สารบัญ

บทนำ

นับเป็นเวลาเนิ่นนานหลายพันปีที่พระมหากษัตริย์ พระราชินี ตลอดจนขุนศึกทั้งหลาย ต้องพึ่งพาการสื่อสารอันทรงประสิทธิภาพเพื่อการปกครองประเทศและบังคับบัญชากองทัพ ในขณะเดียวกัน พวกเขาต่างก็ตระหนักถึงผลกระทบอันอาจเกิดขึ้นหากข้อความเหล่านั้นตกไปอยู่ในเงื้อมมือของฝ่ายตรงข้าม เพราะนั่นหมายถึงการเปิดเผยความลับล้ำค่าให้กับประเทศอริศัตรูคู่แข่ง หรืออาจเป็นการแพร่งพรายข่าวสารชี้เป็นชี้ตายให้กับกองกำลังอีกฝ่ายได้เลย ภัยคุกคามจากการจารกรรมข้อมูลโดยศัตรูนั้นก่อให้เกิดการพัฒนารหัสลับ ซึ่งก็คือเทคนิคในการอำพรางข้อความเพื่อผู้รับที่เราตั้งใจหมายส่งให้เท่านั้นจึงจะอ่านได้

ความจำเป็นในการรักษาความลับทำให้แต่ละประเทศต้องจัดตั้งหน่วยงานสร้างรหัสลับขึ้นมาทำหน้าที่รักษาความปลอดภัยของการสื่อสารโดยการคิดค้นและใช้รหัสลับที่ดีที่สุดเท่าที่มี ในเวลาเดียวกัน นักถอดรหัสฝ่ายศัตรูต่างพยายามแกะรหัสลับเหล่านี้เพื่อล้วงเอาข้อมูลสำคัญออกมาให้จงได้ นักถอดรหัสนั้นเปรียบเสมือนนักเล่นแร่แปรธาตุทางด้านภาษา พวกเขาคือกลุ่มคนลึกลับผู้พยายามเสกข้อความที่มนุษย์เข้าใจได้ขึ้นมา

จากสัญลักษณ์อันไร้ความหมาย ประวัติศาสตร์ของรหัสลับก็คือเรื่องราวการต่อสู้อันยาวนานหลายศตวรรษระหว่างนักสร้างรหัสและนักถอดรหัส การประลองสติปัญญาของทั้งสองฝ่ายส่งผลกระทบอย่างใหญ่หลวงตลอดเส้นทางของประวัติศาสตร์นี้

ในการเขียนหนังสือเล่มนี้นั้น ผมเองมีวัตถุประสงค์หลักอยู่สองประการ ประการแรกคือการนำเสนอให้เห็นถึงวิวัฒนาการของรหัสลับ คำว่าวิวัฒนาการนั้นเป็นคำศัพท์ที่เหมาะสมและให้ความหมายครบถ้วนเพราะการพัฒนารหัสลับต่างๆ ล้วนแล้วแต่เป็นการดิ้นรนต่อสู้ทางวิวัฒนาการดีๆ นั่นเอง เนื่องจากตัวรหัสลับนั้นพร้อมจะถูกนักถอดรหัสโจมตีอยู่ตลอดเวลา เมื่อไหร่ก็ตามที่นักถอดรหัสพัฒนาอาวุธใหม่ที่ช่วยเผยจุดอ่อนของรหัสลับรูปแบบหนึ่งได้แล้ว รหัสลับรูปแบบนั้นก็จะไม่มีประโยชน์อีกต่อไป รหัสลับรูปแบบนั้นหากไม่สูญพันธุ์ไปก็จะต้องมีวิวัฒนาการขึ้นมาเป็นรหัสลับชนิดใหม่ที่แข็งแกร่งกว่าเดิม และรหัสลับใหม่นี้ก็จะสามารถเจริญรุ่งเรืองต่อไปได้ตราบจนนักถอดรหัสหาจุดอ่อนของมันพบอีก เฉกเช่นนี้ไปเรื่อยๆ สถานการณ์ดังกล่าวเทียบเคียงได้กับเรื่องราวของสายพันธุ์แบคทีเรียก่อโรค เชื้อแบคทีเรียจะยังคงอยู่และเติบโตต่อไปได้จนกระทั่งคุณหมอค้นพบยาปฏิชีวนะที่เผยให้เห็นถึงจุดอ่อนของเชื้อเหล่านี้และจัดการล้างบางพวกมันทิ้งเสีย เหล่าแบคทีเรียที่จำต้องอยู่ สู้ เพื่อรอด จึงถูกบีบให้มีวิวัฒนาการเพื่อเอาชนะยาปฏิชีวนะ และหากพวกมันทำสำเร็จ มันก็จะเพิ่มจำนวนกลับมาสร้างชื่อได้อีกครั้ง แบคทีเรียนั้นถูกกดดันให้ต้องมีวิวัฒนาการอยู่ตลอดเวลาเพื่อที่พวกมันจะได้ไม่ถูกโจมตีโดยยาปฏิชีวนะชนิดใหม่ๆ

สงครามอันยืดเยื้อยาวนานระหว่างนักสร้างรหัสและนักถอดรหัสบันดาลให้เกิดการพัฒนาทางวิทยาศาสตร์อันยิ่งใหญ่ขึ้นมาเป็นจำนวนมาก นักสร้างรหัสนั้นต้องพยายามสร้างสรรค์รหัสลับที่แข็งแกร่งยิ่งขึ้นเรื่อยๆ เพื่อปกป้องการสื่อสารของพวกเขา ในขณะเดียวกัน นักถอดรหัสเองก็ต้องประดิษฐ์วิธีการอันทรงพลานุภาพเพื่อหาทางโจมตีรหัสลับให้ได้ ความพยายามของทั้งสองฝ่ายในการรักษาและทำลายความลับคือจุดกำเนิดของวิทยาการและเทคโนโลยีล้ำสมัยนานัปการ นับตั้งแต่คณิตศาสตร์ไปจนถึง

ภาษาศาสตร์ ตลอดจนทฤษฎีข้อมูลไปจนถึงทฤษฎีควอนตัม ทั้งสองฝ่ายช่วยให้วิทยาการเหล่านี้ก้าวหน้าไปอย่างรวดเร็ว งานของพวกเขาส่งผลให้เทคโนโลยีพัฒนาไปด้วยอัตราเร่ง ซึ่งเห็นได้ชัดเจนโดยเฉพาะอย่างยิ่งในกรณีของเครื่องคอมพิวเตอร์สมัยใหม่

ประวัติศาสตร์นั้นเต็มไปด้วยรหัสลับ บ่อยครั้งที่รหัสลับเป็นตัวตัดสินผลลัพธ์ของการศึกอันนำไปสู่จุดจบของราชาและราชินีจำนวนมาก ผมจะพยายามนำกลอุบายต่างๆ รวมไปถึงเรื่องราวของความเป็นความตายมาเล่าเพื่อที่เราจะได้เห็นภาพของจุดเปลี่ยนแห่งวิวัฒนาการของการพัฒนารหัสลับทั้งหลาย แต่ประวัติศาสตร์ของรหัสลับนั้นช่างมีมากมายจนผมจำเป็นต้องตัดเรื่องราวน่าสนใจหลายเรื่องทิ้งไป และนั่นหมายความว่าหนังสือของผมนั้นไม่ได้สมบูรณ์ที่สุด หากคุณต้องการอ่านเรื่องราวที่คุณสนใจหรือประวัติของนักถอดรหัสที่คุณชื่นชอบให้มากขึ้นแล้วละก็ ผมขอให้ไปดูในรายการแหล่งค้นคว้าเพิ่มเติมท้ายเล่ม ซึ่งน่าจะช่วยให้ท่านผู้อ่านสามารถศึกษาหัวข้อที่สนใจได้ละเอียดยิ่งขึ้น

นอกจากการพูดคุยถึงวิวัฒนาการของรหัสลับและผลกระทบต่อหน้าประวัติศาสตร์แล้ว วัตถุประสงค์ประการที่สองของหนังสือเล่มนี้ก็คือการแสดงให้เห็นว่าเรื่องราวเหล่านี้มีความสำคัญต่อชีวิตประจำวันของพวกเรามากยิ่งกว่ายุคไหนๆ เพราะนับวันข้อมูลสารสนเทศก็ยิ่งเป็นทรัพยากรอันมีค่ามากขึ้นเรื่อยๆ และจากการที่การปฏิวัติการสื่อสารได้เปลี่ยนโฉมหน้าสังคมของพวกเรา กระบวนการเข้ารหัสข้อความต่างๆ หรือที่เรียกว่าเอ็นคริปชั่น (encryption) ก็จะยิ่งมีบทบาทสำคัญต่อชีวิตประจำวันเพิ่มมากขึ้น ทุกวันนี้โทรศัพท์ของเรารับส่งสัญญาณจากดาวเทียมดวงต่างๆ และอีเมลของเราต้องเดินทางผ่านคอมพิวเตอร์หลากหลายเครื่องซึ่งกระบวนการสื่อสารทั้งสองประเภทนี้สามารถถูกสกัดกั้นได้โดยง่าย และนั่นถือว่าเป็นภัยต่อความเป็นส่วนตัวของพวกเรา เช่นเดียวกัน มีธุรกิจที่ดำเนินการบนอินเทอร์เน็ตเพิ่มขึ้นจำนวนมาก จึงจำเป็นต้องมีมาตรการป้องกันความปลอดภัยเพื่อปกป้องบริษัทต่างๆ รวมไปถึงลูกค้าของบริษัทเหล่านั้น กระบวนการเข้ารหัสเป็นหนทางเดียวที่จะปกป้องความเป็นส่วนตัว

ของพวกเราและรับประกันความสำเร็จของตลาดบนโลกดิจิทัล ศิลปะแห่งการสื่อสารลับหรือที่รู้จักกันในชื่อวิทยาการรหัสลับ (cryptography) นั้นจึงเปรียบเสมือนแม่กุญแจและลูกกุญแจแห่งยุคสารสนเทศดังเช่นทุกวันนี้

