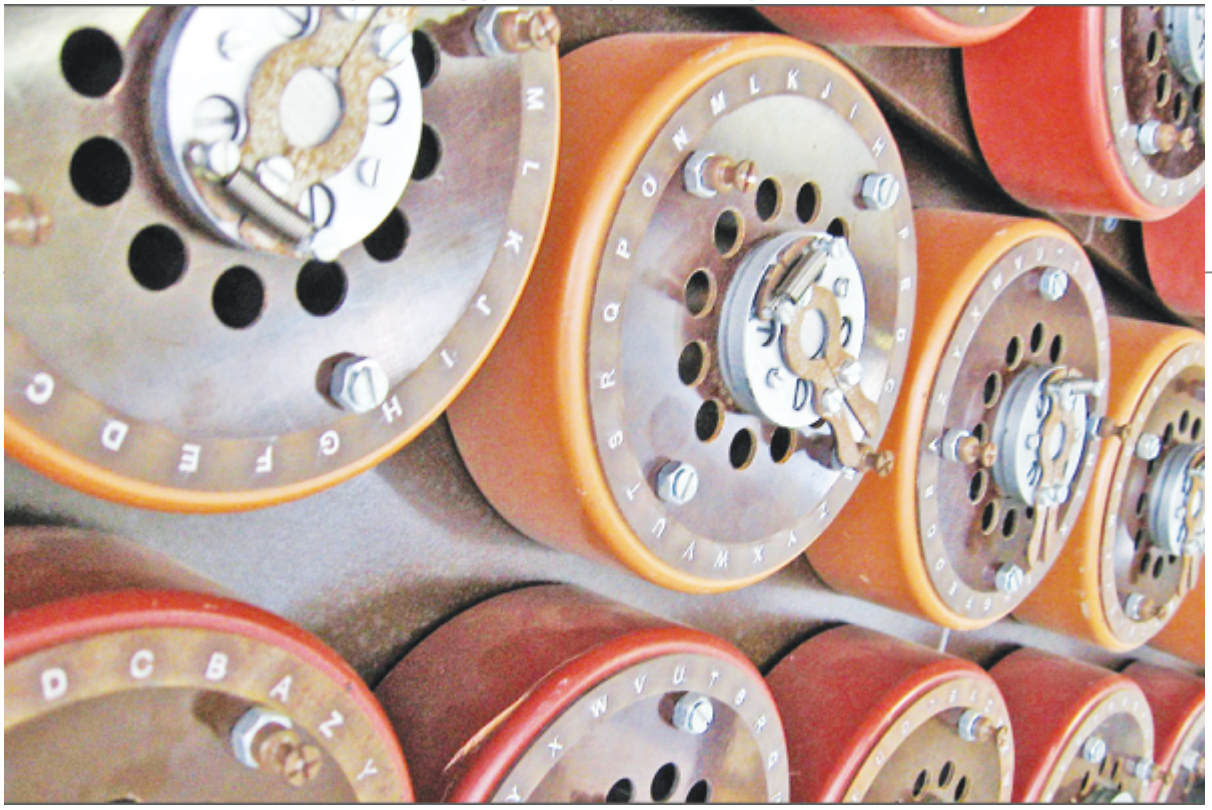
بلچلی پارک، پروژه منهتن از نوع انگلیسی

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



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

نازی‌های سرخورده و خشمگین از ناکامی در جنگ جهانی نخست، همه توان فناوری، اقتصادی و انسانی خود را برای پیروزی در جنگ دوم بسیج کرده‌بودند و در این راه، به زانو در آوردن انگلیس شاید یکی از مهم‌ترین هدف‌ها بود. اما این جزیره با یک نیروی دریایی بسیار قوی حفاظت می‌شود.

