

Zero-Knowledge Protocols

Abhabongse Janthong
สถาพงศ์ จันทรทอง
Associate Visionary Architect, KBTG

Zero-Knowledge Protocols

**HOW TO ACHIEVE A
COMMUNICATION
GOAL WITHOUT
LEAKING JUST
ANYTHING?**

Abhabongse Janthong

สถาพงศ์ จันทรทอง

Associate Visionary Architect, KBTG

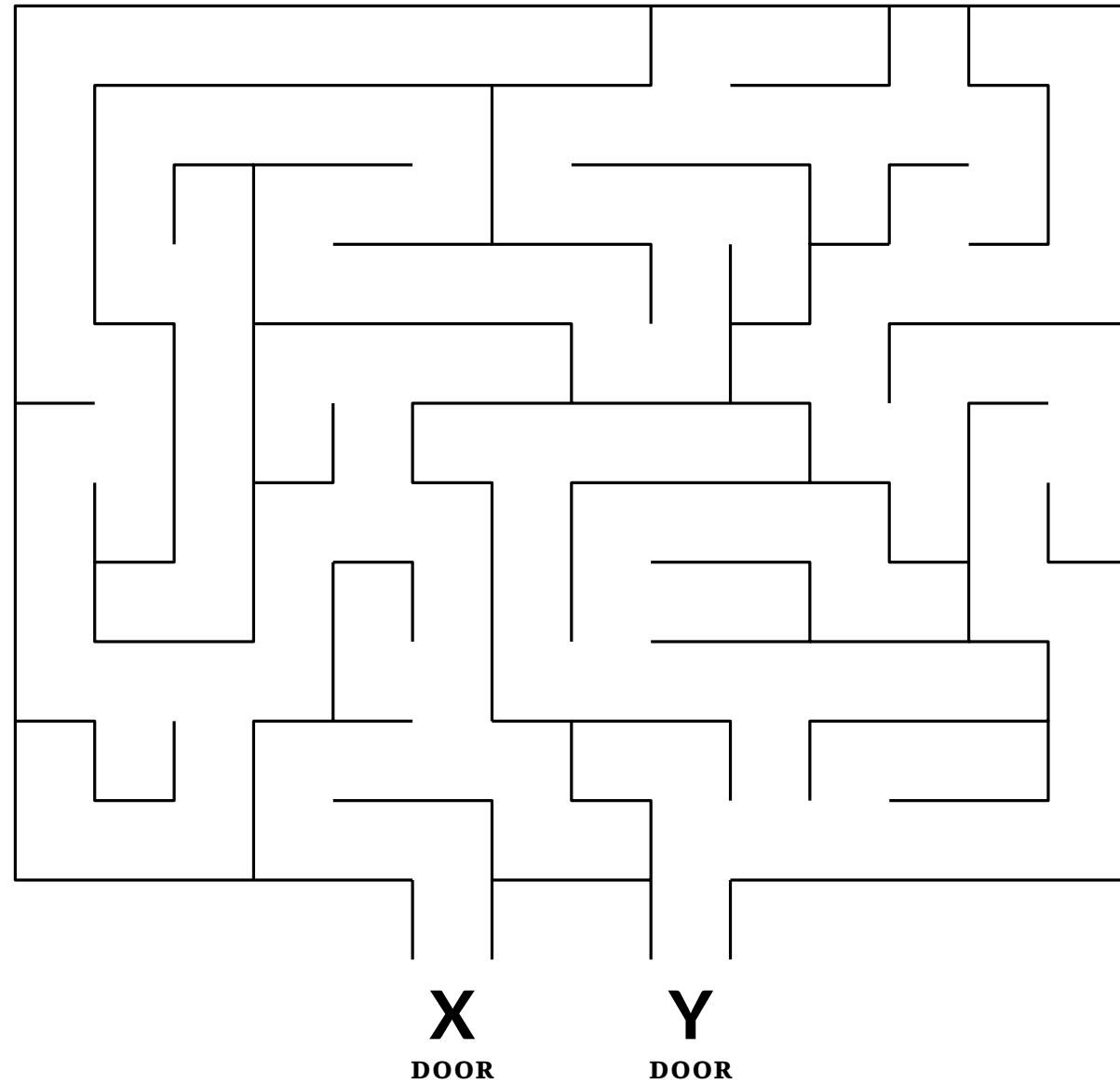
Zero-Knowledge Protocols

ต้องการสื่อสารเพื่อบรรลุ
เป้าหมายบางอย่างโดยไม่
เปิดเผยอะไรนอก
เหนือจากที่จำเป็น

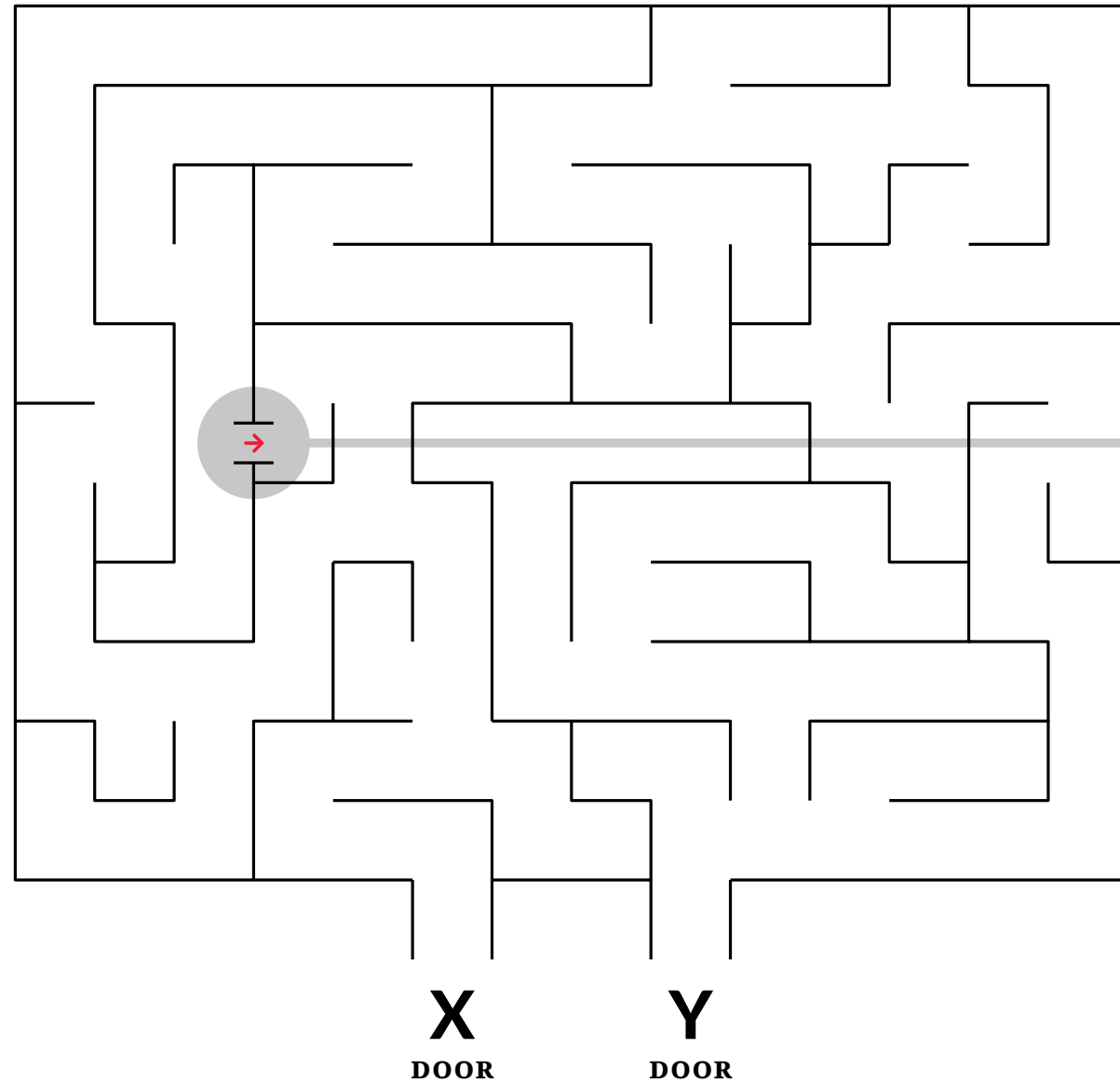
Abhabongse Janthong
อาภาพงศ์ จันทรทอง
Associate Visionary Architect, KBTG

