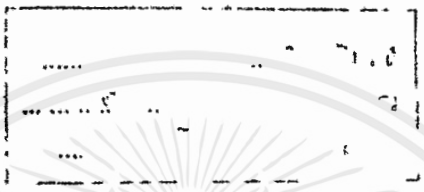
ระบบรหัสลับที่ไม่แสดงความเป็นรหัสลับ

(Non-Revealing Ciphertext Cryptosystem)



โดย

นาย โกวิท ทำมารุ่งเรือง

นาย ญาณพล สายวงศ์นวล

ปริญญานิพนธ์นี้เป็นส่วนหนึ่งของการศึกษาตามหลักสูตรปริญญาวิศวกรรมศาสตร์บัณฑิต

ภาควิชาวิศวกรรมคอมพิวเตอร์

คณะวิศวกรรมศาสตร์

สถาบันเทคโนโลยีพระจอมเกล้าเจ้าคุณทหารลาดกระบัง

ปีการศึกษา 2536

ปริญญานิพนธ์ ปีการศึกษา 2536

ภาควิชา วิศวกรรมคอมพิวเตอร์

คณะ วิศวกรรมศาสตร์ สถาบันเทคโนโลยีพระจอมเกล้าเจ้าคุณทหารลาดกระบัง

เรื่อง ระบบรหัสลับที่ไม่แสดงความเป็นรหัสลับ

ผู้จัดทำ

นาย โกวิท ทำมารุ่งเรือง
นาย ญาณพล สายวงศ์นวล

---------- อาจารย์ที่ปรึกษา
(ดร. เอื้อน ปิ่นเงิน)

---------- อาจารย์ที่ปรึกษา
(ศ.ดร. ศรีศักดิ์ จามรมาน)

ระบบรหัสลับที่ไม่แสดงความเป็นรหัสลับ

NON-REVEALING CIPHERTEXT CRYPTOSYSTEM

โดย นาย โกวิท ทำมารุ่งเรือง
นาย ญาณพล สายวงศ์นวล
อาจารย์ที่ปรึกษา ดร. เอื้อน ปิ่นเงิน
ศ.ดร. ศรีศักดิ์ จามรมาน
ปีการศึกษา 2536

บทคัดย่อ

ปริญญานิพนธ์ฉบับนี้มีวัตถุประสงค์ในการที่จะสร้างระบบรหัสลับที่ไม่แสดงความเป็นรหัสลับ ทั้งนี้ก็เพื่อจะใช้เป็นแนวทางแก่ผู้ที่ต้องการจะพัฒนาโปรแกรมประยุกต์ต่างๆ ที่จะใช้งานระบบรหัสลับที่ไม่แสดงความเป็นรหัสลับให้ได้ทราบถึงหลักการและปัญหาที่อาจจะเกิดขึ้นรวมทั้งแนวทางแก้ไขปัญหาที่อาจจะเกิดขึ้นด้วย

สำหรับเนื้อหาก็จะกล่าวเริ่มต้นตั้งแต่ลักษณะทั่วไปเกี่ยวกับ ระบบการเข้ารหัสลับ หลังจากนั้นจะได้กล่าวถึงวิธีการเขียนโปรแกรมประยุกต์ ด้วยภาษา C เพื่อสร้างระบบรหัสลับที่ไม่แสดงความเป็นรหัสลับ สุดท้ายจะเป็นการสรุปปัญหาที่เกิดขึ้นในการพัฒนาโปรแกรมประยุกต์เพื่อทำงานตามหลักการของระบบรหัสลับที่ไม่แสดงความเป็นรหัสลับและข้อสรุปในการทำงาน

ABSTRACT

The objective of this thesis is to build Non-revealing ciphertext cryptosystem and to guideline how to develop the application software from the Non-revealing ciphertext cryptosystem. The guidelines include basic and possible problems as well as the ways to solve the problems in this project. Interwined with the objective, this thesis describes an introduction to Cryptosystem. Others are the advantage and disadvantage of the primary cryptosystem. Moreover, it also describes the basics of writing programs for Non-revealing ciphertext cryptosystem using the C programming language.

Finally, it summarizes problems and ways to solve them for Non-revealing ciphertext cryptosystem application software.

กิตติกรรมประกาศ

การจัดทำปริญญานิพนธ์ฉบับนี้ สำเร็จลุล่วงไปได้ด้วยดีเนื่องมาจากบุคคลหลาย ๆ ฝ่ายเริ่มตั้งแต่ท่านอาจารย์ที่ปรึกษา ดร. เอื้อน ปิ่นเงิน และ ศ.ดร. ศรีศักดิ์ จามรมาน ที่ได้ดูแลและให้คำปรึกษาชี้แนะมาตั้งแต่เริ่มต้นทำโครงงาน ซึ่งคณะผู้จัดทำขอกราบขอบพระคุณเป็นอย่างสูงมา ณ โอกาสนี้ด้วย ขอขอบคุณทางภาควิชาคอมพิวเตอร์ ที่ได้ให้ใช้คอมพิวเตอร์ยามดึก เพื่อน ๆ นักศึกษาภาควิชาวิศวกรรมคอมพิวเตอร์ ชั้นปีที่ 4 ที่ได้ให้คำปรึกษาและความช่วยเหลือ น้อง ๆ ชุมนุมประชาสัมพันธ์ที่ช่วยให้กำลังใจและให้ยืมคอมพิวเตอร์ใช้ในการทำโครงงาน และทุกท่านที่ไม่ได้กล่าวถึงมา ณ ที่นี้ด้วย

คณะผู้จัดทำ

คำนำ

ปริญญานิพนธ์ฉบับนี้เป็นส่วนหนึ่งของโครงงาน เรื่องระบบรหัสลับที่ไม่แสดงความเป็นรหัสลับ ในวิชา 17418 PROJECT II ซึ่งเป็นโครงงานประจำภาคการศึกษาปลายของนักศึกษาภาควิชาวิศวกรรมคอมพิวเตอร์ชั้นปีที่ 4 โดยมีวัตถุประสงค์เพื่อศึกษาปัญหาและหาข้อสรุปในการสร้างระบบรหัสลับที่ไม่แสดงความเป็นรหัสลับ ทั้งนี้ก็เพื่อที่จะใช้เป็นแนวทางแก่ผู้ที่ต้องการเขียนโปรแกรมประยุกต์ เพื่อที่จะสร้างระบบรหัสลับที่ไม่แสดงความเป็นรหัสลับให้ได้ทราบถึงหลักการและปัญหาที่อาจจะเกิดขึ้นรวมทั้งแนวทางการแก้ไขปัญหาที่อาจเกิดขึ้นด้วยซึ่งในการหาข้อสรุปที่จะใช้เป็นแนวทางการแก้ไขนั้นคณะผู้จัดทำได้ทำการค้นคว้ามาแล้วเป็นอย่างดี ประกอบกับได้ลงมือปฏิบัติในการแก้ไขปัญหาที่เกิดขึ้นให้หมดไปได้ด้วยตนเอง หลังจากที่ได้ศึกษาค้นคว้ารวมทั้งทำการวิเคราะห์มากแล้วตลอดระยะเวลาที่ได้ทำโครงงานนี้มา

คณะผู้จัดทำโครงงานนี้จึงหวังเป็นอย่างยิ่งว่าปริญญานิพนธ์เล่มนี้จะเป็นเครื่องมือที่ช่วยชี้แนะให้แก่ผู้ที่สร้างโปรแกรมประยุกต์ เพื่อที่จะทำระบบรหัสลับที่ไม่แสดงความเป็นรหัสลับได้เป็นอย่างดีหลังจากที่ได้อ่านปริญญานิพนธ์เล่มนี้ อย่างไรก็ดีผลสรุปทั้งหมดนั้นบางส่วนก็มาจากแหล่งข้อมูลที่คณะผู้จัดทำโครงงานได้ค้นคว้าหามาและ บางส่วนก็มาจากประสบการณ์ที่ได้จากการปฏิบัติเพื่อแก้ไขปัญหาของคณะผู้จัดทำเอง ประกอบกับระยะเวลาที่จำกัดในการศึกษาค้นคว้าและจำนวนของคำศัพท์ต่างๆ ที่มีมากมายหลากหลายในภาษาอังกฤษ ดังนั้นคณะผู้จัดทำจึงไม่อาจกล่าวว่าปริญญานิพนธ์นี้จะครอบคลุมถึงแนวทางการแก้ไขปัญหาทั้งหมด ที่อาจเกิดขึ้นได้ในสร้างโปรแกรมประยุกต์แต่ก็หวังว่าจะมีส่วนช่วยให้ผู้ที่ได้ศึกษาปริญญานิพนธ์นี้ได้แนวทางบางส่วนในการแก้ไขปัญหาให้ลุล่วงไปได้ด้วยดีสำหรับความผิดพลาดต่าง ๆ ของปริญญานิพนธ์นี้ทางคณะผู้จัดทำต้องขออภัยท่านผู้อ่านมา ณ ที่นี้ด้วย

สำหรับคุณความดีของปริญญานิพนธ์นี้ขอมอบแด่คณาจารย์ผู้อบรมสั่งสอนความรู้ทั้งหลายทั้งปวงแก่คณะผู้จัดทำ

คณะผู้จัดทำ

สารบัญ

สารบัญรูปภาพ

บทที่ 1

ปฐมบทเกี่ยวกับระบบรหัสลับ

ในปัจจุบันได้มีการใช้คอมพิวเตอร์ในการใช้งานทางธุรกิจมากขึ้นอย่างมาก เนื่องจากความสามารถของคอมพิวเตอร์ที่มีเพิ่มขึ้นในปัจจุบันนั้น มีส่วนช่วยในการทำงานในด้านต่าง ๆ ในธุรกิจอย่างมากมาย จึงทำให้เกิดการเก็บข้อมูลต่าง ๆ ที่ใช้ในธุรกิจนั้นไว้ในคอมพิวเตอร์เพราะฉะนั้น ข้อมูลเก็บไว้ในคอมพิวเตอร์จึงมีความสำคัญและ มีค่ามากต่ออาชญากรทางคอมพิวเตอร์และคู่แข่งทางการค้า ถ้าหากไม่ได้มีการป้องกันข้อมูลที่เป็น ความลับและมีความสำคัญต่อธุรกิจไว้แล้วละก็ ก็จะทำให้อาชญากรทางคอมพิวเตอร์นั้นสามารถที่จะขโมยข้อมูลที่มีความสำคัญที่เก็บเป็นความลับในคอมพิวเตอร์นั้นนำไปใช้ได้ ซึ่งจะทำให้เกิดผลเสียหายอย่างมากกับธุรกิจ จึงทำให้เกิดระบบการรักษาความปลอดภัยให้กับคอมพิวเตอร์เพื่อที่รักษาความปลอดภัยให้กับข้อมูลที่อยู่ในคอมพิวเตอร์ จึงทำให้เกิดระบบรหัสลับในคอมพิวเตอร์ขึ้น ในการรักษาความปลอดภัยให้กับข้อมูลนั้นจะต้องคำนึงถึงความสำคัญของข้อมูล และระยะเวลาการใช้ข้อมูลด้วย เนื่องจากข้อมูลที่อยู่ในคอมพิวเตอร์นั้นจะมีอายุของข้อมูลสั้น ถ้าหากไม่ได้มีทำการเข้ารหัสข้อมูลทำเป็นรหัสลับไว้เอาไว้ คนที่เอาข้อมูลไปนั้นก็สามารถที่จะนำข้อมูลนั้นไปใช้ได้เลย ซึ่งก็จะเป็นผลเสียหายอย่างมาก เพราะฉะนั้นจึงต้องมีการเข้ารหัสข้อมูลทำเป็นรหัสลับเอาไว้ เพื่อที่จะทำให้คนที่เอาข้อมูลไปไม่สามารถนำข้อมูลไปใช้ได้ในทันทีหรือนำไปใช้ไม่ได้เลย แต่ถ้าคนที่นำข้อมูลไปนั้นเป็นพวกอาชญากรมืออาชีพในการถอดรหัสลับแล้วละก็คงจะทำได้เพียงหน่วงเวลาในการที่ถอดข้อมูลที่เข้ารหัสจนข้อมูลที่ได้ไปนั้นหมดค่าไป ซึ่งก็จะทำให้ข้อมูลนั้นไม่มีประโยชน์อีกต่อไปหรืออาจจะป้องกันข้อมูลของเราจากการถอดรหัสของคนพวกนี้ได้ ซึ่งขึ้นอยู่กับอัลกอริทึมที่ใช้ในการเข้ารหัสลับ แต่อย่างไรก็ตามถ้าทำการเข้ารหัสข้อมูลไว้นั้นหากมีใครได้ไปก็จะมีการพยายามที่จะวิเคราะห์หาข้อมูลเดิมก่อนเข้ารหัส จึงต้องมีการป้องกันข้อมูลที่เป็นรหัสลับของเราในวิธีใหม่ที่ดีกว่าวิธีเดิม โดยการใช้ระบบรหัสลับที่ไม่แสดงความเป็นรหัสลับ ซึ่งจะเป็นวิธีที่ดีกว่าวิธีที่ใช้กันอยู่ในปัจจุบัน เนื่องจากถ้าเข้ารหัสลับด้วยวิธีนี้แล้ว คนที่นำข้อมูลไปนั้นจะไม่รู้ว่าข้อมูลที่นำเอาไปนั้นถูกเข้ารหัสข้อมูลเป็นรหัสลับเอาไว้ คนที่ได้ข้อมูลไปนั้นเข้าใจผิดนึกว่าเป็นข้อมูลที่ไม่ได้เข้ารหัส และทำการนำข้อมูลที่ได้เข้ารหัสลับไว้แล้วนั้นนำไปใช้

บทที่ 2

หลักการและทฤษฎีที่ใช้ในการทำโครงงาน

2.1 ความรู้เบื้องต้นเกี่ยวกับภาษาอังกฤษ

ในหัวข้อนี้เราจะพูดถึงความรู้เบื้องต้นเกี่ยวกับภาษาอังกฤษที่สำคัญทั่ว ๆ ไปว่าประกอบไปด้วยอะไรบ้าง เพื่อใช้เป็นพื้นฐานสำหรับการสร้างโปรแกรมเพื่อที่จะทำการเข้ารหัสลับข้อความภาษาอังกฤษให้เป็นรหัสที่ไม่แสดงความเป็นรหัสลับ ว่าแต่ละส่วนเป็นอย่างไร และควรจะทำอย่างไรกับแต่ละส่วนของภาษาอังกฤษนั้น ซึ่งส่วนต่าง ๆ ของภาษาอังกฤษที่สำคัญที่มีส่วนเกี่ยวข้องกับการทำโปรแกรมจะได้นำมาอธิบายดังต่อไปนี้คือ

2.1.1 Article คือ คำที่ใช้นำหน้าคำนาม มี 2 ชนิด คือ

1. Indefinite Article ได้แก่ a, an
2. Definite Article ได้แก่ the

Indefinite Article ใช้กับคำนามเอกพจน์ที่นับได้เท่านั้น

การใช้ a หรือ an

1. ใช้ a นำหน้านามที่ขึ้นต้นด้วยพยัญชนะหรือสระที่ออกเสียงเหมือนพยัญชนะ เช่น a girl, a car, a desk, a European, a university, a uniform, a one-eyed man

2. ใช้ an นำหน้านามที่ขึ้นด้วยสระและออกเสียงสระ เช่น an apple, an umbrella, an egg, an old oak tree

3. ใช้ an นำหน้านามที่ขึ้นต้นด้วย h แต่เวลาอ่านไม่ออกเสียง h คงออกเสียงสระ เช่น an hour, an heir, an honest man

แต่คำที่ขึ้นต้นด้วย h และออกเสียง h ด้วย ก็คงใช้ 'a' นำหน้า เช่น a hut, a human being, a horse

การใช้ Indefinite Article : a, an

1. ใช้นำหน้านามเอกพจน์ทั่วไปที่นับได้ ซึ่งไม่ชี้เฉพาะเจาะจง เช่น

There is a book on the desk.

Bring me a pen, please.

2. ใช้นำหน้านามซึ่งหมายถึงนามนั้นทั้งจำพวก เช่น

A tiger is a fierce animal.

A palmtree is usually tall.

