ภาคที่ 85 เครื่องเข้ารหัสลับ Enigma

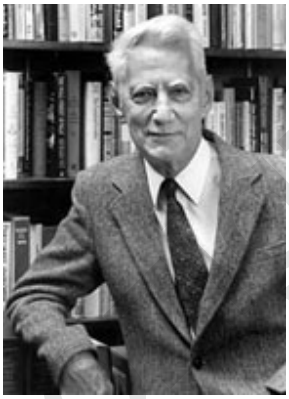
อีนิกมา

เป็นเครื่องเข้ารหัสข้อมูลที่เยอรมันใช้ใน ช่วงสงครามโลกครั้งที่สอง

เยอรมันสื่อสารข้อมูลทาง**วิทยุ**เป็นหลัก เพื่อความสะดวกรวดเร็ว **ข้อมูล**ที่ส่งทาง**วิทยุ**นั้นเป็นสื่อสาธารณะที่ใครๆก็ได้ยินได้ **เยอรมัน**จึงจำเป็นจะต้องแปลงข้อมูลเหล่านั้นด้วย**อีนิกมา**ให้อยู่ในรูปที่อ่าน ไม่รู้เรื่องก่อน

อีนิกมาเป็นรหัสลึกลับน่าสนเท่ห์อย่างชื่อ และเป็นเครื่องมือที่เยอรมันมั่นใจอย่างเหลือเกินว่าจะไม่มีใครทำลายได้สำเร็จ การที่อังกฤษสามารถถอดรหัสอินิกมาได้ ถือเป็นจุดเปลี่ยนของโฉมหน้าของสงครามเลยทีเดียว

อีนิกมาปรากฏโฉม ครั้งแรกในปี 1918 โดยเป็นสินค้าชิ้นหนึ่งของบริษัทรักษาความปลอดภัยที่วางขายในท้องตลาด ผู้คิดค้น**อีนิกมา**คือ **Arthur Scherbius** ซึ่งได้ออกแบบให้**อีนิกมา**ใช้งานง่าย มีหน้าตาคล้ายเครื่องพิมพ์ดีดที่มีแป้นตัวอักษรให้กด



Arthur Scherbius

เวลากดตัว**อักษร** เช่น **Q ตัวอักษร**จะผ่านการแปลงรูปเป็นตัวอื่นเช่น **U** เป็นต้น ในเครื่องมี**แผงไฟ**ที่แสดงตัว**อักษร**ที่ถูกแปลงแล้ว (ในที่นี้คือ U) ที่จะ**สว่างวาบ**ขึ้น **ผู้ใช้เครื่อง**นี้จะต้อง**จดตัว U** เพื่อเอาไปใช้ส่ง**ข้อมูล**ต่อไป ดังนั้น **HELLO** อาจกลายเป็น **BXCYR** เป็นต้น

สังเกต ว่าตัว **L** สองตัวนั้นแปลงได้ต่างกันไปในการกดแต่ละครั้ง (ใน**แป้นพิมพ์**นั้นไม่มี**ตัวเลข** การส่ง**ตัวเลข**จึงต้องใช้การสะกดเอา เช่น **3321** เป็น **DREI DREI ZWO EINS**)

อีนิกมาไม่ประสบความสำเร็จในการขาย แต่**กองทัพเยอรมัน**ให้ความสนใจ และตั้งแต่ปี 1923 **อีนิกมา**ก็ไม่มีวางขายอีกต่อไป แต่กลายเป็นเครื่องมือใช้ในหน่วย**ทหาร**แทน

ข้อ ดีของอีนิกมาคือใช้งานง่าย **เข้าใจง่าย** ผู้ใช้ไม่จำเป็นต้องรู้ว่าข้างในเครื่อง**อีนิกมา** ทำงานอย่างไร ก็รู้ว่าพิมพ์อะไรเข้าไป ก็จะออกมาเป็นอีกอย่างให้เราเอาไปใช้ได้ คนใช้**อีนิกมา** ไม่ต้องผ่านการ**ฝึกฝน**อะไรมาก เพียงอ่าน**หนังสือ**ออกและเรียนรู้การปรับค่าเริ่มต้นของ**ล้อ**หมุน (ที่ทำง่ายๆ ด้วยมือ) ก็ใช้ได้แล้ว