Maze | เขาวงกต

เขาวงกตมีทางเข้า-ออก 2 ทาง และมีเส้นทางภายในที่เชื่อมด้วยกลไกปริศนาอย่างหนึ่ง



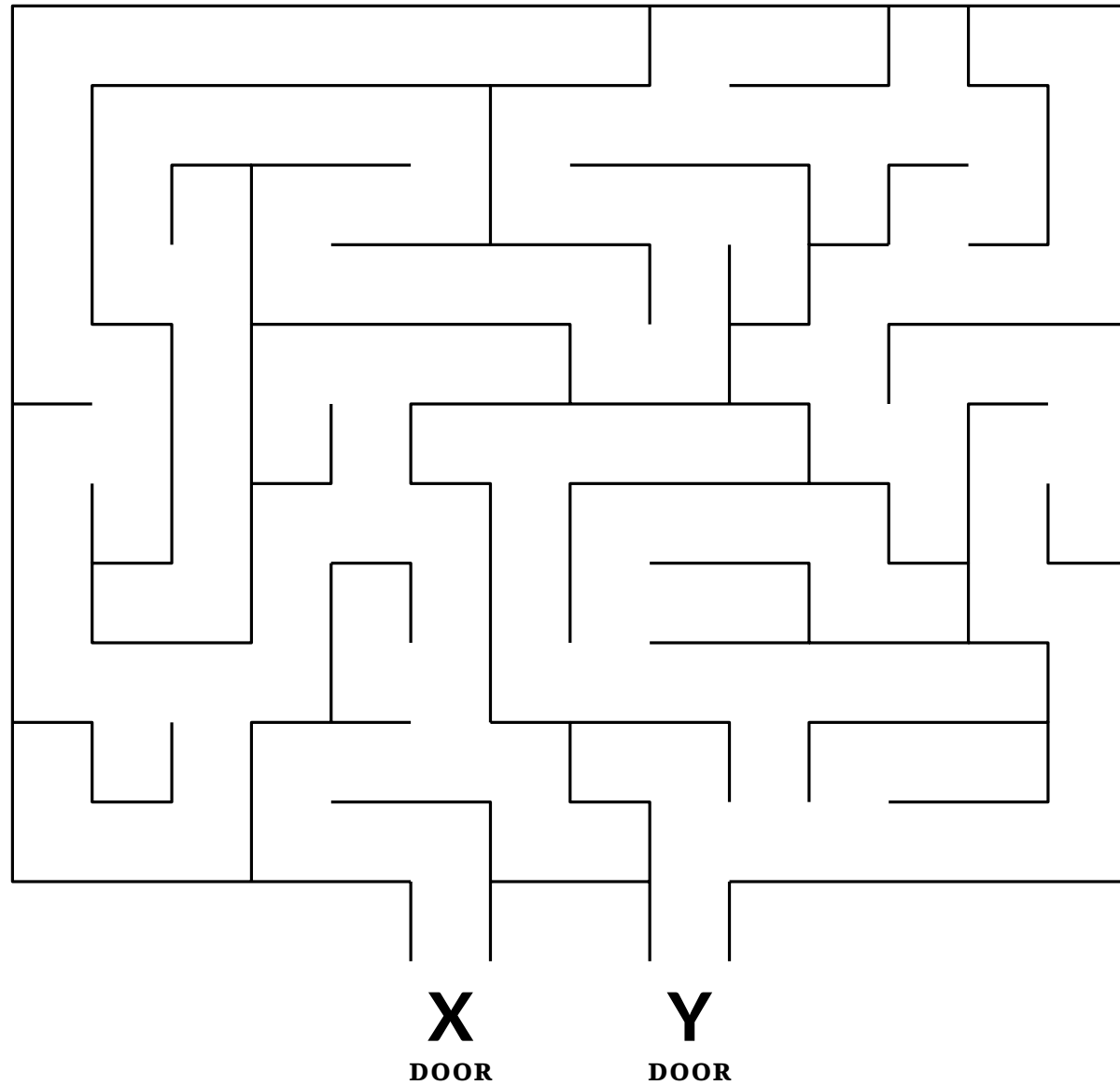
Maze | เขาวงกต



เขาวงกตมีทางเข้า-ออก 2 ทาง และมีเส้นทางภายในที่เชื่อมด้วยกลไกปริศนาอย่างหนึ่ง