3. ใช้นำหน้านามที่เอ่ยถึงเป็นครั้งแรกในการเล่าเรื่องต่างๆ เช่น

Once there was an old woman who lived in a hut near a forest.

4. ใช้นำหน้าคำนามแท้ (Proper nouns) ทำให้มีความหมายเป็น คำนามทั่วไป (Common Noun) เช่น

He thinks he is an Einstein. (= clever)

He is a Superman among his friends. (= very strong)

He is a Hercules in his class. (= very strong)

5. ใช้กับกลุ่มคำที่บอกจำนวน (Numerical expressions) เช่น a hundred, a couple, a dozen, a thousand, a score, a lot of

6. ใช้ในการบอกอัตรา, ราคา, ความเร็ว, น้ำหนัก และเวลา ซึ่งมีความหมายว่า "ต่อ" หรือ "ละ" เช่น

forty miles an hour = สี่สิบไมล์ต่อหนึ่งชั่วโมง หรือ ชั่วโมงละสี่สิบไมล์

three times a day = สามครั้งต่อหนึ่งวัน หรือ วันละสามครั้ง

twenty baht a dozen = ยี่สิบบาทต่อหนึ่งโหล หรือ โหลละยี่สิบบาท

7. ใช้นำหน้านามที่กล่าวถึงอาชีพ หรือ สัญชาติของคน เช่น

He is an engineer. She is a doctor.

He is an America. I am a Thai.

การใช้ Definite Article 'the'

1. เมื่อนามนั้นมีอยู่เพียงสิ่งเดียวในโลก เช่น the sun, the moon, the sky, the world, the universe, the north, the south, the east, the west, the equator, the earth

2. นามที่กล่าวถึงเป็นสิ่งที่ผู้พูดและผู้ฟังเห็นอยู่ใกล้ๆ และรู้ว่าเป็นอันไหน เช่น

Take the chair away.

Put it on the table.

3. นามที่ถือว่าชี้เฉพาะ เนื่องจากผู้พูดและผู้ฟังรู้ว่าหมายถึงคนไหน หรืออันไหน เช่น

Bob is in the garden. (= the garden of this house)

Please pass me the salt. (= the salt on the table)

The Royal Family went to Hua-Hin.

4. ในการเล่าเรื่องใช้นำหน้าเมื่อถูกกล่าวซ้ำเป็นครั้งที่ 2 เช่น

Once there was a queen. She had a son. The queen and the prince lived a very happy life.

5. ใช้นำหน้าคำนามที่มีวลี (phrase) หรืออนุประโยค (Cluase) ที่บอกลักษณะชี้เฉพาะ เช่น

The girl with blue eyes is pretty.

The man standing there is my uncle.

The boy on the donkey is smart.

The girl I met yesterday is beautiful.

6. ใช้นำหน้าคำคุณศัพท์ (Adjectives) หรือคำกริยาวิเศษณ์ (adverbs) ในการเปรียบเทียบขั้นสูงสุด (Superlative degree) เช่น

She is the cleverest girl in this class.

He is the biggest of the tree.

Smith knows the English Grammar the best of all the students.

Mr. Brown explains things the most clearly of all our teachers.

7. ใช้นำหน้าคำคุณศัพท์หรือคำกริยาวิเศษณ์ใน comparative degree แสดงการเปรียบเทียบขั้นกว่า แปลว่า ยิ่ง - ยิ่ง

The more we get together, the happier we'll be.

ยิ่งได้อยู่ด้วยกันมากเท่าไร ยิ่งมีความสุขมากขึ้นเท่านั้น

The more one has, the more one wants.

คนยิ่งมีมาก ยิ่งอยากได้มาก

The fatter the man is, the weaker he becomes.

คนยิ่งอ้วน ยิ่งอ่อนแอ

8. ใช้นำหน้าชื่อเครื่องดนตรีที่มาข้างหลัง Verb to play เช่น

to play the guitar/piano/violin.

She learnt to play the flute.

9. ใช้นำหน้าเมื่อหมายถึงนามนั้นทั้งจำพวก เช่น

The horse is a four-footed animal.

The lion is the king of the beasts.

The cuckoo is very lazy.

แต่มีนามอยู่ 2 คำ ที่ไม่ต้องใช้ the นำหน้าเมื่อใช้ในความหมายทั่วๆ ไป เพื่อเป็นตัวแทนของนามในจำพวกเดียวกัน คือ man และ woman

Man is mortal.

คนทุกคนต้องตาย

Woman is physically inferior to man.

ผู้หญิงย่อมด้วยกว่าผู้ชายในด้านกำลัง

10. ใช้นำหน้านามสกุลที่เป็นพหูพจน์ และมีความหมายว่าครอบครัว

The Fords went to the cinema. ครอบครัวตระกูลฟอร์ด

The Browns invited their friends to the party.

ครอบครัวตระกูลบราวน์

11. ใช้นำคำคุณศัพท์ที่ บอกลำดับที่ เช่น first, second, third, etc. เช่น

I have read the first chapter of that book.

The third unit is difficult to understand.

12. ใช้นำหน้าคำคุณศัพท์ที่ทำหน้าที่เป็นคำนามมีความหมายเป็นพหูพจน์ (ทั้งจำพวก) เช่น the rich, the poor, the dead, the young, the old, the brave, etc. เช่น

We should help the poor . (= poor people)

The English are fond of travel. (= Englishman)

The rich are not always happy.

The brave are to be admired.

13. ใช้นำหน้าชื่อหนังสือสำคัญๆ เช่น

The Bible, The Koran, The Ramayana.

14. ใช้นำหน้า

ชื่อเรือ เช่น The Queen Elizabeth

ชื่อทะเล,มหาสมุทร เช่น The Dead Sea, The Red Sea

The Atlantic Ocean, The Pacific Ocean

ชื่อแม่น้ำ เช่น The Thames, The Chao Phraya River

ชื่อเทือกเขา เช่น The Alps, The Himalayas

ชื่อหมู่เกาะ เช่น The Philippines, The West Indies

ชื่อประเทศ,ชื่อเมือง เช่น The United Kingdom,

The Soviet Union,

The United States of America,

ชื่อสิ่งก่อสร้าง เช่น The Taj Mahal

ชื่ออื่นๆ เช่น The Gulf of Thailand

15. ใช้กับเวลา (Expression of time) เช่น

in the morning / afternoon / evening

in the third of May / April / June / July

16. ใช้นำหน้าชื่อหนังสือพิมพ์รายวัน เช่น

The Bangkok Post, The Nation

17. ใช้นำหน้า

ชื่อโรงภาพยนตร์ เช่น The King's, The Metro

ชื่อโรงแรม เช่น The President Hotel, The Erawan Hotel

ชื่อสโมสร เช่น The Royal Bangkok Sports Club

ชื่อธนาคาร เช่น The Bank of England

เราจะไม่ใช้ articles ในกรณีต่อไปนี้

1. เมื่อคำนามทั่วไปนั้น เป็นพหูพจน์ (Plural) และถูกกล่าวอย่างลอยๆ โดยมิได้ชี้เฉพาะเจาะจงลงไป เช่น

She puts flowers in the vase.

Women like beautiful clothes.

2. ใช้กับคำนามนับไม่ได้ (uncountable nouns)ที่ไม่ชี้เฉพาะเจาะจง ได้แก่

ก. Material Nouns เช่น oil, soil, water, iron, butter, sugar, soap, sand, etc.

Water is composed of hydrogen and oxygen.

ข. อาการนาม เช่น cleverness, wisdom, life, honesty, etc.

What is life ?

แต่เมื่อต้องการชี้เฉพาะลงไป ให้ใช้ 'the' นำหน้า เช่น

I like to drink coffee. (ไม่ชี้เฉพาะเจาะจง)

I like the coffee which comes from Peru. (ชี้เฉพาะเจาะจง)

Gold is a precious metal.

The gold in my ring is very old.

Exercise is good for one's health.

The exercise which he gets from tennis is good for his health.

3. ชื่อวิชาต่างๆ ที่ใช้ในความหมายทั่วๆ ไป เช่น chemistry, history, music, etc.

We are learning English.

แต่ถ้าคำนามเหล่านี้ทำหน้าที่เป็นคำคุณศัพท์ต้องมี 'the' นำหน้า เช่น

She is learning in the history class.

I study the English language.

4. กีฬาหรือสิ่งที่ให้ความบันเทิงใจ เช่น tennis, golf, dancing, singing เป็นต้น เช่น

They like to play golf.

Do you enjoy dancing ?

แต่ถ้าคำนามเหล่านี้ทำหน้าที่เป็นคำคุณศัพท์ ประกอบคำนามอื่นต้องมี articles นำหน้า เช่น

Have you gone to a basket-ball game lately ?

Did you enjoy the basket-ball game that you went to last year ?

5. กับจำนวนนับ เช่น one, two, three, etc. ที่ตามหลังคำนาม เช่น

I am reading Chapter two.

(เปรียบเทียบ I am reading the second Chapter)

He died in World War II.

(He died in the second World War.)

6. กับเวลาต่อไปนี้

at noon/night/midnight/six o'clock

on Sunday/Monday/Friday

last week/month/year

next week/month/year

7. กับคำนามที่ตามหลังคำคัพท์ว่า kind of หรือ sort of ไม่ต้องมี articles นำ แม้ว่าจะเป็นนามนับได้เอกพจน์ก็ตาม เช่น

What kind of man is he ?

What sort of flower do you like ?

What kind of trousers did he buy ?

8. กับชื่ออาหารมื้อต่างๆ คือ breakfast, lunch, dinner, supper เช่น

We have breakfast at 7 o'clock.

My friend invited me to dinner last night. (= the main meal of the day)

I was invited to a dinner last night. (= a dinner-party)

แต่ถ้าต้องการที่จะชี้เฉพาะลงไปก็ใช้ 'the' นำ เช่น

The breakfast I had this morning makes me sick.

9. กับชื่อฤดูต่างๆ เช่น

I like spring more than summer.

แต่ถ้าต้องการที่จะชี้เฉพาะต้องมี 'the' นำหน้า เช่น

The winter of this year is colder than that of last year.

10. กับบางสำนวน เช่น by car, by train, by plane, by taxi, by boat, on foot, at sea, by land, by water, on horseback, at home, at school, in bed, in jail, at sunset, at daybreak, in debt, etc. เช่น

I go to school on foot.

We started our journey at daybreak.

11. คำนามที่แสดงตำแหน่งหน้าที่ ใช้นำหน้าคำนามแท้ (proper noun) เช่น

King Henry, Queen Elizabeth, Saint Paul

(King, Queen, Saint นำหน้าคำนามแท้ Henry, Elizabeth, Paul ตามลำดับใช้แสดงตำแหน่ง จึงไม่ต้องมี article นำหน้า)

12. หน้าคำนามบางคำ. เช่น school, market, church, prison, bed, sea, hospital ในความเฉพาะ เช่น

to go to school = to study ไปเรียนหนังสือ

to go to market = to sell or buy something ไปซื้อหรือขายของ

to go to church = to pray ไปสวดมนต์

to go to prison = ไปเข้าคุกในฐานะที่เป็นนักโทษ

to go to bed = to sleep ไปนอน

to go to sea = to become a sailor ไปเป็นกลาสีเรือ

to go to hospital = to be a patient ป่วยไปโรงพยาบาลในฐานะคนไข้

แต่ถ้ามี 'the' นำหน้าคำนามเหล่านี้ ความหมายจะแตกต่างกันออกไป โดยไปเน้นที่ตัวอาคาร เช่น

They go to school every day.

ไปโรงเรียนทุกวันเพื่อไปเรียนหนังสือ

They go to the school every Saturday.

ไปโรงเรียนทุกวันเสาร์ เพื่อกิจการอื่นที่ไม่ใช่ไปเรียนหนังสือ เช่น ไปประชุม หรือนัดพบกับใครที่นั่น

2.1.2 คำนามแท้ (Proper Nouns)

คำนามแท้นั้นตามปกติไม่มี articles นำ แต่มีหลายกรณีที่ต้องการ articles นำดังหัวข้อต่อไปนี้

1. ชื่อคน โดยปกติไม่ต้องใช้ articles นำ

2. ชื่อประเทศ เมือง ตำบล มหาวิทยาลัย หรือโรงเรียนต่างๆ ไม่มี article นำ

3. คำนามที่แสดงสัญชาติหรือเชื้อชาติ จะมี article หรือไม่นั้นขึ้นอยู่กับวิธีใช้ คือ

ก. เมื่อใช้เป็นคำนามถ้ากล่าวลอยๆ ไม่เฉพาะเจาะจง ใช้ a, an ถ้าชี้เฉพาะเจาะจงใช้ 'the' นำ

ข. เมื่อชื่อ สัญชาติ หรือเชื้อชาติ ใช้เป็น Adjective Complement ก็ไม่ต้องใช้ article นำหน้า

4. ชื่อถนน ไม่ต้องมี article นำหน้า

5. ชื่อเกาะๆ เดียวและภูเขาลูกเดียว ไม่มี article นำ เช่น

6. ชื่อทวีปและภาคพื้นส่วนต่างๆ ของโลกที่แบ่งตามสภาวะภูมิศาสตร์ไม่ต้องมี article

7. ชื่อทะเล มหาสมุทร แม่น้ำ อ่าว เทือกเขา ต้องใช้ 'the' นำหน้า

8. ชื่อวันหยุดต่างๆ ไม่มี article นำหน้า

9. อักษรย่อ

ก. ถ้าออกเสียงทีละตัวใช้ 'the' นำหน้า

ข. ถ้าออกเสียงเป็นพยางค์ ไม่ใช้ 'the' นำ

ค. สายการบินต่างๆ แม้จะออกเสียงทีละตัวก็ไม่ใช้ 'the' นำ

2.1.3 คำนามนับได้และคำนามนับไม่ได้

(Countable nouns and Uncountable nouns)

1. คำนามที่นับจำนวนได้ ได้แก่นามที่มีรูปร่างนับเป็นชิ้นได้ จะใช้ a, an นำหน้าเมื่อไม่เฉพาะเจาะจง และสามารถทำเป็นพหูพจน์ได้ คือ อาจเติมคำ two, three, four etc. ลงหน้านามนั้นได้ เช่น two table, three pencils เป็นต้น

คำนามนับได้ยังแบ่งได้เป็น 2 ชนิด คือ

1.1 นามทั่วไปหรือสามานยนาม (Common nouns)เป็นได้ทั้งเอกพจน์และพหูพจน์ เช่น city, baby, man, desk, etc.

1.2 สมุหนาม (Collective Nouns) คือคำนามของสิ่งที่อยู่รวมกันเป็นหมู่เป็นพวก เช่น head, flock, bunch, etc.

สมุหนามนี้บางคำ เช่น family, group, commitee, class, crowd, jury, cabinet, etc. จะใช้กริยาเป็นเอกพจน์หรือพหูพจน์ก็ได้ ย่อมแล้วแต่ความหมาย ถ้าหมายถึงจำนวนแยกแยะรายตัวรายบุคคล (individual) ก็ใช้กริยาพหูพจน์

2. คำนามที่นับจำนวนไม่ได้ มีรูปเป็นเอกพจน์เสมอ ไม่มี article นำหน้า แต่จะใช้ the นำเมื่อเฉพาะเจาะจง

2.1 Mass Nouns (หรือ material nouns) นามที่อยู่รวมกันเป็นกลุ่มเป็นก้อน แสดงความมากน้อยด้วยปริมาณ (quanity) ไม่ใช่จำนวน (number) เช่น water, air, coffee, meat, suger, salt, pork, ink, chalk, paper, butter, flour, rice, etc.

วิธีใช้ Mass Nouns

ก. ใช้เดี่ยวๆ ได้เลยโดยไม่ต้องไปรวมกับคำอื่น ไม่ต้องมี article นำหน้า ถ้าไม่เฉพาะเจาะจงและใช้กริยาเป็นเอกพจน์ เช่น

She drinks milk every moring.

ข. ใช้คำนามอื่นมาช่วย เมื่อต้องการทราบเป็นหน่วย โดยนับได้จากภาชนะที่บรรจุ หรือจำนวนน้ำหนัก เช่น

a bowl of - rice, sugar

a bottle of - ink, milk, water, beer

2.2 อาการนาม (Abstract Nouns)ได้แก่

ก. นามที่แสดงสภาพ (state) เช่น poverty, richness, plessure, etc.

