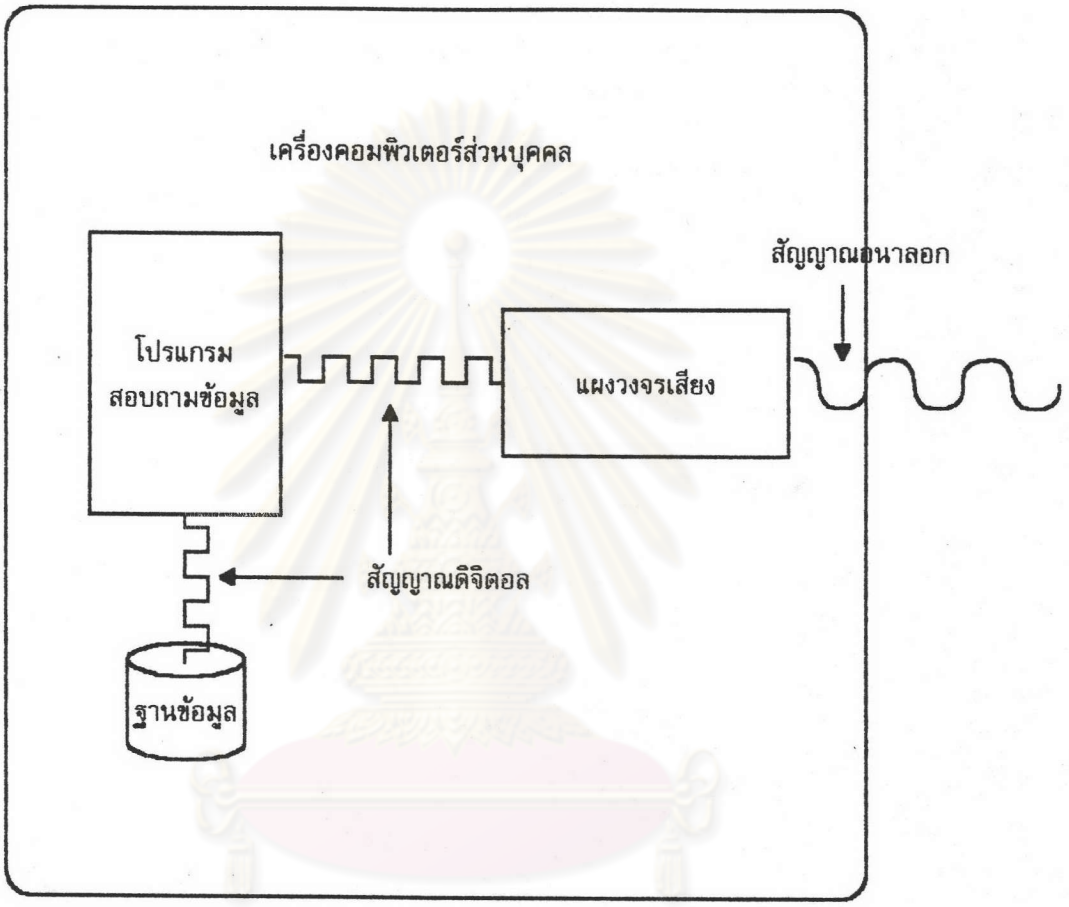
บทที่ 2

แนวคิดพื้นฐานที่เกี่ยวข้อง

การให้บริการสอบถามข้อมูลผ่านทางโทรศัพท์ มีประโยชน์อย่างมากในปัจจุบัน และอนาคตนอกจากช่วยลดภาระเจ้าหน้าที่ตามสาขาของธนาคารที่ต้องคอยตอบคำถามแล้ว ยังทำให้ผู้ใช้บริการรู้สึกว่าข้อมูลของตนปลอดภัย แต่เนื่องจากการปรับปรุงบริการยังต้องอาศัยบริษัทที่ผลิตและ จำหน่ายฮาร์ดแวร์ และซอฟท์แวร์สำเร็จรูป ดังนั้นจึงได้มีการศึกษาซอฟท์แวร์ ฮาร์ดแวร์ราคาถูกที่สามารถปรับปรุงให้ทันสมัยได้ง่ายมาทดแทน ทั้งเพื่อเป็นการรองรับระบบใหม่ที่เกิดขึ้นต่อไปในอนาคต ไม่ต้องผูกติดกับบริษัทที่ผลิตฮาร์ดแวร์ ซอฟท์แวร์สำเร็จรูปอีก จากการศึกษาและทดสอบความเหมาะสมพบว่า สามารถนำเอาคอมพิวเตอร์ส่วนบุคคล และแผงวงจรเสียง มาออกแบบพัฒนาให้ตอบคำถามแทนผู้รับปลายทางได้ ตามความต้องการของผู้ใช้บริการ ตลอดจนควบคุมระบบให้ปลอดภัยจากผู้ที่พยายามเข้ามาใช้บริการโดยไม่ได้รับอนุญาต