(เช่น อาจมีประตูกลที่เปิดได้ทางเดียวซ่อนอยู่ หรือประตูที่ต้องใช้รหัสผ่านลับเพื่อเปิดใช้งาน เป็นต้น)

Maze | เขาวงกต



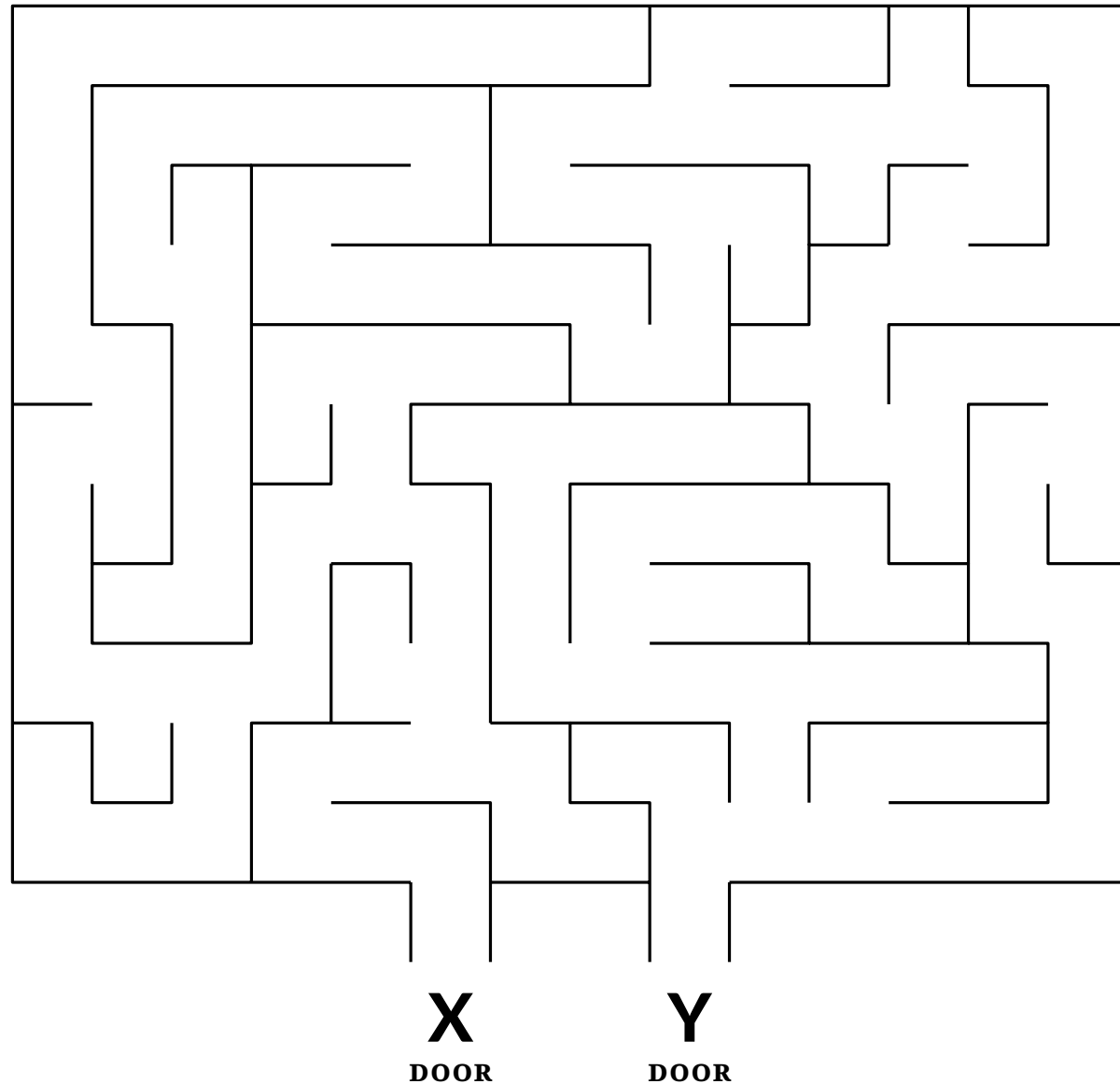
เขาวงกตมีทางเข้า-ออก 2 ทาง และมีเส้นทางภายในที่เชื่อมด้วยกลไกปริศนาอย่างหนึ่ง