ส่วนใหญ่ภารกิจที่ **Enigma** มีส่วนร่วมมากคือ ภารกิจของเรือดำน้ำ **U-boat** ซึ่งทำให้เรือดำน้ำ **U-boat** จมเรือฝ่ายสัมพันธมิตรได้มากมาย จึงทำให้ฝ่ายสัมพันธมิตรต้องเร่งทำการแกะ**รหัส**ของเครื่อง **Enigma** นี้ให้ได้ แต่ก็ไม่ใช่เรื่องง่ายนัก เพราะ นาย **Arthur Scherbius** ได้อ้างว่าถ้านำคน **1000 คน**มาทำการสุ่มถอด**รหัส** โดยใช้อัตรา 4 ทางเลือก ต่อ 1นาที ต้องใช้เวลาถึง **900 ล้านปี** ในการจะถอด**รหัส**ได้ เป็นการเพิ่มความมั่นใจแก่**กองทัพ**นาซี**เยอรมัน**เป็นอย่างมาก

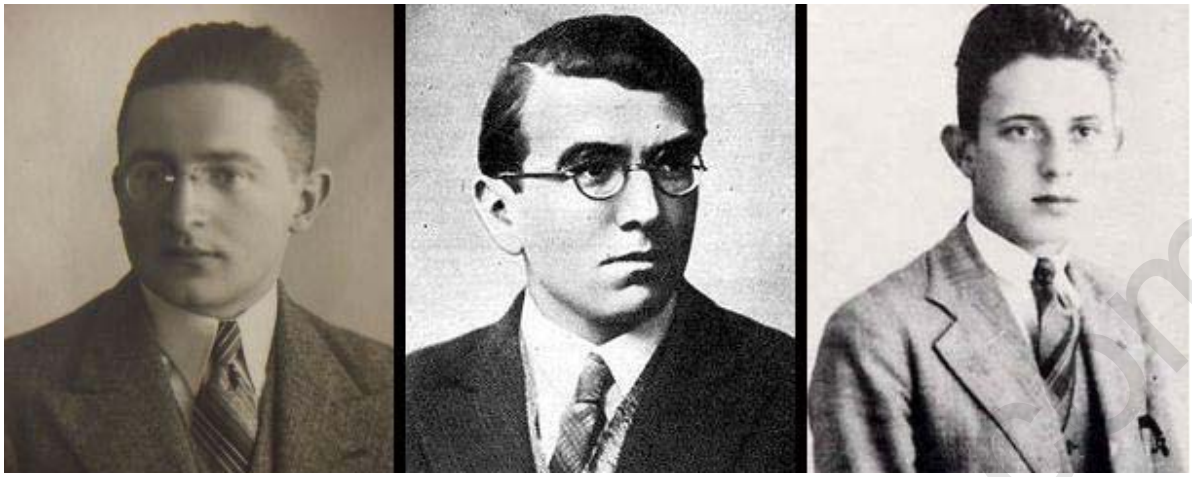
อีกทั้งเครื่องเข้า**รหัส**และถอด**รหัส**ในตัวเดียวกัน**อีนิกมา**มีขนาดเล็ก **พกพา**ไปไหน**สะดวก** จึงสะดวกกับการใช้งานทาง**ทหาร**อย่างยิ่งนอกจาก นั้นหน่วย**ทหาร**แต่ละกองยังสามารถตั้ง**รหัส**ให้เข้าใจได้แต่ในพวกเดียวกัน(เช่น เฉพาะ**กองทัพ**เรือ เฉพาะ**กองทัพ**อากาศ)ซึ่งทำได้ด้วยการตั้งค่าลูก**ล้อ**ให้ต่างกันไปตอนที่สงครามโลกครั้งที่สองเริ่มระอุนั้น**กองทัพเยอรมัน**ก็ใช้งาน**อีนิกมา**อย่างกว้างขวางแล้วตลอดช่วงสงครามโลกครั้งที่สอง **เยอรมัน**ได้พัฒนา**อีนิกมา**อยู่เสมอเช่นเพิ่ม**ล้อ**หมุนจาก 3 เป็น 5 และทำให้**ล้อ**หมุนนี้วิ่งไปลำดับใดก็ได้คือจะตั้งค่าให้ **ล้อ**ไหนจะเป็น **ล้อ**ชั่วโมง **ล้อ**นาที ก็ได้