نبرد آتلانتیک

ماجرا از همان جنگ جهانی اول آغاز شده بود. آلمانی‌ها از قرن نوزدهم طرح‌هایی را برای ساختن زیردریایی آزموده‌بودند و در نهایت در آغاز قرن بیستم توانسته بودند نخستین زیردریایی جنگی خود را بسازند. در طول سالیان، نسل‌هایی پی‌درپی از زیردریایی‌های جنگی در نیروی دریایی آلمان ساخته شد که با حرف U مشخص می‌شدند.
نخستین رده آن در سال 1906 ساخته و U-1 نامیده شد.
رده‌های بعدی تا جنگ جهانی اول به تدریج ساخته شده و تکامل یافتند و از جمله U-9 و SM U-21 نسل‌هایی بودند که در جنگ اول برای غرق کردن کشتی‌های ترابری عازم انگلیس به کار رفتند. این زیردریایی‌ها و نسل‌های پس از آن به طور کلی به نام U-boat معروف شدند، که انگلیسی واژه آلمانی U-Boot بود. کلمه U-Boot خود کوتاه‌شده واژه Unterseeboot به معنی زیردریایی است.
انگلیس در هر دو جنگ جهانی متکی بر کالاها و تسلیحاتی بود که از کانادا، امریکا و مستعمره‌هایش فرستاده می‌شد و بنابراین قطع کردن جریان ترابری دریایی در اقیانوس اطلس، به مفهوم به زانو درآوردن این کشور در جنگ بود، که در واقع آلمان در هر دو جنگ تا مرز آن نیز پیش رفت. در جنگ نخست، از مجموع 360 فروند U-boat ساخته شده،

178 فروند غرق شده بود، اما همه آن‌ها با هم توانسته بودند در مجموع 11 میلیون تن کالا را غرق کنند. براساس بخشی از پیمان ورسای که به جنگ اول رسماً پایان داد، همه U-boatها باید سریع تسلیم می‌شدند و چنین نیز شد و بیشتر آن‌ها پس از امضای این تعهدنامه نابود شدند.

مطلب پیشنهادی

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

با آغاز جنگ دوم، تکرار تجربه U-boatها یکی از راهبردهای اصلی آلمانی‌ها بود و نسل‌های تازه U-boatها وارد کارزار شدند. نبرد دریایی در آغاز جنگ بسیار مؤثر بود و دشواری‌های فراوانی را برای بریتانیا ایجاد کرد، تا جایی که چرچیل بعدها گفت: «تنها چیزی که در دوران جنگ من را واقعاً وحشت‌زده کرد، خطر U-boatها بود.»

شکل 1: ظاهر نخستین نمونه‌های دستگاه انیگما

البته توسعه‌دادن فناوری رادار و سونار و ورود امریکا به جنگ و برخی تدبیرهای دیگر مانند اسکورت نظامی کاروان‌های ترابری دریایی و گسترش محدوده پروازهای پایشی، تهدید U-boatها را کاهش داد، اما آلمانی‌ها هم بیکار ننشستند.
افزون بر پیشرفت‌هایی در فناوری اژدرها و خود زیردریایی‌ها و نیز یافتن روش‌های گوناگونی برای گریز از رادار و سونار، یکی از مهم‌ترین آرایش‌های جنگی برای افزایش قدرت U-boatها، آرایشی بود که با نام «گله گرگ» شناخته می‌شد. در این آرایش، چند U-boat در کنار هم و به‌طور گروهی به کشتی‌های باری حمله می‌کردند که این روش به‌ویژه برای غرق کردن کاروان‌های ترابری اسکورت‌شده مؤثر بود. زیردریایی‌هایی که در این آرایش با هم حمله می‌کردند، بیش از آن‌هایی که به تنهایی گشت می‌زدند، بر ارتباط رادیویی بین خودشان متکی بودند و مقابله با این حمله‌ها نیز بیش از حمله‌های تکی، نیازمند شنود ارتباط میان U-boatها بود. شنود ارتباط رادیویی آلمانی‌ها در جبهه جنگ به طور کلی برای متفقین مهم بود، اما در نبرد آتلانتیک به طور خاص و برای مقابله با «گله‌های گرگ» به طور خاص‌تر، شنود این ارتباط‌ها حیاتی بود. نیروهای متفقین البته می‌توانستند این ارتباط‌های رادیویی را شنود کنند، اما