อย่างไรก็ตาม ความปรารถนาที่มีต่อกระบวนการสร้างรหัสลับของสังคมโดยรวมนั้นขัดกับความต้องการของหน่วยงานที่มีหน้าที่บังคับใช้กฎหมายและรักษาความมั่นคงของประเทศชาติ ตลอดหลายทศวรรษที่ผ่านมา เจ้าหน้าที่ตำรวจและหน่วยสืบราชการลับอาศัยวิธีการดักฟังเพื่อรวบรวมข้อมูลหลักฐานในการจัดการกับบรรดาผู้ก่อการร้ายและองค์กรอาชญากรรมต่างๆ แต่การพัฒนารหัสลับที่แข็งแกร่งมากในช่วงหลังๆ ทำให้การดักฟังนั้นทำได้ยากขึ้น เมื่อเราก้าวเข้าสู่ศตวรรษที่ 21 ฝ่ายที่สนับสนุนสิทธิเสรีภาพพลเมืองพยายามกดดันให้มีการใช้กระบวนการสร้างรหัสลับกันอย่างแพร่หลายเพื่อปกป้องความเป็นส่วนตัวของแต่ละบุคคล ฝ่ายนี้ยังได้รับการสนับสนุนจากธุรกิจต่างๆ ที่ต้องการสร้างรหัสลับอันแข็งแกร่งเพื่อรับประกันความปลอดภัยของธุรกรรมต่างๆ ในโลกของการค้าขายบนอินเทอร์เน็ตที่มีการเติบโตอย่างรวดเร็ว แต่ในเวลาเดียวกัน ฝ่ายกฎหมายและความมั่นคงก็พยายามกดดันและโน้มน้าวให้รัฐบาลจำกัดกระบวนการสร้างรหัสลับ คำถามก็คือ เราให้คุณค่ากับอะไรมากกว่ากัน ระหว่างความเป็นส่วนตัวหรือระบบตำรวจที่มีประสิทธิภาพ แล้วมันพอจะมีหนทางประนีประนอมบ้างหรือไม่

แม้ว่ากระบวนการสร้างรหัสลับจะมีบทบาทต่อกิจกรรมของพลเมืองเป็นอย่างมาก แต่กระบวนการสร้างรหัสลับทางการทหารนั้นก็มีความสำคัญอย่างยิ่งเช่นกัน มีผู้กล่าวว่าสงครามโลกครั้งที่หนึ่งเป็นสงครามของนักเคมีเพราะมีการใช้แก๊สมัสตาร์ดและคลอรีนเป็นครั้งแรก ส่วนสงครามโลกครั้งที่สองนั้นเป็นสงครามของนักฟิสิกส์เพราะมีการจุดระเบิดปรมาณูขึ้นมาด้วยหลักการนี้ สงครามโลกครั้งที่สามจึงน่าจะเป็นสงครามของนักคณิตศาสตร์เพราะนักคณิตศาสตร์จะเป็นผู้ควบคุมสุดยอดอาวุธชิ้นถัดไปด้วยการจัดการกับข้อมูลในสงคราม นักคณิตศาสตร์มีหน้าที่พัฒนารหัสลับที่เราใช้ป้องกันข้อมูลทางการทหารในปัจจุบัน จึงไม่ต้องประหลาดใจว่านักคณิตศาสตร์

ก็จะต้องมีบทบาทสำคัญในแนวหน้าของสงครามทำลายรหัสลับพวกนี้ด้วยเช่นกัน

ระหว่างที่บรรยายถึงวิวัฒนาการของรหัสลับและผลกระทบต่อประวัติศาสตร์อยู่นั้น ผมจะขอออกนอกเรื่องไปสักเล็กน้อย ในบทที่ 5 เราจะกล่าวถึงการถอดข้อความภาษาโบราณต่างๆ อันได้แก่ ลิเนียร์บีและอักษรเฮียโรกลิฟิกของอียิปต์ จริงๆ แล้วกระบวนการสร้างรหัสลับเป็นรูปแบบการสื่อสารที่พัฒนาขึ้นมาเพื่อปกป้องความลับจากศัตรู ทว่าตัวอักษรของอารยธรรมโบราณนั้นไม่ได้ถูกออกแบบมาเพื่อให้เราอ่านไม่รู้เรื่องตั้งแต่ต้น เราแค่สูญเสียวิธีที่จะอ่านมันไปตามกาลเวลาต่างหาก อย่างไรก็ตาม ทักษะที่จำเป็นต่อการค้นหาความหมายในเอกสารโบราณนั้นไม่ต่างอะไรกับศิลปะของการถอดรหัสลับเลย นับตั้งแต่ผมได้อ่านหนังสือเรื่อง *The Decipherment of Linear B* เป็นต้นมา การบรรยายของผู้เขียนอย่างจอห์น แชดวิก ถึงกระบวนการคลายปริศนาของข้อความเมดิเตอร์เรเนียนโบราณนั้นทำให้ผมประทับใจมิรู้ลืมกับผลงานอันน่าทึ่งของบรรดาทีมงานที่ช่วยกันถอดข้อความของบรรพบุรุษของพวกเรา จนทำให้เราเข้าใจอารยธรรมศาสนา ตลอดจนชีวิตประจำวันของพวกเขาเหล่านั้น

สำหรับคนที่ค่อนข้างพิถีพิถันในด้านภาษา ผมต้องขอโทษด้วยนะครับเพราะหนังสือเล่มนี้ที่ชื่อ *The Code Book* ไม่ได้กล่าวถึงเฉพาะโค้ดเท่านั้น คำว่า “โค้ด” หมายถึงวิธีการสื่อสารลับรูปแบบหนึ่งซึ่งเป็นที่นิยมน้อยลงเรื่อยๆ ในโค้ดนั้น คำศัพท์หรือข้อความจะถูกแทนที่ด้วยคำศัพท์ ตัวเลข หรือสัญลักษณ์อื่น ตัวอย่างเช่น สายลับมีโค้ดเนมเป็นของตัวเองซึ่งมีวัตถุประสงค์เพื่อปิดบังชื่อจริงหรืออำพรางตัวตนของพวกเขา เช่นเดียวกันข้อความ Attack at dawn (โจมตีตอนย่ำรุ่ง) นั้นอาจถูกแทนที่ด้วยโค้ด Jupiter (พฤหัส) โดยคำศัพท์นี้อาจถูกส่งไปให้กับผู้บัญชาการในสนามรบเพื่อเป็นการสร้างความสับสนให้กับศัตรู เมื่อผู้รับสารที่เรามุ่งหมายได้รับข้อความแล้วก็จะทราบความหมายของ Jupiter ในทันทีหากศูนย์บัญชาการและผู้บัญชาการรบเคยตกลงโค้ดนี้กันไว้ก่อน แต่ฝ่ายศัตรูที่ดักจับข้อความนี้จะไม่สามารถเข้าใจความหมายอะไรได้เลย วิธีการสื่อสารลับประเภทอื่น

นอกจากโค้ดแล้วยังมีรหัสไซเฟอร์ (cipher) ซึ่งเป็นเทคนิคที่พื้นฐานขึ้นไปอีก ในรหัสไซเฟอร์จะมีการแทนที่ตัวอักษรแต่ละตัวแทนที่จะแทนศัพท์ทั้งคำ ตัวอย่างเช่น เราอาจแทนที่ตัวอักษรแต่ละตัวในข้อความด้วยตัวอักษรตัวถัดไป ดังนั้น A จะถูกแทนที่ด้วย B, B แทนด้วย C เช่นนี้ไปเรื่อยๆ Attack at dawn จึงกลายเป็น Buubdl bu ebxo ไป ทุกวันนี้รหัสไซเฟอร์เป็นหัวใจสำคัญของวิทยาการรหัสลับ เพราะฉะนั้น หนังสือเล่มนี้จึงควรจะชื่อว่า *The Code and Cipher Book* แต่ผมขออนุญาตเลือกใช้ชื่อที่ติดหูมากกว่าความถูกต้องนะครับ

นอกจากนี้ ผมยังพยายามอธิบายถึงศัพท์เทคนิคต่างๆ ที่ใช้กันในวิทยาการรหัสลับตามความจำเป็น และถึงแม้ว่าผมจะพยายามใช้ศัพท์ต่างๆ ให้ถูกต้องตามนิยามเหล่านี้ก็ตาม แต่บางครั้งผมขอเลือกใช้ศัพท์ที่อาจไม่ถูกต้องทางเทคนิคทั้งหมดเสียทีเดียวแต่คนทั่วไปน่าจะคุ้นเคยมากกว่า ตัวอย่างเช่น ในการบรรยายถึงคนที่พยายามถอดรหัสไซเฟอร์ (cipher) ผมมักจะเรียกคนเหล่านี้ว่า *codebreaker* หรือ*นักถอดรหัส (โค้ด)* มากกว่าที่จะใช้ศัพท์ที่ถูกต้องแต่ไม่ติดหูอย่าง*นักถอดรหัสไซเฟอร์*หรือ *cipherbreaker* แต่ผมจะทำแบบนี้เฉพาะกรณีที่ความหมายของคำคำนั้นชัดเจนในบริบทดังกล่าวเท่านั้น ในช่วงท้ายของหนังสือเล่มนี้ยังมีอภิธานศัพท์ให้ด้วย แต่จริงๆ แล้วผมคิดว่าคำศัพท์ในวงการรหัสลับนั้นค่อนข้างตรงไปตรงมาอยู่นะครับ ตัวอย่างเช่น *ข้อความธรรมดา*หรือ *plaintext* นั้นหมายถึงข้อความก่อนเข้ารหัส และ*ข้อความรหัส (ไซเฟอร์)* หรือ *ciphertext* นั้นหมายถึงข้อความที่ผ่านการเข้ารหัสแล้ว

ก่อนที่จะจบบทนำ ผมคงต้องกล่าวถึงปัญหาสำคัญที่นักเขียนเกี่ยวกับวิทยาการรหัสลับทุกคนจะต้องเผชิญ นั่นก็คือ เรื่องราวของวิทยาการด้านความลับส่วนใหญ่ย่อมเป็นความลับ วีรบุรุษจำนวนมากในหนังสือเล่มนี้ไม่เคยได้รับการยกย่องผลงานตลอดช่วงชีวิตของพวกเขา เพราะเราไม่สามารถประกาศเรื่องราวดังกล่าวให้สาธารณชนรับทราบในระหว่างที่นวัตกรรมเหล่านั้นยังมีคุณค่าทางการทูตหรือทางการทหารอยู่ ในการค้นคว้าข้อมูลเพื่อเขียนหนังสือเล่มนี้ ผมมีโอกาสได้พูดคุยกับ

