# 05506232 Mathematics for Computer Science

*Lab 12*

## Objectives

1. เข้าใจการยืนยันการคำนวณความน่าจะเป็นด้วย Counting Techniques ด้วยการเขียนโปรแกรมภาษาไพธอน
2. เข้าใจ RSA Algorithm ด้วยการเขียนโปรแกรมภาษาไพธอน

## Counting Techniques

ให้นักศึกษาตอบคำถามด้านล่างทุกข้อในคอมเมนต์ Assignment ก่อนเขียนโปรแกรมเพื่อยืนยันคำตอบ โดยส่งไฟล์นามสกุล .py หลังจากนั้นแยกตามข้อดังนี้

**ตอบคำถามเหล่านี้ในช่อง Private Comment ก่อน**

1.1 หากโยนเหรียญที่มีน้ำหนักปกติ 1 เหรียญ หากครั้งนี้เหรียญออกหัว โอกาสที่ครั้งต่อไปเหรียญจะออกก้อยมีเท่าไหร่

1.2 ในการแข่งขันฟุตบอลนัดกระชับมิตรนัดหนึ่ง เป็นการพบกันระหว่างทีมชาติไทยกับทีมชาติบราซิล จงเรียงโอกาสที่จะเกิดเหตุการณ์ต่อไปนี้จากมากไปน้อยโดยการอนุมาน

- ทีมชาติไทยจะแพ้ทีมชาติบราซิล
- ทีมชาติไทยจะยิงประตูได้อย่างน้อย 1 ลูก
- ทีมชาติไทยจะชนะทีมชาติบราซิล
- ทีมชาติไทยจะยิงประตูได้อย่างน้อย 1 ลูก แต่จะแพ้ทีมชาติบราซิลในท้ายที่สุด

1.3 เกมโชว์หนึ่ง มีกล่องอยู่ 3 กล่อง จะมีเพียง 1 กล่องเท่านั้นที่มีเงินสด 1 ล้านบาทอยู่ข้างใน เราไม่สามารถทำอะไรกับกล่องได้นอกจากจะเลือกกล่องที่จะเปิด หากเรากล่องใบหนึ่งไปแล้ว พิธีกรเปิดกล่อง 1 ใบจาก 2 กล่องที่เราไม่ได้เลือก พบว่าเป็นกล่องเปล่า และถามว่าเราจะเปลี่ยนกล่องที่เลือกหรือไม่ การเปลี่ยนกล่องที่เลือกจะทำให้โอกาสได้รางวัลมากขึ้น น้อยลง หรือเท่าเดิม

**<u>จงเขียนโปรแกรมเพื่อตรวจสอบคำถามข้างต้นทั้งสามข้อ โดยจำลองสถานการณ์ดังนี้</u>**

1.1 โยนเหรียญแบบสุ่ม 100,000 ครั้ง นับจำนวนครั้งที่เหรียญออกหัวแล้วตามด้วยก้อย เทียบกับจำนวนครั้งที่เหรียญออกหัว คิดเป็นร้อยละ ทำซ้ำ 3 ครั้ง หาค่าเฉลี่ย

1.2 จำลองสถานการณ์ที่ทีมชาติไทยเจอกับทีมชาติบราซิล โดยจำลอง 1 ลูปเท่ากับ 1 นาที (แปลว่า 1 นัดจะวน 90 รอบ) โอกาสที่ทีมชาติไทยจะยิงประตูได้ในแต่ละนาทีคือ 2% โอกาสที่ทีมชาติบราซิลจะยิงประตูได้ในแต่ละนาทีคือ 10% ทำซ้ำการแข่งทั้งหมด 100,000 นัด เรียงลำดับเหตุการณ์ 4 เหตุการณ์ข้างบนว่าเหตุการณ์ใดมีโอกาสเกิดจากมากไปน้อย

1.3 จำลองสถานการณ์ที่มีกล่อง 3 ใบ A B และ C สุ่มให้กล่องใบหนึ่งเป็นกล่องที่ถูกรางวัล เลือกกล่อง A หลังจากนั้นให้เปิดกล่องใบหนึ่งที่ไม่มีรางวัล (B หรือ C) เปรียบเทียบว่าหากทำซ้ำ 100,000 ครั้ง การยืนยันเลือกกล่อง A โดยไม่เปลี่ยน กับการเปลี่ยนไปเลือกกล่องที่ยังไม่ถูกเปิด แบบใดมีโอกาสถูกรางวัลมากกว่ากัน หรือมีโอกาสพอ ๆ กัน

**Deadline: 9 October 2023**

## RSA Algorithm

RSA (Rivest–Shamir–Adleman) เป็นหนึ่งในอัลกอริทึมเข้ารหัสแบบไม่สมมาตรที่เก่าแก่และนิยมใช้มากที่สุด แนวคิดของ RSA คือการเข้ารหัสข้อความด้วยกุญแจที่เปิดเผยต่อสาธารณะ (Public Key) และจะสามารถถูกถอดรหัสได้จากกุญแจเฉพาะ (Private Key) ที่ปลายทาง

- เลือกจำนวนเฉพาะมาสองจำนวน p และ q ในสถานการณ์จริงจะใช้จำนวนเฉพาะที่ขนาดใหญ่มาก ๆ
- คำนวณค่า $n = p \times q$
- คำนวณค่า $phi(n) = (p - 1) \times (q - 1)$
- หาค่า e ซึ่งทำให้ $1 < e < phi(n)$ และ gcd (ห.ร.ม.) ของ phi(n) กับ e เท่ากับ 1 (อาจมีหลายค่าได้ เลือกมา 1 ค่า)
- คำนวณหาค่า d ที่ทำให้ $d \times e$ หารด้วย phi(n) แล้วเหลือเศษ 1
- Public Key คือ {e, n} และ Private Key คือ {d, n}
- ข้อความ M ที่ถูกเข้ารหัสเป็นข้อความ C ด้วย Public Key ดังนี้

  $C = (M^e) \bmod n$

- ข้อความ C จะถูกถอดรหัสเป็นข้อความ M ด้วย Private Key ดังนี้

  $M = (C^d) \bmod n$

จงเขียนโปรแกรมเพื่อจำลองการเข้ารหัสแบบ RSA จากวิธีการด้านบน โดยส่งไฟล์นามสกุล .py แยกตามข้อดังนี้

2.1 เลือกจำนวนเฉพาะ p และ q ที่ไม่เกิน 100 (เพื่อให้ง่ายต่อการจำลอง) แสดงค่า Public Key และ Private Key ออกทางหน้าจอ หลังจากนั้นให้เข้ารหัสรหัสนักศึกษาของตัวเอง และแสดงข้อความที่ถูกเข้ารหัสออกทางหน้าจอ และถอดรหัสออกทางหน้าจอ

**Deadline: 9 October 2023**