دشواری بزرگ در این بود که آلمانی‌ها همه ارتباط‌های رادیویی خود را با دستگاه کدگذاری ویژه‌ای به نام انیگما (Enigma) رمزگذاری می‌کردند و کلید رمزها نیز به طور روزمره و در دوره‌های سنگین‌تر نبرد، گاهی تا سه بار در روز عوض می‌شد. به این ترتیب، پیام‌های شنودشده بدون رمزگشایی بی‌فایده بودند. شاهرگ اقتصادی و تسلیحاتی بریتانیا در گرو شکستن کد انیگما بود و این کار نه برای یک بار، که باید به شکل روزمره و بسیار سریع انجام می‌شد وگرنه ارزش اطلاعات کشف‌شده از بین می‌رفت.

آلمانی‌ها همه ارتباط‌های رادیویی خود را با دستگاه کدگذاری ویژه‌ای به نام انیگما (Enigma) رمزگذاری می‌کردند و کلید رمزها نیز به طور روزمره و در دوره‌های سنگین‌تر نبرد، گاهی تا سه بار در روز عوض می‌شد.

اِنیگما

آلمانی‌ها در جنگ جهانی اول هم ارتباط‌های رادیویی خود را رمزنگاری می‌کردند، اما انیگما بسیار پیشرفته‌تر از سیستمی بود که در جنگ اول به کار گرفته می‌شد. سیستم انیگما را یک مهندس برق آلمانی به نام آرتور شربیوس (Arthur Scherbius) در سال‌های پایانی جنگ اول ساخت و در سال ۱۹۱۸ به ثبت رساند. شربیوس در آغاز موفقیت چندانی در فروختن انیگما به دولت برای استفاده گسترده نظامی نداشت، چرا که دولت سیستم رمزنگاری به کار رفته در جنگ جهانی نخست را به اندازه کافی قوی می‌دانست و انگیزه لازم را برای خریدن سیستم گران‌قیمت او نداشت. ماجرایی که به خریدن انیگما توسط دولت آلمان برای استفاده نظامی انجامید، طنزی تاریخی دارد. در همان زمانی که شربیوس، چند سال پس از پایان جنگ نخست، می‌کوشید سیستم رمزنگاری‌اش را به دولت آلمان بفروشد، کتاب‌هایی در انگلیس نوشته و منتشر شد که به جنگ نخست می‌پرداختند.
یکی از این کتاب‌ها با عنوان «بحران جهانی» را وینستون چرچیل نگاشته بود و در آن توضیح داده بود که یکی از دلیل‌های مهم موفقیت در برابر نیروهای آلمان، توانایی شکستن رمزهای ارتباطی آنان بوده است. انتشار این خبر، دولت آلمان را بهت‌زده و وادار کرد تا برای متوقف کردن شنود، اقدام به خریدن سیستم انیگما و به‌کارگیری آن در ارتباط‌های نظامی کند. این آغاز داستان انیگما در ارتش بود و تا مدتی انگلیس و فرانسه و متحدان‌شان را از رمزگشایی مکاتبه‌های رادیویی آلمانی‌ها بازداشت، اما رمزنگاری انیگما تا پیش از جنگ دوم شکسته شد و در طول جنگ چرچیل باید با سیستم رمزنگاری‌ای مقابله می‌کرد که خود، انگیزه به‌کارگیری‌اش را به آلمانی‌ها داده‌بود! نمونه نخست انیگما، مانند مدلی است که در شکل 1 می‌بینید و در آن به طور کلی یک صفحه کلید (برای تایپ کردن حرف‌های متن)، یک صفحه نمایش‌گر حروف (با لامپی زیر هر حرف) و سه چرخ‌دنده اصلی (مانند کیلومترشمارهای مکانیکی در خودروها) وجود دارد که بر گرد هرکدام، 26 حرف الفبای انگلیسی حک شده‌است.
عملکرد صفحه حروف مانند صفحه نمایشگر کامپیوترها است و با فشردن هر حرف روی صفحه کلید، حرفی روی صفحه حروف روشن می‌شود که بستگی به وضعیت ماشین در هنگام تایپ شدن حرف ورودی دارد، اما در ضمن همواره با آن متفاوت است. برای این که بفهمیم انیگمای اولیه چگونه کار می‌کرد، نخست بیایید ورودی و خروجی آن را مانند یک کاربر درک کنیم. شیوه کار کردن با دستگاه به این صورت است که نخست، باید چرخ‌دنده‌ها را به ترتیب در جای‌شان نصب کنیم. این سه چرخ‌دنده از یک تا سه شماره‌گذاری شده‌اند و می‌توان آن‌ها را به شش ترتیب (فاکتوریل سه) در سه جایگاه قرار داد. ترتیب چرخ‌دنده‌ها، بخشی از کلیدی است که برای رمزگذاری یک پیام و سپس برای رمزگشایی آن به کار می‌رود.
پس از نصب کردن چرخ‌دنده‌ها، باید هر یک را روی حرف مشخصی قرار داد. مثلاً اولی را روی حرف R، دومی را روی حرف H و سومی را روی حرف L قرار می‌دهیم. اکنون دستگاه آماده است و می‌توان تایپ کردن پیام را آغاز کرد. به ازای هر حرفی از پیام که تایپ می‌کنیم، حرف دیگری روی صفحه حروف روشن می‌شود و اگر می‌خواهیم پیامی را رمزگذاری کنیم، به جای هر حرف در پیام نخستین، حرفی را که با تایپ کردن آن روی صفحه حروف روشن می‌شود، ثبت می‌کنیم، تا این که به پایان پیام برسیم و رشته‌ای از حروف را که به دست می‌آید روی خط ارتباطی می‌فرستیم.

