราต้องการ โดย 1 หน้าจะสามารถติดต่อได้ 1 คน โดยการส่งข้อความนั้นจะถูกนำไปเข้ารหัสที่ส่วนการเข้า-ถอดรหัสข้อมูลก่อนที่จะถูกส่งออกไป

6.2.3 ส่วนการเข้า-ถอดรหัสข้อมูล

ในส่วนการเข้า-ถอดรหัสข้อมูลจะใช้งานเฉพาะการสื่อสารโดยตรงกับผู้ใช้งานโปรแกรม IsagQ เท่านั้น โดยเมื่อผู้ส่งต้องการส่งสารที่ต้องการความปลอดภัยไปยังผู้รับซึ่งใช้โปรแกรม IsagQ สารของผู้ส่งจากส่วนการติดต่อกับผู้ใช้งานหน้าสนทนาจะถูกส่งมายังส่วนการเข้า-ถอดรหัสข้อมูลเพื่อทำการเข้ารหัสข้อมูลสาร จากนั้นสารที่ถูกเข้ารหัสจะถูกส่งกลับเพื่อส่งผ่านอินเตอร์เน็ตไปยังส่วนการติดต่อกับผู้ใช้หน้าสนทนาฝั่งผู้รับ เมื่อผู้รับซึ่งใช้โปรแกรม IsagQ ได้รับสารที่มีการเข้ารหัส ส่วนการติดต่อกับผู้ใช้หน้าสนทนาฝั่งผู้รับจะส่งสารนั้นมายังส่วนการเข้า-ถอดรหัสข้อมูลเพื่อทำการถอดรหัส แล้วจึงส่งกลับมาส่วนการติดต่อกับผู้ใช้หน้าสนทนาฝั่งผู้รับเพื่อแสดงข้อความ ซึ่งทำให้สารในการสนทนาสามารถอ่านได้เฉพาะผู้รับและผู้ส่งเท่านั้น

6.2.4 ส่วนติดต่อกับICQ

ในการเข้าสู่ระบบ ICQ และการส่งข้อความไปยังผู้ใช้ ICQ คนอื่นๆนั้น จะต้องติดต่อผ่านส่วนติดต่อกับICQ โดยส่วนนี้จะส่งข้อความไปยัง ICQ Server และผู้ใช้ ICQ คนอื่นๆโดยไม่มีการเข้ารหัส