(เช่น อาจมีประตูกลที่เปิดได้ทางเดียวซ่อนอยู่ หรือประตูที่ต้องใช้รหัสผ่านลับเพื่อเปิดใช้งาน เป็นต้น)

Alice ต้องการจะพิสูจน์ให้ **Bob** ฟังว่า

ฉันรู้จักเส้นทางในเขาวงกตระหว่างประตู **X** และประตู **Y**

Maze | เขาวงกต



เขาวงกตมีทางเข้า-ออก 2 ทาง และมีเส้นทางภายในที่เชื่อมด้วยกลไกปริศนาอย่างหนึ่ง

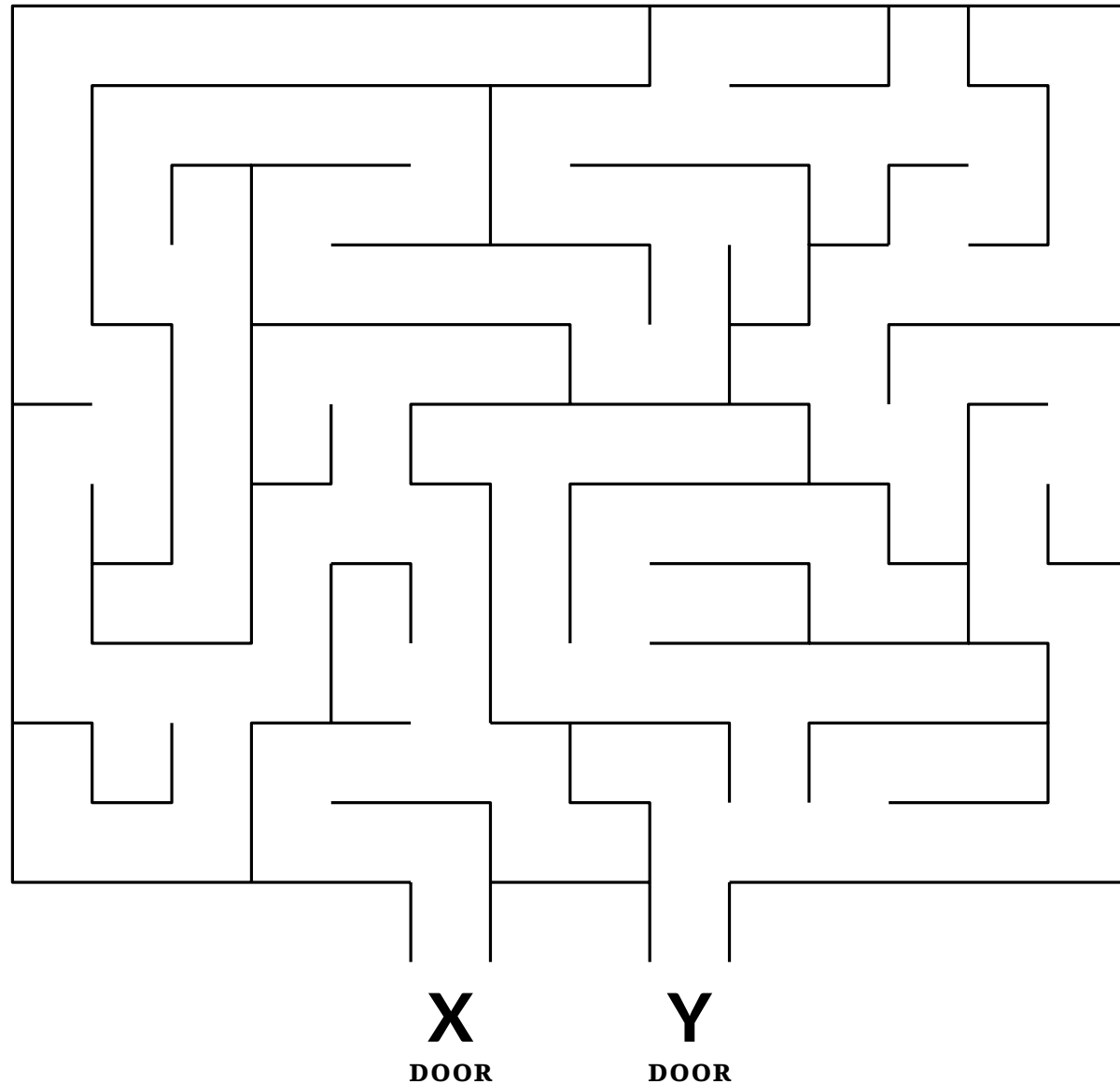
(เช่น อาจมีประตูกลที่เปิดได้ทางเดียวซ่อนอยู่ หรือประตูที่ต้องใช้รหัสผ่านลับเพื่อเปิดใช้งาน เป็นต้น)

Alice ต้องการจะพิสูจน์ให้ **Bob** ฟังว่า

ฉันรู้จักเส้นทางในเขาวงกตระหว่างประตู **X** และประตู **Y**

เราไม่เชื่อแกหรอก!!!

