بلچلی پارک، پروژه منهتن از نوع انگلیسی

روایت شکسته‌شدن کدهای انیگما در جنگ جهانی دوم (بخش سوم و آخر)

بررسی تاریخ دانش و فناوری در قرن بیستم بدون در نظر گرفتن جنگ جهانی دوم، شاید مانند دیدن کوه باشد بدون در نظر گرفتن قله آن. در نیمه نخست قرن بیستم، دگرگونی‌ها و پیشرفت‌هایی فراوان در دانش‌های تجربی و ریاضیات، زمینه را برای جهش‌های بزرگ در حوزه‌های فناوری و دانش کاربردی آماده ساخته‌بودند که جنگ میان ابرقدرت‌ها، راهی ناگزیر برای توسعه دادن آن‌ها فراهم کرد. نمونه این جهش‌ها را شاید آشکارتر از همه‌جا بتوان در فناوری رادار، پردازش ماشینی و رمزنگاری و شکستن کد، مهندسی هوافضا و مکانیک و (با تأسف و دریغ) در توسعه جنگ‌افزارهای کشتار جمعی دید. در این مجموعه مقاله نگاهی خواهیم داشت بر روایت شکسته‌شدن کدهای انیگما در جنگ جهانی دوم.

این مقاله یکی از قسمت‌های سلسله مقالات یادنامه آلن تورینگ است. این مجموع پیش از این در ماهنامه شبکه منتشر شده اما به سایت جدید منتقل نشده بود. با توجه به اهمیت موضوع، این مجموعه را به سایت مجله اضافه می‌کنیم و امیدواریم که مورد توجه علاقمندان قرار بگیرد.

برای مطالعه بخش‌های پیشین این سلسله مقالات اینجا کلیک کنید

برای مطالعه قسمت‌های قبل روایت شکسته‌شدن کدهای انیگما در جنگ جهانی دوم روی لینک‌های زیر کلیک کنید:

مطلب پیشنهادی

بلچلی پارک، پروژه منهتن از نوع انگلیسی

روایت شکسته‌شدن کدهای انیگما در جنگ جهانی دوم (بخش نخست)

مطلب پیشنهادی

بلچلی پارک، پروژه منهتن از نوع انگلیسی
روایت شکسته‌شدن کدهای انیگما در جنگ جهانی دوم (بخش دوم)

بلچلی پارک

بسیاری از انگلیسی‌ها داستان شکستن کد انیگما را از اینجا به بعد برای شما تعریف می‌کنند. تعجبی هم ندارد، چراکه «تاریخ را همواره فاتحان نوشته‌اند»؛ حتی وقتی که با شکست‌خوردگان هم‌پیمان بوده‌اند. ریفسکی و یکی دو تن از همکارانش در پروژه شکستن کد انیگما، پس از آغاز جنگ مدت‌ها سرگردان بودند. آن‌ها مدتی را در فرانسه به شکستن کدهای آلمانی‌ها گذراندند، اما پس از اشغال فرانسه دوباره آواره شدند و در نهایت در اسپانیا دستگیر و از آنجا به پرتغال و در نهایت انگلیس فرستاده شدند که در انگلیس به شکستن برخی کدهای دیگر آلمانی‌ها پرداختند. اما در همین زمان و در نقطه‌ای دیگر از انگلیس، پروژه دیگری برای شکستن کد انیگما در جریان بود.
در بلچلی پارک، صدها ریاضی‌دان، زبان‌شناس، شطرنج‌باز، آماردان و افراد دیگر از هر پیشه و پیشینه‌ای که ممکن بود به کار رمزگشایی بیایند، گرد هم آورده شده بودند تا روی شکستن کدهای آلمانی‌ها کار کنند، اما شکستن کد انیگمای نیروی دریایی آلمان اهمیت ویژه‌ای داشت. گروهی که روی این مسئله کار می‌کرد، دستاوردهای همتایان لهستانی خود را در اختیار داشت و اکنون با استفاده از آن، خود روش‌های دیگری برای رمزگشایی پیدا می‌کردند. برخی از این روش‌ها به شرایط زمانی جنگ نیز بستگی داشتند. برای نمونه، انگلیسی‌ها در سال‌های پایانی جنگ دریافتند اپراتورهای خسته آلمانی گاهی کلید تصادفی آغاز هر پیام را نه به شکل تصادفی، که (برای نمونه) با فشردن سه حرف هم‌جوار روی صفحه کلید انیگما انتخاب می‌کردند (مانند QWE)، یا گاهی اپراتور ممکن بود به جای استفاده کردن از کلیدهای تصادفی مختلف برای پیام‌های گوناگون در یک روز، به طور یکسان از یک کلید استفاده کند (که ممکن بود برای نمونه، حروف اول نام نامزد اپراتور نگون‌بخت باشد!).