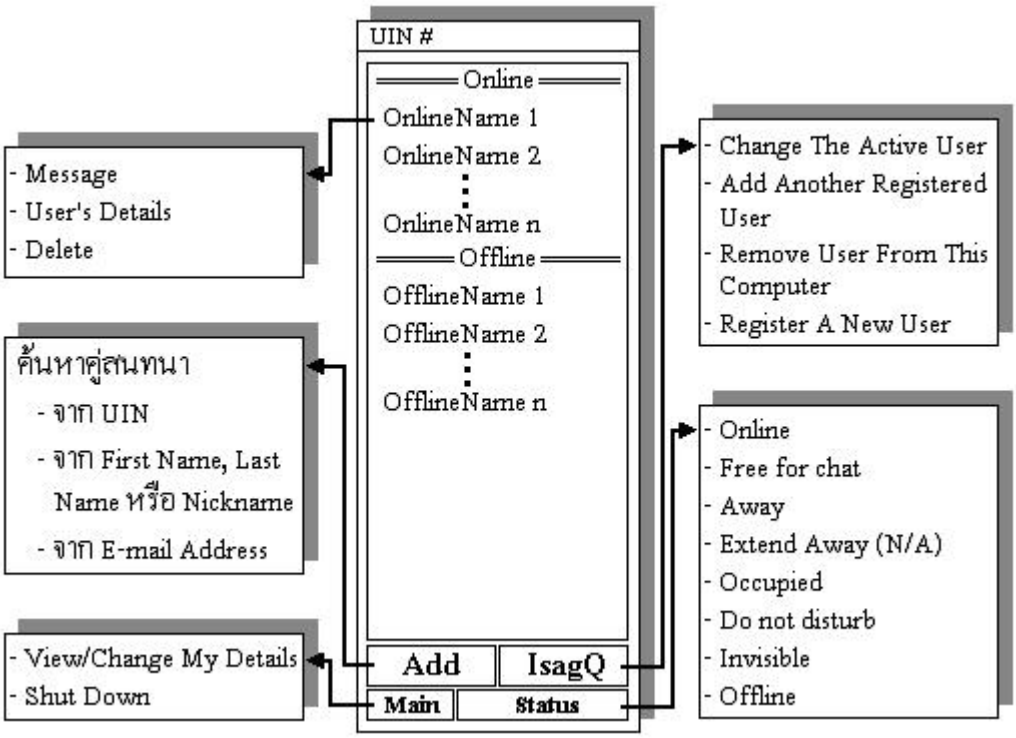
6.2.5 ส่วนติดต่อกับ IsagMQ

ใช้ในการเข้าสู่ระบบของ IsagMQ เพื่อดึง contact list และกระทำการอื่นๆกับ IsagMQ Server เช่น ลบชื่อผู้ใช้งานขอตัวเอง สร้างชื่อผู้ใช้งานใหม่ เป็นต้น โดยส่วนนี้จะรวมส่วนการเข้ารหัสด้วย SSL เข้าไปด้วย

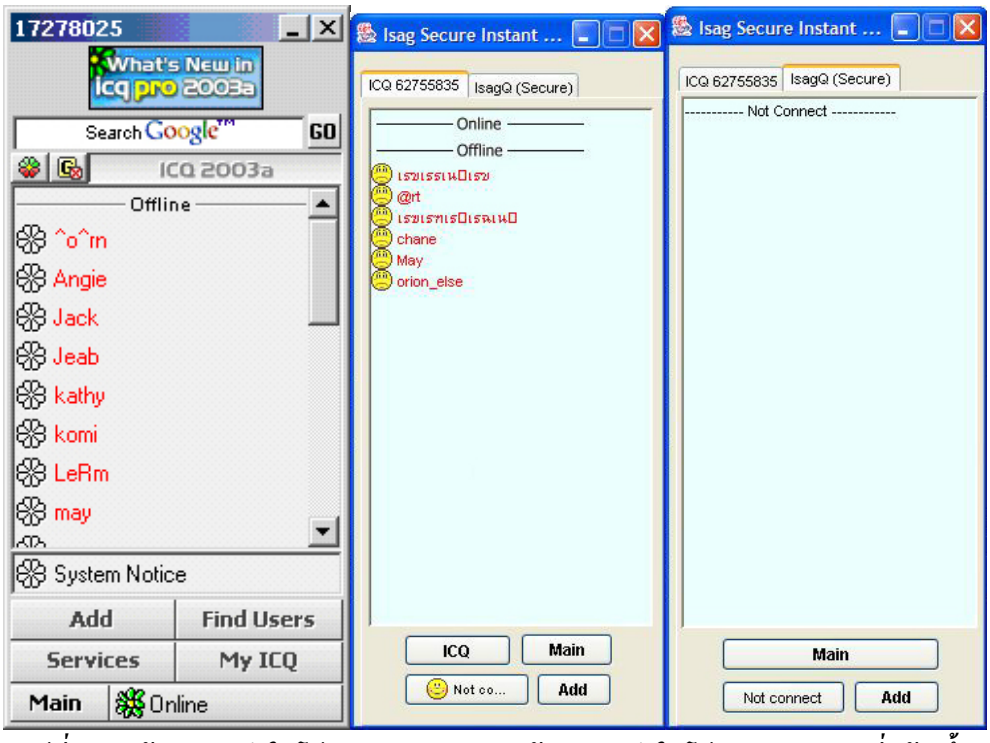
6.3 การออกแบบและสร้างส่วนการติดต่อกับผู้ใช้งาน

ในการออกแบบส่วนการติดต่อกับผู้ใช้งานจะใช้โครงสร้างโปรแกรม ICQ เป็นต้นแบบ เพื่อให้ผู้งานสามารถใช้งานได้ง่ายเหมือนกับโปรแกรม ICQ แต่โปรแกรม IsagQ ได้ทำการลดฟังก์ชันการทำงาน

บางอย่างที่ไม่ค่อยได้ใช้งานออก และเพิ่มหน้าสำหรับแสดงรายชื่อของผู้ใช้งาน IsagQ ซึ่งในการติดต่อกันโดยตรงนั้นจะใช้การเข้ารหัสข้อมูลแบบ DES เพื่อความปลอดภัยของผู้ใช้งาน



รูปที่ 6.4 การออกแบบหน้าจอสำหรับติดต่อกับผู้ใช้งานในโปรแกรม IsagQ ส่วนแสดงรายชื่อของ ICQ