แนวคิดต่าง ๆ ที่กล่าวต่อไปนี้เป็นส่วนหนึ่งของการศึกษาที่ผ่านมา และนำมาใช้พัฒนาระบบการสอบถามข้อมูลทางโทรศัพท์

1. หลักการทำงานของแผงวงจรเสียง ใช้หลักการรู้จำเสียง(Voice recognition) หลักการนี้กล่าวถึงเทคโนโลยีที่ทำให้เครื่องคอมพิวเตอร์สามารถรับรู้ความแตกต่างของเสียงโดยเสียงพูดที่ถูกพูดผ่านไมโครโฟนเข้าไปที่แผงวงจรเสียงเป็นรูปสัญญาณอนาลอก(Analog signals) และถูกเปลี่ยนให้เป็น สัญญาณดิจิตอล(Digital signals) สัญญาณนี้ถูกนำไปปรับปรุงตัดสัญญาณรบกวนออกแล้วนำไปเก็บลงแฟ้มข้อมูลตามชื่อที่กำหนดเพื่อรอการนำไปใช้ เมื่อมีความต้องการใช้แฟ้มข้อมูลของเสียง แฟ้มข้อมูลจะถูกนำมาผ่านแผงวงจรเสียง ทำการเปลี่ยนสัญญาณดิจิตอลให้เป็นสัญญาณอนาลอกออกมาทางโทรศัพท์ ดังรูปที่ 2.1



รูปที่ 2.1 แสดงการทำงานของแผงวงจรเสียง

2. หลักการรักษาความปลอดภัย ระบบการสอบถามข้อมูลทางโทรศัพท์ โดยใช้เครื่องคอมพิวเตอร์ส่วนบุคคล และแผงวงจรเสียง ทำการป้องกันการเข้าถึงข้อมูลจากผู้ที่ไม่ได้รับอนุญาตโดยใช้ รหัสประจำตัว(user id) และรหัสผ่าน(password) ในการเข้ามาขอใช้บริการ ส่วนข้อมูลที่สำคัญของผู้ใช้บริการถูกเก็บไว้ในลักษณะที่ทำการเข้ารหัสลับ(Cryptography) ไว้ เมื่อต้องการใช้ต้องถอดกลับมาเป็นข้อความเดิม ทำให้ผู้ใช้บริการเกิดความเชื่อมั่นในการใช้บริการ

วิธีการสร้างรหัสผ่าน ทำจากรหัสประจำตัวของผู้ใช้บริการ และคีย์สำหรับการเข้ารหัสลับ(Cryptographic Key) เป็นการเข้ารหัสลับแบบการแทนที่(Substitution) โดยใช้ตารางเพื่อแทนตัวอักษรเดิมให้เป็นตัวอักษรอื่น (Charles P. Pfluger, 1989) มีด้วยกันหลายวิธี คือ

2.1 การเข้ารหัสลับแบบตัวอักษรเดียว เช่น

2.1.1 การเข้ารหัสแบบซีซาร์(Caesar Cipher) ตามชื่อของจูเลียต ซีซาร์ โดยใช้วิธีการเลื่อนตัวอักษรไป 3 ตำแหน่งในการเข้ารหัส เขียนเป็นสมการได้ดังนี้