ข. นามที่แสดงคุณสมบัติ เช่น beaty, honesty, kindness, cleverness, etc.

ค. นามที่แสดงการกระทำ เช่น movement, flight, revenge, etc.

สรุปการใช้ Articles กับคำนามนับได้และ คำนามนับไม่ได้

1. คำนามนับได้ที่เป็นเอกพจน์ ต้องมี article เสมอ

ก. ถ้าเป็นสิ่งเดียว ชิ้นเดียว กล่าวถึงทั่วๆ ไป ใช้ a หรือ an

I want a book on ancient history.

Did you buy a hat ?

ข. ถ้าเป็นสิ่งเดียว ชิ้นเดียว ที่ชี้เฉพาะเจาะจงใช้ 'the' นำ

I want the book on your desk.

Did you buy the green hat or the red one ?

2. คำนามพหูพจน์และคำนามที่นับไม่ได้

ก. ถ้ากล่าวถึงทั่วไป ไม่ต้องมี article นำหน้า เช่น

Books are necessary for students.

Paper is scarce in some parts of the world.

ข. ถ้าชี้เฉพาะเจาะจงลงไปใช้ 'the' นำ เช่น

The books that I need are expensive.

The paper in the book is of a good quality.

จากความรู้เกี่ยวกับ Article จะเห็นได้ว่า Article นั้นจะมีข้อกำหนดในการใช้มาก มายเพราะฉะนั้นถ้าหากทำการเปลี่ยนแปลง Article ไปนั้น โอกาสที่จะทำให้เมื่อเราทำการเข้ารหัส ไปนั้นโอกาสที่จะทำให้รูปประโยคแตกต่างออกไปจากรูปประโยคทั่วไปในภาษาอังกฤษนั้นเป็นไป ได้ง่ายมาก อีกทั้งยังสังเกตุได้ง่ายอีกด้วยตัวอย่างก็อย่างเช่น

This is a student.

This is an student.

จะเห็นได้ว่าจะสังเกตุเห็นได้อย่างชัดเจนว่าการใช้ an กับคำว่า student นั้นมันผิด อย่างแน่นอน หรืออย่างเช่นกับคำที่จะเน้นเฉพาะเจาะจงลงไปจะต้องมี the นำหน้าคำนามนั้นแต่ .Possessive Pronouns เช่น mine yours his etc.งไม่มีคำขยายสรรพนามอีกยนก็สังเกตุ ได้ง่ายอีกเช่นกัน เช่น ในประโยคที่มีการเปรียบเทียบขั้นกว่าหรือขั้นสูงสุดจะต้องมี the นำหน้าคำ

house. ะกอบให้เห็นดังต่อไปนี้นเลย จ งไม่สามารถที่จะทำการเปลี่ยนคำพวกนี้ได้

ˇ ˇ pˇ

ละเอียดลงไปมากกว่านั้นคือแบ่งเป็นคำนามให้ย่อยลงไปอีกให้แบ่งกลุ่มให้ย่อยเท่าที่จะมากได้ก็

ˇ ˇxtˇ

2.1.4 คำสรรพนาม (Pronoun)

คำสรรพนาม คือ คำที่ใช้แทนคำนามเพื่อหลีกเลี่ยงการใช้คำซ้ำซาก คำสรรพนามจะ ทำหน้าที่เช่นเดียวกับกลุ่มคำนามที่สรรพนามนั้นไปแทนที่จึงไม่มีคำขยายสรรพนามอีก

ชนิดของคำสรรพนาม

1.Personal pronouns เช่น I, You, He, She

2.Possessive Pronouns เช่น mine, yours, his, etc.

3.Reflexive Pronouns เช่น myself, yourself, etc.

4.Interrogative Pronouns เช่น what, who, whom, which

Who came here this morning.

What did you buy?

5.Relative Pronouns เช่น what, whom, that, whose, of which

The man who robbed you has been arrested.

The boy whom you saw yesterday is Tom.

6.Demonstrative Pronouns คือ this, that, these, those

7.Indenfinite Pronouns คือ สรรพนามที่ไม่ชี้เฉพาะเจาะจงเป็นสรรพนามที่ประสมคำระหว่างคำ some, any, no, every กับคำว่า body, one, thing เช่น somebody, someone, anybody, anyone, anything, everyone, everything, nobody, no, one, nothing

Personal pronouns

1. Nominattive Form คือคำสรรพนาม ที่ใช้เป็นประธานของกิริยา (โดยปกติจะวางอยู่หน้าคำกิริยา) หรือใช้ส่วนเติมเต็ม (complement) มักวางหลัง verb to be เช่น

She knows everything.

I am a student.

How many children has he?

2. Accusative Form คือ คำสรรพนามที่ใช้เป็นกรรม

ก. ใช้เป็นกรรมตรง (direct object) มักจะวางไว้หลังคำกิริยา เช่น

She likes me.

I saw him.

ข. ใช้เป็นกรรมของคำบุพบท (วางไว้หลังคำบุพบท)

She gave it to me.

I shall go with him.

It is for us.

ค. ใช้เป็นกรรมรอง (indirect object)

โดยใช้แทน to + noun (pronoun)

หรือ for + noun (pronoun)

I gave her a pen. = I gave pen to her.

I bought him a football. = I bought a football for him.

3. ใช้ it กับสัตว์, ทารก (baby) และ เด็กเล็ก (child) โดยเฉพาะเมื่อกล่าว โดยไม่คำนึงถึงเพศ

Look at that lovely child?

Is it boy or girl?

4. สัตว์เลี้ยงในบ้านใช้ตามสรรพนามตามเพศมัน

I have lost my cat.

Have you seen + him?

+ her?

5. ในกรณีที่ไม่บ่งเพศ เราจะใช้สรรพนามเพศชาย เช่น

My cousin came to see me last night.

He left his books at my house.

6. everyone, everybody, everything ที่ใช้ใน Question tag จะใช้รูป plural verb + they ? เช่น

A: " Everybody has finished the exercise, haven't they ? "

B: " Yes they have. "

คำศัพท์ที่ทำหน้าที่เป็น คำสรรพนาม ในประโยคจะไม่สามารถทำการเปลี่ยนแปลงได้ เพราะถ้าเปลี่ยนแล้วจะทำให้ความสัมพันธ์ระหว่างคำสรรพนามกับประธานของประโยคที่เปลี่ยนมากพร้อมกันนั้น จะไม่มีความสัมพันธ์กันเลย จึงไม่สามารถที่จะทำการเปลี่ยนคำพวกนี้ได้ ซึ่งจะได้ยกตัวอย่างประกอบให้เห็นดังต่อไปนี้

He left his books at my house.

I left her books at his house.

ซึ่งจากตัวอย่างจะเห็นได้ว่า เพียงแค่เปลี่ยนแค่เฉพาะคำสรรพนามเพียงอย่างเดียว ก็จะเห็นได้ว่าความหมายของประโยคก็จะเสียไปอย่างมาก

2.1.5 คำคุณศัพท์ (Adjective)

คือคำที่ใช้ประกอบนามแบ่งออกเป็นชนิดต่างๆ ตามลักษณะการใช้ดังนี้

1.คำคุณศัพท์ที่แสดงความเป็นเจ้าของ (Possesive Adjective)คือคำที่ใช้ประกอบนามเพื่อแสดงความเป็นเจ้าของ ได้แก่ my, your, our, its, their, his, her, 's

His eye-glasses

Jame's car

2. คำคุณศัพท์ที่ใช้อธิบาย (Descriptive Adjective) เป็นคำคุณศัพท์ประกอบนามเพื่อบอกลักษณะของนามแบ่งออกเป็น 3 อย่าง คือ

- บอกคุณภาพ (quality) เช่น good, delicious, generous (ใจกว้าง), narrow, deep, tame, careful, active
- บอกขนาด (size) และอายุ (age) เช่น big, tall, short, young, old, new
- บอกสี (colour) เช่น brown, pink, yellow, white, green

3. คำคุณศัพท์ที่ใช้กับจำนวน (Number Adjective) แบ่งออกเป็น 2 อย่างคือ

1) บอกจำนวนธรรมดา (Cardinal Numeral Adjective) เช่น one, two, three, ...

2) บอกลำดับที่ (Ordinal Numeral Adjective) เช่น first, second, third, ...

Cardinal	Cardinal Number	Ordinal	Ordinal Number
1	one	1 st	first
2	two	2 nd	second
3	three	3 rd	third
4	four	4 th	fourth
5	five	5 th	fifth
6	six	6 th	sixth
7	seven	7 th	seventh
8	eight	8 th	eighth
9	nine	9 th	ninth
10	ten	10 th	tenth

11	eleven	11 th	eleventh
12	twelve	12 th	twelfth
13	thirteen	13 th	thirteenth
14	fourteen	14 th	fourteenth
20	twenty	20 th	twentieth
30	thirty	30 th	thirtieth
100	a hundred	100 th	a hundredth
1000	a thousand	1000 th	a thousandth
20000	twenty thousand	20000 th	twenty thousand
1000000	a million	1000000 th	a millionth

<u>การอ่านและเขียนตัวเลข</u>

จำนวนนับตั้งแต่ 100 ขึ้นไป ให้อ่านโดยใช้ and เชื่อมหลักสิบ ส่วนจำนวนต่ำกว่านั้น คือ ตั้งแต่ 99 ลงมา ให้ใช้ hypen (-) คั่น เช่น

82 = eighty-two

132 = one hundred and thirty-two

1,234 = one thousand,two hundred and thirty-four

35,613,459 = thirty-five million,six hundred and thirteen thousand,four hundred and fifty-nine.

และมีข้อสังเกตว่า

1. หลัง thousand, million จะมีเครื่องหมาย comma (,)

2. หลัง hundred, thousand, million จะเติม s ไม่ได้ เพราะคำเหล่านี้ถูกใช้เป็น คำคุณศัพท์ ถ้าจะเติม s จะต้องไปเติมหลังคำนามเช่น

I have a hundred pens.

There are two thousand students in our school.

แต่ถ้าคำดังกล่าวถูกใช้อย่างคำนามหรือใช้เป็นสำนวนก็เติม s ได้ และมักจะตามด้วย of (ต้องไม่มีคำบอกจำนวนที่แน่นอนอยู่ข้างหน้า) เช่น

There are <u>thousand of</u> people in the street.

Hundreds and hundreds of birds came in winter.

3. หน้าหนังสือ (page) หรือบทที่ในหนังสือ (chapter หรือ lesson) ให้อ่านนับ ธรรมดา เช่น

page 12 = page twelve

lesson 5 = lesson five

ถ้าจะใช้เรียกแบบ ordinal numbers ก็ได้ เช่น the twelth page, the fifth lesson, the fifteenth chapter, the third part

4. เมื่อทั้ง ordinal และ cardinal numbers ขยายคำนาม จะต้องใช้ ordinal number ขึ้นต้นก่อนเสมอ

ordinal no. + cardinal no. + noun

เช่น The first five lessons are easy.

4. Proper Adjective คือคำคุณศัพท์ที่มาจาก Proper Noun และคำคุณศัพท์ นี้ต้องเขียนขึ้นต้นด้วยตัวใหญ่เสมอ เช่น *Italian* food, *American* style, *Thai* song

5. คำนามที่เอามาใช้เป็นคำคุณศัพท์ประกอบนาม เช่น eletric machine, cotton dress, history book

6. Demonstrative Adjective คือคำคุณศัพท์ประกอบนามเพื่อชี้เฉพาะลงไป ได้แก่ this that those these

7. Indefinite Adjective คือ คำคุณศัพท์ที่บอกจำนวนไม่แน่นอน ได้แก่ all no many several few some any enough

8. Distributive Adjective คือคำคุณศัพท์ที่ประกอบนามเพื่อแบ่งแยกนามออกจากกัน ได้แก่ each every either neither

ในส่วนของคำคุณศัพท์นั้นก็มีหลายชนิดดังที่ได้แจกแจงไปแล้วนั้น ดังนั้นแต่ละชนิดจึงต้องทำการพิจารณากันก่อนว่าคำคุณศัพท์ชนิดใดที่สามารถจะทำการเปลี่ยนแปลงไปได้บ้าง ซึ่งก็มีคำคุณศัพท์ที่ใช้อธิบาย (Descriptive Adjective) ที่สามารถทำการเปลี่ยนแปลงได้ ซึ่งเราทำการแบ่งย่อยคำศัพท์ออกเป็นพวกย่อยๆ ได้ตามอย่างของคำคุณศัพท์ที่ใช้อธิบายเช่นเป็นกลุ่มของคำศัพที่ใช้บอกสี กลุ่มของคำศัพท์ที่ใช้บอกขนาด กลุ่มของคำศัพท์ที่ใช้บอกอายุ กลุ่มของคำศัพท์ที่ใช้บอกคุณภาพ คำศัพท์ที่ใช้บอกคุณลักษณะ ซึ่งในแต่ละกลุ่มนั้นยังสามารถแยกย่อยลงไปอีกได้เพื่อความเหมาะสมในการเปลี่ยน

สำหรับในกรณีคำคุณศัพท์ตัวเลขนั้นจากกฎการใช้ที่ได้บรรยายไว้ เราสามารถที่จะทำการเปลี่ยนค่าตัวเลขและลำดับที่ได้โดยที่จะไม่มีผลใดกับรูปประโยคเลย อีกทั้งสามารถที่จะเปลี่ยนแล้วทำให้เป็นไปตามที่เราต้องการมากที่สุด คือทำให้เกิดการเปลี่ยนแปลงที่จำนวนเท่านั้น ตัวอย่างเช่น

They have three lovely books.

They have five lovely books.

ซึ่งจะเห็นได้ว่าไม่ได้ทำให้รูปประโยคนั้นผิดไวยากรณ์เลยแม้แต่น้อย ทั้งยังช่วยให้ข้อมูลในประโยคนั้นเปลี่ยนไปจากเดิม

ส่วนคำคุณศัพท์ที่ไม่สามารถที่จะทำการเปลี่ยนแปลงได้ก็ได้แก่คำคุณศัพท์ที่แสดงการเป็นเจ้าของ เพราะจะไปมีความสัมพันธ์กับประธานของประโยค และ คำคุณศัพท์ประกอบนามเพื่อชี้เฉพาะลงไป เพราะจะเป็นการเน้นที่เฉพาะลงไปกับสิ่งที่อยู่ในประโยคเดิม ถ้าหากเปลี่ยนก็จะทำให้การเน้นชี้เฉพาะลงไปนั้นผิด

2.1.6 คำบ่งบอกปริมาณ (Quantitative Words)

คำที่แสดงปริมาณของคำนามต่าง ๆ แบ่งได้เป็น 3 ประเภท คือ

1. ใช้เฉพาะกับนามที่นับได้ ได้แก่ a large number of, a good many, several of, few, a few, many, both, every, neither of

2. ใช้เฉพาะกับนามที่นับไม่ได้ ได้แก่ a large amount of, a large quantity of, a great deal of, a good deal of, little, a little, much

3. ใช้ได้กับนามที่นับได้และนับไม่ได้ ได้แก่ a lot of, lots of, plenty of, none of, all of, some, any, most, almost, nearly

การใช้คำบ่งบอกปริมาณ

1. A large number of ใช้กับ Plural noun เท่านั้น ดังรูปประโยคต่อไปนี้

A large number of + plural noun + plural verb

A large number of books are on the shelves in the library.

A large number of boys do so.

A large number of people like to play football.

I bought a large number of knives and forks.

She ate a large number of chocolates.

You will see a large number of other cars on the road.

That library has a large number of books on history.

A large number of และ a great number of มีความหมายคล้ายคลึงกันมาก ที่แตกต่างกันก็เพียงเล็กน้อยเท่านั้น คือ A great number is bigger than a large number.

2. A good many (of) เป็นภาษาพูดใช้ขยายเฉพาะนามนับได้เท่านั้น และกริยาต้องเป็นพหูพจน์เสมอ

A good many of my pupils still make spelling mistakes.

(= a large number of my pupils)

A good many people were there.

(= a large number of people)

3. Several of ใช้ขยายเฉพาะพหูพจน์เท่านั้น และใช้กริยาพหูพจน์เสมอ

Several of us decided to walk home.

Several of the glasses were broken.

Several of Jimmy's books are on the table.