مطلب پیشنهادی

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

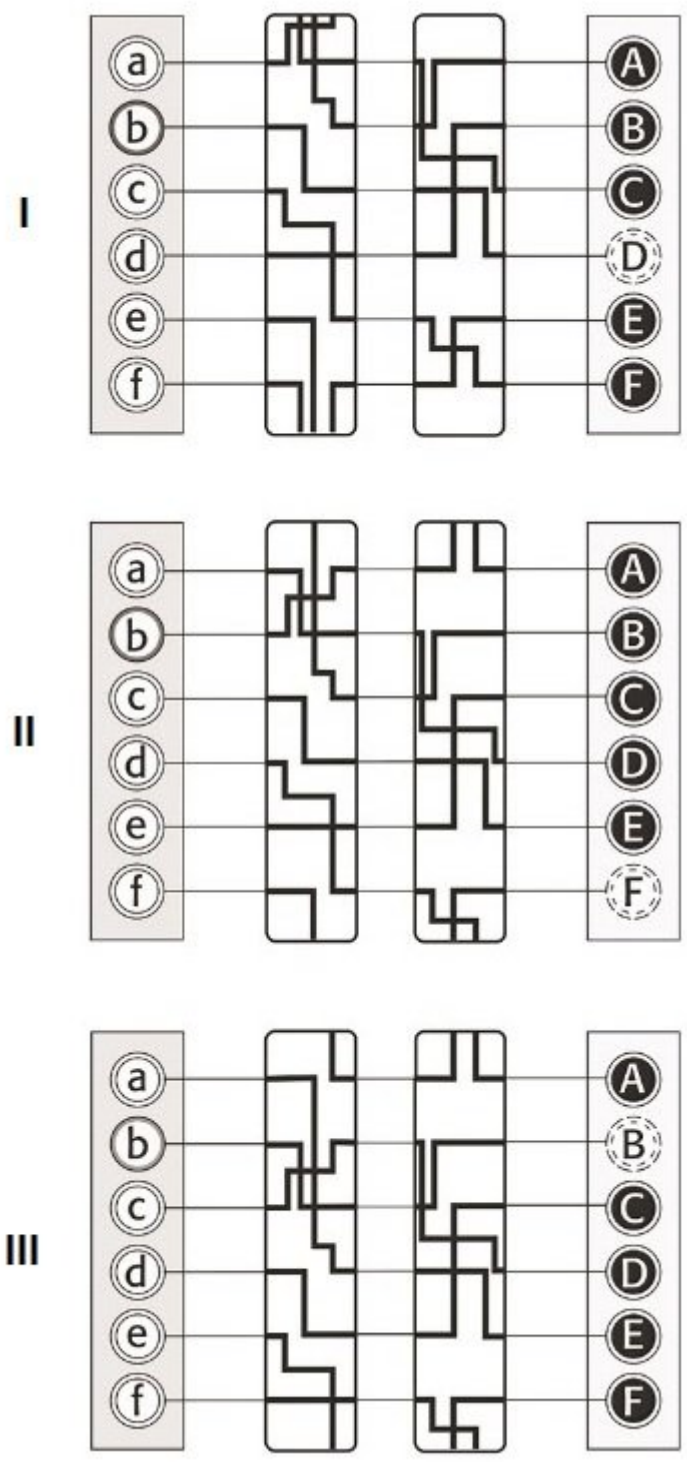
همان‌گونه که گفته شد، یک ویژگی انیگما این است که در آن هیچ گاه هیچ حرفی به خودش رمزنگاری نمی‌شود، مثلاً T به T رمز نمی‌شود، بلکه همیشه به حرف دیگری برگردانده می‌شود. پس از تایپ کردن هر حرف، چرخ‌دنده‌ای که در جایگاه نخست است، یک حرف جابه‌جا می‌شود، مثلاً اگر روی حرف U است، به حرف V می‌رود. اگر چرخ‌دنده نخست روی حرف Z باشد، با تایپ کردن یک حرف، به حرف A می‌رود و سپس چرخ‌دنده دوم نیز یک حرف جلو می‌رود، درست مانند نشانگرهای یکان و دهگان در کیلومترشمار مکانیکی خودروها. به همین ترتیب، اگر چرخ‌دنده دوم به حرف Z برسد، به حرف A می‌رود و چرخ‌دنده سوم هم یک حرف جلو می‌رود (مانند نشان‌گرهای دهگان و صدگان). چیزی که برای شروع کار مهم است، آرایش نخستین چرخ‌دنده‌ها است و این آرایش در طول فرآیند تایپ کردن، تغییر خواهدکرد.