$C_i = E(P_i) = P_i + 3$

P_i = ตัวอักษรเดิม

C_i = ตัวอักษรที่เข้ารหัสแล้ว

ตัวอักษรก่อนเข้ารหัส ABCDEFGHIJKLMNOPQRSTUVWXYZ

ตัวอักษรหลังเข้ารหัส defghijklmnopqrstuvwxyzabc

ข้อความก่อนเข้ารหัส VICHIEN

ข้อความหลังเข้ารหัส ylfklhg

2.1.2 การเข้ารหัสแบบ Permutation จะอยู่ในรูปฟังก์ชั่น ถ้า $a^1, a^2, \ldots, a^k$ แล้ว x เป็น 1, 2, 3,...,k จะแทน C^i ด้วย $a^x(P^i)$

x^1 = 1,3,5,7,9,10,8,6,4,2

x^2 = 10,9,8,7,6,5,4,3,2,1

ตำแหน่งที่ 2 ของ x^1 มีค่า 3 $(x^1(2) = 3)$,

ตำแหน่งที่ 5 ของ x^2 มีค่า 6 $(x^2(5) = 6)$,

<u>ตัวอย่าง</u> การเข้ารหัสลับแบบตัวอักษรเดียว การกำหนดตำแหน่งของตัวอักษร โดยให้อักษร A อยู่ตำแหน่งที่ 0, B อยู่ตำแหน่งที่ 1 ไปจนถึง Z อยู่ตำแหน่งที่ 25

อักษร 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

รหัส 0 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25

ทุกตำแหน่งของตัวอักษรอยู่ระหว่าง 0 ถึง 25 ใช้ฟังก์ชั่น x = 25 - y ในการหาค่า

A เมื่อเข้ารหัสแล้วเป็น Z

B เมื่อเข้ารหัสแล้วเป็น Y

C เมื่อเข้ารหัสแล้วเป็น X

หรือใช้สูตร x(y) = (3y) mod 26 เช่นในการหาว่าค่าของ V แทนด้วยตัวอักษรอะไร ทำได้โดย หาตำแหน่งของ V ในที่นี้อยู่ที่ 21 นั่นคือ y = 21

x(21) = (3x21) mod 26

= 11

ผลลัพธ์ตำแหน่งที่ 11 คือตัวอักษร L

2.2 การเข้ารหัสลับแบบการแทนที่หลายตัวอักษร ขั้นตอนการเข้ารหัสลับของข้อมูล ถูกแบ่งเป็น 2 ชุดแยกจากกัน ชุดแรกเข้ารหัสลับที่ตำแหน่งคี่, ชุดหลังเข้ารหัสลับที่ตำแหน่งคู่ โดยแบ่งสูตรการเข้ารหัสลับเป็น 2 ชุด

การเข้ารหัสลับข้อมูลด้วย สูตร x1(y) = (3y) mod 26 (สำหรับตำแหน่งคี่)

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

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

การเข้ารหัสลับข้อมูลด้วย สูตร x2(y) = ((5y)+13) mod 26 (สำหรับตำแหน่งคู่)

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

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

ผลการเข้ารหัสจาก VICHIEN ได้เป็น lbgwyhn

2.3 การเข้ารหัสลับด้วยการสับเปลี่ยนที่(Transposition) เป็นการกระจายตำแหน่งข้อมูลไม่ให้อยู่ในรูปแบบเดิม เช่น ข้อมูลเดิมเป็น a1, a2, a3,...,a20 จัดให้อยู่ในรูปคอลัมน์ได้ ดังนี้

a_1 a_2 a_3 a_4 a_5

a_6 a_7 a_8 a_9 a_{10}

a_{11} a_{12} a_{13} a_{14} a_{15}

a_{16} a_{17} a_{18} a_{19} a_{20}

ผลลัพธ์ของการเข้ารหัสลับแบบนี้จะได้ข้อมูลในแนวดิ่งคือ a_1, a_6, a_{11}, a_{16}, a_2, a_7, a_{12}, a_{17}, a_3, a_8,..., a_{20}

2.4 การเข้ารหัสลับของอัลกอริทึมเดส(Data Encryption Standard Algorithm หรือ DES) เป็นการนำวิธีพื้นฐานของการเข้ารหัสมาใช้ เช่น การแทนที่ข้อมูล การสับเปลี่ยนตำแหน่ง การมอดูโลสอง หรือ เอกซ์คลูซีฟออร์ ส่วนการสลับตำแหน่งมีด้วยกัน 3 ลักษณะคือ