There are several of my books on the shelf.

4. Few, A few; Little, A little

few และ a few ใช้กับนามพหูพจน์เท่านั้น

			books			
There are	+	few	+	pens	+	left.
		a few		cakes		
				sandwiches		

5. Little และ A little ใช้กับนามนับไม่ได้เท่านั้น

			sugar			
There is	+	little	+	money	+	left.
		a little		time		
				chance		

few = not many; nearly none หมายความว่า น้อยมากหรือแทบจะไม่มี ใช้ขยายนามนับได้พหูพจน์มีความหมายเป็นปฏิเสธ (negative meaning)

a few = some หมายความว่า พอมีอยู่บ้าง แต่ไม่มากนัก ใช้ขยายนามนับได้พหูพจน์มีความหมายเป็นบอกรับ (affirmative meaning)

The room was nearly empty; there were few people.

Although it is 11 p.m., there are still a few people in the street.

He is very selfish man, so he has few friends.

Few of us own five cars. (= Not many of us own .....)

A few of the students went on foot but most of them went by bus.

(= Some of the students went on foot .....)

Little = not much; nearly none หมายความว่าน้อยมาก ใช้ขยายนามนับไม่ได้มีความหมายเป็น ปฏิเสธ

A little = some หมายความว่า พอมีอยู่บ้าง ใช้ขยายนามนับไม่ได้ มีความหมายเป็นบอกรับ

There is little food in the house, so we cannot give you any.

We have a little time before the train arrives. Let's have some coffee.

จากกฎการใช้ข้างต้นจะเห็นได้ว่ากลุ่มของคำบอกปริมาณจะมีอยู่ 3 กลุ่มด้วยกัน ซึ่งในแต่ละกลุ่มนั้นจะมีรูปแบบการใช้ที่เหมือนกันแตกต่างกันที่ความหมายทำให้สามารถที่จะทำการเปลี่ยนแทนที่กันได้

2.1.7 คำกริยา (Verb)

คำกริยานั้นเป็นคำที่ใช้ในการบ่งบอกถึงการกระทำของประธานในประโยค ซึ่งพอจะแบ่งคำกริยาออกได้เป็นดังนี้คือ

1. Transsitive Verbs คือกริยาที่ต้องการกรรมมาต่อท้าย เช่น give, buy, order, bring, etc. เช่น

He gave some money to me.

I bought some novels yesterday.

2. Intransitive Verbs คือ กริยาที่ไม่ต้องมีกรรมตามมา เนื่องจากเป็นกริยาที่มีความหมายสมบูรณ์อยู่ในตัว ไม่ต้องการกรรมมาต่อท้าย ก็ทำให้ประโยคสมบูรณ์ เช่น go, swim, run etc.

When did he go ?

I'd like to swim today.

3. Finite Verbs คือ กริยาแท้ ซึ่งรูปของกริยาจะเปลี่ยนแปลงไปตามประธานและ Tense เช่น

He visits his grandparents every sunday.

They go shopping.

She played tennis yesterday.

4. Non-Finite Verbs คือ คำที่มาจากกริยา แต่ไม่ได้ทำหน้าที่กริยาแท้ หมายความว่ารูปแบบของคำจะไม่เปลี่ยนไปตามประธานและ Tense แบบกริยาแท้นั่นเอง

Non-Finite Verbs จะอยู่ในรูปของ Infinite, Gerund หรือ Participle ก็ได้ เช่น

I want you to go now.

She wanted you to go there.

5. Auxiliary Verbs, Anomalous Verbs หรือ Helping Verbs คือ กริยาช่วยที่ไปทำให้กริยาแท้มีความหมายเปลี่ยนแปลงไป หรือ เปลี่ยนรูปประโยค เช่นจากคำถามเป็นปฏิเสธ ช่วยแสดงกาลเวลา ตลอดจนการคาดคะเน, สัญญา ฯลฯ กริยาช่วยใน Finite forms ทั้ง 24 ตัว นี้เรียกว่า Anomalous verbs ต่างจาก Non-finite forms ก็คือ เราสามารถเติม not หลัง Anomalous verbs ได้เช่น

I haven't finited it yet. have ในประโยคนี้เป็น Anomalous verbs

I don't have breakfast at 8 o'clock. have ในประโยคนี้เป็น Auxiliary non-finite เพราะเราจะไม่พูดว่า I haven't breakfast.

สำหรับกรณีของคำกริยานั้นถ้าหากเปลี่ยนไปจะทำให้ความหมายของประโยคเปลี่ยนแปลงไปจากเดิมอย่างมากอีกทั้งคำกริยานั้นก็ยังแบ่งออกเป็น 5 พวกซึ่งบางพวกต้องมีกรรมมารับข้างท้ายแต่บางพวกไม่มีกรรมมารับข้างท้ายถ้าหากเปลี่ยนมาแทนกันก็จะทำให้ผิดไวยากรณ์ภาษาอังกฤษไปในทันที

2.1.8 คำกิริยาวิเศษณ์ (Adverbs) มีหน้าที่ดังนี้

1. ขยายคำกิริยา เช่น

He work hard.

She play tennis well.

2. ขยายคำกริยาวิเศษณ์ด้วยกัน เช่น

He drives very carefully.

It rain rather heavily.

3. ขยายคำคุณศัพท์ เช่น

They are very intelligent.

His work is good enough.

4. ขยายประโยค เช่น

Frankly, I am hard up.

Fortunately, no one complained.

5. ขยายวลี เช่น

He walked straight to the hut.

They lived nearly on the top of the hill.

ชนิดของคำกริยาวิเศษณ์

1. คำกริยาวิเศษณ์ที่บอกความถี่ (Adverbs of frequency)

ได้แก่ คำหรือกลุ่มคำที่บอกความถี่ของการกระทำหรือตอบคำถามว่า"ทำบ่อยแค่ไหน" (how often) แบ่งออกเป็น

1.1 คำกริยาวิเศษณ์ที่บอกความถี่ที่เป็นคำๆ เดียว เช่น often, usually, ever, never, always, generally, frequently, occasionally, sometime, seldom, rarely, hardly, scarcely

ตำแหน่งของกริยาวิเศษณ์ที่บอกความถี่

1. วางไว้หลัง verb to be เช่น

I am always at home on saturdays.

Betty is occationally a little nervious.

2. วางไว้หน้ากิริยาแท้ เช่น

I rarely go to the cinema.

She often leaves without permission.

3. วางไว้หลังกิริยาช่วย เช่น

He can sometimes find time for reading.

He will never agree to my suggestion.

ถ้าในประโยคมีกิริยาหลายตัวให้วางแทรกหลังกิริยาช่วยตัวแรก เช่น

He has often been praised for his experiment.

4. วางไว้หลัง not เช่น

He does not always work hard.

1.2 คำกริยาวิเศษณ์ที่บอกความถี่ที่เป็นกลุ่มคำ จะใช้ตอบคำถาม How often ? เช่นเดียวกันกับ คำกริยาวิเศษณ์บอกความถี่ที่เป็นคำเดียว เช่น every two months, every other day, as often as, you wish, etc.

ตำแหน่งในการวางคำกริยาวิเศษณ์ประเภทนี้

1. ปรกติจะวางไว้ท้ายประโยค เช่น

His son practices swimming four times a week.

This furnace should be cleared of ash every fourth day.

2. ถ้าต้องการเน้นจะวางขึ้นต้นประโยค เช่น

Again and again I've warned you to be late.

Every ten minutes there are buses to the station.

2. คำกริยาวิเศษณ์เพื่อบอกเวลา (Adverb of time)

ได้แก่คำหรือกลุ่มคำที่ทำหน้าที่ขยายกิริยาเพื่อบอกเวลา หรือตอบคำถามว่า 'when' เช่น

When did you arrive home ?

Yesterday / At three o'clock. / Last night

คำกริยาวิเศษณ์เพื่อบอกเวลามีสองชนิด คือ

2.1 ไม่มีคำบุพบท (preposition) นำหน้า เช่น yesterday, three days ago, tomorrow, evening, etc.

2.2 มีคำบุพบทนำหน้า เช่น on saturday, in summer, at seven o'clock, etc.

ตำแหน่งของคำประเภทนี้คือ

1. ปรกติจะวางทิ้งไว้ท้ายประโยค แต่ถ้าต้องการจะเน้นเวลาก็จะวางคำวิเศษณ์ที่บอกเวลานั้น ๆ ไว้หน้าประโยค

She'll leave for London on Sunday morning.

Where are you likely to be next month.

Last summer we went to Scothland; this summer we're going to Wales.

2. จะวางไว้หน้าประโยคหรือท้ายประโยคก็ได้

We left Bangkok at eight o'clock.

At noon the plane landed at Singapore Airport.

คำกริยาวิเศษณ์เพื่อบอกเวลานั้นนอกจากจะเป็นกลุ่มคำทั้งที่ใช้กับคำบุพบทและใช้ตามลำพังแล้ว ยังสามารถใช้กับ อนุประโยคได้ด้วยซึ่งเราเรียกว่า adverbial clauses of time clause ชนิดนี้จะขึ้นต้นด้วย when, since, after, as soon as, before. ฯลฯ เป็นต้น ซึ่งตำแหน่งของ Adverbial clauses of time นี้จะอยู่ส่วนใดในประโยคก็ได้ เช่น

Come and see me as soon as you can.

When you have time, come and see me.

The crowds of shoppers, after they had heard the warnin about the bomb, ran for shelter.

3. ในกรณีที่มี adverbs of time หลายคำ นิยมวาง adverb of time จากหน่วยเล็กไปหาหน่วยใหญ่ เช่น

Pick me up at 6 o'clock tomorrow morning.

At three o'clock tomorrow I'll meet you at front of the theatre.

3. คำกริยาวิเศษณ์ที่ใช้กับระยะเวลา (Adverbs of duration)

ก็คือคำกริยาวิเศษณ์เพื่อบอกเวลา อย่างหนึ่ง ต่างกันแต่ว่า คำกริยาวิเศษณ์เพื่อบอกเวลาจะตอบคำว่า When ส่วนคำกริยาวิเศษณ์ที่ใช้กับระยะเวลาจะตอบคำว่า how long หรือระยะความยาวของเวลา ซึ่งแบ่งออกได้เป็นสามกลุ่มด้วยกัน

กลุ่มที่1 นำหน้าด้วย for เช่น

We have studied English for ten years.

กลุ่มที่2 นำหน้าด้วย from-to หรือ from-till (utill) เช่น

He works from nine to twelve.

from nine till twelve.

from nine untill twelve.

กลุ่มที่3 นำหน้าด้วย till,untill หรือ up to เช่น

He will stay here till tomorrow morning.

untill tomorrow morning.

up to tomorrow morning.

4. คำกริยาวิเศษณ์เพื่อบอกสถานที่ (Adverb of place)

คำกริยาวิเศษณ์เพื่อบอกสถานที่ได้แก่ คำหรือกลุ่มคำที่ทำหน้าที่ขยายกริยาเพื่อบอกสถานที่ หรือตอบคำถามว่า "where" เช่น

Where will I put these books ?

On that shelf.

He met with an accident at the crossroads.

While we were staying at the hotel, a conference was being held.

ตำแหน่งของคำกริยาวิเศษณ์เพื่อบอกสถานที่

ปกติจะวางไว้ท้ายประโยค และถ้ามี adverbs of place มากกว่า 1 คำ ก็จะเรียงจากสถานที่เล็กไปหาสถานที่ใหญ่ เช่น

He lives in a small village in Bedford.

5. คำกริยาวิเศษณ์ที่เกี่ยวกับวิธีการ (Adverbs of manner)

คือ คำที่ตอบคำถามว่า อย่างไร (How) คำกริยาวิเศษณ์ที่เกี่ยวกับวิธีการมักมาจาก คำคุณศัพท์โดยเติม -ly หลัง คำคุณศัพท์เหล่านั้น เช่น

คำคุณศัพท์	คำกริยาวิเศษณ์
Helen is a slow driver.	She drives slowly.
Matin is a dangerous driver.	He drives dangerously.

Julian is a careful driver. She drives carefully.

ข้อสังเกต คำที่ลงท้ายด้วย ly ไม่ได้หมายความว่าจะเป็นคำกริยาวิเศษณ์ที่เกี่ยวกับวิธีการเสมอไป เช่น lovely, elderly, friendly, likely, etc. ซึ่งถึงจะลงท้ายด้วย -ly แต่เป็นคำคุณศัพท์

ตำแหน่งของคำกริยาวิเศษณ์ที่เกี่ยวกับวิธีการ

ถ้าในประโยคนั้นมีกรรมตรง (direct object) อยู่ด้วย เราจะวาง คำกริยาวิเศษณ์ที่เกี่ยวกับวิธีการไว้หลังกรรมตรง ถ้าในประโยคนั้นไม่มีกรรมตรง คำกริยาวิเศษณ์ที่เกี่ยวกับวิธีการจะอยู่หลังคำกริยา เช่น

She plays tennis beautifully.

He spoke English well.

สำหรับคำกริยาวิเศษณ์นั้นตามหลักของภาษาอังกฤษที่กล่าวมาแล้วนั้นจะเห็นได้ว่าจะมีคำกริยาวิเศษณ์พวกบอกความถี่บ่อยที่สามารถที่จะสามารถนำมาเปลี่ยนแปลงได้โดยที่ยังคงความถูกต้องทางหลักไวยากรณ์ทางภาษาอังกฤษเหมือนเดิม แต่ความหมายของประโยคในด้านจำนวนความถี่ความบ่อยในประโยคเปลี่ยนไป เช่น

He always plays basketball with children.

He never plays basketball with children.

I am always at home on Saturdays.

I am hardly at home on Saturdays.

2.2 การเข้ารหัสและการถอดรหัสเบื้องต้น

ในการที่จะทำระบบรหัสลับที่ไม่แสดงความเป็นรหัสลับนั้นจะต้องมาทำการศึกษาถึงระบบในการเข้ารหัสเสียก่อนว่ามีอะไรบ้าง ประกอบด้วยอะไรบ้าง ในระบบเข้ารหัสลับนั้นจะต้องประกอบไปด้วยข้อความก่อนการเข้ารหัส (Plaintext)ซึ่งเป็นข้อความเริ่มต้นที่จะทำการเข้ารหัสลับ กระบวนการในการเข้ารหัสข้อความของเราเรียกว่าการเข้ารหัส (Encryption) ส่วนข้อความที่ได้จากการ การเข้ารหัสเรียกว่า ข้อความที่เข้ารหัส (Ciphertext) และกระบวนการที่ทำการเปลี่ยนข้อความที่เข้ารหัสไว้นั้น ให้กลับไปเป็นข้อความเดิมก่อนการเข้ารหัสเรียกว่า การถอดรหัส (Decryption) สำหรับในโครงงานนี้จะมุ่งความสำคัญไปที่การเข้ารหัสข้อมูลที่เป็นข้อความ ที่เก็บอยู่ในรูป Text File ปกติที่ใช้กันอยู่ เพื่อเป็นการกำหนดขอบเขตของโครงงาน

จากการศึกษาวิธีในการเข้ารหัสข้อความนั้นจะมีวิธีพื้นฐานอยู่ 2 วิธี คือ

1. การแทนที่ตัวอักษร (Substitutions) ซึ่งเป็นการทีเปลี่ยนอักษรตัวหนึ่งไปเป็นอีกตัวหนึ่ง

2. การจัดเรียงตัวอักษร (Transpositions) จะเป็นวิธีที่จะทำการเรียบเรียงลำดับของตัวอักษรใหม่

ทั้ง 2 วิธีนั้นเป็นวิธีที่ใช้กับตัวอักษรเพียงตัวเดียว ซึ่งไม่สามารถที่จะนำมาใช้งานได้ในโครงงาน เพราะถ้าใช้การสร้างรหัสลับตาม 2 วิธีนั้นก็จะเป็นการเข้ารหัสแบบธรรมดา ซึ่งเมื่อดูแล้วก็จะรู้ว่าเป็นรหัสลับซึ่งจะใช้โดยตรงไม่ได้ จึงต้องทำการประยุกต์นำมาใช้งาน

2.3 การเข้ารหัสแบบแทนที่ตัวอักษร (Substitutions)

