Zero-Knowledge Protocols

Abhabongse Janthong
อาภาพงศ์ จันทร์ทอง
Associate Visionary Architect, KBTG

Zero-Knowledge Protocols

HOW TO ACHIEVE A COMMUNICATION GOAL WITHOUT LEAKING JUST ANYTHING?

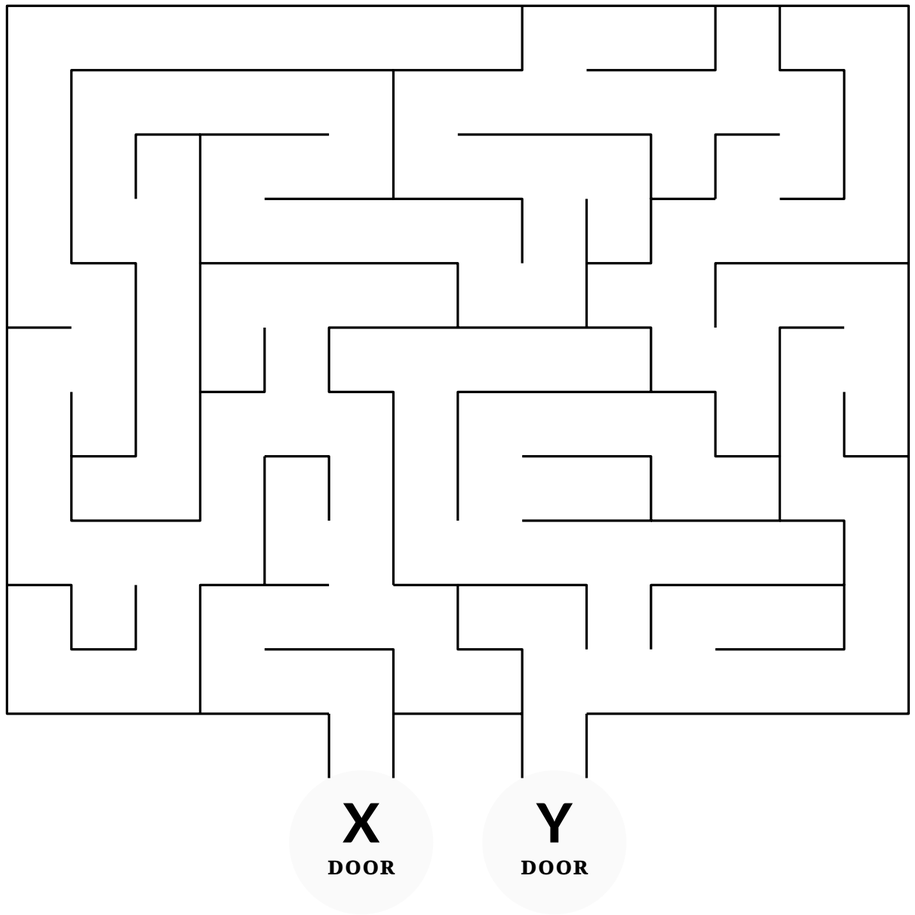
Abhabongse Janthong
อาภาพงศ์ จันทร์ทอง
Associate Visionary Architect, KBTG

Zero-Knowledge Protocols

ต้องการสื่อสารเพื่อบรรลุเป้าหมายบางอย่างโดยไม่เปิดเผยอะไรนอกเหนือจากที่จำเป็น

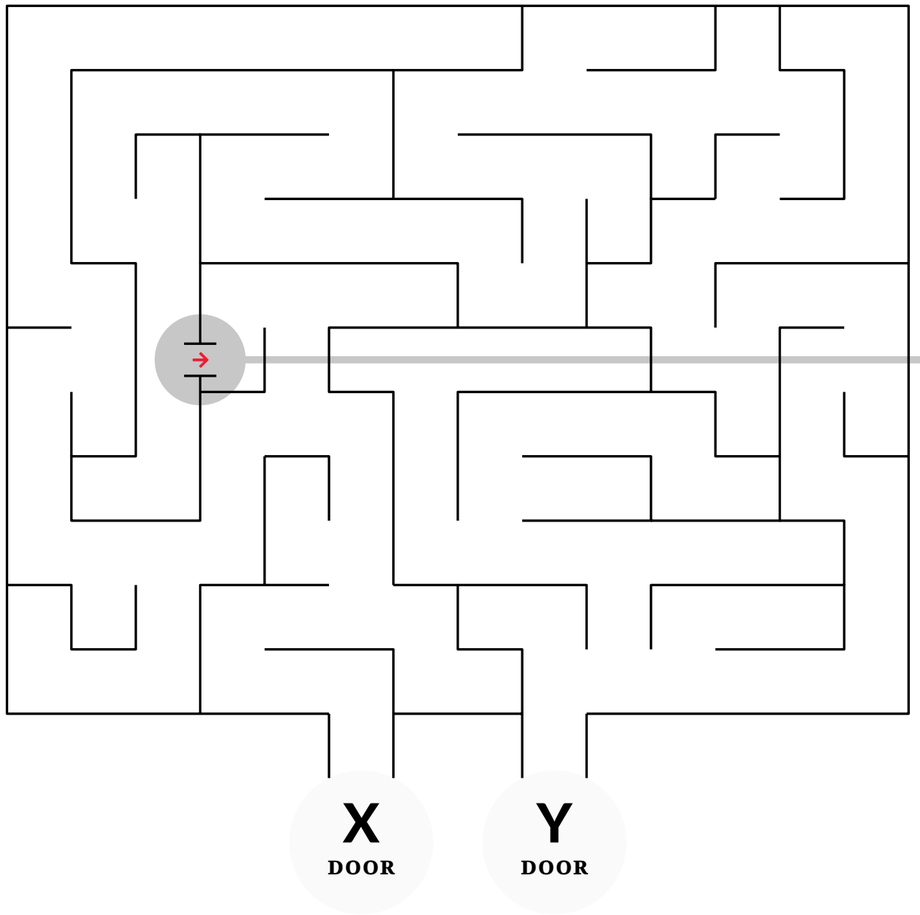
Abhabongse Janthong
อาภาพงศ์ จันทร์ทอง
Associate Visionary Architect, KBTG