Permutation ผลของการเปลี่ยนจะได้ข้อมูลเท่าเดิม

Expanded Permutation ผลของการเปลี่ยนจะได้ข้อมูลเพิ่มขึ้น

Permutation Choices ผลของการเปลี่ยนจะได้ข้อมูลลดลง

ขั้นตอนการทำงานของอัลกอริทึมเดส กลุ่มข้อมูลเข้ารหัส และคีย์สำหรับเข้ารหัสลับ ถูกแบ่งเป็น 64 บิท นำมาเปลี่ยนตำแหน่งของบิทใหม่ตาม ตารางที่ 2.1 ผลลัพธ์ที่ได้แบ่งเป็น 32 บิท (L=0ถึง 31 R=32 ถึง 63) ข้อมูลนี้ถูกส่งมาทำงานที่ฟังก์ชั่น $f(R^{i-1},K^i)$ ซึ่งเป็นวงจรทำงานซ้ำ 16 รอบ ค่า K^i หาได้จาก ฟังก์ชั่น f(i,key) i=1,2,3,..,16

ฟังก์ชั่น $f(R^{i-1},K^i)$ ทำหน้าที่ นำ R^{i-1} มาเอกซ์คลูซีฟออร์กับ K^i นำผลลัพธ์ที่ได้มาผ่านตารางที่ 2.2 ถึง ตารางที่ 2.9

ฟังก์ชั่น f(i,key) ทำหน้าที่ นำคีย์สำหรับเข้ารหัสลับมาเปลี่ยนตำแหน่ง โดยใช้ตารางที่ 2.10 แบ่งข้อมูลที่ได้เป็น 2 ส่วน นำมาเลื่อนบิทแบบเวียนซ้าย (Circular Left Shift) นำข้อมูลที่ได้มาผ่านตารางที่ 2.11 ทำ 16 ครั้ง จึงได้ค่า K^i ในแต่ละรอบ

การถอดรหัสขั้นตอนเดียวกันกับการเข้ารหัส ยกเว้นค่า K เป็นตรงข้ามคือ เริ่มจาก K^{16} K^{15}... K^1 อัลกอริทึมเดสเป็นอัลกอริทึมที่ได้รับความนิยมสูงในขณะนี้ซึ่งได้รับการรับรองมาตรฐานจาก NBS (National Bureau of Standard) ทาง NBS ได้เสนอคุณสมบัติของอัลกอริทึมสำหรับการเข้ารหัสลับ (Meyer and Matyas, 1982) ดังนี้

ก. อัลกอริทึมที่ออกแบบต้องสมบูรณ์ ชัดเจน

ข. ต้องทราบว่าอัลกอริทึมมีความสามารถในการป้องกันข้อมูลได้แค่ไหน

ค. ประสิทธิภาพในการป้องกันข้อมูลขึ้น กับคีย์สำหรับการเข้ารหัสลับไม่ใช่อัลกอริทึม

ง. การทำงานของ อัลกอริทึม ต้องไม่กระทบกระเทือนต่อการทำงานของผู้ใช้

58	50	42	34	26	18	10	2
60	52	44	36	28	20	12	4
62	54	46	38	30	22	14	6
64	56	48	40	32	24	16	8
57	49	41	33	25	17	9	1
59	51	43	35	27	19	11	3
61	53	45	37	29	21	13	5
63	55	47	39	31	23	15	7

ตารางที่ 2.1 แสดง Initial permutation

	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
0	14	4	13	1	2	15	11	8	3	10	6	12	5	9	0	7
1	0	15	7	4	14	2	13	1	10	6	12	11	9	5	3	8
2	4	1	14	8	13	6	2	11	15	12	9	7	3	10	5	0
3	15	12	8	2	4	9	1	7	5	11	3	14	10	0	6	13

ตารางที่ 2.2 แสดง S-boxes (s1)

	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
0	15	1	8	14	6	11	3	4	9	7	2	13	12	0	5	10
1	3	13	4	7	15	2	8	14	12	0	1	10	6	9	11	5
2	0	14	7	11	10	4	13	1	5	8	12	6	9	3	2	15
3	13	8	10	1	3	15	4	2	11	6	7	12	0	5	14	9

ตารางที่ 2.3 แสดง S-boxes (s2)