ซึ่งทำให้การถอด**รหัส**ยากขึ้นไปอีก ไม่เพียงเท่านั้น**เยอรมัน**จะเลือกใช้**ล้อ**หมุนเพียงสามตัวจากห้าตัวที่มีอยู่การ จะแกะ**รหัส**ด้วยการเดาจึงต้องเดาทั้งลูก**ล้อ**ไหนที่จะใช้ และใช้ในลำดับใดด้วยคุณสมบัติเหล่านี้ **เยอรมัน**จึงเชื่อมั่นว่าไม่มีใครจะแกะ**รหัสอีนิกมา**ออกได้เลย มีการเริ่มต้นศึกษาเครื่องอินิกมา ในปี ค.ศ. 1930 ก่อนที่**เยอรมัน**จะบุก**โปแลนด์** ในปี ค.ศ. 1939 โดยหน่วยราชการลับของ**โปแลนด์** โดยการรวบรวมข้อมูล รูปภาพและสร้างเครื่องจำลองอินิกมา (Enigma Replica)ได้สำเร็จ แต่การถอด**รหัส**ก็ยังไม่ใช่เรื่องง่าย ทีมงานถอด**รหัส**ของ**โปแลนด์**ประกอบไปด้วยนักคณิตศาสตร์ นักถอด**รหัส** ในปี ค.ศ. 1939ที่**เยอรมัน**บุก**โปแลนด์**ทำให้ ผลงานการวิจัยศึกษาอินิกมา ถูกส่งต่อไปยังฝ่ายพันธมิตรคือฝรั่งเศสและสหราชอาณาจักร แต่การบุกของ**เยอรมัน**ได้รุกคืบมายังฝรั่งเศสอย่างรวดเร็วฝรั่งเศสยังไม่ได้พัฒนาต่อ ทีม**โปแลนด์**ที่พยายามแกะ**อีนิกมา**ประกอบด้วย Marian Rejewski, Jerzy Rozycki และ Henryk Zygalski ทีมนี้มีที่มาตั้งแต่ต้นปี **1929** เมื่ออาจารย์ Krygowski แห่งภาคคณิตศาสตร์ มหาวิทยาลัย Poznan ได้รวบรวมรายชื่อนักเรียนปีสามและสี่ที่รู้ภาษา**เยอรมัน** และมีผลการเรียนในเกณฑ์ดี มาร่วมเรียนวิชา Cryptology (การเข้า**รหัส**และถอด**รหัส**ข้อมูล) ในโครงการลับที่มี**ทหาร**มาร่วมด้วย นักเรียนราวยี่สิบคนที่ได้รับเลือกจะต้อง**ปฏิญาณ**ตนว่า จะเก็บเรื่องนี้เป็น **ความลับ** สาเหตุที่**มหาวิทยาลัย**นี้ได้รับเลือกเป็นที่ตั้ง**ทีม** ก็เพราะ**นักเรียน** ส่วนใหญ่มาจาก**ดินแดน**ที่เคยถูกครอบครองโดย**เยอรมัน**มาก่อน และผ่านการเรียนใน**โรงเรียน**ที่สอนเป็นภาษา**เยอรมัน** ในวิชา Cryptology นั้น **อาจารย์**นำโค้ดยากๆ มาลองให้**นักเรียน**แก้เล่น และสอนความรู้ไปด้วยพร้อมกัน**นักเรียน**จำนวนมากต้องยก**เลิกกลางคัน** บ้างเพราะตามไม่ทัน บ้างเพราะรู้สึกไม่ถนัดทางศาสตร์นี้ และ**สามคนที่เหลือรอดอยู่**ก็ได้กลายมาเป็นทีม**อีนิกมา**นั่นเอง ในตอนนั้น Rejewski อายุ 27 ปี Rozycki อายุ 23 และ Zygalski อายุ 25 ปี