ผู้เชี่ยวชาญจากกองบัญชาการสื่อสารของรัฐบาลอังกฤษ (Government Communications Headquarters หรือ GCHQ) ซึ่งได้ให้รายละเอียดเกี่ยวกับงานวิจัยต่างๆ ในช่วงทศวรรษที่ 1970 ซึ่งเปิดเผยต่อสาธารณชนไปเมื่อไม่นานมานี้ และจากการเปิดเผยข้อมูลดังกล่าวทำให้นักวิทยาการรหัสลับผู้ยิ่งใหญ่ของโลกสามท่านเพิ่งได้รับการยกย่องให้สมเกียรติยศที่พวกเขาพึงได้รับมานานแล้ว อย่างไรก็ตาม การเปิดเผยดังกล่าวก็ช่วยเตือนให้ผมทราบว่าในวงการนี้ยังมีอะไรอีกมากมายซึ่งผมหรือนักเขียนหนังสือแนววิทยาศาสตร์คนอื่นๆ ไม่มีทางจะทราบได้ องค์กรอย่างเช่น GCHQ และสำนักงานความมั่นคงแห่งชาติของสหรัฐ (National Security Agency หรือ NSA) นั้นยังคงดำเนินการวิจัยลับในศาสตร์ของวิทยาการรหัสลับอย่างต่อเนื่อง นั่นหมายความว่าความก้าวหน้าในเรื่องนี้จะยังเป็นความลับและบรรดานักวิจัยในวงการนี้จะยังคงเป็นบุคคลนิรนามอยู่ต่อไป

และถึงแม้ว่าจะต้องเผชิญกับอุปสรรคจากความลับของรัฐบาลตลอดจนงานวิจัยลับทั้งหลาย ในบทสุดท้ายของหนังสือเล่มนี้ผมได้พยายามที่จะพยากรณ์อนาคตของรหัสลับ เราจะลองมาคาดการณ์กันว่าสุดท้ายแล้วใครจะเป็นผู้ชนะในสงครามการดิ้นรนทางวิวัฒนาการระหว่างนักสร้างรหัสกับนักถอดรหัส นักสร้างรหัสจะเป็นฝ่ายออกแบบรหัสลับอันแข็งแกร่งไร้เทียมทานและสามารถเก็บรักษาความลับขั้นสุดยอดเอาไว้ตลอดกาลได้หรือไม่ หรือจะเป็นนักถอดรหัสที่สามารถสร้างเครื่องมือที่ถอดรหัสลับประเภทใดๆ ได้ทั้งหมด อย่าลืมว่าเรามีสุดยอดอัจฉริยะจำนวนหนึ่งที่กำลังทำงานในห้องปฏิบัติการลับอยู่ และคนเหล่านี้ล้วนได้รับทุนวิจัยปริมาณมหาศาล แน่นอนว่าข้อความบางตอนในบทสุดท้ายของผมอาจมีข้อผิดพลาด ตัวอย่างเช่น ผมกล่าวว่า ควอนตัมคอมพิวเตอร์ซึ่งเป็นเครื่องมือที่สามารถถอดรหัสในยุคปัจจุบันได้ทั้งหมดยังคงอยู่ในระยะเริ่มต้นเท่านั้น แต่มันก็เป็นไปได้ว่าอาจมีใครสักคนประดิษฐ์ควอนตัมคอมพิวเตอร์ขึ้นมาได้แล้ว ทว่าคนที่จะออกมาบอกว่าผมพูดผิดพลาดตรงไหนบ้างนั้นล้วนแล้วแต่ไม่สามารถเปิดเผยตัวตนได้ทั้งสิ้น

บทที่ 1

รหัสลับของแมรี ราชินีแห่งสกอต

The Cipher of Mary Queen of Scots

เช้าวันเสาร์ที่ 15 ตุลาคม 1586 สมเด็จพระราชินีนาถแมรีเสด็จเข้าไปยังห้องพิจารณาคดีอันแน่นขนัดคลาคล่ำไปด้วยฝูงชนภายในปราสาทฟอเทอริงเกย์ แม้จะทรงถูกคุมขังมาโดยตลอดระยะเวลาหลายปี อีกทั้งยังประชวรพระโรครูมาติสซั่มรุมเร้า ถึงกระนั้นพระสิริโฉมอันงดงาม กอปรด้วยพระจริยวัตรอันสุขุมสมขัตติยนารียังคงเป็นที่ประจักษ์ต่อสายตา แพทย์ประจำพระองค์คอยประคองพระนางให้เสด็จผ่านผู้พิพากษา ขุนนาง ตลอดจนบรรดาผู้สังเกตการณ์ พระองค์เสด็จมุ่งตรงไปยังบัลลังก์ที่ตั้งอยู่กึ่งกลางห้องโถงแคบยาว ทรงมีพระราชดำริว่าพระแท่นบัลลังก์นี้เป็นเครื่องแสดงความเคารพต่อพระองค์ หากแต่พระนางทรงเข้าพระทัยผิด เพราะพระแท่นบัลลังก์ดังกล่าวเป็นสัญลักษณ์แทนพระองค์ในสมเด็จพระราชินีนาถเอลิซาเบธ ผู้เป็นศัตรูและโจทก์ของพระนางต่างหาก สมเด็จพระราชินีนาถแมรีทรงถูกเชิญให้เสด็จออกจากพระแท่นบัลลังก์ไปยังฝั่งตรงข้ามของห้อง ซึ่งมีเก้าอี้กำมะหยี่สีแดงสดอันเป็นที่ประทับของฝ่ายจำเลย

แมรี ราชินีแห่งสกอตทรงถูกดำเนินคดีในข้อหากบฏ พระนางทรงถูกกล่าวหาว่ามีส่วนร่วมในการวางแผนลอบปลงพระชนม์สมเด็จพระราชินีนาถเอลิซาเบธเพื่อแย่งชิงราชบัลลังก์อังกฤษ เซอร์ฟรานซิส วอลซิงแฮม ราชเลขานุการในสมเด็จพระราชินีนาถเอลิซาเบธได้ทำการจับกุมผู้สมรู้ร่วมคิดรายอื่น ทั้งยังทำการสอบเค้นจนได้คำสารภาพและสั่งประหารชีวิตไปเรียบร้อยแล้ว ตอนนี้เขาจะต้องพิสูจน์ให้ได้ว่าสมเด็จพระราชินีนาถแมรีทรงเป็นหัวใจสำคัญของแผนการนี้ จึงสมควรมีความผิดในระดับที่เท่าเทียมและควรต้องโทษประหารด้วยเช่นกัน

วอลซิงแฮมทราบดีว่าก่อนจะสำเร็จโทษสมเด็จพระราชินีนาถแมรีได้นั้น เขาจะต้องทำการพิสูจน์ให้สมเด็จพระราชินีนาถเอลิซาเบธทรงประจักษ์ถึงความผิดของสมเด็จพระราชินีนาถแมรีเสียก่อน แม้ว่าสมเด็จพระราชินีนาถเอลิซาเบธจะทรงรังเกียจเดียดฉันท์สมเด็จพระราชินีนาถแมรีมากเพียงใดก็ตาม แต่พระองค์ทรงมีหลายเหตุผลที่ยังไม่กล้าประกาศพระราชโองการให้มีการสำเร็จโทษสมเด็จพระราชินีนาถแมรีเสีย ข้อแรกคือ แมรีทรงเป็นราชินีแห่งสกอตแลนด์ คงเป็นที่กังขาของผู้คนจำนวนมากว่าศาลของอังกฤษมีสิทธิสั่งประหารประมุขของประเทศอื่นด้วยหรือ ข้อสอง การสำเร็จโทษสมเด็จพระราชินีนาถแมรีนั้นอาจเป็นการสร้างบรรทัดฐานอันแปลกประหลาดขึ้นมา เพราะถ้ารัฐหนึ่งๆ สามารถสั่งประหารพระราชินีได้แล้ว ในอนาคตกลุ่มกบฏก็คงไม่มีความลังเลที่จะสั่งประหารประมุข ซึ่งก็คือสมเด็จพระราชินีนาถเอลิซาเบธได้ด้วยเช่นกัน ข้อสาม สมเด็จพระราชินีนาถเอลิซาเบธและสมเด็จพระราชินีนาถแมรีนั้นทรงเป็นพระญาติกัน ความสัมพันธ์ทางสายพระโลหิตนั้นอาจทำให้สมเด็จพระราชินีนาถเอลิซาเบธต้องหนักพระทัยมิใช่น้อยหากจะต้องมีพระบรมราชโองการให้ประหารสมเด็จพระราชินีนาถแมรี โดยสรุปก็คือ สมเด็จพระราชินีนาถเอลิซาเบธคงจะต้องทรงคัดค้านการสั่งประหารอย่างแน่นอน หากวอลซิงแฮมไม่สามารถพิสูจน์ชัดจนสิ้นข้อสงสัยว่าสมเด็จพระราชินีนาถแมรีทรงมีส่วนร่วมในแผนลอบปลงพระชนม์จริง

กลุ่มผู้สมรู้ร่วมคิดนั้นประกอบด้วยเหล่าขุนนางหนุ่มของอังกฤษฝ่ายคาทอลิกที่หวังจะโค่นบัลลังก์เอลิซาเบธซึ่งเป็นโปรเตสแตนต์ แล้วตั้งแมรี

ซึ่งเป็นคาทอลิกด้วยกันขึ้นมาแทน ผลการพิจารณาคดีออกมาชัดเจนว่า กลุ่มผู้สมรู้ร่วมคิดยกย่องแมรีให้เป็นประธาน แต่มันยังไม่ชัดเจนว่าสมเด็จพระราชินีนาถแมรีเองนั้นแท้จริงแล้วทรงเป็นผู้สนับสนุนขบวนการดังกล่าวด้วยหรือไม่ ในความเป็นจริงก็คือสมเด็จพระราชินีนาถแมรีมีพระบรมราชานุญาตให้ดำเนินแผนดังกล่าว ดังนั้น ความท้าทายของวอลซิงแฮมจึงอยู่ที่ว่าเขาจะพิสูจน์สายสัมพันธ์ระหว่างพระนางและกลุ่มผู้ก่อการได้หรือไม่