Maze | เขาวงกต



เขาวงกตมี**ทางเข้า-ออก 2 ทาง** และมีเส้นทางภายในที่เชื่อมด้วย**กลไกปริศนา**อย่างหนึ่ง

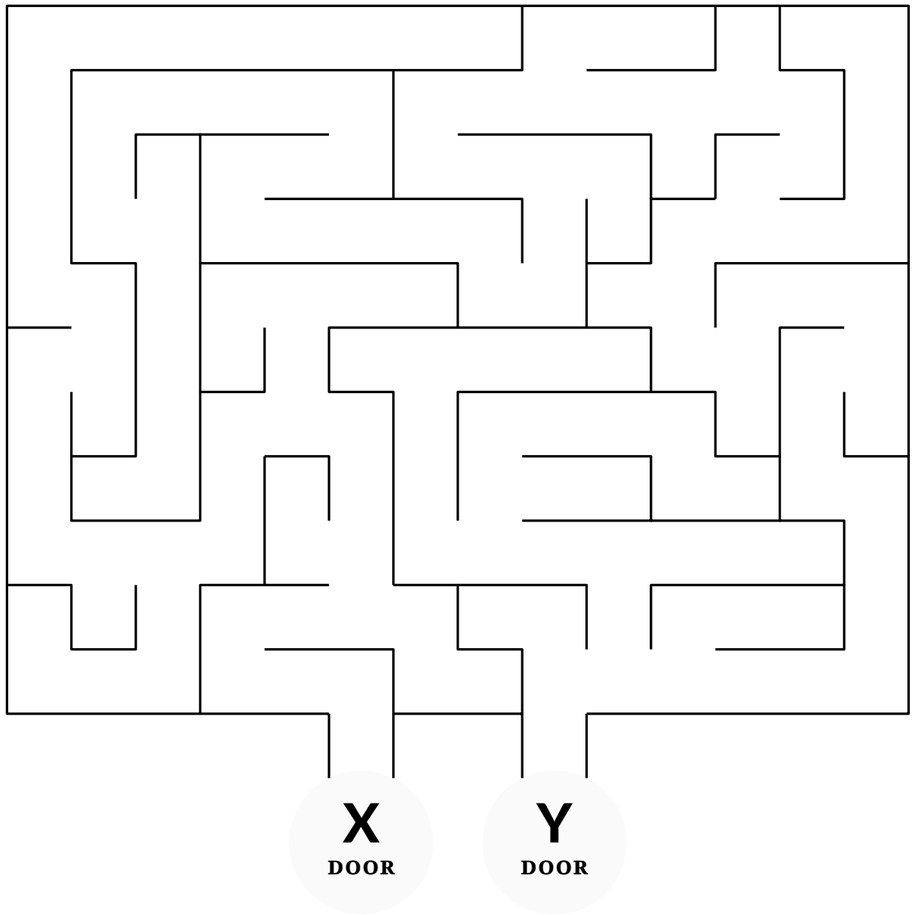
Maze | เขาวงกต



เขาวงกตมี**ทางเข้า-ออก 2 ทาง** และมีเส้นทางภายในที่เชื่อมด้วย**กลไกปริศนา**อย่างหนึ่ง

(เช่น อาจมีประตูกลที่เปิดได้ทางเดียวซ่อนอยู่ หรือประตูที่ต้องใช้รหัสผ่านลับเพื่อเปิดใช้งาน เป็นต้น)