در آن سوی خط، به دستگاهی نیاز داریم که آرایش (ترتیب) چرخ‌دنده‌های آن و نیز حرف روی نشانگر برای هر چرخ‌دنده، مانند دستگاه رمزگذاری فرستنده باشد. مجموعه این دو (ترتیب چرخ‌دنده‌ها و حرف روی نشان‌گر برای هر کدام) کلید رمز را تشکیل می‌دهد. کاربری که در آن سوی خط است، رشته پیام رمزشده را دریافت می‌کند و آن را روی دستگاهی که با همان کلید رمز تنظیم شده، تایپ می‌کند و با نگاشتن یک به یک حرف‌هایی که با فشردن هر حرف از رشته رمز شده، روی صفحه نمایش‌گر حرف‌ها پدیدار می‌شود، پیام نخست را به دست می‌آورد. این یک درک بیرونی از شیوه کار کردن با انیگمای نخستین است. اکنون ببینیم درون جعبه چه می‌گذرد.

سازوکار انیگما

در مدلی که در شکل 1 می‌بینید، ساده‌ترین نوع دستگاه انیگما شبیه‌سازی شده است. برای فهمیدن سازوکار آن، بیایید مدل را باز هم ساده‌تر کنیم. دستگاهی را در نظر آورید که تنها دو چرخ‌دنده دارد و الفبایی شش‌حرفی را رمزنگاری و رمزگشایی می‌کند. سه مرحله کاری چنین دستگاهی در شکل 2 نشان داده شده است.