ในปี 1926 **โปแลนด์** ที่จับตาดู**เยอรมัน**อยู่ พบว่าตัวเองแกะข้อความที่**เยอรมัน**ใช้สื่อสารไม่ได้อีกต่อไป จึงรู้ว่า**เยอรมัน** ได้ใช้วิธีการเข้า**รหัส**ข้อมูลแบบใหม่แล้ว สปาย**โปแลนด์**สืบพบเกี่ยวกับ**อีนิกมา** อีกทั้งได้ครอบครอง เครื่อง**อีนิกมา**ที่เคยวางขายตามท้องตลาดด้วย Rejewski หนึ่งในผู้แกะโค้ด**อีนิกมา**เขียนในบทความของเขาฉบับหนึ่ง (Wiadomosci matematyczne 23) ว่าในราวปี 1927 ศุลกากรวอร์ซอได้รับ**พัสดุ**จาก**เยอรมัน** ระบุว่าเป็นอุปกรณ์วิทยุ แต่บริษัทจัดส่งยื่นคำขาดอย่างเอาเป็นเอาตายให้คืน**พัสดุ**นี้กลับ**เยอรมัน**ก่อนจะถูกเปิดตรวจ โดยบอกว่า**พัสดุ**นี้จัดส่งพลาด

อาการร้อนรนนี้ทำให้ศุลกากร**โปแลนด์**เอะใจและส่งพัสดุนี้ไปให้หน่วยแกะ**รหัส** ข้อมูล ซึ่งเป็นผู้ดูแลอุปกรณ์วิทยุอยู่ในตอนนั้น **โปแลนด์**พบว่าสิ่งที่อยู่ในกล่องคือ**อีนิกมา** เหตุการณ์นั้นเกิดขึ้นในเที่ยงวันเสาร์ และ**โปแลนด์**ก็มีเวลาทั้งสุดสัปดาห์ทำความรู้จักกับ**อีนิกมา** ก่อนจะบรรจุลงกล่องแล้วจัดส่งคืน**เยอรมัน**อย่างเรียบร้อยแต่ถึง **โปแลนด์**จะมี**อีนิกมา**รุ่นที่เคยวางขาย แต่การแกะ**รหัส**ก็ยังเป็นไปไม่ได้เพราะ**กองทัพเยอรมัน**ได้ดัดแปลง**อีนิกมา**ที่ใช้ใน**ทหาร**ให้ต่างจากรุ่นที่วางขายในท้องตลาด