เช้าของวันไต่สวนคดีนั้น แมรีในฉลองพระองค์กำมะหยี่สีดำทรงประทับอยู่อย่างเดียวดายภายในคอกจำเลย ในคดีกบฏนั้น จำเลยจะถูกห้ามไม่ให้ปรึกษาบุคคลอื่น ไม่ได้รับอนุญาตให้เรียกพยาน กระทั่งไม่ได้รับอนุญาตให้เลขานุการส่วนพระองค์ช่วยตระเตรียมเอกสารในคดีให้ด้วยซ้ำ ถึงกระนั้นสถานการณ์ของพระองค์ก็ไม่ได้สิ้นหวังเสียทีเดียว เพราะแมรีทรงมีความระมัดระวังในการติดต่อกับบรรดาผู้ร่วมอุดมการณ์ด้วยกันเป็นอย่างยิ่ง พระราชหัตถเลขาทุกฉบับจะถูกเข้ารหัสลับเสมอ และรหัสลับช่วยเปลี่ยนให้ข้อความของพระองค์กลายเป็นสัญลักษณ์ต่างๆ ที่ไร้ความหมาย แมรีทรงเชื่อว่าแม้วอลซิงแฮมจะดักเอาพระราชหัตถเลขาของพระองค์ไปได้ เขาก็คงไม่เข้าใจข้อความในนั้นอยู่ดี และถ้าเนื้อความนั้นเป็นปริศนา จดหมายดังกล่าวก็จะไม่สามารถใช้เป็นหลักฐานดำเนินคดีกับพระนาง แต่นั่นขึ้นอยู่กับว่ารหัสลับของพระนางจะต้องไม่ถูกฝ่ายตรงข้ามถอดรหัสออกมาได้

ภาพที่ 1 สมเด็จพระราชินีนาถแมรีแห่งสกอตแลนด์

ความโชคร้ายของแมรีก็คือ วอลซิงแฮมมิได้เป็นเพียงราชเลขานุการเท่านั้น หากแต่เขายังเป็นหัวหน้าสายลับของ

อังกฤษอีกด้วย เขาดักสกัดพระราชหัตถเลขาของแมรีที่ทรงมีถึงผู้ก่อการได้ และเขารู้ด้วยว่าใครจะสามารถถอดรหัสนี้ได้ โทมัส ฟีลิปส์ คือนักถอดรหัสที่เก่งที่สุดของประเทศ ตลอดหลายปีที่ผ่านมา เขาคือผู้ถอดรหัสข้อความในแผนการลอบปลงพระชนม์สมเด็จพระราชินีนาถเอลิซาเบธ และเพื่อให้มีหลักฐานหนักแน่นพอที่จะจัดการกับคนกลุ่มนี้ ถ้าเขาสามารถถอดรหัสในจดหมายซึ่งเป็นหลักฐานกล่าวโทษแมรีได้สำเร็จ แมรีคงไม่สามารถพ้นจากเงื้อมมือของพญามัจจุราชไปได้ ในขณะเดียวกัน หากรหัสลับของแมรีมีความแข็งแกร่งมากพอที่จะรักษาความลับของพระนางเอาไว้ได้ พระนางก็จะมีโอกาสรอดพระชนม์ชีพ นี่ไม่ใช่เหตุการณ์แรกในประวัติศาสตร์ที่ชะตาชีวิตของคนคนหนึ่งจะขึ้นอยู่กับความแข็งแกร่งของรหัสลับ

วิวัฒนาการของการรักษาความลับ

หลักฐานเกี่ยวกับการรักษาความลับที่เก่าแก่ที่สุดนั้นสามารถสืบสาวย้อนไปได้ถึงเฮโรโดตัส ผู้ที่ได้รับการยกย่องจากซิเซโร นักปรัชญาและรัฐบุรุษชาวโรมันว่าเป็น “บิดาแห่งประวัติศาสตร์” ในผลงานหนังสือของเขาเรื่อง *The Histories* เฮโรโดตัสได้เรียบเรียงเรื่องราวความขัดแย้งระหว่างกรีกและเปอร์เซียเมื่อ 500 ปีก่อนคริสต์ศักราช ในทัศนะของเฮโรโดตัสนั้น นี่คือการประจันหน้าระหว่างเสรีภาพและระบอบทาส ระหว่างรัฐกรีกซึ่งเป็นอิสระและเปอร์เซียผู้รุกราน เฮโรโดตัสระบุว่า ศาสตร์แห่งการรักษาความลับช่วยให้กรีกรอดพ้นจากการยึดครองโดยเซอร์ซีส ราชาแห่งราชันย์ทั้งปวงผู้ทรงไว้ซึ่งอาชญาสิทธิ์แห่งเปอร์เซีย

ความบาดหมางอันยาวนานระหว่างกรีกและเปอร์เซียพุ่งสู่ระดับสูงสุดภายหลังจากที่เซอร์ซีสทรงสถาปนากรุงเปอร์เซโปลิสเป็นราชธานีแห่งใหม่ประจำอาณาจักรของพระองค์ ในการนี้ เครื่องบรรณาการล้ำค่าหลั่งไหลมาจากทั่วทุกสารทิศทั้งจากดินแดนในจักรวรรดิตลอดจนรัฐข้างเคียง ขาดก็แต่เพียงเอเธนส์และสปาร์ตา นั่นจึงทำให้เซอร์ซีสตัดสินพระทัยส่งกองกำลัง

ไปปราบปราม พร้อมกับทรงมีประกาศิตว่า “ข้าจักขยายอาณาเขตของจักรวรรดิเปอร์เซียออกไปจนสุดขอบฟ้าของพระผู้เป็นเจ้า เพื่อที่ดวงตะวันจะไม่มีทางสิ้นแสงในดินแดนของพวกเรา” พระองค์ทรงใช้ระยะเวลาราวห้าปีเพื่อตระเตรียมกองกำลังอันเข้มแข็งเกรียงไกรที่สุดในประวัติศาสตร์อย่างลับๆ และเมื่อ 480 ปีก่อนคริสต์ศักราช ก็ทรงพร้อมแล้วที่จะทำการบุกโจมตีอย่างไม่คาดฝัน

ทว่าข่าวการรวบรวมกำลังพลของเปอร์เซียนั้นไม่อาจรอดพ้นสายตาของเดมาราตัส ชาวกรีกผู้ถูกเนรเทศจากแผ่นดินเกิดมาอาศัยอยู่ ณ เมืองซูซาในจักรวรรดิเปอร์เซีย ถึงแม้ตัวจะถูกเนรเทศ แต่ใจยังคงจงรักภักดีต่อแผ่นดินเกิดมิเสื่อมคลาย เดมาราตัสตัดสินใจส่งข้อความเตือนชาวสปาร์ตาถึงแผนการบุกโจมตีของเซอร์ซีส ความท้าทายอยู่ที่ว่าเขาจะต้องส่งข้อความอย่างไรไม่ให้ถูกทหารเปอร์เซียดักสกัด เฮโรโดตัสได้บรรยายไว้ว่า

> อันตรายจากการถูกตรวจพบนั้นหนักหนาสาหัสยิ่ง มีแค่เพียงหนทางเดียวเท่านั้นที่เขาอาจส่งข้อความออกไปได้ นั่นคือก่อนอื่นจักต้องขูดขี้ผึ้งออกจากกระดานเขียนข้อความ แล้วเขียนบรรยายแผนการของเซอร์ซีสลงบนนั้น จากนั้นจึงใช้ขี้ผึ้งพอกทับลงไปบนข้อความอีกครั้ง ด้วยวิธีนี้จะทำให้กระดานขี้ผึ้งนั้นดูว่างเปล่า จึงอาจรอดพ้นจากสายตาทหารเปอร์เซียที่คอยตรวจตราความเรียบร้อยระหว่างเส้นทางไปได้ เมื่อข้อความไปถึงยังปลายทางแล้ว เท่าที่ข้ารู้มาก็ยังไม่มีผู้ใดทราบความลับในทันที ต้องรอจนกระทั่งกอร์โก พระธิดาของเคลโอเมเนส ผู้เป็นมเหสีของเลโอนิดาสทอดพระเนตรเห็นนิมิต และรับสั่งว่าหากมีคนขูดเอาขี้ผึ้งออก ก็จักพบข้อความบางอย่างซ่อนอยู่ข้างใต้ ซึ่งเมื่อดำเนินการแล้ว ก็ได้พบข้อความดังกล่าวจริงๆ ข้อความทั้งหมดจึงถูกอ่าน และส่งต่อไปยังชาวกรีกคนอื่นๆ ต่อไป

ด้วยคำเตือนดังกล่าวทำให้ชาวกรีกผู้ไร้ซึ่งการเตรียมตัวรับมือข้าศึกอยู่แต่เดิมนั้นต้องหันมาเตรียมความพร้อม ผลกำไรจากเหมืองเงินของรัฐที่เมื่อก่อนจะนำมาแบ่งปันกันในระหว่างบรรดาพลเมือง ก็ถูกนำมาใช้เป็นทุนรอนสำหรับการต่อเรือรบจำนวนสองร้อยลำเพื่อเสริมความแข็งแกร่งให้กับกองทัพเรือ