شکل2: دیاگرامی ساده شده از نحوه کار انیگما



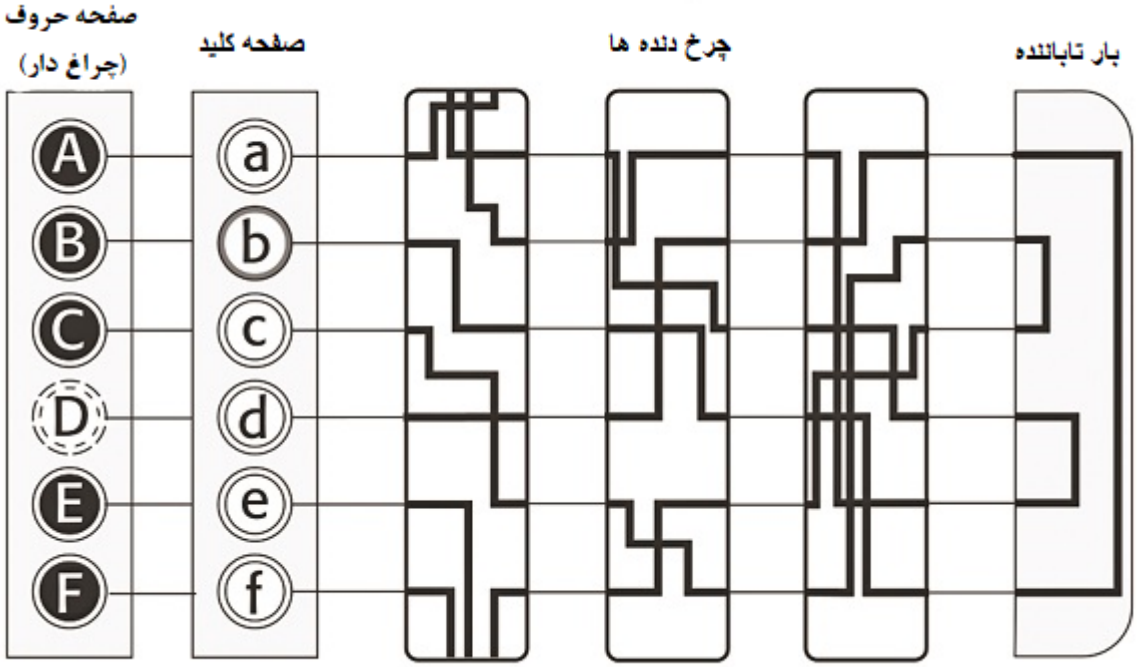
درون هر چرخ‌دنده، سیم‌کشی متقاطعی وجود دارد که شش ورودی و شش خروجی دارد (در نمونه واقعی، این عدد 26 است). روشن شدن لامپ زیر یک حرف با فشردن کلیدی روی صفحه کلید، نتیجه بسته شدن مداری است که از چرخ‌دنده‌ها می‌گذرد تا به صفحه کلید برسد. خط‌های تیره روی مقطع هر چرخ‌دنده، مسیر سیم‌کشی‌های درون آن را نشان می‌دهند.

در جایی که یک خط به انتهای بالا یا پایین مقطع می‌رسد، امتداد آن را باید در انتهای دیگر چرخ‌دنده دنبال کرد، مانند آنچه که در انتهای بالایی و پایینی چرخ‌دنده نخست در بخش ا شکل 2 می‌توان دید. یافتن مسیر سیم‌ها در این مدل ساده‌شده، آسان است و طرز کار کلی دستگاه
را نشان می‌دهد.