เป็นวิธีการที่ใช้การแทนที่ตัวอักษรแต่ละตัวด้วยตัวอักษรตัวอื่นหรือสัญลักษณ์อื่น สำหรับเทคนิคในการเข้ารหัสแบบต่อไปนี้เรียกว่า monoalphabetic cipher หรือ simple substitution ซึ่งก็มีอยู่ด้วยกันหลายชนิดซึ่งจะได้อธิบายดังต่อไปนี้

2.3.1 รหัสลับแบบ Caesar (Caesar Cipher)

รหัสลับแบบ Caesar เป็นชื่อที่ตั้งเป็นเกียรติแก่ Julius Caesar ซึ่งเป็นบุคคลที่คิดค้นวิธีนี้ขึ้นเป็นวิธีการของรหัสลับแบบ Caesar นั้นแต่ละตัวอักษรนั้นจะถูกเปลี่ยนไปอีกตัวอักษรหนึ่งโดยที่ระยะห่างระหว่างตัวอักษรที่เปลี่ยนไปกับตัวอักษรเดิมนั้นเป็นเลขคงที่จำนวนหนึ่ง ดังนั้นถ้าใช้วิธีการ Caesar นั้นเลื่อนไป 3 ตัวอักษร ดังนั้นตัวข้อความต้นฉบับ

แทนด้วย p_i นั้นถูกเปลี่ยนเป็นข้อความที่เข้ารหัสแทนด้วย c_i แล้ว สามารถแทนได้ด้วยสมการดังต่อไปนี้

$$c_i = E(p_i) = p_i + 3$$

รูปแสดงการเปลี่ยนของตัวอักษรโดยวิธี Caesar นั้นจะได้ดังนี้

plaintext letter :

A B C D E F G H I J K L M N O P Q R S T U V W X Y Z

ciphertext letter :

d e f g h i j k l m n o p q r s t u v w x y z a b c

ถ้าใช้วิธีการเข้ารหัสแบบ Caesar กับข้อความ

TREATY IMPOSSIBLE

เราก็จะได้ข้อความที่เข้ารหัสแล้วดังนี้

TREATY IMPOSSIBLE

wuhdwb lpsrvvleoh

2.3.2 ข้อดีและข้อเสียของการเข้ารหัสแบบ Caesar

การเข้ารหัสแบบ Caesar นั้นเป็นวิธีการเข้ารหัสที่ง่ายวิธีหนึ่ง แต่ก็เป็นวิธีที่ใช้ได้ดีในสมัยของ Julius Caesar ก็เพราะในสมัยก่อนนั้นมีคนมีความรู้ความสามารถที่จะอ่านตัวอักษรธรรมดาออกนั้นมีน้อย สำหรับวิธีการเข้ารหัสแบบ Caesar นั้นจะมีรูปแบบ $p_i + 3$ ซึ่งง่ายในการจำ ทำให้การใช้งานง่าย ผู้ส่งข้อความสามารถที่จะเข้ารหัสข้อความเดิมไปเป็นรหัสลับได้ง่าย แล้วทำลายข้อความเดิมได้ง่าย แต่เนื่องจากความที่เป็นรูปแบบแน่นอนนี้เองที่เป็นจุดอ่อนที่สำคัญของวิธีการเข้ารหัสแบบ Caesar การเข้ารหัสเพื่อรักษาความปลอดภัยในเครื่องคอมพิวเตอร์นั้นไม่ควรที่จะมีคุณสมบัติแบบนี้ เพราะถ้าหากมีคนได้ส่วนของรหัสลับนี้ไปเพียงส่วนน้อย ก็สามารถที่จะเดารูปแบบทั้งหมดของการเข้ารหัสได้

2.3.3 วิธีการวิเคราะห์รหัสที่เข้ารหัสแบบ Caesar

ลองมองดูผลจากการเข้ารหัสของตัวอย่างก่อนหน้านี้จะเห็นได้ว่า ร่องรอยจากข้อความเดิมจะมาปรากฏที่ข้อความที่เข้ารหัส ดูตรงที่ ss ของข้อความเดิมจะถูกเปลี่ยนเป็น vv และ ตัวอักษรที่ใช้ซ้ำกันบ่อยๆ เช่น T, I, E ซึ่งจะถูกเปลี่ยนเป็นตัว w, l และ h ซึ่งร่องรอยนี้ช่วยให้การหาข้อความเดิมนั้นเป็นไปโดยง่าย

สมมุติว่าคุณพยายามหาข้อความเดิมของข้อความที่เข้ารหัสต่อไปนี้

wklv phvvdjh lv qrw wrr kdug wr euhdn

โดยปกติแล้วข้อความที่จะเข้ารหัสนั้นจะใช้ตัวอักษรอยู่ทั้งหมด 27 ตัวคือ A ถึง Z และช่องว่าง(blank) ซึ่งเป็นตัวแยกระหว่างคำ ในกรณีที่แย่ที่สุดนั้นช่องว่างจะไม่เปลี่ยนแปลง แต่ในการเข้ารหัสจริงๆ แล้วนั้นจะตัดช่องว่างทิ้ง เพราะจากข้อสมมุติที่ว่าถ้าหากเป็นผู้รับที่ถูกต้องแล้วก็สามารถที่จะแยกแต่ละคำได้โดยไม่ยาก

ในภาษาอังกฤษนั้นจะมีความสัมพันธ์กับคำสั้นๆอย่างเช่น "am", "is", "to", "be", "he", "we", ... , "and", "are" , "you", "she" เป็นต้น ดังนั้นในตอนที่จะทำการวิเคราะห์รหัสลับก็คือพยายามแทนคำสั้นๆ ที่เรารู้จักลงในตำแหน่งที่เหมาะสมของข้อความที่เข้ารหัส และพยายามแทนให้เข้ากับตัวอักษรที่เหมือนกันในตำแหน่งอื่นๆ ของข้อความนั้น

สำหรับร่องรอยที่ชัดเจนก็คือ r ที่ซ้ำกันในคำ wrr คำที่เจอได้บ่อยสำหรับคำที่มีตัวอักษร B ตัว ที่มีรูปแบบเป็น xyy คือ "SEE" และ "TOO" จะมีโอกาสน้อยที่จะเป็น "ADD", "ODD" หรือ "OFF" ถ้า wrr เป็นคำว่า SEE เราก็จะแทน wr ได้เป็น SE ซึ่งมันไม่

ใช่ แต่ถ้าเราแทน wrr เป็น TOO ก็จะได้ wr เป็นคำว่า TO ซึ่งมีเหตุผลดี แล้วแทนที่ T แทน w และ O แทน r

wklv phvvdjh lv qrw wrr kdug wr euhdn

T--- ------- -- -OT TOO ---- TO -----

เพราะฉะนั้นจะได้ประโยคเป็น จะเห็นว่า ตรงคำ -OT นั้นสามารถที่จะเป็น "cot" หรือ "dot" หรือ "got"หรือ "hot" หรือ "lot" หรือ "not" หรือ "pot" หรือ "rot" หรือ "tot" แต่ตัวเลือกนี้น่าจะเป็น "not" โชคไม่ดีที่ q = N ไม่ได้ให้ร่องรอยอะไรเลย มาดูคำว่า lv ซึ่งก็มีอยู่ในตอนท้ายของคำว่า wklv ซึ่งเริ่มต้นด้วย T คราวนี้ลองมาดูว่าคำที่มี 2 ตัวอักษร และสามารถเป็นตัวท้ายของคำที่ยาวกว่าได้มีอะไรบ้าง ก็จะได้คำว่า SO, IS, IN อย่างไรก็ตาม SO นั้นเป็นไปไม่ได้ เพราะเมื่อแทนเป็น T-SO แล้วไม่มีคำแบบนี้แน่ ลองมาดู

IN ใช้คำนี้ไม่ได้ เพราะจะขัดกับตอนแรกที่ให้ q = N ดังนั้นคำว่า IS จึงเหมาะสมที่จะแทน lv จากนั้นก็ทำการวิเคราะห์ข้อความต่อ ในลักษณะแบบนี้ต่อไป

2.3.4 การวิเคราะห์หาข้อความเดิมของการเข้ารหัสแบบแทนที่

เทคนิคการหาข้อความเดิมของ Caesar Cipher นั้นสามารถใช้กับวิธีการเข้ารหัสแบบแทนที่อย่างอื่นได้ คำสั้นๆ คำซ้ำ ซึ่งเป็นเบาะแสให้เดาหาข้อความเดิม ซึ่งก็แน่นอนว่าคุณจะต้องพยายามเดาและแทนที่ตัวอักษรที่เดานั้น จนกระทั่งได้คำทั้งหมด หรือจนกว่าจะเจอที่ขัดแย้ง ถ้าข้อความนั้นยาวมากๆ การทำอย่างนี้เป็นเรื่องที่น่าเบื่อที่สุด แต่โชคดีที่ยังมีวิธีในการวิเคราะวิธีอื่นอยู่

การกระจายความถี่

ในภาษาอังกฤษนั้นจะมีตัวอักษรบางตัวที่จะใช้บ่อยมากกว่าตัวอื่น ดังในตารางที่ 2.1 จะแสดงจำนวนและความถี่ของตัวหนังสือในหนังสือที่สุ่มมา

จากตารางนั้นสามารถที่จะใช้วิเคราะห์ข้อความที่เข้ารหัสต่อไปนี้

	English		Pascal	
Letter	Count	Percent	Count	Percent
a	3312	7.49	664	4.7
b	573	1.29	197	1.39
c	1568	3.54	878	6.22
d	1602	3.62	511	3.61
e	6192	14	1921	13.6
f	966	2.18	5.4	3.57
g	769	1.74	294	2.08
h	1869	4.22	478	3.39
i	2943	6.65	1215	8.6
j	119	0.27	6	0.04
k	206	0.47	87	0.61
l	1579	3.57	722	5.11
m	1500	3.39	270	1.91
n	2982	6.74	1157	8.19
o	3261	7.37	835	5
p	1074	2.43	340	2.41
q	116	0.26	12	0.08
r	2716	6.14	1147	8.12
s	3072	6.95	594	4.21
t	4358	9.85	1311	9.28
u	1329	3	377	2.66
v	512	1.16	127	0.89
w	748	1.69	193	1.36
x	123	0.28	139	0.98
y	727	1.64	137	0.96
z	16	0.04	5	0.03
ALL	44232		14121	

รูปที่ 2.1 ตารางการกระจายของตัวอักษรในภาษาอังกฤษและภาษาปาสคาล

Letter	Count		Letter	Count	Percent
a	0	0	n	0	0
b	3	1.8	o	4	2.41
c	0	0	p	5	2.99
d	11	6.59	q	16	9.58
e	2	1.2	r	9	5.39
f	6	3.61	s	3	1.8
g	4	2.4	t	0	0
h	26	15.56	u	8	4.79
i	2	1.2	v	17	10.18
j	5	2.99	w	14	8.38
k	5	2.99	x	5	2.99
l	16	9.58	y	4	2.4
m	0	0	z	2	1.2
ALL	167				

รูปที่ 2.2 ตารางแสดงความถี่ของรหัสในตัวอย่างที่สุ่มขึ้น

จากทั้ง 2 ตารางจะสังเกตุความสัมพันธ์ระหว่างข้อมูลของ 2 ตารางได้ดังนี้ คือ ค่าความถี่ของตัวอักษรในตารางแรกจะมีค่าใกล้เคียงกับตัวอักษรที่ถัดจากอักษรในตารางแรก 3 ตัวอักษร ซึ่งในตัวอย่างนั้นเข้ารหัสแบบ Caesar โดยที่เลื่อนไปทางขวา 3 ตำแหน่ง เพราะฉะนั้นสามารถใช้ตารางความถี่ช่วยวิเคราะห์ได้

2.3 การเข้ารหัสแบบจัดเรียงตัวอักษร (Transpositions)

จุดประสงค์ของการเข้ารหัสแบบแทนที่นั้นก็เพื่อทำให้เกิดความสับสนและพยายามให้วิธีที่จะทำให้ ข้อความและคีย์นั้นเปลี่ยนเป็นรหัสลับให้ยากไว้ ส่วนวิธี Transpositions ของการเข้ารหัสลับของตัวอักษร ในข้อความนั้นมาจัดเรียงตัวอักษรใหม่ ซึ่งจุดประสงค์ของการจัดเรียงใหม่นั้นก็เพื่อทำให้เกิดการกระจายออก ของข้อมูลจากข้อมูลของข้อความเดิม

แต่วิธีการ Transpositons นี้สามารถทำการวิเคราะห์ได้ง่ายเนื่องจากมีรูปแบบที่แน่นอนตายตัว เพราะว่าวิธีนี้ก็คือการจัดเรียงของสัญลักษณ์ต่างๆ ในข้อความใหม่ซึ่งเราก็เรียกว่าการจัดเรียงลำดับ (Permutation)

2.4.1 การเข้ารหัสแบบจัดเรียงอักษรแบบคอลัมน์ (Columnar Transpositions)

เราจะเริ่มต้นด้วยการศึกษาวิธีที่ง่ายๆ ก่อนนั่นก็คือการเข้ารหัสแบบจัดเรียงอักษรแบบคอลัมน์ ซึ่งเป็นการจัดเรียงลำดับของตัวอักษรในข้อความเดิมก่อนเข้ารหัสลงเป็นคอลัมน์ ซึ่งจากตัวอย่างต่อไปนี้จะเป็นการจัดเรียงเป็น 5 คอลัมน์ ตัวอักษรนั้นจะกระจายเป็น 5 บล็อค ส่วนของตัวอักษรที่เหลือก็จะถูกจัดเป็นบล็อคต่อจากบล็อคนี้ ซึ่งจะได้แสดงดังนี้

C_1 C_2 C_3 C_4 C_5

C_6 C_7 C_8 C_9 C_{10}

C_{11} C_{12} C_{13} C_{14} C_{15}

ข้อความรหัสลับที่ได้จากวิธีการจัดเรียงเป็นคอลัมน์เป็นดังนี้คือ

$C_1\ C_6\ C_{11}\ \ldots C_2\ C_7\ C_{12}\ \ldots\ C_3\ C_8\ C_{13}$, etc.