Maze | เขาวงกต



เขาวงกตมีทางเข้า-ออก 2 ทาง และมีเส้นทางภายในที่เชื่อมด้วยกลไกปริศนาอย่างหนึ่ง

(เช่น อาจมีประตูกลที่เปิดได้ทางเดียวซ่อนอยู่ หรือประตูที่ต้องใช้รหัสผ่านลับเพื่อเปิดใช้งาน เป็นต้น)

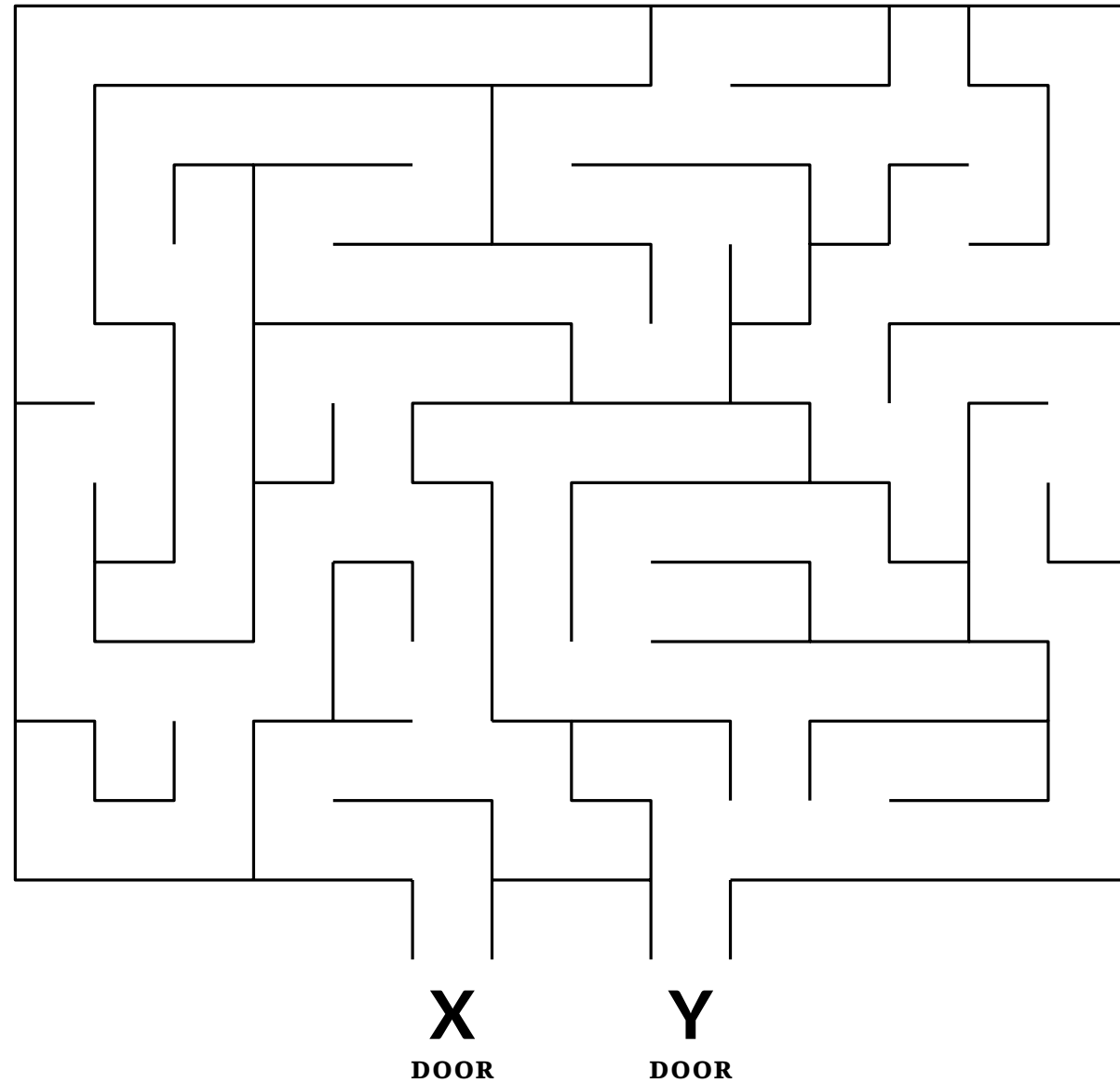
Alice ต้องการจะพิสูจน์ให้ **Bob** ฟังว่า

ฉันรู้จักเส้นทางในเขาวงกตระหว่างประตู **X** และประตู **Y**

เราไม่เชื่อแกหรอก!!!