مطلب پیشنهادی

آزمون تورینگ؛ غایتی که در گنجه خاک می‌خورد
آزمون تورینگ چیست و چه کاربردی دارد؟

ترکیب متنوعی از تخصص‌های مختلف که در بلچلی پارک وجود داشت و محیط غیررسمی آن که امکان همکاری آنان را با یکدیگر فراهم می‌کرد، کمک کرد تا در طول جنگ دوم و با وجود دگرگونی تدریجی انیگما، انگلیسی‌ها همچنان بتوانند بسیاری از کدهای آن را بشکنند، اما آلن تورینگ بود که بزرگ‌ترین ضعف انیگما را دریافت و از آن بهره گرفت. با این کشف تورینگ، رمزگشایی از انیگما حتی در دشوارترین شرایط نیز ممکن شد، به خصوص زمانی که آلمانی‌ها تصمیم گرفتند کلید تصادفی را تنها یک بار در آغاز پیام بفرستند، که به معنی بی‌اثر شدن روش ریفسکی بود. تورینگ در آغاز جنگ از کمبریج به بلچلی آمده بود و در اندیشگاه (think tank) آن جای گرفته بود.
در اینجا متخصصان رمزگشایی روی دشواری‌های تازه یا دشواری‌هایی که ممکن بود در آینده اتفاق بیفتد، کار می‌کردند. تورینگ به اندیشیدن روی این مسئله پرداخت که اگر آلمانی‌ها دگرگونی بزرگی در شیوه استفاده کردن از انیگما بدهند، چگونه می‌توان آن را رمزگشایی کرد. روند جاری در بلچلی پارک بر پایه کار ریفسکی ایجاد شده بود که متکی بر استفاده از کلید تکراری در آغاز هر پیام بود. بریتانیایی‌ها می‌توانستند حدس بزنند که آلمانی‌ها به‌زودی متوجه ناامنی این شیوه می‌شوند و آن را کنار می‌گذارند. یافتن شیوه تازه‌ای برای شکستن کد انیگما که بی‌نیاز از تکرار کلید تصادفی در آغاز پیام باشد، بر عهده تورینگ نهاده شد. برخی از همکاران تورینگ در بلچلی پارک گفته‌اند که او کار کردن روی این مسئله را اساساً به این دلیل انتخاب کرد که دیگران از حل کردنش ناامید بودند و او می‌توانست کل مسئله را برای خودش داشته باشد.

دلیله

آلن‌تورینگ ماشین قابل حملی را ابداع کرد که دلیله (**Delilah**) نامیده می‌شد. این ماشین با استفاده از شیوه‌ای که محاسبات ماجولار (**Modular Arithmetic**) نامیده می‌شود،پیام‌های صوتی را رمزنگاری می‌کرد.

تورینگ ساعت‌های بسیاری را صرف مطالعه کدهای رمزگردانی‌شده پیشین در بلچلی کرد و دریافت گاهی می‌تواند از روی زمان فرستادن پیام و منبع آن، بخشی از متن آن را از روی رشته رمزی‌اش حدس بزند. برای نمونه، می‌دانستند که آلمانی‌ها معمولاً هر روز صبح کمی پس از ساعت ۶، یک گزارش هواشناسی می‌فرستند. پس پیامی که در ساعت شش و پنج دقیقه صبح فرستاده می‌شد، به احتمال بسیار حاوی واژه wetter (واژه آلمانی برای آب و هوا) می‌بود. فرمت رسمی مکاتبه‌های نظامی باعث می‌شد که تورینگ بتواند در چنین پیامی، حتی جای واژه wetter را با اطمینان در پیام رمزگذاری‌شده بیابد. وقتی در یک پیام بتوان بخشی از متن رمزگذاری‌شده را با متن عادی پیام متناظر ساخت (مثلاً kpjdf با wetter)، آن بخش را crib می‌نامند. تورینگ به شکل ریاضی ثابت کرد که دانستن یک crib، مجموعه کلیدهای ممکن برای ماشین رمزگذاری را بسیار محدود می‌کند، به این مفهوم که برای یافتن کلید، باید شمار بسیار کمتری از کلیدهای ممکن را جست‌وجو کرد. اما همچنان برای یافتن کلید باید در میان هزاران کلید، جست‌وجو کرد و یک‌به‌یک آن‌ها را آزمود. برای این کار تورینگ ماشینی طراحی کرد و نام آن را به پیروی از همتای پیشین لهستانی‌اش، Bombe نهاد. ساختن بمب به مهندسی به نام هرولد کین سپرده شد.