โปแลนด์อาจจะทำอะไรไม่ได้ไปมากกว่านี้ ถ้า**เยอรมัน**จะไม่มีหนอนบ่อนไส้ Hans Thilo-Schmidt (* ชื่อจริงนี้ปรากฏต่างๆ กันไป ข้อมูลที่ทราบแน่ชัดประการเดียวคือเขาเป็นที่รู้จักกันทั่วไปในนามแฝง Asche) เป็นชาว**เยอรมัน**ที่มาเสนอขายข้อมูล**อีนิกมา**ให้ฝรั่งเศส บางข้อมูลบอกว่าเขาเกิดตกอับ และได้ไปของานทำจากพี่ชายที่เป็นนาย**ทหาร**มียศในศูนย์ข้อมูลของ**เยอรมัน** งานที่ได้รับมอบหมายคือการ**ทำลาย**โค้ด**อีนิกมา**ที่ไม่ใช้แล้ว ฮานส์มีข้อมูลทั้งข้อความก่อนเข้า**รหัส**และข้อความที่เข้า**รหัส**แล้ว ซึ่งเขานำไปขายให้หน่วยสปาย**ฝรั่งเศส** แถมด้วยการเขียน**คู่มือ**อธิบายการติดตั้งใช้งาน**เครื่อง**ให้พร้อมสรรพ แต่ฮานส์ก็ไม่ได้บอกว่า**อีนิกมา**มีวงจรการทำงานภายในอย่างไร นายฮานส์นั้นทำงานได้ดีมาก จนกระทั่ง**ฝรั่งเศส**เชิญให้ไป**ปารีส**ครั้งหนึ่งในปี 1938 เพื่อให้**รางวัล**เป็นการ**ท่องราตรี** ในฐานะที่ **ปฏิบัติหน้าที่และจงรักภักดีเป็นเลิศ**



(รูปจากซ้ายไปขวา Marian Rejewski , Henryk Zygalski , Jerzy Rozycki)

ฝรั่งเศสนำข้อมูลที่ได้ไปปรึกษากับ**อังกฤษ** ซึ่งได้ลงความเห็นว่าถึงจะมี**ข้อมูล**พวกนี้ไปก็ไร้ประโยชน์ **ฝรั่งเศส**จึงเสนอ**ข้อมูล**นี้ให้ทีม**อีนิกมาโปแลนด์**ที่ยินดีเป็นอันมาก ทีม**โปแลนด์**มี**ข้อความ**ให้ลองเล่นแล้ว แต่ต้องแก้**ปริศนา**ว่าลูก**ล้อ**ในนั้นหมุนอย่างไร จึงลองถามทาง**ฝรั่งเศส**ว่าขอคีย์ หรือค่าตั้ง**เริ่มต้น**ของลูก**ล้อ**ด้วยได้ไหม เพื่อจะได้รู้ว่า AXEBY = HELLO เมื่อค่าเริ่มต้นลูก**ล้อ**เป็น ABN เป็นต้น ซึ่งฮานส์ก็ตอบรับและส่ง**ข้อมูล**คีย์มาให้ด้วยความ**เต็มใจ** ทีม**โปแลนด์** พิจารณาข้อมูล และพบด้วยว่า**ล้อ**หมุนทั้งสามต้องหมุนด้วยความเร็วไม่เท่ากัน เพราะจากข้อความส่วนใหญ่นั้น **ล้อ**ชั่วโมงและนาทีจะไม่หมุน (ไม่มีใครเรียก**ล้ออีนิกมา**ว่าชั่วโมงและนาทีนอกจากผู้เขียน จริงๆ จะกันเรียกว่า**ล้อ**ซ้ายกลางขวา หรือ LMN หรือ**ล้อ**หมุนช้า **ล้อ**หมุนเร็ว)