Maze | เขาวงกต



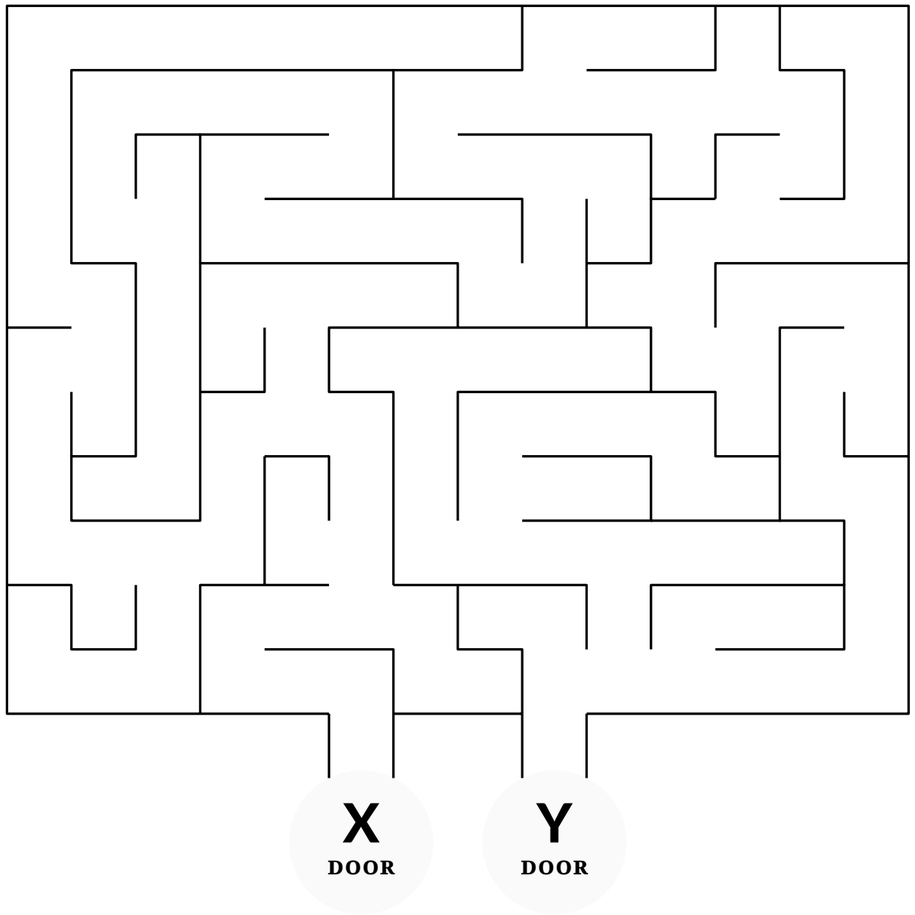
เขาวงกตมี**ทางเข้า-ออก 2 ทาง** และมีเส้นทางภายในที่เชื่อมด้วย**กลไกปริศนา**อย่างหนึ่ง

(เช่น อาจมีประตูกลที่เปิดได้ทางเดียวซ่อนอยู่ หรือประตูที่ต้องใช้รหัสผ่านลับเพื่อเปิดใช้งาน เป็นต้น)

Alice ต้องการจะพิสูจน์ให้ **Bob** ฟังว่า

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

Maze | เขาวงกต



เขาวงกตมี**ทางเข้า-ออก 2 ทาง** และมีเส้นทางภายในที่เชื่อมด้วย**กลไกปริศนา**อย่างหนึ่ง

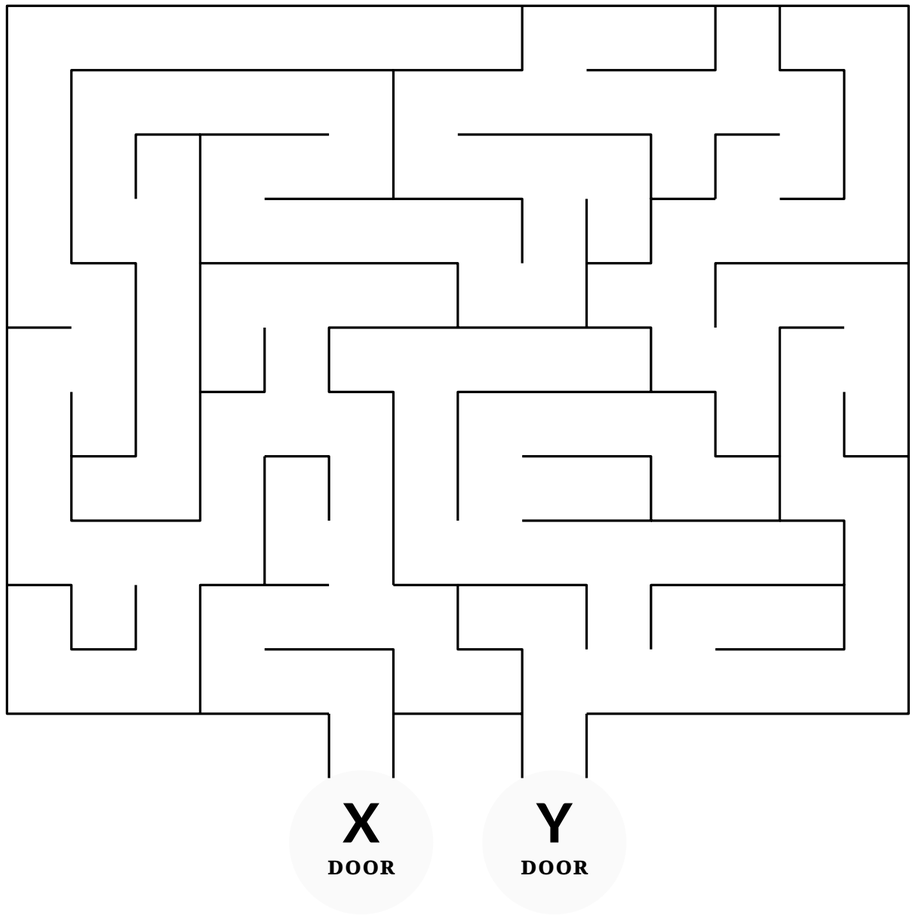
(เช่น อาจมีประตูกลที่เปิดได้ทางเดียวซ่อนอยู่ หรือประตูที่ต้องใช้รหัสผ่านลับเพื่อเปิดใช้งาน เป็นต้น)