تا زمانی که ساختن بمب به پایان برسد، تورینگ در بلچلی به کار کردن روی مسائل دیگر پرداخت و در همین زمان آوازه وی در بلچلی پیچید. یکی از همکارانش در بلچلی به نام پیتر هیلتون، وی را این‌گونه توصیف کرده است: «آلن

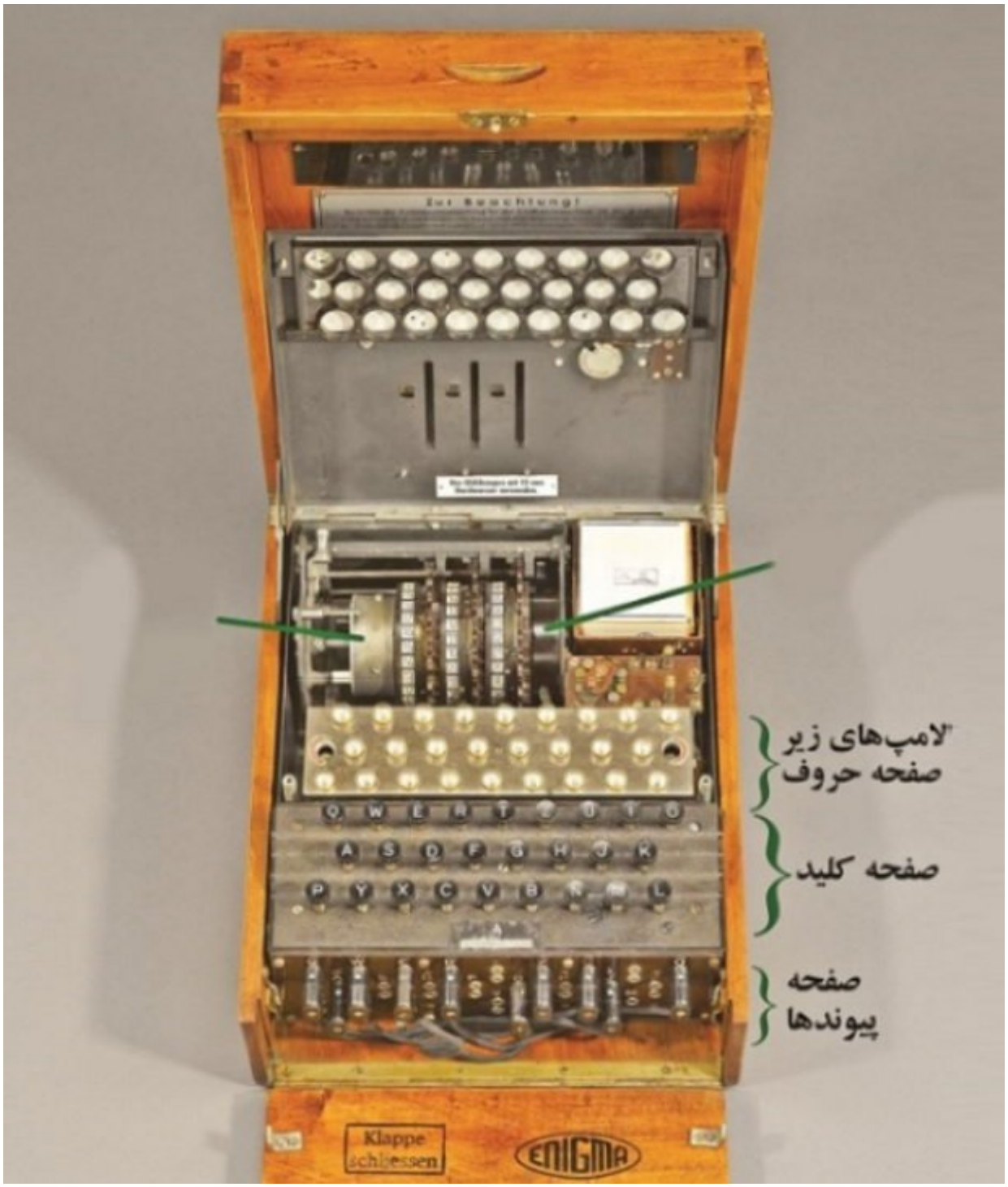
تورینگ به راستی یک نابغه بود، اما نابغه‌ای مهربان و قابل معاشرت. همیشه می‌خواست وقت بگذارد و ایده‌هایش را برای بقیه توضیح دهد؛ اما یک متخصص کوته‌اندیش نبود و از این روی اندیشه تطبیق‌پذیرش بر گستره وسیعی از دانش‌های دقیق گسترده بود.»
به دلیل سرشت بسیار محرمانه پروژه بلچلی پارک، در بیرون از محیط آن کسی نمی‌دانست تورینگ (یا دیگرانی که در آنجا کار می کردند) یک رمزگشا است، چه رسد به این که بدانند او برترین رمزگشای کشورش در آن زمان است. به مادرش گفته بود در گونه‌ای پژوهش نظامی مشغول است و مادرش تنها افسوس می‌خورد که چرا حتی درگیری با کار نظامی نتوانسته آرایش موی فرزند ژولیده‌اش را بهتر کند. اگرچه بلچلی را ارتش اداره می‌کرد، اما هنجارگریزی شخصیت‌های دانشگاهی‌ای مانند تورینگ در محیط آن تحمل می‌شد. تورینگ معمولاً زحمت اصلاح کردن به خود نمی‌داد، ناخن‌هایش آلوده بود و جامه‌اش چروک.
تا پایان سال 1941، پانزده دستگاه بمب مشغول کار بودند. در شرایط خوب، یک ماشین بمب ممکن بود کلید انیگما را یک ساعته بیابد و این برای رمزگشایی از بقیه پیام‌های آن روز کافی بود. اما در عمل دشواری‌های گوناگونی پیش می‌آمد.