รูปที่ 6.5 หน้าจอกราฟิกในโปรแกรม ICQ และหน้าจอกราฟิกในโปรแกรม IsagQ ที่สร้างขึ้น

เมื่อได้ทำการออกแบบโครงสร้างส่วนของการติดต่อกับผู้ใช้งานแล้ว เราได้ทำการสร้างโดยใช้ภาษาจาวาซึ่งการสร้างโปรแกรมจะใช้ class library ของจาวาที่ให้มาคือ java.swing.*; เป็นส่วนมาก ซึ่งทำให้มีลักษณะคล้ายกับโปรแกรม ICQ เพื่อสะดวกของผู้ใช้งาน และสามารถแสดงผลได้เหมือนกันในทุกแพลตฟอร์มที่สนับสนุน JVM ในรูปที่ 6.5 จะแสดงหน้าจอกราฟิกในส่วนการติดต่อกับผู้ใช้งานที่ได้สร้างขึ้นจากภาษาจาวา แต่จากรูปแรกจะเห็นว่ายังไม่มีการเข้าใช้งานของผู้ใช้ที่มีความปลอดภัย ซึ่งในส่วนนี้ก็จะยังไม่มีการแสดงชื่อใดๆ นอกจากการออนไลน์แบบธรรมดาและการออฟไลน์ รูปต่อมาจะเป็นรูปหน้าจอกราฟิกของ IsagQ ในหน้ารายชื่อของ ICQ ในกรณีที่มีการเรียกให้ใช้งาน ส่วนรูปทางขวาสุดคือรูปหน้าจอกราฟิกของ IsagQ ในหน้ารายชื่อของ IsagQ ในกรณีที่ไม่มีการเรียกให้ใช้งาน

6.4 การติดต่อเครือข่ายอินเทอร์เน็ต

ในการเขียนโปรแกรมสำหรับติดต่อเครือข่ายอินเทอร์เน็ต จะเริ่มจากการเขียนโปรแกรมเพื่อทำการติดต่อขอใช้บริการจากเซิร์ฟเวอร์ ซึ่งจะต้องแก้ไขและปรับปรุงการทำงานอย่างต่อเนื่องไปโดยเริ่มที่การล็อกอินเพื่อขอเข้าใช้บริการ การเรียกขอรายการคอนแทคลิสต์ การร้องขอข้อมูลรายการผู้ใช้งานที่ทำการออนไลน์จากเซิร์ฟเวอร์ การเปลี่ยนแปลงสถานะ การส่งข้อความผ่านทางเซิร์ฟเวอร์ การค้นหาคู่สนทนา การเรียกขอดูข้อมูลของคู่สนทนาเป็นต้น ซึ่งสามารถดูรายละเอียดคำสั่งได้จากบทที่ 5