Alice ต้องการจะพิสูจน์ให้ **Bob** ฟังว่า

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

เราไม่เชื่อแกหรอก!!!

Maze | เขาวงกต



เขาวงกตมี**ทางเข้า-ออก 2 ทาง** และมีเส้นทางภายในที่เชื่อมด้วย**กลไกปริศนา**อย่างหนึ่ง

(เช่น อาจมีประตูกลที่เปิดได้ทางเดียวซ่อนอยู่ หรือประตูที่ต้องใช้รหัสผ่านลับเพื่อเปิดใช้งาน เป็นต้น)

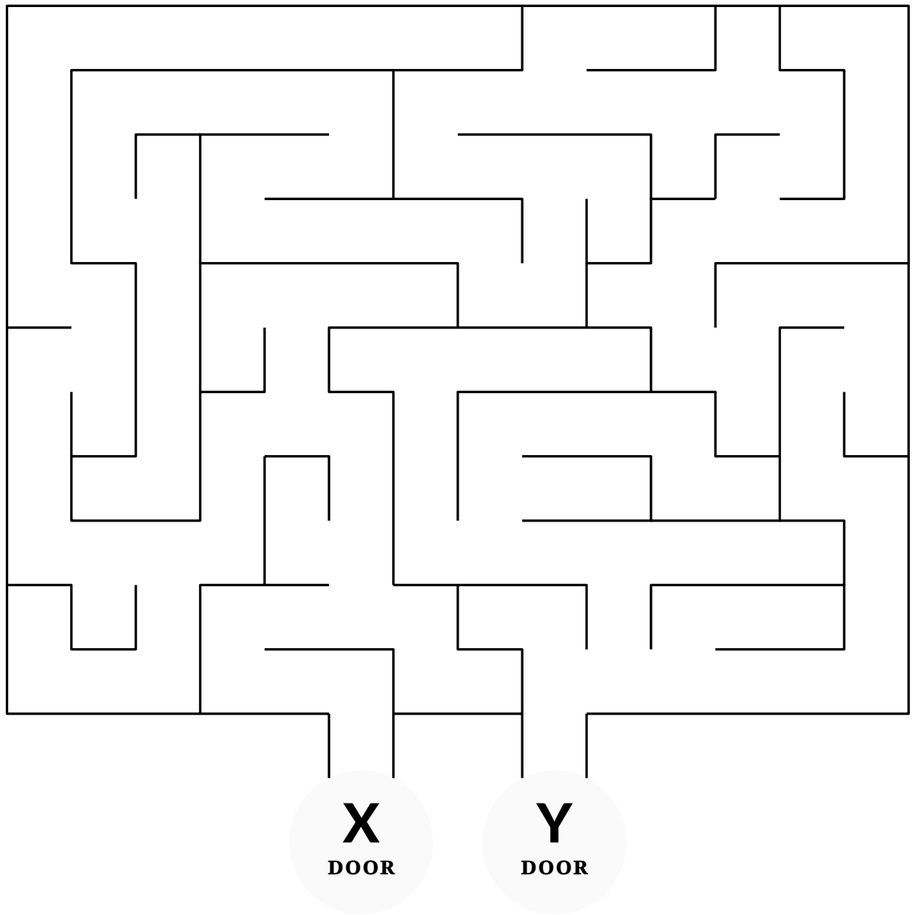
Alice ต้องการจะพิสูจน์ให้ **Bob** ฟังว่า

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

เราไม่เชื่อแกหรอก!!!