เพราะเหตุนี้ เซอร์ซีสจึงทรงสูญเสียความได้เปรียบจากการโจมตีโดยไม่ทันตั้งตัวไป และในวันที่ 23 กันยายน 480 ปีก่อนคริสต์ศักราช เมื่อกองทัพเปอร์เซียเดินทางมาถึงอ่าวซาลามิส ใกล้กับนครรัฐเอเธนส์ ชาวกรีกก็เตรียมความพร้อมเสร็จสมบูรณ์ เซอร์ซีสทรงเชื่อว่ากองกำลังของพระองค์ได้ล้อมกองทัพเรือของกรีกเอาไว้แล้ว แต่ที่จริงคือทางกรีกจงใจล่อให้เรือของเปอร์เซียเข้ามาในอ่าว ชาวกรีกทราบดีว่าเรือของพวกเขาที่ลำเล็กกว่าและมีจำนวนน้อยกว่ามากนั้นย่อมต้องถูกบดขยี้ในทะเลเปิดโดยกองทัพเปอร์เซียที่มีจำนวนมากมายมหาศาลอย่างแน่นอน ทว่าในอ่าวแคบๆ นั้น พวกเขาอาจพลิกเกมกลับมาชนะเปอร์เซียได้ เมื่อลมเปลี่ยนทิศ กองทัพเปอร์เซียจึงพบว่าพวกตนถูกลวงเข้ามาในอ่าวและโดนกองกำลังของกรีกปิดล้อมไว้ อาร์เทมิเซีย เจ้าหญิงแห่งเปอร์เซียทรงพบว่าเรือของพระนางถูกล้อมไว้ถึงสามด้าน จึงทรงพยายามหันหัวเรือออกไปยังทะเลกว้าง แต่กลับพาให้เรือของพระองค์ไปชนกับเรือพวกเดียวกันเองเสียอย่างนั้น การนี้ทำให้พวกเปอร์เซียปั่นป่วน เรือของเปอร์เซียพุ่งชนกันเอง และกองทัพกรีกเข้าโจมตีอย่างดุเดือด ภายในระยะเวลาเพียงวันเดียว กองทัพเปอร์เซียอันเกรียงไกรกลับต้องถูกสยบลงอย่างราบคาบ

กลยุทธ์ในการรักษาความลับของเดมาราตัสอาศัยการซ่อนเร้นข้อความเป็นสำคัญ เฮโรโดตัสยังบรรยายถึงการส่งข้อความโดยอาศัยแต่เพียงการซ่อนความลับอีกเหตุการณ์หนึ่ง ซึ่งก็คือเรื่องราวของฮิสไตเอียสผู้ที่ต้องการให้อริสตาโกรัสแห่งเมืองมิเลตุสลงมือปฏิวัติกษัตริย์เปอร์เซีย โดยวิธีการที่ฮิสไตเอียสใช้คือ เขาทำการโกนผมของผู้นำสารออกทั้งหมด จากนั้นจึงสักข้อความลงบนหนังศีรษะ แล้วรอให้ผมงอกกลับขึ้นมาใหม่ (ช่วงเวลาในประวัติศาสตร์ยุคนั้นช่างไม่ต้องเร่งรีบเอาเสียเลย) ต่อจากนั้น

ผู้นำสารซึ่งไม่ได้พกสิ่งของต้องสงสัยอื่นๆ ติดตัวไปด้วยจึงสามารถเดินทางถึงจุดหมายได้อย่างปลอดภัย เมื่อเขาไปถึงปลายทางก็จะทำการโกนผมอีกครั้งเพื่อให้ผู้รับสารมองเห็นข้อความบนหนังศีรษะ

วิธีการรักษาความลับด้วยการซ่อนข้อความไม่ให้เห็นนั้นเรียกว่า *การอำพรางข้อมูล (steganography)* ซึ่งมีรากศัพท์มาจากภาษากรีก *steganos* ที่หมายความว่า **"ปิดบัง"** และ *graphein* ที่หมายความว่า **"เขียน"** ตลอดระยะเวลาสองพันปีนับตั้งแต่เฮโรโดตัสเป็นต้นมา โลกของเรามีวิธีการอำพรางข้อมูลหลากหลายรูปแบบ ตัวอย่างเช่น ชาวจีนโบราณเขียนข้อความลงบนผ้าไหมขนาดเล็ก จากนั้นจึงม้วนให้เป็นก้อนเล็กๆ แล้วเคลือบด้วยขี้ผึ้ง เพื่อให้ผู้นำสารกลืนก้อนขี้ผึ้งนั้นลงไป ในศตวรรษที่ 16 นักวิทยาศาสตร์ชาวอิตาลีชื่อโจวานนี ปอร์ตา บรรยายวิธีการซ่อนข้อความไว้ในไข่ต้มโดยใช้หมึกชนิดพิเศษที่ทำจากสารส้มหนึ่งออนซ์และน้ำส้มสายชูหนึ่งไพนต์ เมื่อใช้หมึกดังกล่าวเขียนข้อความลงบนเปลือกไข่ น้ำหมึกจะซึมทะลุรูพรุนที่อยู่บนเปลือกไข่ ทิ้งข้อความไว้บนผิวนอกของไข่ขาว ซึ่งเราสามารถอ่านข้อความดังกล่าวได้โดยการปอกเปลือกไข่ต้มออก ศาสตร์แห่งการอำพรางข้อมูลยังอาศัยการเขียนด้วยหมึกล่องหน ซึ่งได้มีการบรรยายเอาไว้อย่างน้อยก็ตั้งแต่ศตวรรษที่ 1 แล้ว โดยไพลนีผู้อาวุโสกล่าวว่าเราสามารถใช้ **"น้ำนม"** ของต้นสลัดไดในการทำหมึกล่องหนได้ ถ้าเราปล่อยให้หมึกแห้งแล้วจะมองไม่เห็น แต่เมื่อเรานำไปอังกับความร้อน ข้อความที่เขียนด้วยหมึกดังกล่าวจะเปลี่ยนเป็นสีน้ำตาล ของเหลวที่เป็นสารอินทรีย์หลายชนิดมีคุณสมบัติแบบเดียวกัน เนื่องจากมีองค์ประกอบหลักเป็นคาร์บอนจึงสามารถกลายเป็นถ่านได้ง่าย สายลับในยุคปัจจุบันล้วนทราบกันดีว่าหากไม่มีหมึกล่องหนให้ใช้แล้ว ก็อาจลองด้นสดด้วยการนำปัสสาวะของตัวเองมาทำเป็นหมึกล่องหนไปพลางก่อนได้

การที่การอำพรางข้อมูลสามารถอยู่ยั้งยืนยงมาได้อย่างยาวนานแสดงว่ามันช่วยตอบโจทย์เรื่องการรักษาความปลอดภัยได้ดีพอสมควร แต่ว่าวิธีการนี้มีจุดอ่อนสำคัญอยู่ประการหนึ่ง นั่นก็คือ ถ้าผู้นำสารถูกตรวจค้นโดยละเอียดและข้อความดังกล่าวถูกค้นพบ ความลับทั้งหมดจะ

ถูกเปิดเผยออกมาทันที การดักสกัดเอาข้อความมาได้นี้อาจทำให้ความมั่นคงต้องพังทลายลงไปในทันใด เจ้าหน้าที่รักษาการณ์ที่ละเอียดรอบคอบอาจทำการตรวจสอบผู้ที่เดินทางข้ามพรมแดนทุกคนอย่างละเอียด โดยขูดขี้ผึ้งออกจากแผ่นกระดานทั้งหมด ลองนำกระดาษเปล่าไปอังกับไฟปอกเปลือกไข่ต้ม โกนผมของทุกคน ฯลฯ ซึ่งแน่นอนว่าจะต้องมีบางครั้งที่ข้อความลับถูกตรวจพบ

ดังนั้น นอกจากจะมีการพัฒนาในศาสตร์ของการอำพรางข้อมูลแล้ว ยังต้องมีการพัฒนาศาสตร์ของ*การสร้างรหัสลับ*หรือ *cryptography* ควบคู่กันไปด้วย คำศัพท์ดังกล่าวมีรากศัพท์มาจากภาษากรีก *kryptos* ที่หมายความว่า “ซ่อน” วัตถุประสงค์ของการสร้างรหัสลับนั้นไม่ได้อยู่ที่การซ่อนข้อความไม่ให้หาพบ หากแต่อยู่ที่การซ่อนความหมายของข้อความนั้นโดยอาศัยกระบวนการที่เรียกว่า*การเข้ารหัส*หรือ *encryption* ซึ่งจะเปลี่ยนข้อความให้ดูไร้ความหมายด้วยการแปลงตัวอักษรผ่านกระบวนการเฉพาะที่ผู้ส่งและผู้รับได้ตกลงกันไว้ล่วงหน้า เมื่อผู้รับได้รับสารแล้วจึงสามารถย้อนกลับกระบวนการนั้นเพื่อที่จะอ่านข้อความได้รู้เรื่อง ประโยชน์ของการใช้รหัสลับคือถึงแม้ว่าฝ่ายศัตรูจะดักสกัดเอาข้อความที่ผ่านการเข้ารหัสไปได้ก็ไม่ได้แปลว่าจะเข้าใจความหมายในข้อความนั้น การที่ฝ่ายตรงข้ามไม่รู้ว่าข้อความผ่านการเข้ารหัสด้วยกระบวนการใด ทำให้พวกเขาต้องเผชิญกับความยากลำบากในการถอดเอาเนื้อหาดั้งเดิมก่อนการเข้ารหัสออกมา ซึ่งอาจเป็นไปไม่ได้เลยที่จะถอดรหัสลับดังกล่าวได้สำเร็จ

แม้ว่าการสร้างรหัสลับและการอำพรางข้อมูลจะเป็นคนละแนวทางที่ไม่เกี่ยวข้องกัน แต่เราสามารถใช้ทั้งการแปลงข้อความร่วมกับการซ่อนข้อความไปพร้อมกันเพื่อความปลอดภัยสูงสุดได้ ตัวอย่างเช่น ไมโครดอทเป็นวิธีการอำพรางข้อมูลที่นิยมใช้ในช่วงสงครามโลกครั้งที่สอง สายลับเยอรมันในลาตินอเมริกาจะทำการย่อภาพถ่ายของทั้งหน้าเอกสารลงจนกลายเป็นจุดขนาดจิ๋วที่มีเส้นผ่านศูนย์กลางน้อยกว่า 1 มิลลิเมตร จากนั้นจึงทำการซ่อนจุดดังกล่าวไว้แทนเครื่องหมายมหัพภาค (จุด full stop) ในจดหมายที่ดูไม่ได้มีพิษภัยอะไร เอฟบีไอตรวจพบไมโครดอทอันแรก