6.5 การสร้างคีย์สำหรับทำการเข้ารหัสข้อมูล

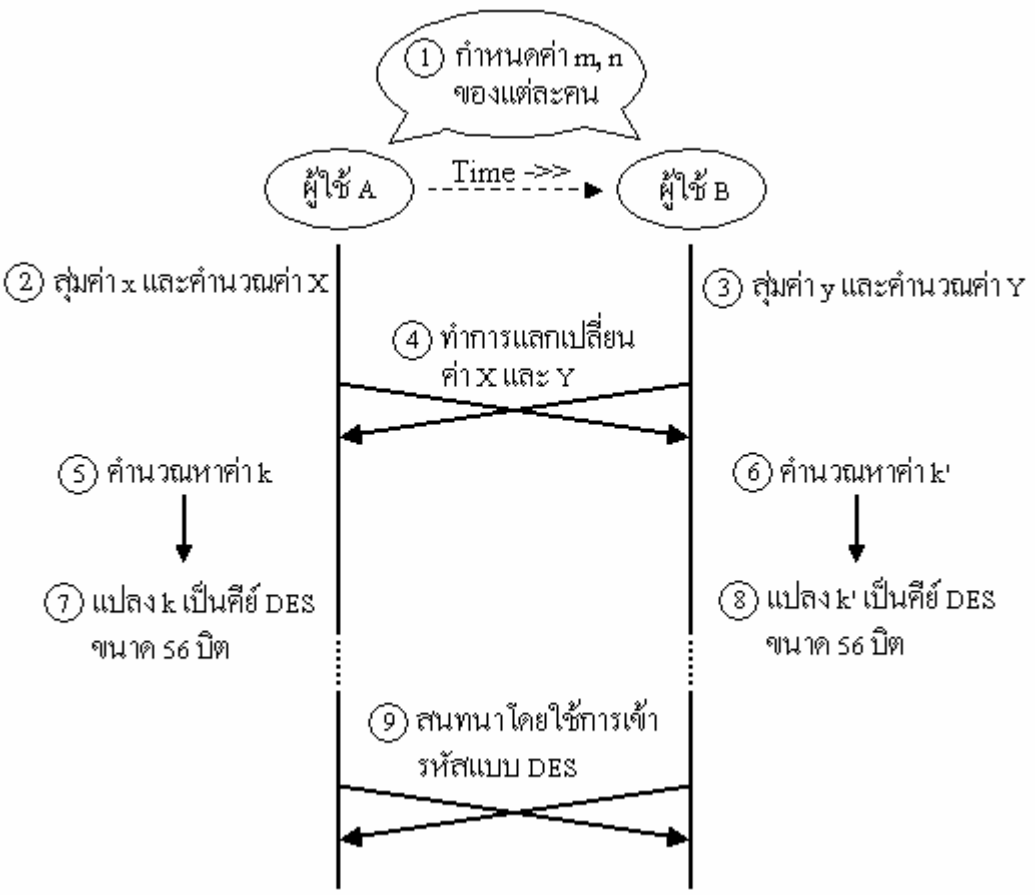
เมื่อผู้ใช้งานโปรแกรม IsagQ ทำการออนไลน์จะต้องทำการสร้างคีย์ความลับระหว่างกัน โดยในโครงงานนี้จะใช้วิธี Deffie-Hellman ในการสร้างคีย์ความลับแล้วนำค่าคีย์ที่ได้มาแปลงเป็นคีย์ DES ขนาด 64 บิต และใช้คีย์ที่ได้นี้ทำการเข้ารหัสข้อความที่ต้องการรับส่งระหว่างกัน ทำให้ผู้ใช้งานโปรแกรม IsagQ ทั้งสองฝั่งสามารถทำการรับส่งสารได้อย่างปลอดภัย

ลำดับขั้นตอนในการรับส่งคีย์ต่อไปนี้จะแสดงถึงเหตุการณ์ที่ผู้ใช้ A และผู้ใช้ B ซึ่งเป็นผู้ใช้งานโปรแกรม IsagQ ทำการสร้างคีย์ DES ด้วยวิธี Deffie-Hellman เพื่อทำการรับส่งสารได้อย่างปลอดภัย ซึ่งมีขั้นตอนต่อไปนี้

1. ผู้ใช้ A และผู้ใช้ B ทำการกำหนดค่า m และ n ของแต่ละผู้ใช้โดยที่ $1 < n < m$ โดยเลขทั้งสองนี้ไม่จำเป็นต้องปกปิด
2. ผู้ใช้ A สุ่มตัวเลขที่มีค่ามากๆ มาตัวหนึ่งกำหนดให้เป็นค่า x แล้วหาค่า $X = n^x \bmod m$ และให้ผู้ใช้ A เก็บค่า x เอาไว้เป็นความลับ
3. ให้ผู้ใช้ B ทำเหมือนกับผู้ใช้ A ในข้อ 2 สุ่มตัวเลขที่มีค่ามากๆ มาตัวหนึ่งกำหนดให้เป็นค่า y แล้วหาค่า $Y = n^y \bmod m$ และให้ผู้ใช้ B เก็บค่า y เป็นความลับ
4. ให้ผู้ใช้ A และผู้ใช้ B ทำการแลกค่า X และ Y กัน
5. ผู้ใช้ A คำนวณหาค่า $k = Y^x \bmod m$
6. ผู้ใช้ B คำนวณหาค่า $k' = X^y \bmod m$
7. ผู้ใช้ A ทำการแปลงค่า k ที่คำนวณได้ให้เป็นค่าขนาด 56 บิต

8. ผู้ใช้ B ทำการแปลงค่า k' ที่คำนวณได้ให้เป็นค่าขนาด 56 บิต ซึ่งค่าคีย์ซึ่งแปลงจากค่า k ของผู้ใช้ A และค่าคีย์ซึ่งแปลงจากค่า k' ของผู้ใช้ B จะมีค่าเท่ากัน ซึ่งสามารถนำค่าที่ได้มาเป็นคีย์ในการเข้ารหัสแบบ DES ในการสนทนา
9. ผู้ใช้ A และผู้ใช้ B ทำการสนทนาโดยการใช้คีย์ DES ที่แปลงมาจากค่า k และ k' ซึ่งมีค่าเท่ากันคือ n^{xy} mod m ใช้เป็นคีย์ความลับในการสนทนาระหว่างกัน