มา! เดี๋ยวฉันนำทางเธอเอง

Maze | เขาวงกต



Alice ต้องการจะพิสูจน์ให้ **Bob** ฟังว่า

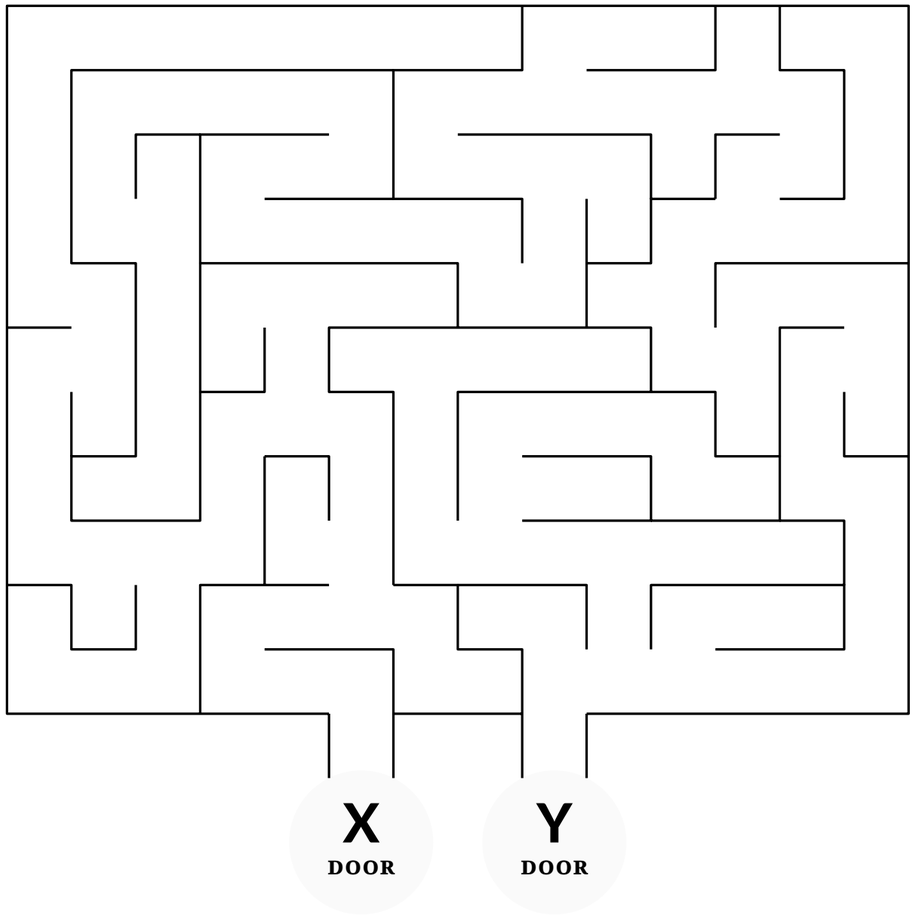
ฉันรู้จักเส้นทางในเขาวงกตระหว่างประตู **X** *และประตู* **Y**

เราไม่เชื่อแกหรอก!!!

มา! เดี๋ยวฉันนำทางเธอเอง

ไม่เอาหรอก เราไม่อยากโดนสปอยล์อะ -_-

Maze | เขาวงกต



Alice ต้องการจะพิสูจน์ให้ **Bob** ฟังว่า

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

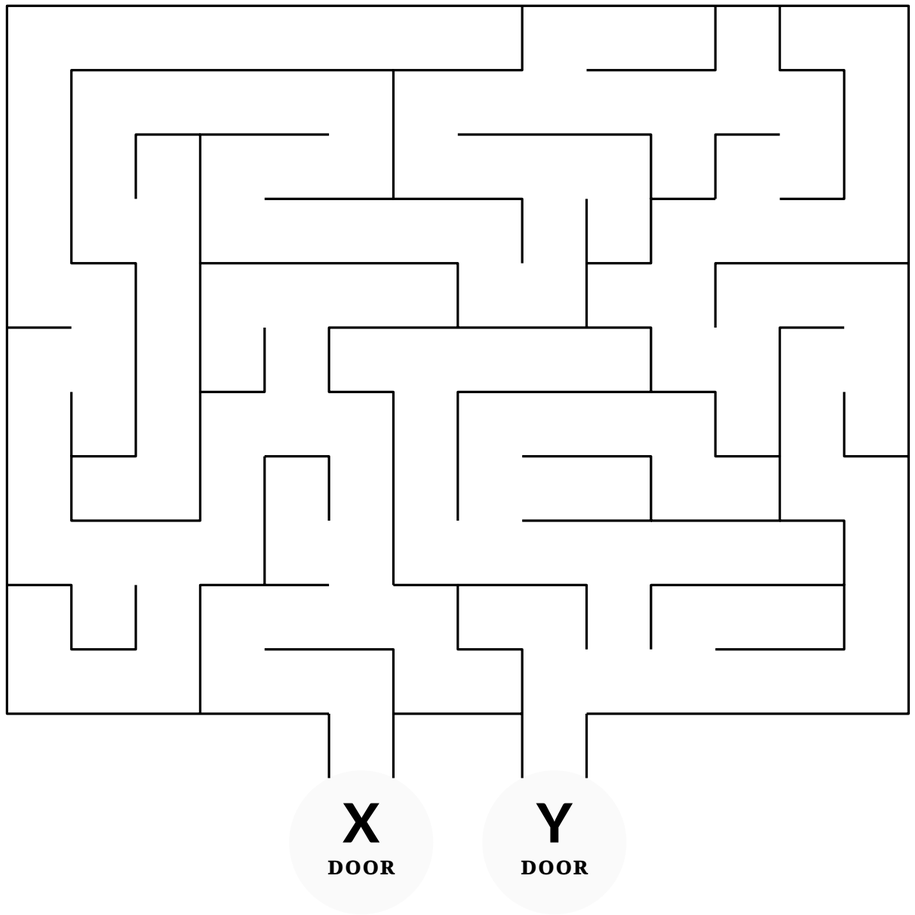
เราไม่เชื่อแกหรอก!!!