Rejewski ใช้หลักการสลับลำดับของข้อมูล (Permutation) มาสร้างสมการ ค่อยๆ แกะรอยการทำงานของลูก**ล้อ** จนรู้ว่าลูก**ล้อ**ทำงานอย่างไร **โปแลนด์**พยายามสร้าง**อีนิกมา**จำลองขึ้นมา แต่ปัญหาหนักหน่วงที่ต้องเดาใจ**เยอรมัน** ก็คือการเดินสายไฟจากปุ่มคีย์บอร์ดแต่ละปุ่มไปยังตัวอักษรแต่ละตัวที่ลูก**ล้อ** **เยอรมัน**อาจจะลากสายจากปุ่ม A ไปที่ลูก**ล้อ**ซี่ X ก็ได้ และความเป็นไปได้ที่จะลากสายแบบต่างๆ กันนี้ เป็นไปได้แปดล้านล้านแบบ ในเครื่อง**อีนิกมา**ที่วางขายในท้องตลาดที่**โปแลนด์**มีอยู่นั้น ลากสายจากปุ่มคีย์บอร์ด Q ไป Aและ W ไป B คือเรียงลำดับตามแป้นของคีย์บอร์ด และไม่ว่า**โปแลนด์**จะพยายามเท่าไหร่ **ก็ไม่ได้ผลออกมาเลย** ทีม**โปแลนด์**เกือบจะสิ้นหวังอยู่แล้ว กับการต้อง**เดาใจหนึ่งในล้านล้าน**นี้ แต่ Rejewski ก็ลองนึกว่าสมมติว่า**เยอรมัน**จะลากสายแบบตรงไปตรงมา จาก A ไป A และ B ไป B ล่ะ และพอลองเข้าก็ได้ผลจริงๆ เมื่อใส่ HELLO และตั้งค่าลูก**ล้อ**เป็น ABN ข้อความที่ได้ก็จะเป็น AXEBY **ไม่น่าเชื่อเลยว่า**ในบรรดาทางเลือก**นับล้านล้านแบบ** **เยอรมัน**จะเลือกวิธีนี้ ที่จริงแล้ว ตอนที่**อังกฤษ**เจอทีม**โปแลนด์**เป็นครั้งแรก คำถามแรกที่**อังกฤษ**เอ่ยปากถามคือ **เยอรมัน**ลากสายนี้อย่างไร และก็ ได้รับคำตอบอันสร้าง**ความประหลาดใจยิ่งยวด**นี้ อย่างไรก็ตาม ตอนนี้**โปแลนด์**ก็มี**อีนิกมา**จำลองอยู่กับตัว

แล้วแต่ถึงจะสร้าง**อีนิกมา** เทียมได้สำเร็จ การแกะโค้ดก็ยังเป็น**เรื่องยาก** เราต้องไม่ลืมว่า**อีนิกมา**จะตั้งค่าเริ่มต้นของลูก**ล้อ**ใหม่ทุกวัน แถมลูก**ล้อ**สามตัวนี้ยังจับมาสลับว่า**ล้อ**ไหนจะเร็วจะช้าได้ตามใจอีกด้วยหากจะให้เดาค่าเริ่มต้นลูก**ล้อ**ให้ถูก ก็ต้องเดาให้ถูกหนึ่งใน**หนึ่งแสนห้าพันกว่าวิธี** และจะต้องเดากันทุกวัน การเดาหนึ่งจากแสนฟังดูง่ายดาย ใน**ยุคคอมพิวเตอร์**

แต่ใน**สมัยนั้น** การลองหนึ่งทางเลือก หมายถึงการปรับลูก**ล้อ**ด้วยมือ และการตั้งลำดับ**ความเร็ว**ของลูก**ล้อ** ก็ต้องลาก**เดินสาย**กันใหม่จริงๆ ดังนั้นการ**แกะโค้ด**ด้วยการเดาสุ่มจึงไม่เป็นผล หากจะต้องเดา ก็ขอให้เป็นการเดาแค่**หนึ่งในร้อย**แทนที่จะเป็นหนึ่งในแสน **โปแลนด์**จะต้องรู้ให้ได้ว่าค่า**เริ่มต้น**ของลูก**ล้อ** และลำดับการใช้ลูก**ล้อ**เป็นอย่างไร และผู้ที่ช่วยให้คำตอบนี้แก่**โปแลนด์**ก็ไม่ใช่ใครเลย นอกจาก**เยอรมัน**

ส่วน ทาง**สหราชอาณาจักร**ได้มีการก่อตั้งหน่วยงานที่ Bletchley Park เพื่องานถอด**รหัส**โดยเฉพาะ