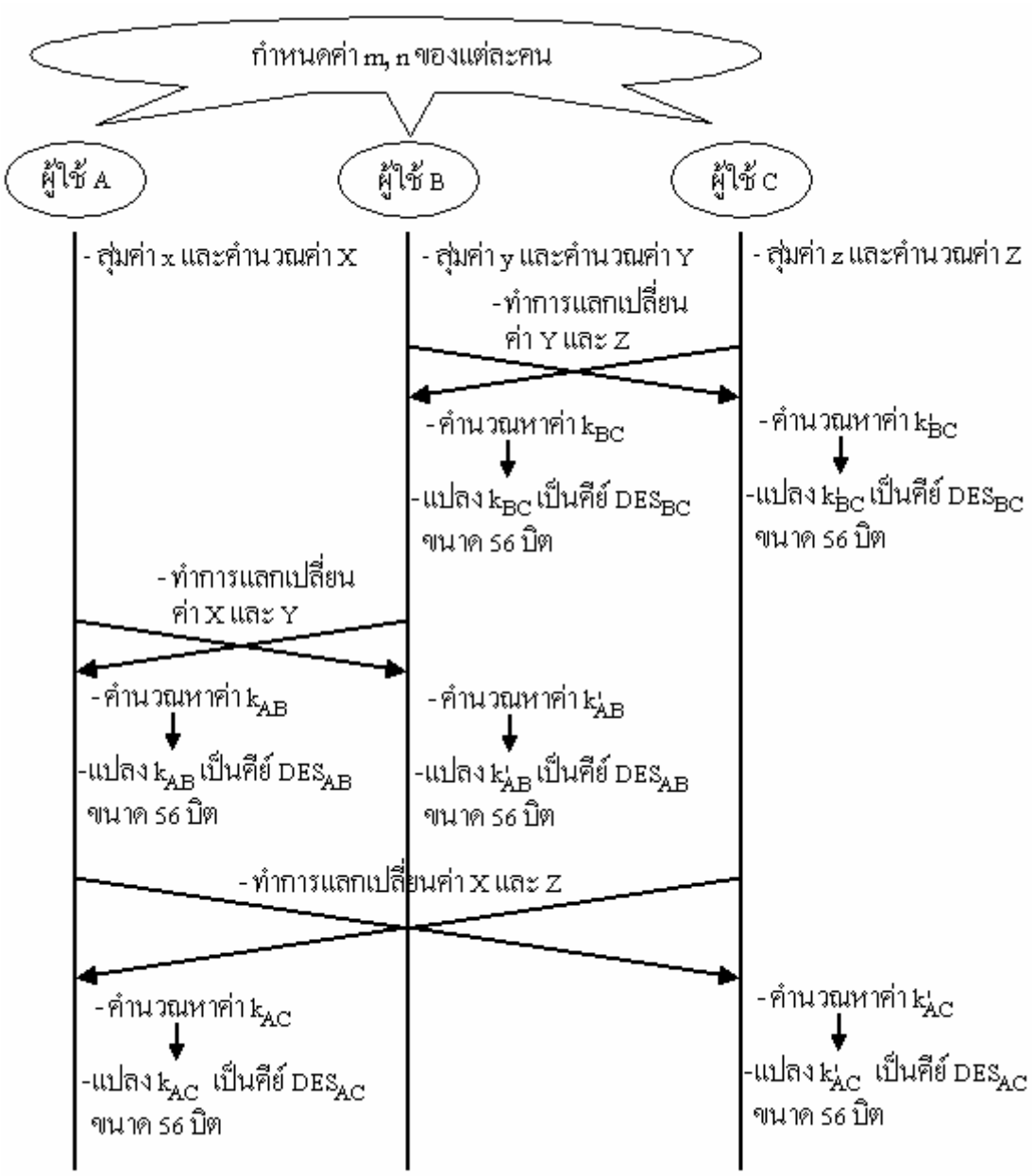
จากการทำงานดังกล่าวนี้จะเกิดขึ้นทุกครั้งเมื่อผู้ใช้งานโปรแกรม IsagQ ทำการออนไลน์ และหากผู้ใช้งานผู้อื่นซึ่งใช้โปรแกรม ICQ ก็จะไม่ต้องทำการรับส่งคีย์นี้ สามารถทำการรับส่งสารโดยตรงได้ทันที แต่การรับส่งสารจะไม่ปลอดภัย