มา! เดี๋ยวฉันนำทางเธอเอง

ไม่เอาหรอก เราไม่อยากโดนสปอยล์อะ -_-

เธอนี่เรื่องมากจังนะ :(จะเอาไง

Maze | เขาวงกต



Alice ต้องการจะพิสูจน์ให้ **Bob** ฟังว่า

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

เราไม่เชื่อแกหรอก!!!

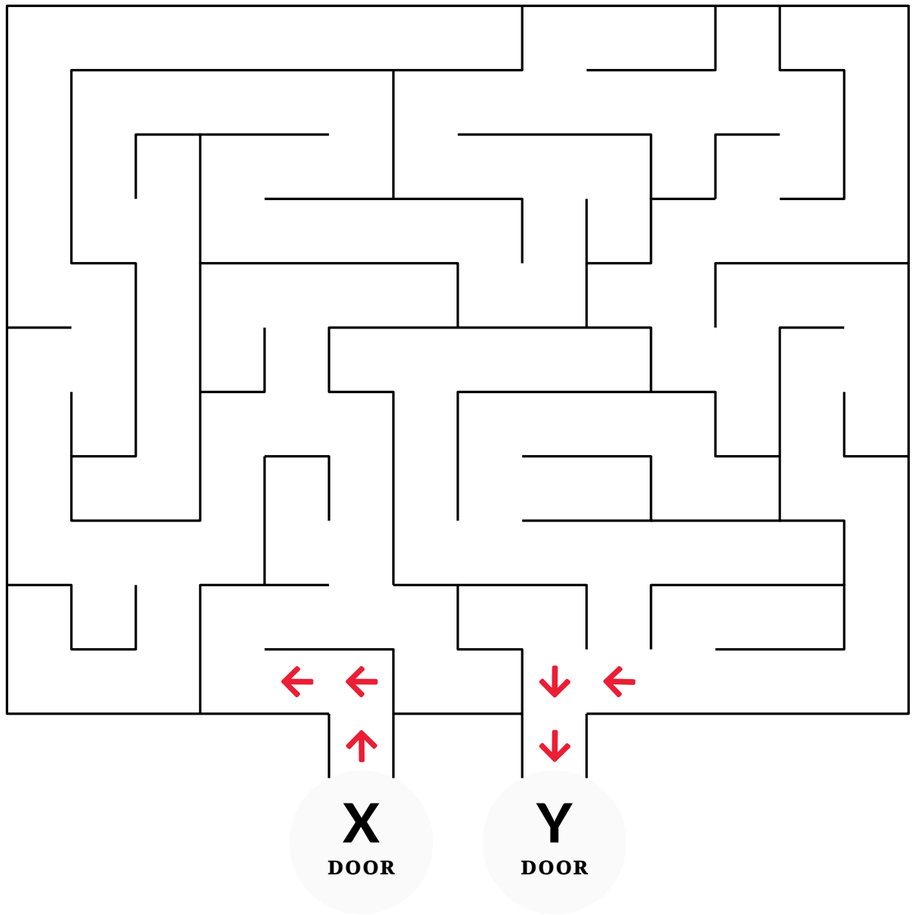
มา! เดี๋ยวฉันนำทางเธอเอง

ไม่เอาหรอก เราไม่อยากโดนสปอยล์อะ -_-

เธอนี่เรื่องมากจังนะ :(จะเอาไง

จริง ๆ มันก็มีวิธีอยู่นะ

Maze | เขาวงกต



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

เราไม่เชื่อแกหรอก!!!