เมื่อปี 1941 ภายหลังได้รับคำแนะนำว่าหน่วยงานของอเมริกาควรพยายามมองหาแสงสะท้อนเล็กๆ จากพื้นผิวของจดหมาย ซึ่งแสดงว่ามีการใช้ฟิล์มบางๆ บริเวณนั้น นับแต่นั้นเป็นต้นมา หน่วยงานของอเมริกาก็สามารถอ่านข้อความส่วนใหญ่จากไมโครดอทที่ดักสกัดไว้ได้ เว้นแต่ว่าสายลับเยอรมันนั้นจะใช้ความระมัดระวังเพิ่มขึ้นไปอีกขั้นด้วยการแปลงข้อความเสียก่อนที่จะทำการย่อส่วน ในกรณีที่มีการใช้รหัสลับร่วมกับการอำพรางข้อมูล หน่วยงานของอเมริกาอาจจะดักเอาข้อความหรือสกัดกั้นการสื่อสารได้ก็จริง แต่พวกเขาจะไม่ได้ข้อมูลเกี่ยวกับกิจกรรมของสายลับเยอรมันเพิ่มเติมเลย ถ้าจะให้เปรียบเทียบแนวทางการรักษาความลับทั้งสองแขนงแล้ว การสร้างรหัสลับนับว่าเป็นวิธีการที่ปลอดภัยกว่าเพราะมันสามารถป้องกันข้อมูลสำคัญไม่ให้ตกไปอยู่ในมือของศัตรูได้

การสร้างรหัสลับนั้นยังสามารถแบ่งออกเป็นสองแขนง ได้แก่ *การสลับอักษร (transposition)* และ*การแทนที่อักษร (substitution)* ในการสลับอักษรนั้น ตัวอักษรในข้อความจะถูกจัดเรียงตำแหน่งใหม่ ทำให้เกิดเป็นคำใหม่ที่เรียกว่าอะนาแกรม (anagram) ขึ้นมา สำหรับข้อความสั้นๆ เช่น คำศัพท์คำเดียวนั้น วิธีการนี้จะไม่ค่อยปลอดภัยเพราะการสลับตัวอักษรทำได้แค่เพียงไม่กี่รูปแบบ ตัวอย่างเช่น คำศัพท์ที่ประกอบด้วยตัวอักษรสามตัวจะสามารถสลับอักษรออกมาได้เพียงหกรูปแบบเท่านั้น ดูอย่างคำว่า cow, cwo, ocw, owc, wco, woc แต่ถ้าข้อความยาวขึ้น จำนวนรูปแบบการสลับอักษรจะยิ่งเพิ่มขึ้นเป็นทวีคูณ ทำให้เราไม่สามารถคาดเดาข้อความต้นฉบับได้หากไม่รู้กระบวนการสลับอักษรที่ใช้ ดูอย่างประโยคว่า For example, consider this short sentence (ตัวอย่างเช่น ลองดูประโยคสั้นๆ แค่นี้) ข้อความนี้มีเพียง 35 ตัวอักษร แต่มันมีวิธีการสลับอักษรได้มากกว่า 50,000,000,000,000,000,000,000,000,000,000,000 รูปแบบ ซึ่งถ้าคนหนึ่งคนลองตรวจสอบข้อความที่สลับตัวอักษรแต่ละรูปแบบด้วยความเร็วหนึ่งข้อความต่อหนึ่งวินาที ต่อให้คนทั้งโลกร่วมมือกันตรวจสอบข้อความสลับอักษรทั้งวันทั้งคืนโดยไม่หยุดหย่อน ก็ยังต้องใช้เวลามากกว่าอายุของเอกภพถึงหนึ่งพันเท่าเพื่อที่จะตรวจสอบรูปแบบการสลับอักษรได้ทั้งหมด

การสลับอักษรแบบสุ่มนั้นดูเหมือนจะเป็นวิธีการที่มีความปลอดภัยสูง เพราะมันแทบเป็นไปไม่ได้เลยที่ศัตรูผู้ดักสกัดเอาข้อความมาได้นั้นจะถอดข้อความดั้งเดิมกลับมาได้ ถึงแม้จะเป็นเพียงประโยคสั้นๆ ก็ตาม แต่วิธีดังกล่าวก็มีข้อด้อยอยู่อย่างหนึ่งเช่นกัน เพราะถ้าหากการสลับอักษรนั้นสร้างอะนาแกรมที่ยากมากๆ ขึ้นมา โดยที่แต่ละตัวอักษรเรียงกันมั่วไปหมด ไม่มีความคล้องจองกันหรือดูไม่สมเหตุสมผลเลยแม้แต่น้อย การถอดข้อความย้อนกลับก็จะเป็นเรื่องที่ยากมากสำหรับผู้รับสารด้วยเช่นกัน ไม่ต่างอะไรกับศัตรู การสลับอักษรที่มีประสิทธิภาพนั้นจึงต้องเป็นไปตามระบบซึ่งผู้ส่งและผู้รับสารได้ตกลงกันไว้อย่างชัดเจนมาก่อนแล้ว และต้องปกปิดกระบวนการดังกล่าวจากศัตรู ตัวอย่างเช่น เด็กนักเรียนนิยมส่งข้อความหากันด้วยการสลับอักษรแบบ “สลับฟันปลา” ซึ่งข้อความที่ได้ถูกเขียนขึ้นโดยสลับตัวอักษรไปมาระหว่างแถวบนและแถวล่าง แล้วจึงนำตัวอักษรที่ผ่านการสลับแล้วในแถวล่างมาเรียงต่อจากตัวอักษรแถวบนอีกทีหนึ่ง กลายเป็นข้อความเข้ารหัสขั้นสุดท้าย ดังตัวอย่างต่อไปนี้

THY SECRET IS THY PRISONER; IF THOU LET IT GO, THOU ART A PRISONER TO IT

(ความลับของเจ้าคือนักโทษของเจ้า หากเจ้าปล่อยมันไป เจ้าย่อมกลายเป็นนักโทษของมัน)

↓

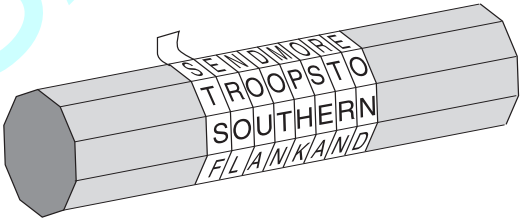
T H Y S E C R E T I S T H Y P R I S O N E R I F T H O U L E T I T G O T H O U A R T A P R I S O N E R T O I T

↓

TYERTSHPIOEITOLTTOHURARSNROTHSCEITYRSNRFHUEIGTOATPIOETI

ผู้รับสารสามารถถอดข้อความได้โดยการย้อนกระบวนการดังกล่าว ทั้งนี้วิธีการสลับอักษรอย่างเป็นระบบนั้นมีหลายรูปแบบ เช่น สลับฟันปลาสามแถว โดยข้อความจะถูกเขียนด้วยสามแถวแทนที่จะเป็นสองแถวตามแบบเดิม นอกจากนี้ เรายังอาจสลับตัวอักษรแต่ละคู่ โดยตัวอักษรตัวแรกจะสลับตำแหน่งกับตัวอักษรตัวที่สอง ตัวอักษรตัวที่สามสลับตำแหน่งกับตัวอักษรตัวที่สี่ เช่นนี้ไปเรื่อยๆ

การสลับอักษรอีกรูปแบบหนึ่งที่พบในเครื่องมือเข้ารหัสทางการทหารชิ้นแรกของโลกคือ *ไซเทล (scytale)* ของชาวสปาร์ตา ซึ่งมีใช้กันมาตั้งแต่ 500 ปีก่อนคริสต์ศักราช ไซเทลนั้นเป็นท่อนไม้สำหรับให้เอาสายหนังหรือกระดาษหนังมาพัน ดังตัวอย่างในภาพที่ 2 ผู้ส่งสารจะเขียนข้อความตามความยาวของไซเทล แล้วจึงแกะเอาสายหนังออกซึ่งตอนนี้กลายเป็นตัวอักษรที่อ่านไม่รู้เรื่องแล้ว เพราะตำแหน่งของตัวอักษรในข้อความอยู่สลับที่กันมั่วไปหมด ผู้นำสารจะพกสายหนังติดตัวไว้ โดยอาจใช้วิธีอำพรางข้อความเพิ่มเติม ตัวอย่างวิธีที่นิยมกันคือการใช้สายหนังดังกล่าวแทนเข็มขัดโดยซ่อนฝั่งที่มีตัวอักษรเอาไว้ด้านใน สำหรับวิธีการถอดข้อความออกมานั้น ผู้รับสารจะต้องนำสายหนังที่ได้มาพันรอบไซเทลซึ่งมีขนาดเส้นผ่านศูนย์กลางเท่ากันกับอันที่ผู้ส่งสารใช้ เมื่อ 404 ปีก่อนคริสต์ศักราช แม่ทัพไลแซนเดอร์แห่งสปาร์ตาพบกับผู้นำสารคนหนึ่งซึ่งถูกทรมานจนเลือดท่วมทั้งตัว ผู้นำสารคนดังกล่าวเป็นผู้รอดชีวิตเพียงหนึ่งเดียวจากคณะที่มีห้าคน ซึ่งเดินทางมาจากเปอร์เซียอย่างลำบากยากเข็ญ ผู้นำสารยื่นเข็มขัดของเขาให้กับไลแซนเดอร์ เมื่อไลแซนเดอร์ได้รับเข็มขัดมาแล้วจึงนำไปพันรอบไซเทลของเขา ทำให้ทราบว่าฟาร์นาบาซัสแห่งเปอร์เซียกำลังวางแผนที่จะบุกโจมตีสปาร์ตา ข้อมูลดังกล่าวช่วยให้ไลแซนเดอร์เตรียมพร้อมรับมือจากการโจมตีและสามารถขับไล่พวกเปอร์เซียไปได้ในที่สุด



ภาพที่ 2 เมื่อแกะแผ่นหนังออกจากไซเทล (ท่อนไม้) ของผู้ส่งสารแล้ว ตัวอักษรที่ได้จะดูเหมือนเรียงกันมั่วๆ S, T, S, F,... ทำให้อ่านไม่รู้เรื่อง ผู้รับสารจะต้องพันสายหนังเข้ากับไซเทลที่มีขนาดเส้นผ่านศูนย์กลางเท่ากันเท่านั้น ข้อความจึงจะปรากฏขึ้นมา (SEND MORE TROOPS TO SOUTHERN FLANK AND... [ส่งกองกำลังเพิ่มเติมมายังแนวรบด้านใต้และ...])