مطلب پیشنهادی

یادنامه آلن تورینگ
در ذهن پدر هوش مصنوعی جهان آلن تورینگ چه می‌گذشت؟

یک مشکل متداول این بود که جست‌وجو برای یافتن کلید، بر پایه دانستن crib انجام می‌گرفت که خود تنها با حدس زدن انجام می‌شد. تضمینی نبود که یک crib مشخص، حتماً درست باشد و اگر هم بود، تضمینی نبود که حتماً در بخش درست، در مطابقت با رشته پیام اصلی باشد (یعنی امکان جابه‌جایی به اندازه یک یا چند حرف وجود داشت.). البته یک روش مؤثر برای آزمودن جای crib در رشته پیام، مقایسه کردن حرف‌به‌حرف آن با رشته رمزشده بود. همان‌گونه که دیدیم، یک ویژگی انیگما آن است که هیچ گاه یک حرف را به خودش رمزگردانی نمی‌کند. پس اگر در تطبیق دادن یک رشته crib با رشته پیام رمزشده، دو حرف یکسان در جایگاه یکسانی از دو رشته دیده می‌شد (مانند wetter و oeylq) مشخص می‌شد که مکان crib در رشته درست حدس زده نشده‌است.
اطلاعات محرمانه‌ای که از پروژه رمزگشایی انیگما به دست می‌آمد، بخشی از پروژه فراگیرتری با نام رمز اولترا (Ultra) بود، که شامل رمزگشایی از پیام‌های رمزی ارتش‌های ایتالیا و ژاپن نیز می‌شد. این اطلاعات در مجموع کمک زیادی به برتری متفقین در جنگ دوم کرد و یافتن مواضع، زمان‌های عملیات و اطلاعات دیگر بارها باعث شد متفقین دست برتر را در نبرد داشته باشند یا در برابر حمله‌ها آماده باشند.

شکل5: نمونه‌ای واقعی از دستگاه انیگما



شکل6: نمونه‌ای دیگر از دستگاه انیگما

چرچیل که خوب می‌دانست مخفی نگه داشتن توانایی‌های رمزگشایی متفقین چه قدر اهمیت دارد (کتاب او یک بار آلمانی‌ها را به برگرفتن انیگما سوق داده بود و گویا همین درس برای او کافی بود)، دستور داده بود از اطلاعات به‌دست‌آمده به گونه‌ای استفاده شود که بدگمانی آلمانی‌ها و متحدان‌شان را برنیانگیزد. برای نمونه، رمزگشایی از پیام‌های انیگمای نیروی دریایی آلمان بارها باعث شد موقعیت برخی از U-boatها کشف شود. اما حمله کردن به همه آن‌ها عاقلانه نبود. پس در چنین موردهایی، معمولاً نیروهای انگلیس اجازه می‌دادند برخی از U-boatها از حمله‌شان در امان بمانند.