มา! เดี๋ยวฉันนำทางเธอเอง

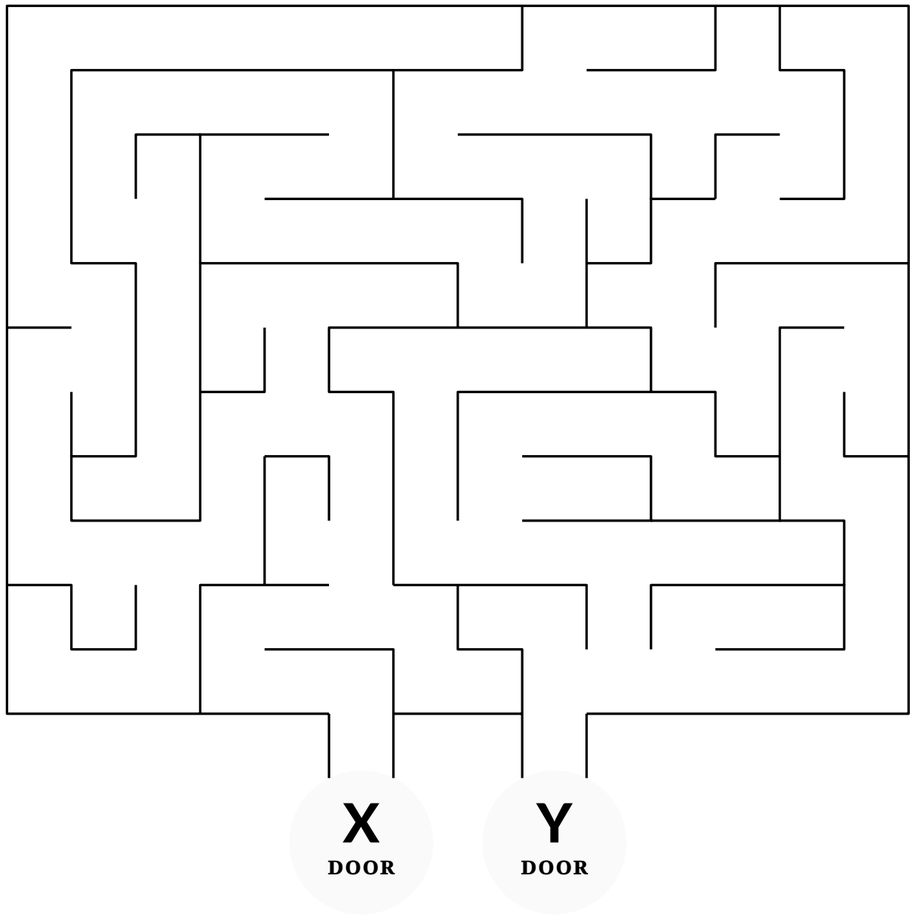
ไม่เอาหรอก เราไม่อยากโดนสปอยล์อะ -_-

เธอนี่เรื่องมากจังนะ :(จะเอาไง

จริง ๆ มันก็มีวิธีอยู่นะ

แกก็เข้าประตู **X** ไป แล้วออกทางประตู **Y** ให้เราเห็น
เดี๋ยวเราเฝ้าดูจากข้างนอกนี้นี่แหละ

Maze | เขาวงกต



เราไม่เชื่อแกหรอก!!!

มา! เดี๋ยวฉันนำทางเธอเอง

ไม่เอาหรอก เราไม่อยากโดนสปอยล์อะ -_-

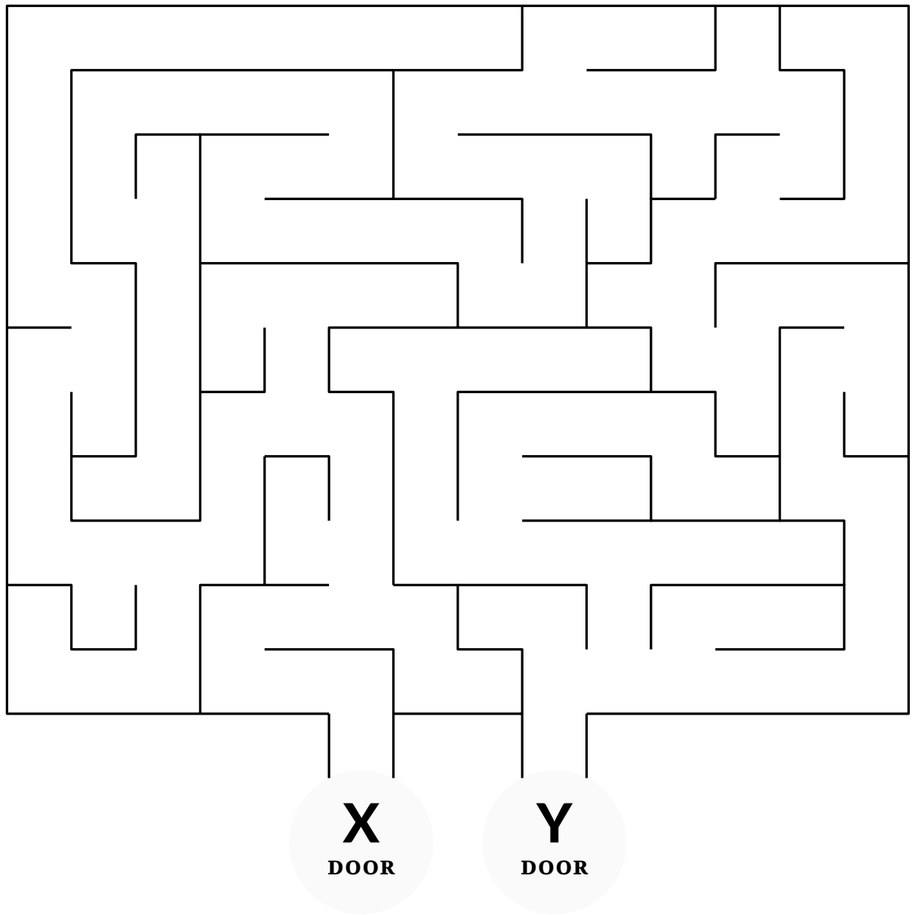
เธอนี่เรื่องมากจังนะ :(จะเอาไง

จริง ๆ มันก็มีวิธีอยู่นะ

*แกก็เข้าประตู **X** ไป แล้วออกทางประตู **Y** ให้เราเห็น*
เดี๋ยวเราเฝ้าดูจากข้างนอกนี้นี่แหละ