รูปที่ 6.6 ขั้นตอนในการสร้างคีย์ความลับสำหรับสนทนาระหว่างผู้ใช้โปรแกรม IsagQ

จากการรับส่งคีย์ดังกล่าวที่ได้ออกแบบนี้ โปรแกรม IsagQ จะต้องทำการสร้างคีย์สำหรับสนทนาระหว่างผู้ใช้งานใหม่ทุกครั้งเมื่อผู้ใช้งานโปรแกรม IsagQ ทำการออนไลน์ ซึ่งการสร้างคีย์ความลับขึ้นมาใหม่นี้จะทำให้การสนทนาเป็นความลับระหว่างผู้ใช้งานเพียง 2 คนเท่านั้น

การรับส่งคีย์ในรูปที่ 6.7 จะเป็นการแสดงการสร้างคีย์เมื่อผู้ใช้ A, B และ C ต้องการสนทนาระหว่างกัน ซึ่งในการใช้งานจริงนั้นจะต้องมีคีย์ความลับ 3 คู่คือ คีย์ระหว่าง A กับ B, คีย์ระหว่าง A กับ C และคีย์ระหว่าง B กับ C เพื่อให้การสนทนานั้นเป็นความลับระหว่างผู้ใช้งาน 2 คน



รูปที่ 6.7 การสร้างคีย์ความลับเมื่อมีผู้ใช้งานโปรแกรม IsagQ หลายคน

6.6 การรวมส่วนประกอบของโปรแกรมเข้าด้วยกัน

เมื่อสามารถเขียนโปรแกรมพื้นฐานได้ครบทั้งห้าส่วนแล้ว ก็จะนำมาทดลองใช้งาน โดยจะเริ่มจากการนำส่วนการติดต่อกับผู้ใช้งานหน้ารายชื่อกับส่วนติดต่อ ICQ และส่วนติดต่อ IsagQ มารวมกันก่อน ซึ่งจะต้องปรับปรุงให้ส่วนการติดต่อกับผู้ใช้งานหน้ารายชื่อติดต่อกับเครือข่ายอินเทอร์เน็ตผ่านทางส่วนติดต่อ ICQ และ IsagQ ได้ จากนั้นจึงทำการทดลองใช้คำสั่งต่างๆ ตามที่ได้ออกแบบกับเซิร์ฟเวอร์เช่น การล็อกอินเพื่อขอเข้าใช้บริการ การเรียกขอรายการคอนแทคลิสต์ การร้องขอข้อมูลรายการผู้ใช้งานที่ทำการออนไลน์จากเซิร์ฟเวอร์ การเปลี่ยนแปลงสถานะ การค้นหาคู่สนทนา การเรียกขอดูข้อมูลของคู่สนทนา เป็นต้น

จากนั้นจึงทำการเขียนโปรแกรมการรับส่งสารผ่านทางเซิร์ฟเวอร์และการรับส่งสารโดยตรง ซึ่งในส่วนนี้จะทำให้ได้โปรแกรมที่มีลักษณะการทำงานเหมือนกับโปรแกรม ICQ สามารถสนทนากับผู้ใช้งานโปรแกรม ICQ ได้

เมื่อรวมการทำงานในส่วนการติดต่อกับผู้ใช้งานหน้ารายชื่อและส่วนติดต่อ ICQ กับ IsagQ เข้ากันได้แล้ว จะนำส่วนการติดต่อกับผู้ใช้งานหน้าสนทนากับส่วนการเข้า-ถอดรหัสข้อมูลเข้ามารวมกับโปรแกรมในข้างต้น โดยในขั้นตอนนี้จะต้องทดลองโดยมีผู้ใช้งานโปรแกรม IsagQ อย่างน้อย 2 คนทำการออนไลน์และต่างมีรายชื่อของอีกคนหนึ่งอยู่ใน contact list จากนั้นจึงทำการทดลองการสร้างคีย์ของโปรแกรมตามลักษณะที่ได้กล่าวมาแล้ว เมื่อสามารถทำการสร้างคีย์ได้แล้ว จึงทดลองนำสารที่ต้องการส่งระหว่างผู้ใช้งานโปรแกรม IsagQ มาทำการเข้ารหัสและทดลองส่งสารให้กับผู้ใช้งานโปรแกรม IsagQ เมื่อผู้ใช้งานโปรแกรม IsagQ สามารถสนทนากันได้อย่างถูกต้องแล้วจึงทำการแก้ไขและตกแต่งโปรแกรมให้น่าใช้งานมากขึ้น