มา! เดี่ยวฉันนำทางเธอเอง

Maze | เขาวงกต



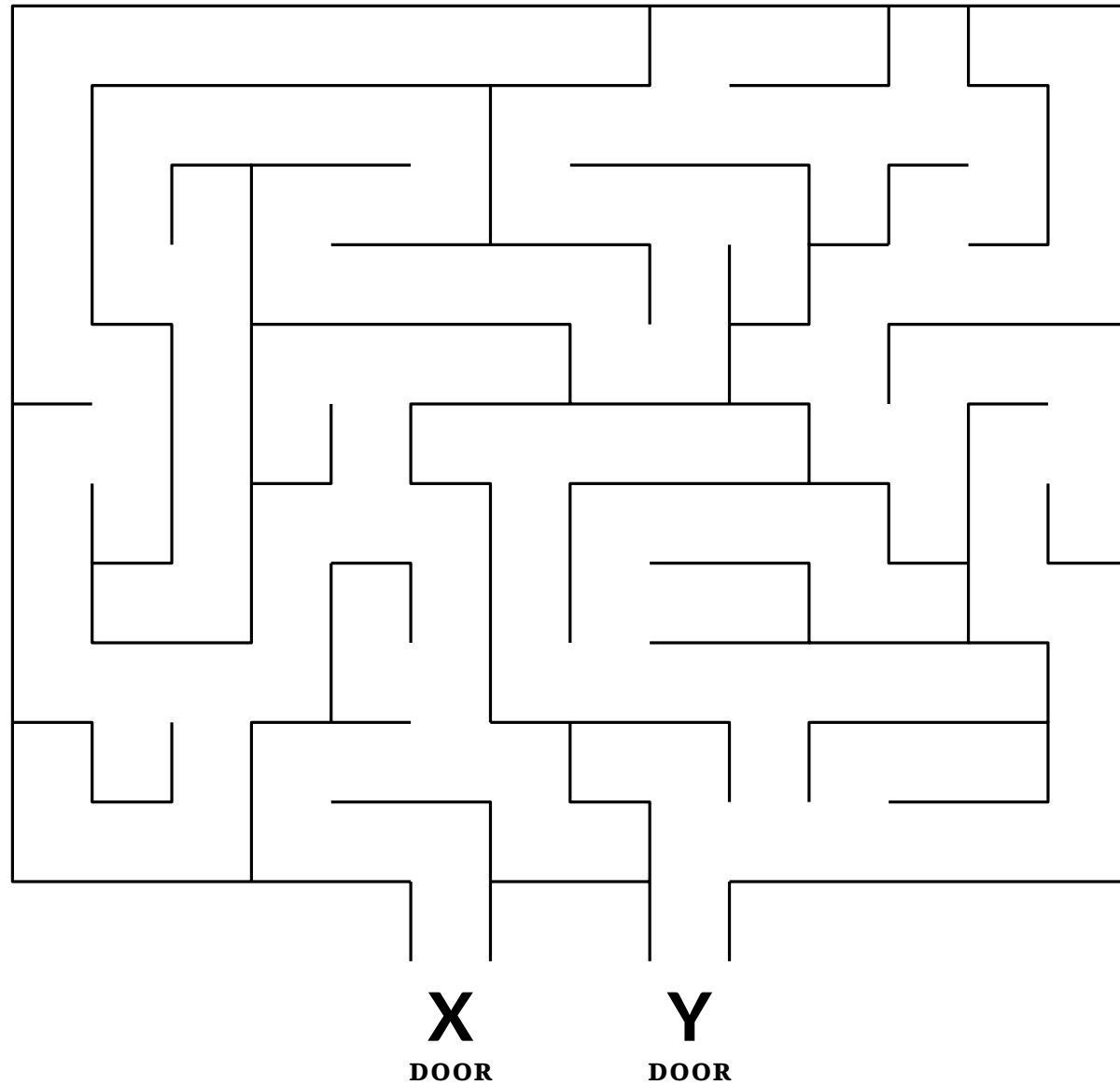
ฉันรู้จักเส้นทางในเขาวงกตระหว่างประตู **X** และประตู **Y**

เราไม่เชื่อแกหรอก!!!

มา! เดี่ยวฉันนำทางเธอเอง

ไม่เอาหรอก เราไม่อยากโดนสปอยล์อะ --

Maze | เขาวงกต



ฉันรู้จักเส้นทางในเขาวงกตระหว่างประตู **X** และประตู **Y**

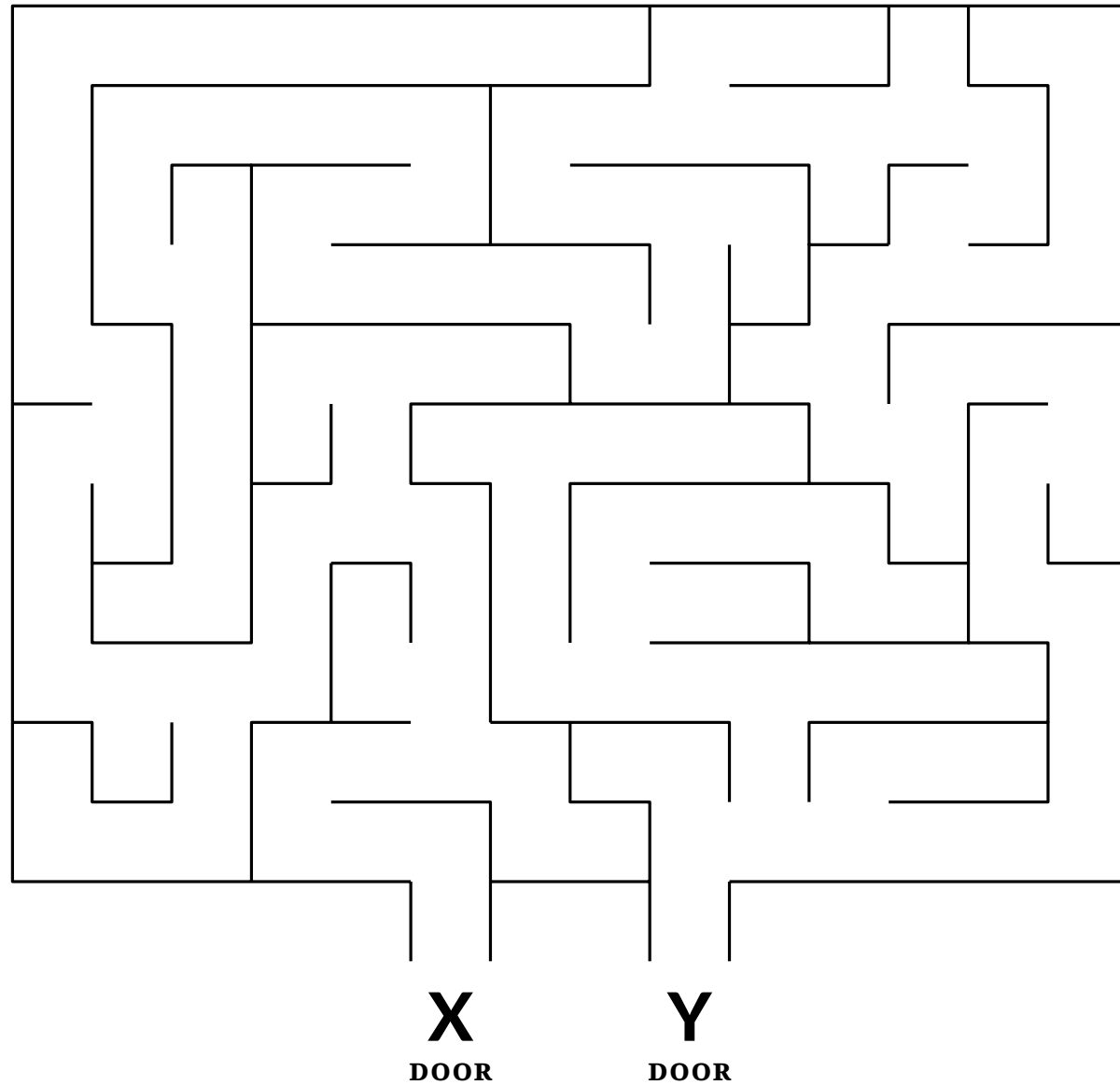
เราไม่เชื่อแกหรอก!!!