گاهی هم یک هواپیمای شناسایی به محدوده‌ای که یک یا چند U-boat قرار داشتند فرستاده می‌شد و سپس نیروهای رزمی برای شکار کردن U-boatها فرستاده می‌شدند، تا این پندار برای آلمانی‌ها پیدا شود که از بدشانسی مورد شناسایی تصادفی هوایی قرار گرفته‌اند. البته گاهی هم کار از دست انگلیسی‌ها در می‌رفت. در یک مورد، کدهای انیگما موقعیت 9 کشتی ترابری و سوخت‌رسان آلمانی را فاش کرد. اما برای احتیاط، تنها مختصات 7 کشتی به نیروها داده شد که آن‌ها را با موفقیت غرق کردند، اما ناوچه‌های انگلیسی تصادفاً به دو کشتی دیگر هم برخوردند و

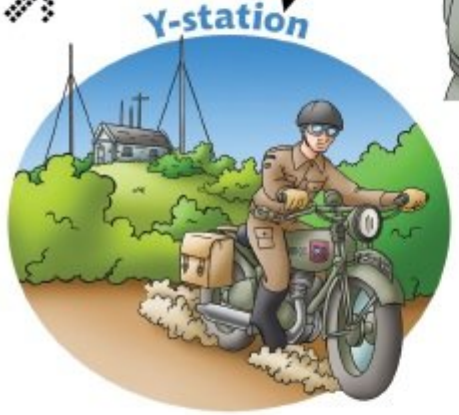
آن‌ها را هم غرق کردند! این رخداد بدگمانی آلمانی‌ها را برانگیخت و دستور یک بررسی داده شد. اما در گزارش نهایی علت‌های ممکن برای این رخداد، بدشانسی یا نفوذ یک جاسوس انگلیسی دانسته شد.
احتمال شکسته شدن کد انیگما ظاهراً دور از تصور آلمانی‌ها بود و مدارک تاریخی هم نشانی از این که آن‌ها به شکسته شدن کد انیگما در طول جنگ پی برده باشند، به دست نمی‌دهد. تردیدی نیست که برتری اطلاعاتی متفقین از راه خواندن کدهای انیگما، کمک فراوانی به کوتاه‌تر شدن جنگ کرد، همچنان که دشوار می‌توان تصور کرد شبه جزیره انگلیس می‌توانست بدون رمزگشایی انیگما، از حمله U-boatها به خط‌های ترابری کالا جان سالم به در برده و در جنگ تاب آورد.

روند کشف رمز

۱- افسر آلماني مسئول، يك پيغام رمزنگاري شده با ماشين انيگما را با استفاده از علامت‌هاي مورس مخابره مي‌كند.

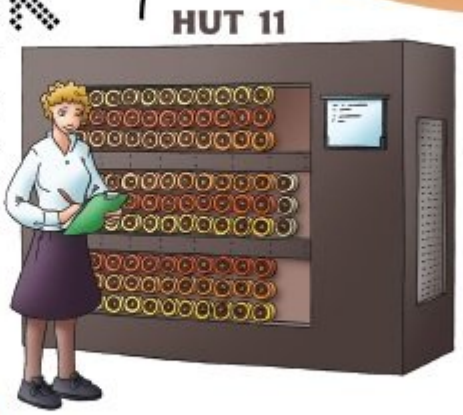
۲- سربازان متصدي آلماني حاضر در ميدان جنگ، پيغام را دريافت كرده و با تايپ در ماشين انيگما، آن‌را رمزگشايي مي‌كنند.

۳- سيگنال‌هاي راديويي آلمانی‌ها در يك مركز شنود محرمانه (موسوم به Y-Station) تحت رديگيري و شنود قرار مي‌گيرد و توسط يك قاصد موتورسوار (بعدها ماشين تحرير تلگرافی يا تله‌پرينتر) به بلچلي پارك (X-Station) ارسال می‌شود.