การสร้างรหัสลับอีกแขนงหนึ่งนั้นก็คือการแทนที่อักษร หลักฐานที่เก่าแก่ที่สุดของการเข้ารหัสด้วยการแทนที่อักษรปรากฏอยู่ในคัมภีร์กามสูตร ซึ่งเป็นคัมภีร์ที่เขียนขึ้นในศตวรรษที่ 4 โดยพราหมณ์ชื่อว่าวาตฺสฺยายน โดยอ้างอิงจากคัมภีร์โบราณที่ย้อนกลับไปได้ราว 400 ปีก่อนคริสต์ศักราช คัมภีร์กามสูตรแนะนำให้สตรีทั้งหลายพึงศึกษาศิลปวิทยาการ 64 แขนง เช่น การทำอาหาร การแต่งกาย การนวด ตลอดจนการทำน้ำหอม นอกจากนี้ยังกล่าวถึงศิลปะที่คนทั่วไปอาจนึกไม่ถึง เช่น มนตร์คาถา หมากรุก การทำหนังสือ ตลอดจนงานไม้ ศิลปะในลำดับที่ 45 คือ*มเลจฺฉิตวิกลฺปา*หรือ*ศิลปะแห่งการเขียนอักษรลับ* ซึ่งสอนให้สตรีปกปิดรายละเอียดของชู้รัก หนึ่งในวิธีการที่แนะนำคือ ให้ทำการจับคู่ตัวอักษรโดยการสุ่ม แล้วจึงแทนที่ตัวอักษรในข้อความดั้งเดิมด้วยคู่ของตัวอักษรนั้นๆ หากเราลองนำเทคนิคดังกล่าวมาใช้กับตัวอักษรโรมัน เราอาจสร้างคู่ตัวอักษรขึ้นมาได้ดังนี้

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

ดังนั้น เมื่อจะส่งข้อความว่า meet at midnight (พบกันตอนเที่ยงคืน) ผู้ส่งจึงเขียนว่า CUUZ VZ CGXSGIBZ แทน รูปแบบการเขียนข้อความลับแบบนี้เรียกว่า*รหัสไซเฟอร์แทนที่อักษร* (substitution cipher) เนื่องจากตัวอักษรแต่ละตัวในข้อความดั้งเดิมถูกแทนที่ด้วยตัวอักษรที่แตกต่างออกไป วิธีดังกล่าวจึงแตกต่างจากรหัสไซเฟอร์สลับอักษร (transposition cipher) ในกระบวนการสลับอักษรนั้น อักษรแต่ละตัวยังคงเป็นตัวเดิมเพียงแต่อยู่ในตำแหน่งที่เปลี่ยนไป ในขณะที่กระบวนการแทนที่อักษรนั้น ตัวอักษรแต่ละตัวจะเปลี่ยนรูปไปแต่ยังอยู่ในตำแหน่งเดิม

การใช้รหัสไซเฟอร์แทนที่อักษรทางการทหารเป็นครั้งแรกนั้นปรากฏหลักฐานในสงครามระหว่างจูเลียส ซีซาร์ กับชนเผ่ากอล (Gallic Wars) ซีซาร์ได้บรรยายถึงวิธีการที่เขาใช้ในการส่งข้อความหาซิเซโร ซึ่งกำลัง

ถูกปิดล้อมอยู่และจวนเจียนที่จะต้องยอมแพ้อยู่รอมร่อ โดยซีซาร์แทนที่ตัวอักษรโรมันทั้งหมดด้วยตัวอักษรกรีก ทำให้ศัตรูไม่สามารถเข้าใจเนื้อหาของข้อความ นอกจากนั้น ซีซาร์ยังได้บรรยายถึงวิธีการส่งข้อความอันน่าตื่นตาตื่นใจไว้ดังนี้

> ซีซาร์กำชับกับผู้นำสารว่า ถ้าหากเขาไม่สามารถเข้าไปใกล้กับค่ายทหารได้ ให้เขวี้ยงหอกที่พันจดหมายไว้ด้วยสายหนังเข้าไปยังบริเวณสนามเพลาะของค่ายทหาร ผู้นำสารชาวกอลเกรงกลัวอันตราย จึงปาหอกทิ้งไว้ตามคำสั่ง แต่บังเอิญว่าหอกนั้นไปโดนหอคอยแล้วติดอยู่อย่างนั้นถึงสองวันโดยไม่มีใครเห็น จนเข้าวันที่สาม มีทหารนายหนึ่งมาพบ จึงนำหอกนี้ลงมาและมอบให้กับซิเซโร เมื่อซิเซโรอ่านข้อความแล้วจึงนำมาประกาศให้ทั้งกองทัพได้รับทราบในระหว่างการสวนสนาม นำความยินดีมาให้กับทุกคน

ซีซาร์ใช้รหัสลับบ่อยมาก ถึงขนาดที่วาเลเรียส โปรบัส สามารถเขียนตำราว่าด้วยรหัสลับของซีซาร์ขึ้นมาได้เลย เป็นที่น่าเสียดายว่าเนื้อหาดังกล่าวได้สูญหายไปตามกาลเวลา แต่ยังโชคดีที่เรามีบันทึกของซูเอโตนิอุสเรื่อง *The Lives of the Twelve Caesars* ซึ่งเขียนขึ้นในศตวรรษที่ 2 โดยในตอนที่ 56 มีรายละเอียดของการแทนที่อักษรวิธีหนึ่งที่จูเลียส ซีซาร์ นิยมใช้ ซีซาร์แทนที่ตัวอักษรแต่ละตัวในข้อความด้วยตัวอักษรที่อยู่ในสามลำดับถัดไป นักถอดรหัสเรียกตัวอักษรที่ใช้ในข้อความธรรมดาหรือข้อความดั้งเดิมก่อนเข้ารหัสว่า *ตัวอักษรธรรมดา (plain alphabet)* และเรียกตัวอักษรที่ใช้แทนที่ตัวอักษรธรรมดาว่า *ตัวอักษรรหัส (cipher alphabet)* เมื่อเรานำตัวอักษรมาเรียงเป็นแถว โดยให้ตัวอักษรธรรมดาอยู่แถวบนและตัวอักษรรหัสอยู่แถวล่างดังภาพที่ 3 เราจะเห็นชัดเจนว่าตัวอักษรรหัสนั้นเลื่อนจากตำแหน่งของตัวอักษรธรรมดาไปสามตำแหน่ง ดังนั้น รูปแบบการแทนที่อักษรประเภทนี้จึงได้ชื่อว่า *รหัสเลื่อนของซีซาร์ (Caesar shift cipher)* เรียกสั้นๆ ว่า *รหัสซีซาร์หรือซีซาร์ไซเฟอร์*

(Caesar cipher) โดยคำว่าไซเฟอร์นั้นหมายถึงการแทนที่ตัวอักษรแต่ละตัวด้วยตัวอักษรหรือสัญลักษณ์อื่น

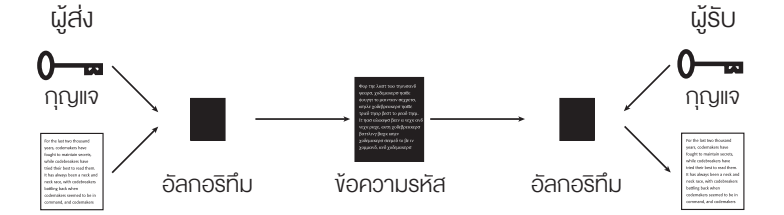
แม้ว่าซูเอโตนิอุสจะพูดถึงแต่การที่ซีซาร์เลื่อนตัวอักษรไปสามตำแหน่ง แต่ในชีวิตจริง เราอาจเลื่อนตัวอักษรไปกี่ตำแหน่งก็ได้ตั้งแต่ 1-25 ตำแหน่ง ดังนั้น เราจึงสร้างรหัสไซเฟอร์ได้มากถึง 25 รูปแบบ ยิ่งไปกว่านั้น ถ้าเราไม่จำกัดอยู่เฉพาะการเลื่อนตัวอักษรแต่เพียงอย่างเดียว โดยแทนที่ตัวอักษรธรรมดาด้วยตัวอักษรอะไรก็ได้แล้วละก็ เราจะสามารถสร้างรหัสไซเฟอร์ที่แตกต่างกันได้มากกว่า 400,000,000,000,000,000,000,000,000 รูปแบบเลยทีเดียว

ตัวอักษรธรรมดา	**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**
ตัวอักษรรหัส	**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**
ข้อความธรรมดา	**v e n i, v i d i, v i c i** (ข้ามา ข้าเห็น ข้าพิชิต)*
ข้อความรหัส	**Y H Q L, Y L G L, Y L F L**

ภาพที่ 3 ตัวอย่างของรหัสซีซาร์เมื่อใช้กับข้อความสั้นๆ รหัสซีซาร์นั้นอาศัยตัวอักษรรหัสซึ่งเลื่อนจากลำดับของตัวอักษรธรรมดาไปด้วยตำแหน่งที่แน่นอน (ในกรณีนี้คือสามตำแหน่ง) ตามปกติแล้วในวงการวิทยาการรหัสลับ เรานิยมเขียนตัวอักษรธรรมดาด้วยตัวพิมพ์เล็ก และเขียนตัวอักษรรหัสด้วยตัวพิมพ์ใหญ่ เช่นเดียวกัน ในข้อความธรรมดาหรือข้อความดั้งเดิมนั้น เราจะใช้ตัวพิมพ์เล็ก ส่วนข้อความเข้ารหัสหรือข้อความไซเฟอร์นั้นจะเขียนด้วยตัวพิมพ์ใหญ่

เราอาจพิจารณารหัสไซเฟอร์แต่ละรูปแบบผ่านกระบวนการเข้ารหัสโดยทั่วไป อันประกอบด้วย *อัลกอริทึม (algorithm)* และ*กุญแจ (key)* ในกรณีนี้อัลกอริทึมคือกระบวนการแทนที่ตัวอักษรธรรมดาแต่ละตัวด้วยตัวอักษรรหัส โดยตัวอักษรรหัสนั้นมาจากการจัดเรียงตัวอักษรธรรมดาอย่างไรก็ได้ กุญแจจะเป็นตัวบอกเราว่าตัวอักษรรหัสอะไรใช้แทนตัวอักษรธรรมดาตัวไหน ความสัมพันธ์ระหว่างอัลกอริทึมและกุญแจสามารถแสดงให้เห็นได้ดังภาพที่ 4