มา! เดี่ยวฉันนำทางเธอเอง

ไม่เอาหรอก เราไม่อยากโดนสปอยล์อะ --

เธอนี้เรื่องมากจังนะ :(จะเอาไง

Maze | เขาวงกต



ฉันรู้จักเส้นทางในเขาวงกตระหว่างประตู **X** และประตู **Y**

เราไม่เชื่อแกหรอก!!!

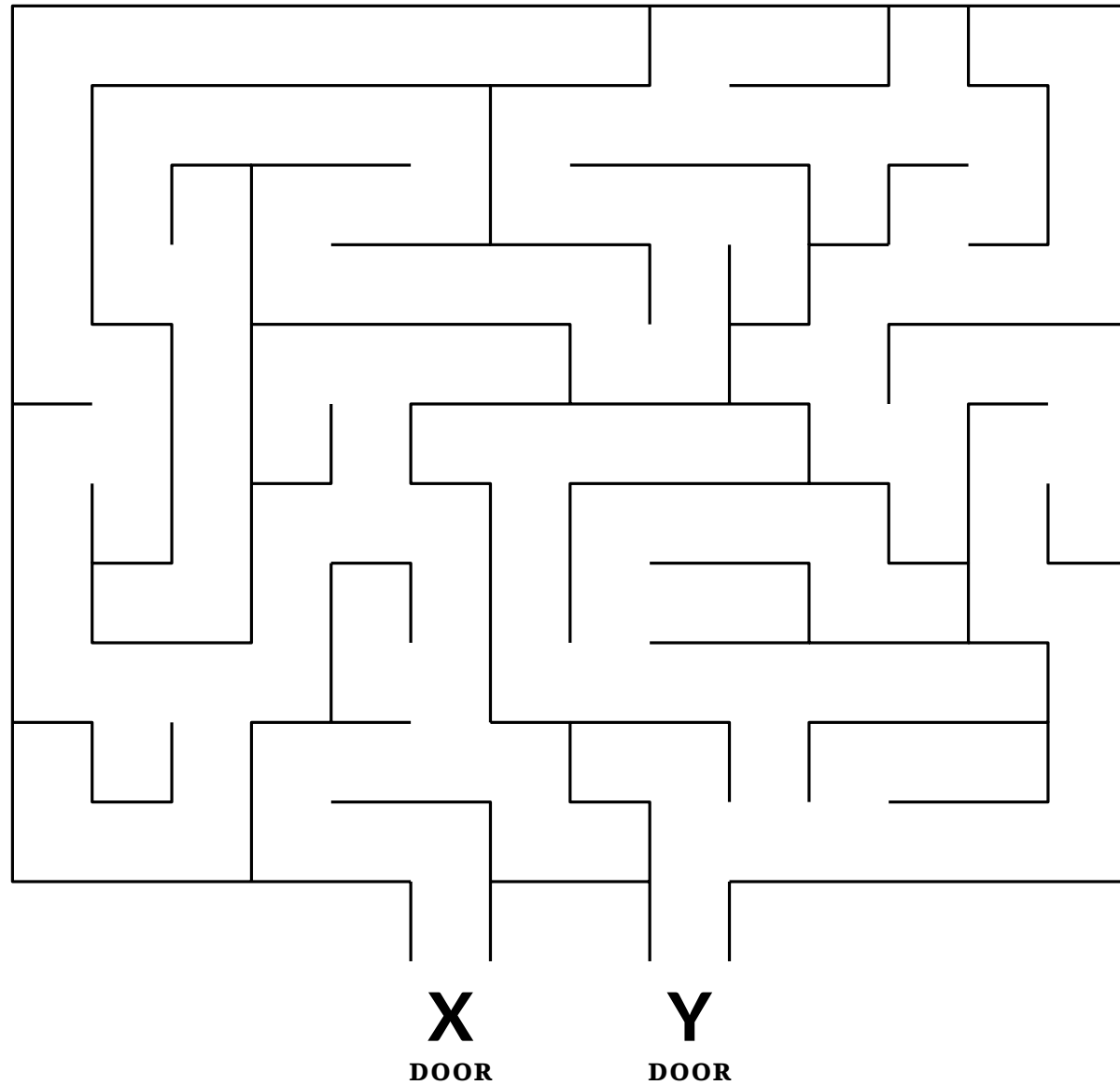
มา! เดี่ยวฉันนำทางเธอเอง

ไม่เอาหรอก เราไม่อยากโดนสปอยล์อะ --

เธอนี้เรื่องมากจังนะ :(จะเอาไง

จริง ๆ มันก็มีวิธีอยู่นะ

Maze | เขาวงกต



ฉันรู้จักเส้นทางในเขาวงกตระหว่างประตู **X** และประตู **Y**

เราไม่เชื่อแกหรอก!!!