ถ้าแบบนั้น ก็เท่ากับให้คำใบ้หนะสิ

Maze | เขาวงกต



มา! เดี๋ยวฉันนำทางเธอเอง

ไม่เอาหรอก เราไม่อยากโดนสปอยล์อะ -_-

เธอนี่เรื่องมากจังนะ :(จะเอาไง

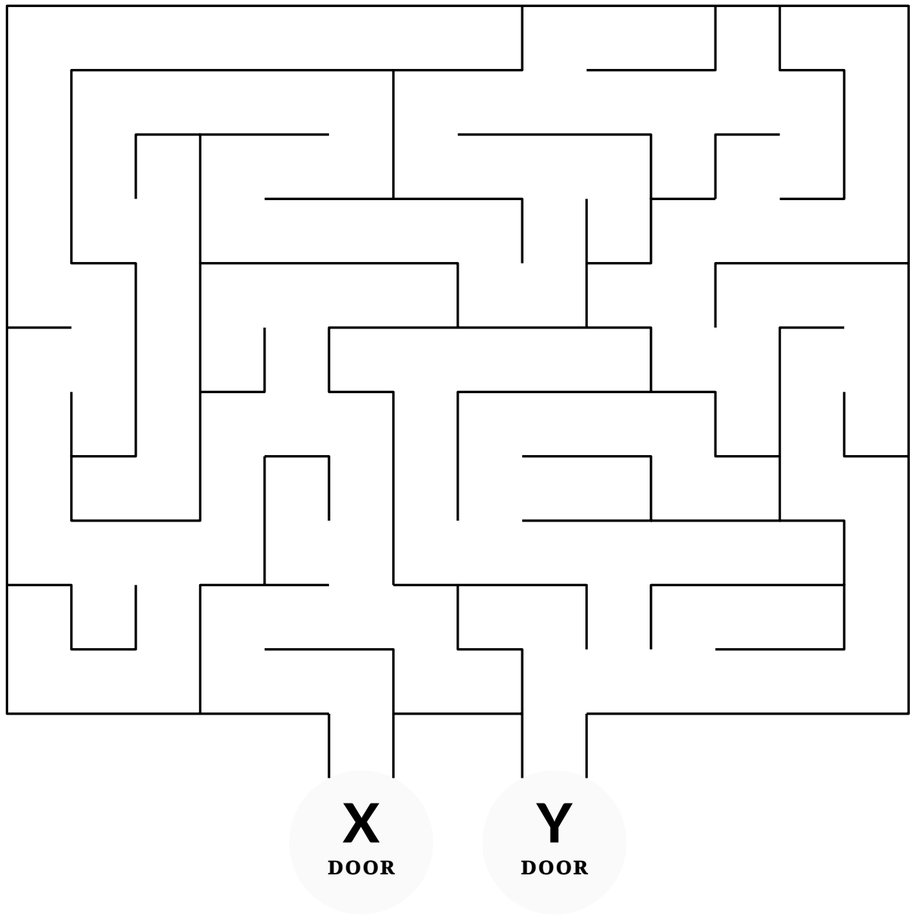
จริง ๆ มันก็มีวิธีอยู่นะ

แกก็เข้าประตู **X** ไป แล้วออกทางประตู **Y** ให้เราเห็น
เดี๋ยวเราเฝ้าดูจากข้างนอกนี้นี่แหละ

ถ้าแบบนั้น ก็เท่ากับให้คำใบ้หนะสิ

. . . ว่ามีทางเข้า-ออกเขาวงกต ที่ต้องเข้าจาก
ประตู **X** แล้วออกทางประตู **Y**

Maze | เขาวงกต



ไม่เอาหรอก เราไม่อยากโดนสปอยล์อะ -_-

เธอนี่เรื่องมากจังนะ :(จะเอาไง

จริง ๆ มันก็มีวิธีอยู่นะ

แกก็เข้าประตู **X** *ไป แล้วออกทางประตู* **Y** *ให้เราเห็น เดี๋ยวเราเฝ้าดูจากข้างนอกนี้นี่แหละ*

ถ้าแบบนั้น ก็เท่ากับให้คำใบ้หนะสิ

. . . ว่ามีทางเข้า-ออกเขาวงกต ที่ต้องเข้าจากประตู **X** *แล้วออกทางประตู* **Y**

เธอไม่ควรรู้ด้วยซ้ำว่ามีเส้นทางแบบนั้น มันก็คือสปอยล์รูปแบบหนึ่งนะ