	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
0	10	0	9	14	6	3	15	5	1	13	12	7	11	4	2	8
1	13	7	0	9	3	4	6	10	2	8	5	14	12	11	15	1
2	13	6	4	9	8	15	3	0	11	1	2	12	5	10	14	7
3	1	10	13	0	6	9	8	7	4	15	14	3	11	5	2	12

ตารางที่ 2.4 แสดง S-boxes (s3)

	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
0	7	13	14	3	0	6	9	10	1	2	8	5	11	12	4	15
1	13	8	11	5	6	15	0	3	4	7	2	12	1	10	14	9
2	10	6	9	0	12	11	7	13	15	1	3	14	5	2	8	4
3	3	15	0	6	10	1	13	8	9	4	5	11	12	7	2	14

ตารางที่ 2.5 แสดง S-boxes (s4)

	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
0	2	12	4	1	7	10	11	6	8	5	3	15	13	0	14	9
1	14	11	2	12	4	7	13	1	5	0	15	10	3	9	8	6
2	4	2	1	11	10	13	7	8	15	9	12	5	6	3	0	14
3	11	8	12	7	1	14	2	13	6	15	0	9	10	4	5	3

ตารางที่ 2.6 แสดง S-boxes (s5)

	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
0	12	1	10	15	9	2	6	8	0	13	3	4	14	7	5	11
1	10	15	4	2	7	12	9	5	6	1	13	14	0	11	3	8
2	9	14	15	5	2	8	12	3	7	0	4	10	1	13	11	6
3	4	3	2	12	9	5	15	10	11	14	1	7	6	0	8	13

ตารางที่ 2.7 แสดง S-boxes (s6)

	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
0	4	11	2	14	15	0	8	13	3	12	9	7	5	10	6	1
1	13	0	11	7	4	9	1	10	14	3	5	12	2	15	8	6
2	1	4	11	13	12	3	7	14	10	15	6	8	0	5	9	2
3	6	11	13	8	1	4	10	7	9	5	0	15	14	2	3	12

ตารางที่ 2.8 แสดง S-boxes (s7)

	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
0	13	2	8	4	6	15	11	1	10	9	3	14	5	0	12	7
1	1	15	13	8	10	3	7	4	12	5	6	11	10	14	9	2
2	7	11	4	1	9	12	14	2	0	6	10	13	15	3	5	8
3	2	1	14	7	4	10	8	13	15	12	9	0	3	5	6	11

ตารางที่ 2.9 แสดง S-boxes (s8)

57	49	41	33	25	17	9
1	58	50	42	34	26	18
10	2	59	51	43	35	27
19	11	3	60	52	44	36
63	55	47	39	31	23	15
7	62	54	46	38	30	22
21	13	5	28	20	12	4

ตารางที่ 2.10 แสดง PC1

14	17	11	24	1	5
3	28	15	6	21	10
23	19	12	4	26	8
16	7	27	20	13	2
41	52	31	37	47	55
30	40	51	45	33	48
44	49	39	56	34	53
46	42	50	36	29	32

ตารางที่ 2.11 แสดง PC2

3. หลักการทดสอบความเหมาะสมของระบบด้านจำนวนคู่สายที่ให้บริการ โดยทดสอบจากระยะเวลา ตั้งแต่ผู้ใช้บริการโทรเข้ามาจนระบบสามารถให้บริการแก่ผู้ใช้บริการครบตามความต้องการ วิธีการทดสอบ แบ่งข้อมูลออกเป็น 2 กลุ่มคือ กลุ่มแรก เป็นข้อมูลที่ได้จากผู้วิจัยโทรศัพท์เข้ามาใช้บริการเองเพื่อหาค่าเฉลี่ยของเวลาที่ให้บริการแต่ละรหัสบริการ ส่วนกลุ่มหลังเป็นกลุ่มที่เปิดให้ผู้ใช้บริการโทรศัพท์เข้ามาใช้บริการจริงในระยะเวลา 1 วัน การทดสอบอ้างอิงจากทฤษฎีรอคอย (Queueing Theory) ที่กล่าวถึง ความสัมพันธ์ของเวลาที่ใช้รอคอยก่อนเข้าระบบ เวลาที่ใช้ภายในระบบ จำนวนระบบที่มารองรับผู้ใช้บริการ(Allen, A.O., 1978)