มา! เดี่ยวฉันนำทางเธอเอง

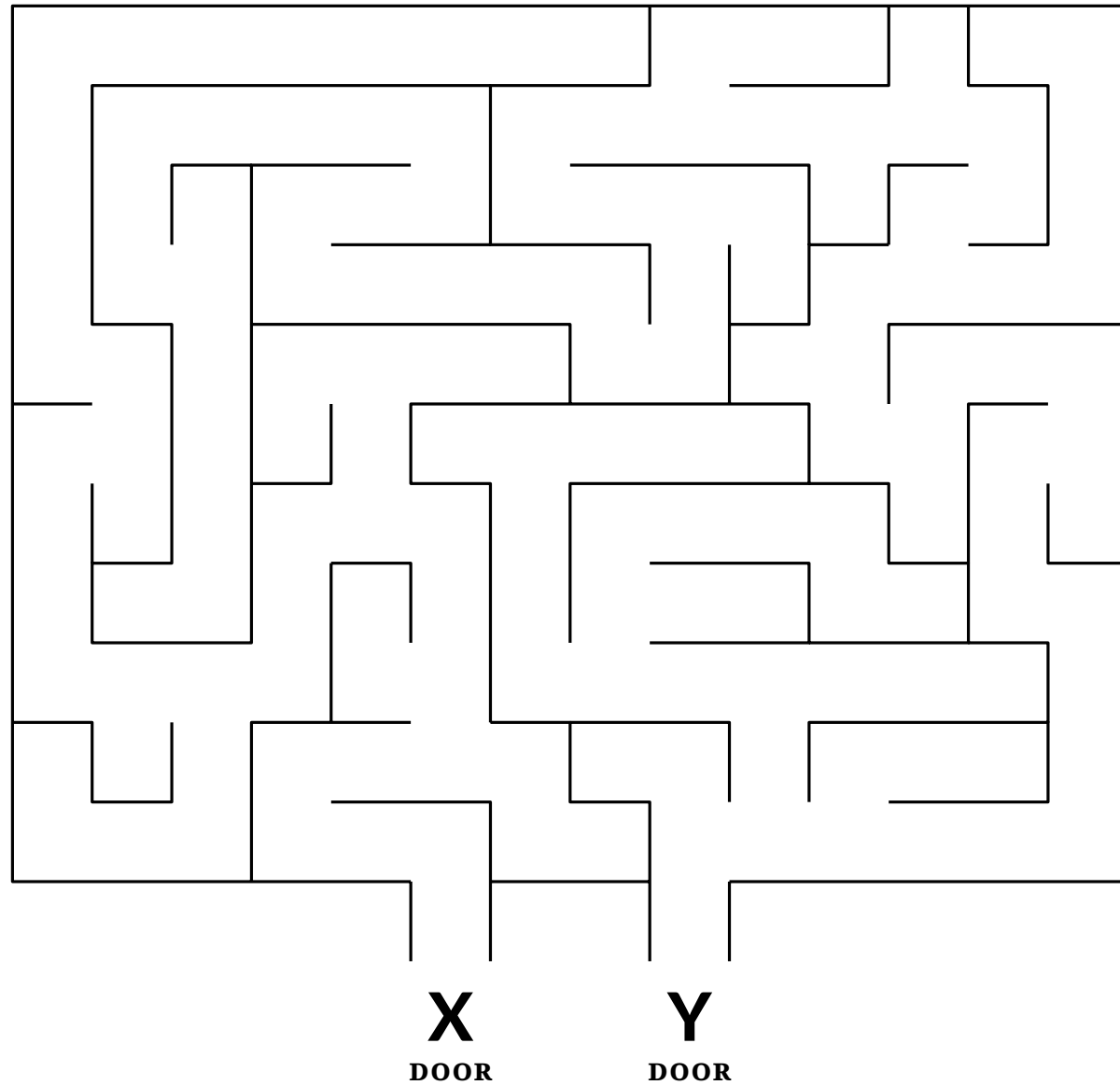
ไม่เอาหรอก เราไม่อยากโดนสปอยล์อะ --

เธอนี้เรื่องมากจังนะ :(จะเอาไง

จริง ๆ มันก็มีวิธีอยู่นะ

แกก็เข้าประตู **X** ไป แล้วออกทางประตู **Y** ให้เราเห็น
เดี๋ยวเราเฝ้าดูจากข้างนอกนี่แหละ

Maze | เขาวงกต



ฉันรู้จักเส้นทางในเขาวงกตระหว่างประตู **X** และประตู **Y**

เราไม่เชื่อแกหรอก!!!

มา! เดี่ยวฉันนำทางเธอเอง

ไม่เอาหรอก เราไม่อยากโดนสปอยล์อะ --

เธอนี้เรื่องมากจังนะ :(จะเอาไง

จริง ๆ มันก็มีวิธีอยู่นะ

แกก็เข้าประตู **X** ไป แล้วออกทางประตู **Y** ให้เราเห็น
เดี๋ยวเราเฝ้าดูจากข้างนอกนี่แหละ

แต่ว่า ... ฉันทำแบบนั้นไม่ได้หรอก