ซึ่ง Bletchley Park นี้เป็น Mansion สไตล์ วิคทอเรีย อยู่ทางเหนือของ ลอนดอน ประเทศ**อังกฤษ**ประมาณ 50 ไมล์ ซึ่งเป็นแหล่งของ**บุคคล**ที่มีความสามารถในการถอด**รหัส**นับเป็น **หมื่นๆ คน** ประกอบด้วย เล่นเกม**อักษรไขว้ แชมป์หมากรุก นักคณิตศาสตร์ นักเรียน นักอักขระอียิปต์** และใครก็ตาม**ที่มีวี่แวว**ว่าจะแกะ**รหัส**ได้ ทุกคนทำงานด้วยความ**สนุกสนาน** ด้วยความ**ท้าทาย**กับ**รหัส**ที่ต้องการจะถอด **ยิ่งเป็นความมั่นคงระดับชาติและหมายถึงความเป็นความตายของชีวิตมนุษย์**ด้วย แล้ว พวกเขาจะทำงานหามรุ่งหามค่ำกันเลยทีเดียว

ความประสบความสำเร็จ ของ Bletchley Park นั้นได้รับความช่วยเหลือจากหลายทาง หนึ่งในนั้นคือ **นักคณิศาสตร์**จากมหาวิทยาลัยเคมบริดช์ชื่อ **Alan Turing (แอลัน ทัวริง)**ซึ่งเป็นที่ยอมรับว่าเป็น**บิดา**ของ**วิทยาการคอมพิวเตอร์** ซึ่งได้สร้างเครื่องมือถอด**รหัส**ชื่อ The **bombe** (มาจากภาษาอังกฤษว่า **Bomb** เพราะเป็นเครื่องมือที่เสียงดังมากนั้นเอง) ช่วงแรกๆ เครื่อง **Bombe** ทำงานได้ช้ามากๆ **แต่ด้วยความประมาท**ของฝ่าย**เยอรมัน**ที่**โอเปเรเตอร์มักง่าย**ไม่ยอมเปลี่ยนการตั้งเครื่องทุกวันประจวบกับในเดือนพฤษภาคม 1941 ฝ่าย**อังกฤษ**ได้จับกุมเรือดำน้ำ **U-boat** ที่นอกฝั่งกรีนแลนด์ทางฝ่ายอังกฤษก็ได้เข้าไปค้นและเจอเครื่อง **Enigma** โมเดลล่าสุดพร้อมกับ หนังสือถอด**รหัส**(Code Book)อีกหลายเล่มด้วย จึงทำให้เครื่องถอด**รหัส**ของ**ฝ่ายสัมพันธมิตรพัฒนา**ไปมาก**ทีเดียว**

โดย เฉพาะ ช่วง **ดีเดย์** ซึ่งการสื่อสารของ**เยอรมัน**ในช่วงนั้น **ฝ่ายสัมพันธมิตร**ก็ได้ถอด**รหัส**ได้แล้ว

Alan Turing

ซึ่งเครื่องมือถอด**รหัส**ในช่วงดีเดย์นั่น ได้สร้างมาจากต้นแบบ **Bombe** เป็นหนึ่งในเครื่อง **BinaryComputer** เครื่องแรกๆ ของโลก ซึ่งกินพื้นที่หลายๆห้องและใช้**หลอดสูญญากาศ**มากกว่า 1500 หลอด เครื่องนี้ชื่อว่า **Colossus** ซึ่งเริ่มใช้งานเดือนมิถุนา ปี 1944 ก่อน**ดีเดย์**ไม่กี่วัน

ความผิดพลาดข้อสำคัญที่สุดของเยอรมันก็คือ ความเชื่ออย่างสุดจิตสุดใจในตัวอีนิกมานี่เองซึ่งเป็นเหตุของความผิดพลาดและเลินเล่อในการใช้งาน

บทสรุปของเรื่องนี้ ก็คือ จะทำการสิ่งใดก็ขอให้ มีสติ อย่าประมาท