ตัวอย่างของข้อความเดิมนั้นนำมาเขียนเป็นคอลัมน์ได้ดังนี้

T	H	I	S	I
S	A	M	E	S
S	A	G	E	T
O	S	H	O	W
H	O	W	A	C
O	L	U	M	N
A	R	T	R	A
N	S	P	O	S
I	T	I	O	N
W	O	R	K	S

รูปที่ 2.3 แสดงการเรียงของตัวอักษรในการเข้ารหัสแบบจัดเรียง

เพราะฉะนั้นข้อความรหัสลับที่ได้คือ

tssoh oaniw haaso lrsto imghw

utpir seeoa mrook istwc nasns

ความยาวของข้อความนี้จะเป็นผลคูณของ 5 ถ้าข้อความที่เราเข้ารหัสนั้นน้อยกว่าที่จะทำให้เต็มทุกคอลัมน์ ตัวอักษรที่นำมาใช้เติมให้เต็มคือตัวอักษร X

2.5 ส่วนของการวิเคราะห์คำ (Lexical Analysis)

ส่วนแรกในการทำงานคือส่วนของการวิเคราะห์คำเพื่อที่จะทำการแยกข้อความออกเป็นคำๆ โดยที่จะต้องแยกให้ออกว่าในประโยคนั้น แต่ละคำนั้นมีหน้าที่อะไร

ตัวอย่างเช่น ประโยค "the cat ate a mouse." อย่างน้อยเราจะต้องรู้ว่าคำว่า the นั้นทำหน้าที่เป็น article ของประโยคและ a นั้นก็ทำหน้าที่เป็น article เช่นกัน โดยการแยกออกเป็นคำ ๆ นี้เราเรียกแต่ละคำว่าโทเคน (token)

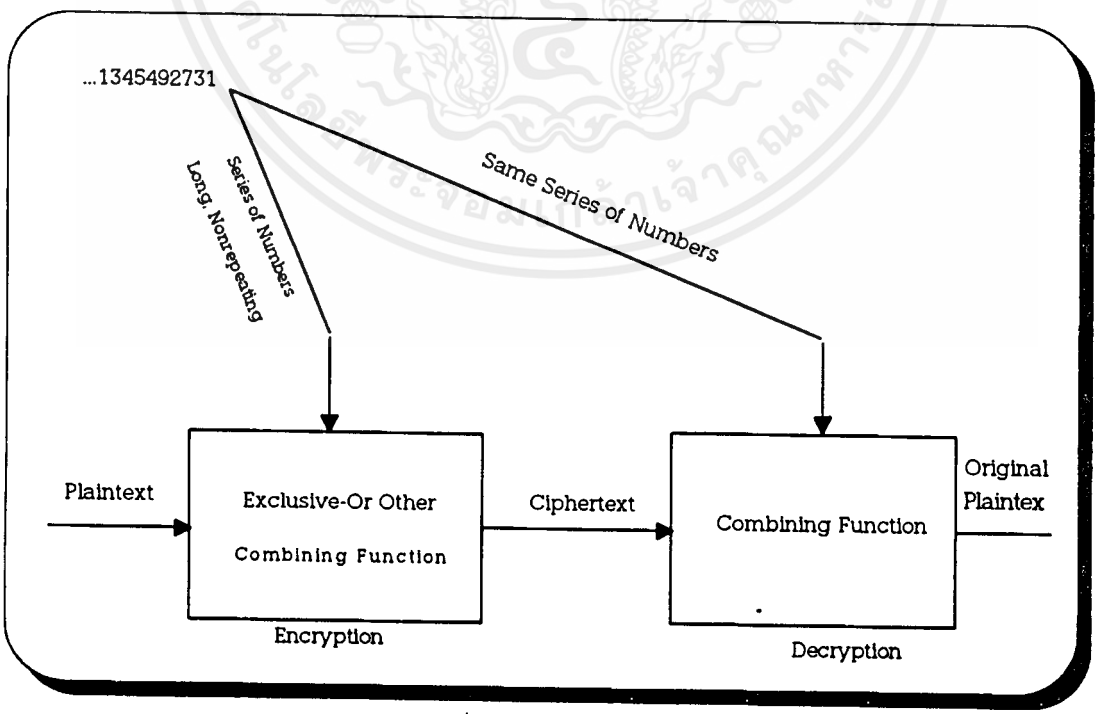
ในขั้นตอนของการทำส่วนของการวิเคราะห์คำนั้น โดยที่แต่ละ token นั้นจะตรวจสอบดูว่ามีหน้าที่อะไรในภาษาอังกฤษ โดยที่จะทำการตรวจสอบโดยการค้นหาในพจนานุกรมที่ได้สร้างเอาไว้ก่อนหน้านี้แล้ว แต่จะเห็นว่าคำนามทั่ว ๆ ไปหรือคำกิริยานั้นมีมากมายยากที่เราจะระบุความแตกต่างหรือกำหนดลงไปให้มีหมายเลขเฉพาะได้ ซึ่งสิ่งที่อาจจะทำได้ก็คือ วิธีแรกเราจะใช้วิธีการค้นหาคำนั้นในตารางของพจนานุกรมที่มีอยู่ เช่น คำว่า cat ซึ่งเป็นคำที่ตามหลัง article 'the' ซึ่งโดยมากแล้วคำที่ตามหลัง article ก็มักจะเป็นคำนามหรือคำคุณศัพท์ หรือเป็นช่วงของวลีของคำนาม (Noun Phrase) หรือ วลีของประธาน (Subject Phrase) นั่นเอง ซึ่งเราก็จะใช้วิธีการค้นหาในตารางของคำนาม ถ้าไม่เจอก็จะไปหาที่ตารางของคำคุณศัพท์ เมื่อมีการค้นหาเจอแล้วเราก็สามารถกำหนดหมายเลขเฉพาะให้กับโทเคนนั้นได้หรืออีกวิธีหนึ่งก็คือเราจะส่งโทเคนนั้นไปโดยที่ยังไม่แยกความแตกต่างของโทเคนของคำทั่ว ๆ ไปเช่น คำนามหรือคำกริยา โดยจะไปแยกอีกทีหนึ่ง

2.6 การสร้างรหัสลับ

การสร้างรหัสลับจากประโยคที่มีความถูกต้องตามหลักไวยากรณ์ ขึ้นให้เหมาะสมกับประโยคในข้อความของข้อความเดิมก่อนที่จะเข้ารหัส โดยในการสร้างรหัสลับนี้ทำได้โดยการนำประโยคที่กระจายคำ โดยที่ทำการเปรียบเทียบกับคำในฐานข้อมูลที่มีอยู่นั้นเพื่อที่จะได้รู้ถึงหน้าที่ของคำศัพท์คำนั้นว่าทำหน้าที่อะไรในประโยคภาษาอังกฤษ ซึ่งถ้าหากคำศัพท์คำนั้นเท่าหน้าที่เป็นคำศัพท์ที่เปลี่ยนแปลงได้ ก็จะนำมาทำการผ่านการเข้ารหัสลับทีละคำ โดยที่ในการทำการเข้ารหัสลับ นั้นจะต้องมีฐานข้อมูลที่เก็บคำศัพท์ต่างๆ ที่มีอยู่ในภาษาอังกฤษไว้โดยที่จะเก็บรวมกลุ่มกันตามแต่ละหน้าที่ในภาษาอังกฤษ เช่น เป็นคำศัพท์เฉพาะในส่วนของประธานเป็นคำศัพท์ในส่วนของกริยา ส่วนของขยายประธาน ส่วนของขยายกริยา ส่วนของขยายกรรมโดยจะทำการเข้ารหัสลับทีละตัวเริ่มจากคำซ้ายมือสุดดูว่าทำหน้าที่เป็นอะไรในประโยค จากนั้นนำคำ ๆ นั้นไปเทียบค่า

ในฐานข้อมูลที่มีอยู่ว่ามีค่าเท่าไหร่ จากนั้นก็ทำการผ่านการเข้ารหัสลับซึ่งก็จะได้ ข้อความที่เป็นรหัสลับเป็นคำ ๆ ใหม่ขึ้นมา แล้วก็ดูตัวต่อไปว่าทำหน้าที่อะไรแล้วก็ดูค่ามันว่ามีค่าเท่าไหร่แล้วก็ทำการเข้ารหัสลับอีก ทำอย่างนี้จนหมดประโยค ซึ่งผลลัพธ์ก็จะเป็นประโยคใหม่ตามที่ต้องการ ในส่วนของการเข้ารหัสลับนั้นก็จะใช้วิธีการที่เรียกว่า รหัสลับแบบเวอร์แนม (Vernam Cipher) ซึ่งก็เป็นวิธีที่ป้องกันการวิเคราะห์เพื่อการถอดรหัสที่ดีวิธีหนึ่ง วิธีนี้ทำได้โดยใช้ลำดับของตัวเลขสุ่มที่ไม่ซ้ำกันซึ่งเรียกว่าคีย์ มาบวกกับค่าที่ได้จากคำในข้อความเดิมก่อนที่จะเข้ารหัสที่หาได้จากฐานข้อมูล เพื่อใช้ในการสร้างรหัสลับ สำหรับตัวเลขที่สุ่มขึ้นมานั้นจะถูกเก็บไว้เป็นตาราง เพื่อที่จะได้สามารถเรียกใช้ได้ง่าย และ ที่สำคัญควรจะมีลำดับของตัวเลขสุ่มที่ไม่ซ้ำกันนี้ยาวพอสำหรับข้อความทั้งหมด เพราะจะเป็นการป้องกันการวิเคราะห์เพื่อถอดรหัส การใช้ รหัสลับแบบเวอร์แนมนี้จะป้องกันการวิเคราะห์เพื่อถอดรหัสได้ดีที่สุดก็ต่อเมื่อไม่มีคีย์ที่ซ้ำกันหรือ ไม่มีการนำคีย์เก่ากลับมาใช้ใหม่ ซึ่งถ้าทำได้ก็จะทำให้การทำเข้ารหัสลับนั้นดีที่สุด เพราะถ้าหากมีการซ้ำกันของคีย์เกิดขึ้น ในข้อความของเราอาจจะเป็นไปได้ที่คีย์เดียวอาจจะเจอกับคำ ๆ เดียวกัน ซึ่งก็จะทำให้อาชญากรทางคอมพิวเตอร์วิเคราะห์และสามารถถอดรหัสจนรู้ถึงคำเดิมก่อนทำรหัสลับได้ หรือการนำคีย์เดิมมาใช้ก็เช่นกันก็จะทำให้เกิดผลที่เหมือนกับ การใช้คีย์ซ้ำ

การเข้ารหัสลับโดยใช้วิธี รหัสลับแบบเวอร์แนมนั้นได้แสดงไว้ดังนี้



รูปที่ 2.4 Virnam Cipher

สำหรับในระบบรหัสลับแล้วเมื่อมีการเข้ารหัสลับแล้วก็ต้องมีการทำการถอดรหัสลับ เพื่อที่จะให้ได้ข้อความเดิมก่อนการเข้ารหัสลับ คืนมาเมื่อต้องการที่จะใช้โดยการถอดรหัสลับ นั้น จะทำตรงกันข้ามกับที่ทำในการทำเข้ารหัสลับโดยที่จะทำใน 2 ขั้นตอนแรกเหมือนการสร้างรหัสลับ คือแยกคำออกมาดูว่าเป็นคำที่ทำหน้าที่อะไรเพื่อที่จะได้ไปใช้ฐานข้อมูลถูกอัน แล้วก็ทำการหาค่าของคำๆนั้นแล้วทำการลบค่าด้วยค่าคีย์ประจำตำแหน่งนั้น ในตารางที่เก็บค่าคีย์เอาไว้ก็จะได้ค่าของคำ ๆ เก่าออกมา ทำให้ได้คำ ๆ เดิมจากการถอดรหัสลับซึ่งก็เป็นอันว่าเสร็จสิ้นการของระบบการเข้ารหัสลับที่เข้ารหัสแล้วยังเป็นคำในภาษาอังกฤษเหมือนเดิม

ในส่วนที่จะทำการพัฒนาต่อไป ก็คือการนำเอาหลักการต่างๆ เหล่านี้มาประกอบกันเพื่อใช้ในการสร้างแอพพลิเคชันขึ้นมาใช้งานจริง ซึ่งก็จะมีปัญหาปลีกย่อยเกิดขึ้นอีกมากมาย ซึ่งก็จะได้ทำการศึกษาปัญหา และแก้ไขไปพร้อม ๆ กันด้วย ซึ่งแอพพลิเคชันที่ได้ทำเสร็จสมบูรณ์นั้นอาจจะใช้ได้เฉพาะงานในเบื้องต้น ซึ่งคำในประโยคนั้นอาจจะไม่มีความซับซ้อนมากนัก

บทที่ 3

การคำนวณและการสร้าง

ในการทำงานของการเข้ารหัสในรูปแบบนี้นั้น ในขั้นตอนแรกจะทำการแยกข้อความออกเป็นคำ ๆ โดยถือแต่ละคำเป็นโทเคน (token) แล้วจึงทำการเข้ารหัสโดยการแทนที่คำเหล่านั้นด้วยการแทนที่ให้ตรงกับรูปแบบของโครงสร้างประโยคแต่ในการทำงานจริงจะพบว่าการที่จะแทนที่คำต่าง ๆ ลงในประโยคตามอัลกอริธึมการเข้ารหัสแบบต่าง ๆ ซึ่งในที่นี้จะเลือกใช้วิธีการเข้ารหัสแบบเวอร์แนมนั้น ถึงแม้ว่าคำต่าง ๆ ที่เลือกมาแทนนั้นจะตรงตามรูปแบบของโครงสร้างประโยค เช่น คำนามแทนคำนาม กริยาแทนกริยา แต่ภาษาที่ใช้กันทั่วไปนั้น แต่ละคำจะมีความสัมพันธ์ซึ่งกันและกัน ดังนั้นการจะเลือกคำต่าง ๆ มาแทนที่ตามอัลกอริธึมโดยตรงนั้นจึงเป็นการยากและไม่สามารถที่จะทำให้แต่ละคำที่เลือกมานั้นมีความสัมพันธ์กันเมื่อได้ทำการทดสอบและทดลองวิธีต่าง ๆ แล้ว จึงได้เลือกวิธีการทำงานโดยการใช้วิธีการแทนที่เฉพาะในส่วนสำคัญซึ่งเมื่อทำการแทนที่แล้วจะไม่ทำให้โครงสร้างของประโยคเสียไปซึ่งได้แก่ส่วนที่เป็นคำนามคำคุณศัพท์และคำกริยาวิเศษณ์โดยทั่ว ๆ ไปนอกจากนี้ส่วนที่เป็นตัวเลขก็เป็นส่วนสำคัญที่จะทำการเปลี่ยนแปลงด้วย สำหรับส่วนที่เหลือของประโยคที่จะไม่ทำการเปลี่ยนแปลงนั้น คือ พวก Article , คำบุพบท , คำสรรพนาม และ คำกริยา นั้น จากที่ได้ทำการทดสอบและค้นคว้าพบว่าเป็นส่วนที่เป็นโครงสร้างหลักของประโยค ซึ่งเมื่อเปลี่ยนแปลงแล้วจะมีผลกระทบกระเทือนต่อความสัมพันธ์ในประโยคอย่างมาก โดยเฉพาะในส่วนที่เป็นคำกริยาเนื่องจากโดยส่วนใหญ่คำกริยาจะทำหน้าที่เป็นตัวเชื่อมความสัมพันธ์ระหว่างประธานและกรรม รวมไปถึงบุพบทและส่วนอื่น ๆ ทั้งหมดในประโยคด้วย ดังตัวอย่าง เช่น

He always read that red book.

ถ้าทำการเปลี่ยนคำกริยา read ไปเป็นคำอื่นเช่น drive แล้ว จะพบว่ากรรมของประโยคซึ่งได้แก่ book ควรที่จะต้องเปลี่ยนไปเป็นกลุ่มที่เป็นยานพาหนะซึ่งสมมติว่าเปลี่ยนไปเป็น car แต่ในขั้นตอนการแปลงกลับการที่จะหาความสัมพันธ์ ระหว่างคำว่า car กับคำว่า book เพื่อให้คำว่า car แปลงกลับไปเป็นคำว่า book ในขณะที่คำว่า drive ต้องเปลี่ยนกลับไปเป็นคำว่า read นั้น ในขั้นตอนการทำงานจริงพบว่าเป็นไปได้ยากมาก เนื่องจากคำต่าง ๆ เหล่านี้ไม่ได้มีความสัมพันธ์กัน และอยู่ต่างกลุ่มกัน และคำกริยาที่มีในภาษามนุษย์นั้นก็มีมากมาย ดังนั้นการที่จะหาอัลกอริธึมที่จะมากำหนดความสัมพันธ์ของกลุ่มคำกริยาและคำนามพร้อม ๆ กันนั้นจึงเป็นเรื่องที่ยากมาก แต่ถ้าลองทำการเปลี่ยนเฉพาะส่วนที่เป็นคำคุณศัพท์ คำนาม และ คำกริยา

วิเศษณ์ซึ่งสามารถที่จะทำการแบ่งเป็นหมวดหมู่คือการกำหนดความสัมพันธ์ได้ ก็จะทำให้ได้ประโยคข้อความที่มีความหมายที่แท้จริงผิดไปจากเดิมแต่ยังคงโครงสร้างเดิมไว้ได้ เช่น

He always read that red book.

He hardly read that white magazine.

สำหรับรูปแบบของการแทนที่นั้นจะมีการแบ่งหมวดหมู่ของคำศัพท์ต่าง ๆ เอาไว้ด้วยกัน โดยที่คำศัพท์แต่ละคำที่จะถูกแทนที่นั้นจะถูกกำหนดรูปแบบของคำศัพท์คำนั้นว่าอยู่ในหมวดหมู่อะไร เช่น คำว่า car จะอยู่ในหมวดหมู่ ยานพาหนะ Saturday อยู่ในหมวดหมู่ของ วัน old อยู่ในหมวดหมู่ของ คุณสมบัติเป็นต้นจะเห็นว่าในการแทนที่โดยเลือกเฉพาะคำนามและคำคุณศัพท์นี้จะไม่ทำให้โครงสร้างโดยรวมของภาษาเสียไปและการเปลี่ยนทั้งคำนามและคุณศัพท์นั้นก็จะทำให้ความหมายและสาระสำคัญข้อมูลผิดเปลี่ยนไปได้มากพอสมควรแต่ทั้งนี้ทั้งนั้นในด้านความหมายของประโยคนั้นเมื่อแทนที่แล้วในบางประโยคก็อาจจะมีความหมายที่แปลก ๆ ไปบ้างขึ้นอยู่กับว่าจะสามารถออกแบบหมวดหมู่ของกลุ่มคำชนิดเดียวกันได้ครอบคลุมเพียงใดแต่โดยทั่วไปแล้วจะยังสามารถคงรูปประโยคให้เป็นประโยคที่มีความหมายได้พอสมควร เช่น

It is Saturday Afternoon. อาจจะถูกแทนที่ได้เป็น

---> It is Wednesday Evening.