مطلب پیشنهادی

رایگان دانلود کنید: کتاب الکترونیکی «یادگیری ماشینی؛ سفری به اعماق هوشمندی»

در شکل 3، نمونه‌ای را می‌بینیم که همچنان 6 حرفی است (برای ساده‌سازی)، اما از هر نظر دیگر شبیه نمونه نخست انیگما است. در اینجا 3 چرخ‌دنده داریم و نیز یک دیسک بازتاباننده. نقش بازتاباننده چیست؟ بازتاباننده سیم‌کشی درونی ساده‌تری دارد و نقش آن متقارن کردن سیستم انیگما است. یعنی هرگاه دستگاه روی کلید مشخصی تنظیم شده‌باشد و برای نمونه حرف G به حرف B رمزنگاری شود، اگر دستگاه را در همان آرایش قرار دهیم، با فشردن حرف B روی صفحه کلید، حرف G را روی صفحه حرف‌ها روشن خواهدکرد. اهمیت این تقارن در چیست؟



شکل۳: نمونه ساده شده انیگما با دیسک بازتابانند ه

فرض کنید شما دستگاه را در آرایش 312 و با تنظیم نخستین BDA قرار می‌دهید، یعنی در جایگاه نخست (از سمت چپ) چرخ‌دنده شماره3، در جایگاه میانی چرخ‌دنده شماره 1 و در جایگاه سوم چرخ‌دنده شماره 2 را قرار می‌دهید و چرخ‌دنده سوم که در جایگاه نخست قرار دارد را روی حرف B، چرخ‌دنده میانی (شماره ۱) را روی حرف D و چرخ‌دنده سمت راستی (شماره 2) را روی حرف A تنظیم می‌کنید و کلمه BEE (به معنی زنبور عسل) را تایپ می‌کنید. روی صفحه حروف، ممکن است حرف A را برای حرف نخست کلمه، حرف F را برای E میانی و حرف D را برای حرف آخر ببینید.

مطلب پیشنهادی

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

چرا دو حرف آخر که یکسان بودند به حرف یکسانی رمزنگاری نشدند؟ به یاد آورید که با وارد کردن هر حرف،

چرخ‌دنده‌ها در وضعیت تازه‌ای قرار می‌گیرند که در واقع یک کلید تازه است، پس دو حرف یکسان متوالی را به حرف یکسانی کد نخواهند کرد. اگر غیر از این بود، یعنی با یک کلید اولیه مشخص، هر حرف همیشه به حرف یکسانی کد می‌شد، انیگما سیستم بسیار ضعیفی می‌بود و از روی الگوهای تکراری درون پیام‌ها می‌شد کلمه‌ها را حدس زد و کلید را یافت.

انیگما دو ویژگی مهم داشت. نخست این که هیچ حرفی را به خودش کد نمی‌کرد. دوم این که حروف یکسان را نیز به حروفی متفاوت کد می‌کرد.

اکنون کلمه رمز شده را به همراه کلید رمزنگاری‌تان برای شخص دیگری می‌فرستید. گیرنده، ترکیب 312 و BDA را به عنوان کلید و رشته AFD را به عنوان متن پیام رمزنگاری شده دریافت می‌کند (پیامی بسیار کوتاه!). او دستگاهش را طبق کلید شما تنظیم می‌کند و سپس شروع به تایپ کردن متن پیام (AFD) می‌کند و به ترتیب حروف B و E و E را می‌بیند که روی صفحه نمایشگر روشن می‌شوند، چراکه متقارن بودن سازوکار درونی انیگما که به کمک بازتاباننده ممکن شده، باعث می‌شود که اگر شما با کلید مشخصی حرف B را به A رمزنگاری کرده باشید، با همان کلید حرف A به B رمزنگاری شود. در ضمن، کلیدهای بعدی دستگاه هم که در اثر چرخش‌های متوالی چرخ‌دنده‌ها ایجاد شده‌اند، تنها بستگی به کلید نخست و شمار حرف‌های وارد شده دارند و بنابراین نیازی نیست که برای رمزگشایی رشته پیام، دستگاه را برای هر حرفی تنظیم کرد. به این ترتیب، سیستم سریعی برای رمزگذاری و رمزگشایی پیام‌های متنی داریم.

برای مطالعه قسمت بعدی 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 دوم)

تاریخ انتشار:
18 دی 1396

نشانی منبع:
https://www.shabakeh-mag.com/cover-story/10935/%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-%D9%86%D8%AE%D8%B3%D8%AA