۴- از آنجا كه پيغام، يك نامه نظامي است به واحد۶ بلچلي پارك (Hut 6) تحويل داده مي‌شود؛ جايي كه كار دشوار رمزگشايي انجام مي‌شود. در اين واحد، به دنبال يافتن بخش‌هايی از پيام رمزنگاری شده كه بتوان آن را با متن عادی متناظر ساخت (به‌اصطلاح Crib) می‌گردند.

۵- در واحد۱۱ بلچلي پارك (Hut 11)، متون متناظر سازي شده در ماشين Bombe آزمايش مي‌شوند و نتيجه به واحد۶ بازگردانده می‌شود.



۶- پيغام‌هاي رمزگشايي شده خام به واحد۳ (Hut 3) انتقال مي‌يابند؛ جايي كه متخصصان بلچلي پارك پيغام‌ها را ترجمه و بررسی می‌كنند و آن را به شيوه‌اي قابل درك براي مقامات بالا بازنويسي می‌كنند.

مطلب پیشنهادی

مردی که بسیار می‌دانست
زندگی‌نامه آلن تورینگ؛ پدر علوم کامپیوتر (قسمت اول)

پس از جنگ

اگر می‌توانید مکاتبه‌های دشمن‌تان را رمزگشایی کنید و بخوانید، احتمالاً نمی‌خواهید آن‌ها از این توانایی شما باخبر شوند. پروژه بلچلی پارک با پایان جنگ عملاً پایان یافت. چرچیل دستور داد ماشین‌های بمب اوراق شوند، تا حدی که هیچ قطعه‌ای از آن، بزرگ‌تر از اندازه بازوی یک انسان نباشد. وی همچنین دستور داد همه دستاوردهای بلچلی پارک برای همیشه محرمانه بماند.
البته توانایی رمزگشایی انیگما بازنشسته نشد. در واقع، انگلیسی‌ها خود چندین دستگاه انیگمای به دست آمده از آلمانی‌ها را به مستعمره‌های‌شان دادند تا دولت‌های آن‌ها (به پندار امن بودن انیگما) از آن برای مکاتبه‌های خود استفاده کنند! انگلیس هیچ کوششی برای تغییر دادن این پندار نکرد و تا سال‌ها به مکاتبه‌های آنان گوش می‌داد.

در اوایل دهه 1970، کاپیتان وینتربات‌هام (F.W. Winterbotham) که در زمان جنگ مسئول توزیع اطلاعات به دست‌آمده از پروژه اولترا بود، از دولت انگلیس خواست تا اجازه بازگویی تاریخ پروژه به او داده شود، چراکه تا آن زمان دیگر هیچ کشوری از انیگما استفاده نمی‌کرد و مخفی نگه داشتن این اطلاعات دیگر لزوم یا سودی نداشت. این اجازه (با بی‌میلی) صادر شد و وی در سال ۱۹۷۴ کتابی با عنوان The Ultra Secret در این زمینه منتشر کرد. تا این زمان، آلن تورینگ تنها به عنوان ریاضی‌دانی برجسته و مؤثر در پیدایش علوم کامپیوتر و ساختن نخستین ماشین‌های حساب‌گر دیجیتال شناخته می‌شد و از آن پس بود که وی به عنوان بزرگ‌ترین رمزگشای بریتانیا در جنگ دوم و یک قهرمان ملی شناخته شد. البته چنان که می‌دانیم، او دیگر زنده نبود تا مورد قدردانی قرار گیرد (و چه بسا که اگر هم زنده بود، چندان اهمیتی به هیاهوی همگانی نمی‌داد). دو دهه پیش‌تر، سیبی زهرآلود به زندگی کوتاه و پربار وی پایان داده بود!

تاریخ انتشار:

22 دی 1396

نشانی منبع:

https://www.shabakeh-mag.com/are-network/11364/%D8%B1%D9%88%D8%A7%D9%8A%D8%AA-%D8%B4%D9%83%D8%B3%D8%AA%D9%87%E2%80%8C%D8%B4%D8%AF%D9%86-%D9%83%D8%AF%D9%87%D8%A7%DB%8C-%D8%A7%D9%86%D9%8A%DA%AF%D9%85%D8%A7-%D8%AF%D8%B1-%D8%AC%D9%86%DA%AF-%D8%AC%D9%87%D8%A7%D9%86%DB%8C-%D8%AF%D9%88%D9%85-%D8%A8%D8%AE%D8%B4-%D8%B3%D9%88%D9%85-%D9%88-%D8%A2%D8%AE%D8%B1