ทฤษฎีรอคอยเป็นที่นิยมมากในปัจจุบัน แบ่งความสัมพันธ์ออกเป็น

ก. Average arrival (A) : เวลาเฉลี่ยที่ผู้ใช้บริการมาถึง

ข. Service Times (s) : เวลาที่ให้บริการ

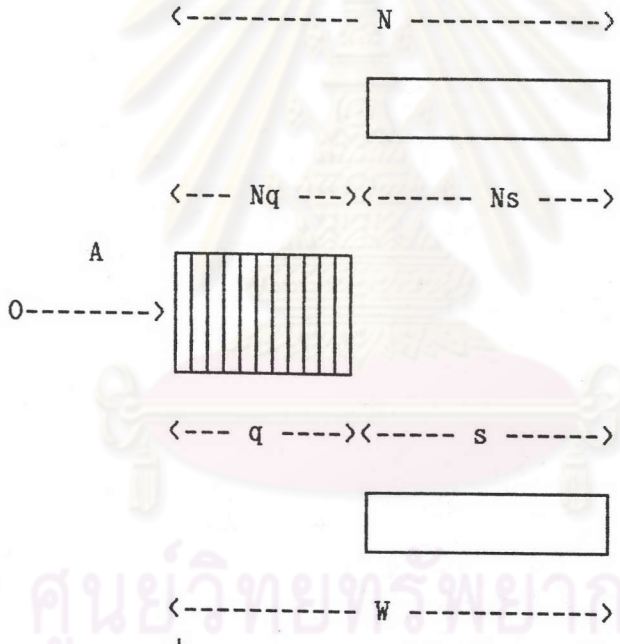
ค. Number of service (Ns) : จำนวนบริการที่มี

ง. Times spent in the queue (q): เวลาที่อยู่ในคิว

จ. Numbers of customers in the queue (Nq) : จำนวนผู้ใช้บริการในคิว

ฉ. Total number of customers in the queueing system (N): จำนวนผู้ใช้บริการที่อยู่ในระบบ

ช. Total time a customer spends in the queueing system (W): เวลาทั้งหมดที่ผู้ใช้บริการใช้ในระบบ



รูปที่ 2.2 แสดงความสัมพันธ์ของทฤษฎีรอคอย

จากรูปที่ 2.2 เห็นได้ว่า ระยะเวลาทั้งหมดที่ผู้ใช้บริการเข้ามาใช้ระบบ มีความสัมพันธ์กับระยะเวลาที่ผู้ใช้บริการรอคอยใช้บริการ และระยะเวลาที่ผู้ใช้บริการใช้บริการ

$$W = Q + S$$

W : ระยะเวลาทั้งหมดที่ผู้ใช้บริการเข้ามาใช้ระบบ

Q : ระยะเวลาที่ผู้ใช้บริการรอคอยใช้บริการ

S : ระยะเวลาที่ผู้ใช้บริการใช้บริการ

เมื่อได้เวลาทั้งหมดที่ผู้ใช้บริการเข้ามาใช้ระบบแล้วนำมาหาความสัมพันธ์กับ Little's Result ที่กล่าวว่า จำนวนผู้ใช้บริการในระบบ เท่ากับ ค่าเฉลี่ยของการมาถึง คูณด้วยระยะเวลาทั้งหมดที่ผู้ใช้บริการเข้ามาใช้ระบบ

$$L = A \times W$$

L = จำนวนผู้ใช้บริการในระบบ

A = ค่าเฉลี่ยของการมาถึง (งาน/หน่วยเวลา)

W = ระยะเวลาทั้งหมดที่ผู้ใช้บริการเข้ามาใช้ระบบ

ในที่นี้เราสามารถหาจำนวนผู้ใช้บริการในระบบ ได้จากจำนวนคู่สายโทรศัพท์ที่ใช้ในการทดสอบนั่นคือ 2 คู่สาย ส่วนระยะเวลาทั้งหมดที่ผู้ใช้บริการเข้ามาใช้ระบบหาได้จากที่กล่าวข้างต้นผลลัพธ์ที่ต้องการคือ ค่าเฉลี่ยของการมาถึง ซึ่งบอกให้เราทราบว่า ผู้ใช้บริการมีโอกาสในการโทรเข้ามาใช้บริการง่าย หรือยาก ดังที่จะกล่าวละเอียดในบทที่ 5