จะเห็นได้ว่ารูปแบบของโครงสร้างของประโยคจะยังคงอยู่ แต่จะเปลี่ยนความหมายที่แท้จริงไป

3.1 ขั้นตอนในการทำงาน

ที่กล่าวมาแล้วนั้นเป็นการกล่าวถึงวิธีที่จะใช้ในการทำงานซึ่ง ในการทำงานจริงนั้นจะต้องมีขั้นตอนต่าง ๆ ดังนี้

1 การออกแบบและสร้างฐานข้อมูลของคำศัพท์คือพจนานุกรม

2 การสร้างโปรแกรมในการทำการเข้ารหัสข้อความ

3.2 การออกแบบและสร้างฐานข้อมูลของคำศัพท์

ในการที่จะทำงานการเข้ารหัสกับประโยคข้อความในภาษาอังกฤษได้นั้น จำเป็นอย่างยิ่งที่เราจะต้องรู้ว่าแต่ละคำนั้นมีหน้าที่ในประโยคนั้นอย่างไร และคำ ๆ นั้นมีรูปแบบจัดอยู่ในหมวดหมู่ของคำประเภทไหน ซึ่งเป็นส่วนของข้อมูลที่จำเป็นที่จะต้องใช้ในการทำงานเช่น

Saturday มีหน้าที่เป็น คำนาม และจัดอยู่ในหมวดหมู่ของ วัน (day) Afternoon มีหน้าที่เป็น คำนาม และจัดอยู่ในหมวดหมู่ของช่วงเวลา

นอกจากนี้ ในการทำงานยังต้องออกแบบให้มีพจนานุกรมแยกออกเป็น 2 ชุดก็คือ พจนานุกรมที่ใช้เก็บคำศัพท์ที่เป็นรูปแบบโครงสร้างของประโยคที่จะพบเห็นโดยทั่วไป เช่น คำที่ทำหน้าที่เป็น article (a, an,the) คำที่ทำหน้าที่เป็นบุพบท (in,on,at,of) คำที่ทำหน้าที่เป็น สรรพนาม (he, she, it) ฯลฯ ซึ่งในที่นี้จะขอเรียกว่า คำสงวน (reserved word) และพจนานุกรมที่ใช้เก็บคำศัพท์ที่เป็นคำทั่ว ๆไป คือ คำนาม คำกริยา คำคุณศัพท์และคำกริยาวิเศษณ์

3.2.1. การสร้างพจนานุกรมของคำสงวน

ในการที่จะสร้างพจนานุกรมขึ้นมานั้นจำเป็นที่จะต้องกำหนดรูปแบบของการเก็บคำศัพท์ว่าจะเก็บอย่างไร ซึ่งสำหรับพจนานุกรมสำหรับคำสงวนส่วนของข้อมูลที่จำเป็นจะต้องใช้คือ คำศัพท์ หน้าที่ของคำศัพท์และรูปแบบว่าเป็นเอกพจน์หรือพหูพจน์และเพื่อความสะดวกและรวดเร็วในการที่จะค้นหาคำศัพท์ที่เก็บในพจนานุกรม จึงได้ทำการออกแบบให้เก็บคำศัพท์ไว้ตามหมวดตัวอักษร คือคำศัพท์ที่ขึ้นต้นด้วยตัวอักษร a จะถูกเก็บในไฟล์ reserv_a.dic และคำศัพท์ที่ขึ้นต้นด้วยตัวอักษร b จะถูกเก็บในไฟล์ reserv_b.dic ดังนี้ จะทำให้ขอบเขตของกลุ่มคำที่จะทำการค้นหามีขนาดแคบลง จะประหยัดเวลาในการค้นหาได้มาก

ตัวอย่างของรูปแบบการเก็บในพจนานุกรมของคำสงวนในไฟล์ reserv_t.dic

this 2 1

that 2 1

the 1 3

3.2.2 การสร้างพจนานุกรมของคำศัพท์ทั่ว ๆ ไป

ในการสร้างพจนานุกรมของคำศัพท์ทั่ว ๆ ไปนั้นจะมีรูปแบบของการเก็บคำศัพท์คล้าย ๆ กับพจนานุกรมของคำสงวนจะมีต่างไปบางจุดคือการระบุหน้าที่ของคำศัพท์และการกำหนดหมวดหมู่ของคำศัพท์เนื่องจากพจนานุกรมของคำศัพท์ทั่ว ๆ ไปนั้นจะใช้เก็บเฉพาะคำศัพท์ที่เป็น คำนาม คำกริยา คำคุณศัพท์ และคำกริยาวิเศษณ์ 4 แบบนี้เท่านั้นดังนั้นการกำหนดความหมายของตัวเลขที่ระบุหน้าที่ของคำศัพท์จึงต้องเปลี่ยนไป และในพจนานุกรมของคำศัพท์โดยทั่ว ๆ ไปนี้ จะมีการระบุชนิดของคำนามที่แบ่งเป็น 4 แบบคือ

1) นามทั่วไปหรือสามานยนาม (common nouns)

2) สมุหนาม (collective nouns)

3) นามที่อยู่รวมกันเป็นกลุ่มก้อน (mass nouns)

4) อาการนาม (abstract noun)

และมีรูปแบบของการกำหนดความหมายของแต่ละบิทดังนี้

บิทที่ 1 -> common nouns

บิทที่ 2 -> collective nouns

บิทที่ 3 -> mass nouns

บิทที่ 4 -> abstract nouns

บิทที่ 5 -> verb

บิทที่ 6 -> adjective

บิทที่ 7 -> adverb

เมื่อกำหนดความหมายของบิทต่างๆแล้วก็จะสามารถระบุหน้าที่ของคำศัพท์ได้โดยการเซ็ทบิทนั้นๆ ให้เป็น 1โดยที่แต่ละคำอาจจะมีหลายหน้าที่ก็ได้แต่สำหรับการระบุหมวดหมู่ของคำศัพท์ของพจนานุกรมของคำศัพท์ทั่ว ๆ ไปนั้น ถ้าหากเป็นคำนาม คำคุณศัพท์ หรือคำกริยาวิเศษณ์ จะต้องมีการระบุหมวดหมู่ของคำ โดยหมวดหมู่ที่ระบุจะถูกนำหน้าด้วยตัวเลข 1- 4 ตามลำดับคือ คำนาม คำกริยา คำคุณศัพท์ และคำกริยาวิเศษณ์ ดังตัวอย่าง เช่น

car x 1 1drive

old x 3 1quality

afternoon x 1rtime

* x หมายถึงสัญลักษณ์แทนตัวอักษรที่เก็บค่าบิทที่ติด

เมื่อได้มีการสร้างพจนานุกรมทั้ง 2 แบบแล้วก็จะสามารถทำการค้นหาข้อมูลเกี่ยวกับรูปแบบของคำแต่ละคำได้ นอกจากพจนานุกรม 2 แบบดังที่ได้กล่าวมาแล้วนั้น ยังต้องมีการจัดทำฐานข้อมูลของคำศัพท์ที่จัดแยกเป็นไฟล์ตามหมวดหมู่ของคำ ซึ่งในที่นี้จะเรียกแต่ละไฟล์ว่าตาราง เช่น ตารางของคำนามที่อยู่ในหมวดหมู่ของยานพาหนะ ตารางของคำนามที่อยู่ในหมวดหมู่ของสัตว์ ตารางของคำคุณศัพท์ที่อยู่ในหมวดหมู่ของคุณลักษณะเป็นต้น ซึ่งในส่วนที่เป็นตารางของหมวดหมู่นี้จะเก็บเฉพาะคำศัพท์เท่านั้น

ตัวอย่าง ของตารางของคำนามที่อยู่ในหมวดหมู่ของยานพาหนะ

CAR

BUS

VAN

3.3 การสร้างโปรแกรมในการทำการเข้ารหัสข้อความ

ในการสร้างโปรแกรมเพื่อที่จะทำการเข้ารหัสข้อความนั้น จะมีขั้นตอนและรายละเอียดปลีกย่อยแยกออกไปอีกมากมาย แต่พอที่จะสรุปขั้นตอนในการสร้างโปรแกรมเพื่อทำการเข้ารหัสได้ดังนี้

1 ขั้นตอนของการแยกคำหรือการวิเคราะห์คำ (LEXICAL ANALYSIS)

2 ขั้นตอนของการค้นหาคำและระบุคุณลักษณะ

3 ขั้นตอนของการเข้ารหัสด้วยการแทนที่คำนามและคุณศัพท์

3.3.1 ขั้นตอนการแยกคำหรือการวิเคราะห์คำ (LEXICAL ANALYSIS)

ขั้นตอนนี้เป็นขั้นตอนแรกในการทำงาน ก่อนอื่นเราต้องอ่านประโยคมาจากไฟล์ก่อน ในที่นี้จะอ่านข้อมูลมาทีละประโยคจากไฟล์ซึ่งแต่ละประโยคจะแยกกันด้วยจุดฟูลสตอป (FULL STOP) แล้วจึงนำมาทำการแยกคำในประโยคออกเป็นคำ ๆ ซึ่งแต่ละคำในประโยคนี้จะถูกนำไปเก็บในลิสต์ (ลิงก์ลิสต์) เพื่อที่จะนำไปใช้งานต่อไป

3.3.2 ขั้นตอนการค้นหาคำและระบุคุณลักษณะ

ขั้นตอนของการค้นหาคำนี้ถ้าหากว่าถ้าฐานข้อมูลของคำศัพท์ที่จะทำการค้นหามีขนาดใหญ่ก็จะทำให้การค้นหาคำแต่ละคำนั้นต้องใช้เวลานาน ดังนั้นในขั้นตอนของการสร้างพจนานุกรมนั้นก็ได้ทำการแยกฐานข้อมูลออกเป็นไฟล์แยกกันตามหมวดหมู่ตัวอักษรเพื่อความสะดวกและรวดเร็วของการค้นหาเนื่องจากขอบเขตของการค้นหาจะมีขนาดแคบลง แต่ถึงแม้ว่าจะใช้วิธีแยกไฟล์แล้วก็ตามถ้าหากใช้วิธีการอ่านไฟล์เข้ามาทีละคำแล้วทำการเปรียบเทียบหาก็ต้องเสียเวลานานพอสมควรในการค้นหาแต่ละคำ ดังนั้นจึงได้ทำการค้นหาวิธีที่จะค้นหาคำในพจนานุกรมด้วยวิธีที่รวดเร็วและสะดวกกว่า และได้พบว่า ในภาษาซีที่เป็นภาษาที่ใช้ในการเขียนโปรแกรมนี้นั้นมีฟังก์ชันที่ใช้ค้นหาคำในสตริงอยู่ฟังก์ชันหนึ่งคือ ฟังก์ชัน STRSTR

ซึ่งจะทำการค้นหาส่วนของสตริงในอีกสตริงหนึ่งซึ่งถ้าหากพบก็จะทำการส่งค่าพอยน์เตอร์ที่ชี้ไปที่ต้นของส่วนของสตริงนั้น ดังรูปแบบดังนี้

CHAR *STRSTR(CHAR *STR1,CHAR *SUBSTR2);

ด้วยฟังก์ชันนี้ก็จะทำให้การค้นหาข้อมูลในส่วนของตัวคำศัพท์สามารถทำได้ด้วยความเร็วมาก แต่ก่อนอื่นต้องมองไฟล์ของฐานข้อมูลที่เราเปิดขึ้นมาในฐานะของชุดสตริงก่อน แต่ในการเปิดไฟล์ข้อมูลของภาษาซีนั้นจะทำการอ่านข้อมูลในไฟล์เข้ามาไว้ในบัฟเฟอร์ก่อนซึ่งข้อมูลที่อยู่ในบัฟเฟอร์จะถูกปิดท้ายด้วย

\0 ทำให้สามารถมองบัฟเฟอร์ของไฟล์นั้นในรูปของสตริง และสามารถใช้ฟังก์ชัน STRSTR ค้นหาคำศัพท์ได้โดยไม่ต้องอ่านไฟล์เข้ามาในเมมโมรีเลย สามารถค้นหาจากบัฟเฟอร์ได้โดยตรง ด้วยวิธีนี้ประกอบกับการแยกไฟล์ตามหมวดหมู่ของตัวอักษรก็จะทำให้การค้นหาคำศัพท์เป็นไปด้วยความสะดวกและรวดเร็ว

ในขั้นตอนของการค้นหาคำศัพท์นั้นจะทำการตรวจสอบคำที่เป็นตัวเลขก่อน จากนั้นหากคำศัพท์อยู่ในรูปพหูพจน์ก็จะทำการแปลงให้อยู่ในรูปของเอกพจน์เพื่อการค้นหาก่อน จากนั้นจะค้นหาคำในพจนานุกรมของคำสงวนก่อน หากไม่เจอจึงค่อยไปหาในส่วนของพจนานุกรมของคำศัพท์ทั่ว ๆ ไป ถ้าหากยังไม่เจอคำศัพท์ก็จะถือว่าเป็นส่วนของชื่อหรือสัญลักษณ์ทั่ว ๆ ไปที่ไม่ใช่คำศัพท์ในพจนานุกรม ถ้าหากว่าเป็นชื่อทั่ว ๆ ไปเช่น JOHN ROBERT ก็จะมีตารางของชื่อทั่ว ๆ ไปเพื่อการตรวจสอบและแทนที่ แต่ถ้าหากว่าเป็นชื่อสถานที่เฉพาะก็จะทำการคงคำศัพท์นั้นไว้ เช่น คำว่า HUAHIN หรือ SUKHUMWIT แต่ในการใช้งานจริงหากมีชื่อเฉพาะที่ต้องการให้ทำการเข้ารหัส ก็สามารถที่จะสร้างตารางของคำเหล่านั้นเพื่อจุดมุ่งหมายในการเข้ารหัสก็ได้

เมื่อพบคำศัพท์ที่ทำการค้นหาแล้ว ก็สามารถที่จะระบุหน้าที่ของมันในประโยคได้ เนื่องจากข้อมูลที่ระบุหน้าที่ของคำศัพท์และข้อมูลที่ระบุหมวดหมู่ของคำศัพท์นั้นได้ถูกเก็บต่อเนื่องจากตัวคำศัพท์ สำหรับในกรณีที่คำศัพท์เป็นคำนามหรือคำคุณศัพท์ที่จะต้องทำการแปลง ถ้าหากว่าคำศัพท์นั้นมีหลายหน้าที่จะต้องทำการระบุหน้าที่ ๆ แท้จริงของคำศัพท์นั้นในประโยค โดยจะมีฟังก์ชันในการกำหนดหน้าที่ ๆ แท้จริงของคำศัพท์ โดยการตรวจสอบรูปแบบตามโครงสร้างของไวยากรณ์ภาษาอังกฤษ เมื่อได้กำหนดคุณลักษณะต่าง ๆ ให้กับคำศัพท์แล้ว ก็จะเข้าสู่ขั้นตอนการเข้ารหัส

3.3.3 ขั้นตอนการเข้ารหัสด้วยการแทนที่คำนามและคำคุณศัพท์

เมื่อได้กำหนดคุณลักษณะต่าง ๆ ของคำศัพท์แต่ละคำในประโยคแล้ว เมื่อจะทำการเข้ารหัสก็จะทำการตรวจสอบว่าคำศัพท์ตัวได้บ้างที่เป็นคำนามหรือคำคุณศัพท์ (รวมทั้งเลขจำนวนและคำกริยาวิเศษณ์บางตัว) เมื่อตรวจพบแล้วก็จะทำการแทนที่ศัพท์คำนั้นโดยจะเลือกคำศัพท์ที่จะมาแทนที่จากตารางของหมวดหมู่ของคำศัพท์นั้น ๆ โดยจะเลือกตัวใดจากตารางก็จะทำการนำค่า ๆ หนึ่งที่ได้จากตารางของตัวเลข

ตามกรรมวิธีของการเข้ารหัสแบบเวอร์แนมไซเฟอร์ดังที่ได้กล่าวมาในทฤษฎีข้างต้น มาบวกเข้ากับลำดับของคำศัพท์นั้น ๆ ในตารางก็จะได้ตำแหน่งของคำศัพท์คำใหม่ที่จะนำไปแทนที่

3.3.4 การถอดรหัส

เมื่อได้ทำการเข้ารหัสและจะทำการถอดรหัสนั้นก็จะทำการแยกคำและระบุคุณลักษณะต่าง ๆ แบบเดียวกับการทำการเข้ารหัสจากนั้นจึงนำค่าจากตารางตัวเลขชุดเดียวกับที่ใช้ในการเข้ารหัสมาลบออกจากลำดับที่ของคำศัพท์นั้นในตารางก็จะทำให้ได้ตำแหน่งของคำศัพท์เดิมกลับคืนเหมือนเดิม

บทที่ 4

การทดลองและผลการทดลอง

ในการดำเนินการสร้างโปรแกรมเพื่อทำการเข้ารหัสโดยวิธีนี้นั้น เราได้ทำการทดลองและพบกับอุปสรรคและปัญหามากมาย เพราะเป็นการทำงานในส่วนที่เป็นภาษาที่มนุษย์ใช้งาน จึงเป็นงานที่มีความละเอียดอ่อนอย่างมากและมีรูปแบบและเงื่อนไขปลีกย่อยต่าง ๆ มากมาย

ในการทำการสร้างโปรแกรมทดลองขั้นแรก ๆ ของการทำโครงงานนั้นจะพบว่าหากใช้วิธีเข้ารหัสโดยการแทนที่คำตามหน้าที่ของคำในประโยค จะพบว่าความสัมพันธ์ระหว่างคำต่าง ๆ จะไม่เข้ากันเพราะว่า ภาษานั้นสามารถแปลงไปในรูปแบบต่าง ๆ มากมาย มีคำศัพท์อยู่เป็นจำนวนมาก ซึ่งเป็นการยากที่จะนำมาเขียนโปรแกรมให้เป็นฟังก์ชันมีขั้นตอนการทำงานที่แน่นอนได้ ดังตัวอย่างเช่น

I GIVE THE BOOK TO SUE.