* veni, vidi, vici (ข้ามา ข้าเห็น ข้าพิชิต) เป็นคำพูดที่มีชื่อเสียงของจูเลียส ซีซาร์



ภาพที่ 4 ในการเข้ารหัสข้อความธรรมดา ผู้ส่งจะนำข้อความนั้นไปผ่านอัลกอริทึม อัลกอริทึมคือระบบทั่วไปที่ใช้ในการเข้ารหัส โดยต้องอาศัยรายละเอียดที่ชัดเจนจากกุญแจ เมื่อเราใช้ทั้งกุญแจและอัลกอริทึมพร้อมกันก็จะเป็นการเข้ารหัส เพื่อเปลี่ยนข้อความธรรมดาให้กลายเป็นข้อความรหัสหรือข้อความไซเฟอร์ ศัตรูอาจดักสกัดเอาข้อความรหัสของผู้ส่งไปได้ แต่ศัตรูจะไม่สามารถถอดรหัสข้อความนั้นได้ ส่วนผู้รับซึ่งทราบทั้งกุญแจและอัลกอริทึมที่ผู้ส่งใช้จะสามารถเปลี่ยนข้อความรหัสกลับไปเป็นข้อความธรรมดาได้

เมื่อฝ่ายศัตรูทำการวิเคราะห์ข้อความที่ดักสกัดมาได้แต่อ่านไม่รู้เรื่อง พวกเขาอาจสงสัยว่าข้อความดังกล่าวคงต้องผ่านอัลกอริทึมอะไรมาสักอย่าง แต่พวกเขาย่อมไม่ทราบกุญแจที่ถูกต้อง ตัวอย่างเช่น พวกเขาอาจสงสัยว่าตัวอักษรแต่ละตัวในข้อความธรรมดาน่าจะถูกแทนที่ด้วยตัวอักษรรหัสรูปแบบใดรูปแบบหนึ่ง แต่พวกเขาไม่น่าจะรู้ว่าตัวอักษรรหัสตัวไหนใช้แทนอะไร ถ้าทั้งผู้ส่งและผู้รับเก็บรักษากุญแจไว้เป็นความลับ ฝ่ายศัตรูก็คงไม่สามารถถอดรหัสข้อความที่ดักสกัดเอาไว้ได้ กุญแจนั้นคือสิ่งสำคัญที่ทำให้ศาสตร์ของการเข้ารหัสอยู่ยั้งยืนยงมาได้ ไม่ใช่อัลกอริทึม โดยเรื่องราวดังกล่าวได้ถูกเขียนไว้อย่างชัดเจนโดยเอากุสต์ เคิร์กฮอฟส์ ฟอน นิวเวนฮอฟ นักภาษาศาสตร์ชาวดัตช์ ในหนังสือของเขาเรื่อง *La Cryptographie militaire* เมื่อปี 1883 ดังนี้ “หลักการของเคิร์กฮอฟส์ก็คือ ความปลอดภัยของระบบรหัสนั้นหาได้อยู่ที่การรักษาความลับของอัลกอริทึมเข้ารหัสไม่ หากแต่อยู่ที่การเก็บรักษากุญแจให้เป็นความลับ”

นอกจากการรักษาความลับของกุญแจแล้ว ระบบรหัสลับที่ปลอดภัยจะต้องมีความเป็นไปได้ของกุญแจจำนวนมากอีกด้วย ตัวอย่างเช่น ถ้าผู้ส่งใช้รหัสเลื่อนของซีซาร์ในการเข้ารหัสข้อความ รหัสลับที่ได้จะค่อนข้างอ่อนแอ

เพราะมันมีกุญแจที่เป็นไปได้แค่เพียง 25 รูปแบบเท่านั้น ในมุมมองของศัตรูแล้ว หากพวกเขาดักสกัดข้อความเอาไว้ได้แล้วสงสัยว่าอัลกอริทึมที่ใช้คือรหัสเลื่อนของซีซาร์ สิ่งที่พวกเขาต้องทำก็คือตรวจสอบความเป็นไปได้เพียง 25 รูปแบบ แต่ถ้าผู้ส่งเลือกใช้อัลกอริทึมแทนที่อักษรที่กว้างกว่านั้น โดยใช้ตัวอักษรรหัสแทนตัวอักษรธรรมดาตัวใดก็ได้ แบบนี้จะมีกุญแจที่เป็นไปได้มากกว่า 400,000,000,000,000,000,000,000,000 รูปแบบให้ตรวจสอบ ดังตัวอย่างในภาพที่ 5 ซึ่งในมุมมองของศัตรูแล้ว ถึงจะดักสกัดเอาข้อความมาได้และรู้ว่าอีกฝ่ายใช้อัลกอริทึมอะไร มันก็ยังเป็นงานช้างที่จะต้องมาตรวจสอบความเป็นไปได้ของกุญแจทั้งหมดอยู่ดี ถ้าสายลับของศัตรูใช้เวลาหนึ่งวินาทีในการตรวจสอบแต่ละกุญแจ การที่จะตรวจสอบกุญแจทั้งหมด 400,000,000,000,000,000,000,000,000 รูปแบบเพียงเพื่อที่จะถอดรหัสข้อความนี้ให้ได้นั้นต้องใช้เวลาประมาณหนึ่งพันล้านเท่าของอายุเอกภพเลยทีเดียว

ตัวอักษรธรรมดา	**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**
ตัวอักษรรหัส	**J L P A W I Q B C T R Z Y D S K E G F X H U O N V M**
ข้อความธรรมดา	**e t t u, b r u t e ?** (เจ้าด้วยหรือ บรูตัส?)*
ข้อความรหัส	**W X X H, L G H X W ?**

ภาพที่ 5 ตัวอย่างของอัลกอริทึมแทนที่อักษรทั่วไป โดยอักษรธรรมดาแต่ละตัวในข้อความธรรมดาจะถูกแทนที่ด้วยตัวอักษรอื่นตามที่ปรากฏในกุญแจ กุญแจนั้นถูกกำหนดโดยตัวอักษรรหัส ซึ่งในที่นี้ตัวอักษรรหัสแต่ละตัวอาจใช้แทนตัวอักษรธรรมดาตัวใดก็ได้

ความสวยงามของรหัสไซเฟอร์ประเภทนี้อยู่ที่ความง่ายในการใช้งาน โดยที่ยังสามารถรักษาความปลอดภัยได้ในระดับสูง ผู้ส่งข้อความสามารถกำหนดกุญแจขึ้นมาได้อย่างง่ายดาย ซึ่งกุญแจก็คือลำดับของตัวอักษร

* et tu, brute? (เจ้าด้วยหรือ บรูตัส?) เป็นคำพูดสุดท้ายก่อนที่จูเลียส ซีซาร์ จะถูกสังหารตามบทประพันธ์ของวิลเลียม เชกสเปียร์

ทั้ง 26 ตัวในตัวอักษรรหัส โดยที่ศัตรูนั้นไม่สามารถไล่ตรวจสอบกุญแจทุกรูปแบบจนหมดได้ ความยากง่ายของกุญแจนั้นสำคัญมาก เพราะทั้งผู้ส่งและผู้รับจะต้องรู้กุญแจดังกล่าว ยิ่งกุญแจนั้นง่ายเท่าไหร่ โอกาสเกิดความผิดพลาดก็จะยิ่งลดลงไปเท่านั้น

ในการจะสร้างกุญแจที่ง่ายนั้น ผู้ส่งอาจจะต้องยอมลดทอนความเป็นไปได้ของรูปแบบกุญแจทั้งหมดลงไปบ้าง แทนที่จะสุ่มลำดับของตัวอักษรรหัสที่ใช้แทนที่ตัวอักษรธรรมดาทั้งหมด ผู้ส่งอาจกำหนดให้มี*คำกุญแจ (keyword)* หรือ*ข้อความกุญแจ (keyphrase)* ก็ได้ ตัวอย่างเช่น ถ้าเราจะใช้ JULIUS CAESAR เป็นข้อความกุญแจ ก่อนอื่นให้เราลบวรรคตอนและตัวอักษรที่ซ้ำกันออก (จะได้เป็น JULISCAER) แล้วกำหนดให้มันเป็นจุดเริ่มต้นของตัวอักษรรหัสที่เราจะใช้ ส่วนตัวอักษรรหัสอื่นๆ นั้นก็คือตัวอักษรที่เหลือเรียงตามลำดับปกติของมัน โดยเริ่มต้นตั้งแต่ตอนท้ายของข้อความกุญแจ ดังนั้นตัวอักษรรหัสของเราตามตัวอย่างจะมีหน้าตาเช่นนี้

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

ข้อดีของการสร้างตัวอักษรรหัสด้วยวิธีนี้ก็คือมันง่ายต่อการจดจำคำกุญแจหรือข้อความกุญแจ ทำให้เราทราบลำดับของตัวอักษรรหัสได้ไม่ยาก ซึ่งถือเป็นสิ่งที่สำคัญมาก เพราะถ้าผู้ส่งต้องจดตัวอักษรรหัสลงบนกระดาษแล้วศัตรูสามารถยึดกระดาษนั้นเอาไว้ได้ กุญแจก็จะถูกเปิดเผย ศัตรูจึงสามารถอ่านข้อความที่เราสื่อสารกันผ่านการเข้ารหัสได้ทันที แต่ถ้าหากเราสามารถจำกุญแจไว้ในหัวได้แล้ว โอกาสที่กุญแจจะตกไปอยู่ในมือของศัตรูก็จะลดลงไปมาก แน่นอนว่าจำนวนรูปแบบของตัวอักษรรหัสที่สร้างขึ้นจากคำกุญแจนั้นน้อยกว่าจำนวนรูปแบบของตัวอักษรรหัสที่สร้างขึ้นจากการสุ่มโดยไร้ข้อจำกัด แต่ถึงกระนั้นจำนวนของรูปแบบก็ยังมากมายมหาศาลอยู่ดี และมันก็แทบเป็นไปไม่ได้เลยที่ศัตรูจะพยายามถอดรหัสด้วยการตรวจสอบข้อความกุญแจที่เป็นไปได้ทั้งหมด