และทำการเปลี่ยนตามหน้าที่ คือ

I	GIVE	THE	BOOK	TO	SUE.
pron.	v.t.	art.	n.	prep.	n.

อาจจะได้เป็น

HE	LOOK	THE	PENCIL	TO	JOE.

ซึ่งจะเห็นได้ว่า ความหมายที่ได้นั้นจะไม่ได้ใจความ

4.1 การทดลองการทำงาน

เราทำการทดลองการเข้ารหัสใหม่โดยจะทำการเปลี่ยนเฉพาะคำนาม คำคุณศัพท์ และ คำกริยาวิเศษณ์ที่บอกความถี่ ซึ่งจากการทดลองดังกล่าวแล้วให้ผลเป็นที่น่าพอใจเป็นอย่างมาก ซึ่งจะได้แสดงการการทดลองดังที่ได้กล่าวนั้น โดยที่ทำการป้อนข้อความเข้าไปให้โปรแกรมที่เขียนขึ้นมาทำการเข้ารหัส โดยที่ข้อความที่ใช้ในการทดลองนั้นเป็นดังต่อไปนี้

It is Saturday afternoon. Earl and Shirley Gatsby are at the Bensons' house. They are studying with Jennifer. They don't usually study on Saturdays, but this Saturday is different. Their school examination are on Monday.

4.2 ผลการทดลอง

จากการทำงานของโปรแกรมที่ได้เขียนขึ้นผลที่ได้จากการทดลองป้อนข้อมูลของข้อความดังข้างต้นเป็นดังนี้

It is Wednesday evening. Arthur and Janny Fraser are at the Frasers' villa. They are studying with Sonia . They don't always study on Tuesdays, but this Wednesday is strange. Their university parties are on Tuesday.

ซึ่งจากผลการทดลองจะเห็นได้ว่าความหมายของประโยคยังได้ใจความอยู่ และเมื่ออ่านเปรียบเทียบกับข้อมูลจากข้อความเดิมแล้วจะเห็นได้ว่าข้อมูลที่สำคัญในข้อความนั้นได้เปลี่ยนไปแล้ว

บทที่ 5

บทสรุปและวิจารณ์

5.1 ความเห็นต่อโครงงาน

โครงงานนี้เป็นโครงงานที่เกี่ยวกับการค้นคว้าพัฒนาเป็นส่วนใหญ่ เป็นโครงงานที่ไม่มีใครเคยทำเป็นลายลักษณ์อักษรมาก่อน ดังนั้นเอกสารที่ใช้ค้นคว้าและอ้างอิงจึงเป็นเอกสารเกี่ยวกับพื้นฐานองค์ประกอบที่ต้องใช้ในการทำงานเช่น หนังสือ Compiler writing , Security In Computing , Successful English Grammar เป็นต้น ในส่วนของการคิดค้นเพื่อการใช้งานจริง จึงเป็นส่วนที่ต้องคิดค้นขึ้นเอง แล้วทำการทดลอง ลองผิดลองถูกเอาเอง ซึ่งในช่วงแรก ๆ จะใช้เวลาในการออกแบบหาวิธีอยู่นานพอสมควร เช่นรูปแบบของการสร้างพจนานุกรม วิธีการเข้ารหัสให้ได้ใจความพออ่านได้โดยการแทนที่คำนามและคำคุณศัพท์ ซึ่งในส่วนเหล่านี้จะไม่มีอยู่ในหนังสือเลย ส่วนที่จะหาได้จากหนังสือก็คือ พื้นฐานของวิธีการเข้ารหัสแบบเวอร์แนมไซเฟอร์ การทำเลกซิคอล อนาไลซิส เป็นต้น

สำหรับผลการทำงานของการทำการเข้ารหัสแล้วนี้จากที่ได้พยายามปรับปรุงโดยวิธีการแทนที่คำนามและคำคุณศัพท์ ก็จะทำให้ประโยคแต่ละประโยคในข้อความมีใจความสมบูรณ์ขึ้น แต่ถ้าหากจะอ่านเอาใจความกันจริง ๆ แล้วประโยคที่ทำการเข้ารหัสแล้วนั้นจะมีความหมายที่ไม่เฉพาะเจาะจงและเมื่อรวมความของแต่ละประโยคเข้าด้วยกันก็จะพบว่าใจความของข้อความชุดนั้นอาจจะไม่สัมพันธ์กัน แต่อย่างไรก็ตามจุดประสงค์หนึ่งของการเข้ารหัสก็คือ ผู้ที่ไม่พึงประสงค์ไม่สามารถที่จะได้ข้อมูลที่ครบสมบูรณ์ไป และไม่สามารถนำข้อมูลนั้นไปใช้งานได้ และการทำการเข้ารหัสแบบแทนที่คำนี้จะทำให้ ผู้ที่ไม่พึงประสงค์ไม่สามารถจะหาวิธีการในการทำการถอดรหัสได้ถ้าหากไม่รู้ข้อมูลของชุดตารางตัวเลขที่ใช้ในการเข้ารหัสแบบเวอร์แนมไซเฟอร์ และนอกจากนั้นการแปลงข้อมูลแต่ละคำนั้นก็ขึ้นอยู่กับลำดับต่าง ๆ ของคำที่อยู่ในตารางของคำศัพท์แต่ละหมวดหมู่ด้วย (ถ้าเข้ารหัสตามตัวอักษรลำดับจะเรียงกันจาก A-Z) ดังนั้นหากผู้ที่ไม่พึงประสงค์ไม่มีข้อมูลของตารางชุดตัวเลขและข้อมูลของตารางหมวดหมู่ของคำศัพท์จะไม่สามารถถอดรหัสของข้อความที่แท้จริงได้เลย

5.2 ปัญหาที่พบ

ปัญหาต่าง ๆ ที่พบในการทำโครงงานนี้มีมากมาย โดยส่วนมากจะเกี่ยวข้องกับรูปแบบของภาษาซึ่งมีความละเอียดอ่อนมาก สามารถที่จะเปลี่ยนแปลงไปได้มากมายตามความ

สัมพันธ์ในรูปแบบต่าง ๆ ที่กำหนดขึ้นโดยไวยากรณ์ของภาษาอังกฤษ ซึ่งมีคำศัพท์ต่าง ๆ มากมาย ในการที่เราจะสร้างประโยคขึ้นมาให้เกิดความหมายได้ใจความถูกต้องและสัมพันธ์กันนั้นจึงเป็นการยากอย่างยิ่ง เพราะแม้แต่มนุษย์เราเองถ้าหากว่ายังไม่คล่องในไวยากรณ์ภาษาอังกฤษ การที่จะพูดหรือเขียนประโยคขึ้นให้ได้ใจความและความหมายยังเป็นการยาก ดังนั้นการที่จะกำหนดให้คอมพิวเตอร์ทำงานในการสร้างประโยคขึ้นใหม่ถึงแม้ว่าจะมีพื้นฐานจากรูปประโยคเดิม ก็จึงเป็นไปได้ยากอย่างยิ่ง เนื่องจากแต่ละคำในประโยคอาจจะไม่สัมพันธ์กัน ถึงแม้ว่าเราจะพยายามจัดหมวดหมู่ของคำไว้ให้ก็ตาม และในการจัดหมวดหมู่ถ้าเราแบ่งแยกย่อยจนเกินไปนั้นก็จะทำให้ความหมายของประโยคเปลี่ยนไปไม่มากพอซึ่งอาจจะทำให้เดาข้อความเดิมออกได้ ดังนั้นในการจัดหมวดหมู่ของคำนั้นต้องจัดให้มีปริมาณของคำศัพท์ในตารางมากพอสมควรที่จะทำให้การแทนที่ได้ใจความแต่มีความหมายผิดไปจากเดิม

ส่วนปัญหาที่พบหลังจากที่ได้ทำการเข้ารหัสไปแล้วคือ ความสัมพันธ์ในประโยคซึ่งเป็นเหตุเป็นผลกับในตอนก่อนที่จะเข้ารหัส คือเมื่อเข้ารหัสแล้วจะทำให้ประโยคนั้นเกิดการขัดแย้งกันซึ่งจะทำให้ความหมายของประโยคนั้นแปลกไปจากความหมายที่ใช้อยู่ในภาษาอังกฤษทั่วไป ดังเช่นประโยคต่อไปนี้

Jim and Earl don't talk about love stories because they never read them.

จิม และเอิร์ลไม่คุยเกี่ยวกับนวนิยายรัก เพราะว่าพวกเขาไม่อ่านมัน

John and Teddy don't talk about love magazines because they always read them.

จอห์น และเท็ดดี้ไม่คุยเกี่ยวกับนิตยสารรัก เพราะว่าพวกเขาอ่านมันเป็นประจำ

จะเห็นได้ว่า หลังจากที่เข้ารหัสแล้ว ประโยคหลังจะเกิดความขัดแย้งกันเองในประโยค ซึ่งก็เป็นปัญหาหนึ่งซึ่งจะต้องทำการแก้ไขต่อไป

5.3 ข้อเสนอแนะในการทำโครงงานต่อไป

โครงงานนี้เป็นครั้งแรกที่มีการจัดทำขึ้นมาจึงยังมีข้อจำกัดต่าง ๆ อยู่อีกมาก ข้อจำกัดอย่างหนึ่งก็คือ การแทนที่คำศัพท์เฉพาะในส่วนที่เป็นคำนาม และคำคุณศัพท์ ซึ่งเป็นส่วนหนึ่งที่ได้คิดขึ้นมาเพื่อแก้ไขปัญหาของความไม่สัมพันธ์กันระหว่างคำต่าง ๆ ในประโยค ด้วยวิธีนี้จะทำให้รูปแบบโครงสร้างของประโยคไม่เสียไป แต่ในกรณีที่ต้องการจะให้ประโยคเปลี่ยนไปโดย

สิ้นเชิงนั้นเป็นไปไม่ได้ ดังนั้นในการที่จะให้ประโยคเปลี่ยนแปลงมาก ๆ จึงอาจจะต้องมีการเปลี่ยนแปลงคำกริยาด้วย ซึ่งการเปลี่ยนคำกริยานี้เป็นเรื่องที่ยุ่งยากเนื่องจากหากต้องการให้ประโยคได้ใจความนั้นประธานและกรรมจะต้องมีความสัมพันธ์กับคำกริยานั้น ๆ ซึ่งวิธีการทำอาจจะต้องมีตารางในการเก็บความสัมพันธ์ของคำกริยาแต่ละคำว่าสัมพันธ์กับคำนามชุดไหนอย่างไร เป็นต้น ซึ่งต้องใช้ฐานข้อมูลที่ได้ออกแบบมาอย่างดีเพื่อการใช้งาน จึงเป็นงานที่ยากและอาจต้องใช้เวลานาน แต่ก็พอมีทางที่จะทำได้ ถ้าทำการศึกษาอย่างจริงจัง

ข้อจำกัดอีกอย่างหนึ่งของชิ้นงานก็คือความสัมพันธ์กันระหว่างประโยคแต่ละประโยคในชุดข้อความ ซึ่งกรณีนี้เป็นกรณีที่ยากที่จะทำการแก้ไข เนื่องจากการเขียนประโยคขึ้นมาเป็นชุดของข้อความโดยมนุษย์นั้น ผู้เขียนมีจุดมุ่งหมายที่แน่นอนในการเขียนว่าจะเขียนอย่างไร จะเขียนในทิศทางไหนต่างจากการแทนที่คำโดยฟังก์ชันที่กำหนดไว้ในคอมพิวเตอร์ เป็นการยากที่จะกำหนดความสัมพันธ์ของแต่ละประโยค ยากที่จะหากฎเกณฑ์มากำหนดความสัมพันธ์ได้ ข้อเสนอแนะเกี่ยวกับเรื่องนี้ก็อาจจะเป็นการตรวจสอบข้อความทั้งหมดแล้ววิเคราะห์ดูว่ามีคำศัพท์คำนาม คำไหนที่ใช้บ่อย ๆ แล้วใช้วิธีการแทนที่ คำศัพท์คำนั้นทั้งหมดในชุดข้อความทีเดียวด้วยคำศัพท์คำอื่น อย่างไรก็ตามวิธีนี้อาจจะไม่ได้ผลก็ได้

5.4 บทสรุป

โครงงาน ๆ นี้เป็นครั้งแรกที่มีการจัดทำขึ้นมา ดังนั้นแหล่งข้อมูลที่จะได้ทำการศึกษามีน้อย ทางคณะผู้จัดทำได้พยายามทำการค้นคว้าโดยการสอบถามจากอาจารย์ที่ปรึกษาและทำการคิดค้นวิธีการขึ้นเองโดยการลองผิดลองถูก ดังนั้นผลลัพธ์ที่ได้จากโครงงานชิ้นนี้อาจจะไม่สมบูรณ์ถูกต้องตามวัตถุประสงค์ทั้งหมด แต่ก็หวังเป็นอย่างยิ่งว่า จะได้วางแนวทางไว้เพื่อการศึกษาและพัฒนาโครงงานชิ้นนี้ให้เสร็จสมบูรณ์ต่อไป

หนังสืออ้างอิง

Jean - Paul Tremblay and Pual G. Sorenson , " The theory and practice of compiler writing " , Mc Graw-Hill, 796 p., 1985

Charles P. Pfleeger , " Security in Computing ", Prentice-Hall International Editions , 537 p., 1989

James Allen , " Natural Language Understanding " , The Benjamin/Cumming Publishing Company , 574 p. , 1987

Ethel Brinton ,Paul Davies, " หนังสือเรียนภาษาอังกฤษ Junior active context English Book II ", สำนักพิมพ์อักษรเจริญ, 248 หน้า , 2533

รองศาสตราจารย์ สุวรรณี เต็งอำนวย และ ผู้ช่วยศาสตราจารย์ อรสา รุ่งแสง, "Successful English Grammar ", สำนักพิมพ์ภูมิบัณฑิต, 558 หน้า, 2533