بلچلی پارک، پروژه منهتن از نوع انگلیسی

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

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 قسمت 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)

امنیت انیگما

دیدیم که کار کردن با انیگما آسان است. اما امنیت آن چه اندازه است؟ یک ویژگی بسیار مهم انیگما آن است که هیچ حرفی را به خودش کد نمی‌کند، و نیز دو حرف یکسان متوالی را به حرف‌های متفاوتی برمی‌گرداند. اما در

انیگمای واقعی (با 26 حرف الفبای انگلیسی) به چند شیوه می‌توان کلید رمز ساخت؟ سه چرخ‌دنده را در مجموع به 6 شیوه مختلف می‌توان در جایگاه‌شان نصب کرد و هر یک را هم می‌توان روی یکی از 26 حرف الفبا قرار داد. پس در مجموع 6×26×26×26 آرایش نخستین ممکن است که برابر با 105456 خواهد بود. با افزودن به شمار دیسک‌ها (کاری که بعدها در دوران جنگ دوم آلمانی‌ها انجام دادند) می‌توان بر این شمار افزود. اما شیوه بسیار مهم دیگری هم برای افزودن بر شمار کلیدهای ممکن وجود دارد، که با افزودن بخشی به نام صفحه پیوندها (یا اتصال‌ها) ممکن می‌شود.
کارکرد و جایگاه صفحه پیوندها را می‌توانید در شکل 4 ببینید، و همان گونه که در شکل‌های 5 و 6 (نمونه‌های واقعی انیگما)می‌بینید، صفحه پیوندها در جلوی دستگاه، زیر صفحه کلید قرار داشت. برای هر حرف، یک جفت سوراخ (مانند پریز برق) روی صفحه پیوندها وجود داشت و کابل‌های ویژه‌ای برای این صفحه در نظر گرفته شده که در هر سر آن‌ها یک دوشاخه وجود داشت. با وصل کردن کابلی میان دو حرف روی این صفحه، جای آن دو حرف پیش از رفتن به آرایش چرخ‌دنده‌ها عوض می‌شد. برای نمونه، اگر کابلی را میان حرف‌های F و Y وصل کنیم، با فشردن کلید F روی صفحه کلید، پالس حرف Y به سوی چرخ‌دنده‌ها می‌رود و با فشردن Y نیز پالس F فرستاده می‌شود. فایده این کار چیست؟ این کار لایه دیگری بر رمزگذاری انیگما می‌افزاید که به خودی خود (یعنی به عنوان یک شیوه رمزگذاری مستقل) روش به‌نسبت ضعیفی است، اما در ترکیب با آرایش چرخ‌دنده‌ها، تعداد کلیدهای ممکن برای دستگاه را چندین مرتبه افزایش می‌دهد. در ابتدای افزوده شدن صفحه پیوندها، شش کابل پیوندی برای هر کلید رمز در نظر گرفته‌شد که باید میان شش جفت حرف وصل می‌شد (مثلاً H به P و مانند آن). اکنون بخش دیگری هم به کلید رمز افزوده شده‌بود: آرایش صفحه پیوندها.
پس کلید رمز اکنون شامل ترتیب چرخ‌دنده‌ها و حرف روی نشانگر دستگاه برای هر کدام بود، به اضافه شش جفت حرف که باید با یک کابل روی صفحه پیوندها به هم وصل شوند. کلیدهای رمز انیگما برای هر یک از نیروهای ارتش آلمان معمولاً به شکل ماهانه چاپ و توزیع می‌شد. هر واحدی با در اختیار داشتن ماشین انیگما و تنظیم کردن آن طبق کلید روز، می‌توانست با بقیه واحدها ارتباط برقرار کند و آشکار است که محرمانه نگاه داشتن کلیدها اهمیت اساسی داشت.

مطلب پیشنهادی

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

اما شمار کلیدهای ممکن چند تا است؟ از میان 26 حرف، به چند شیوه می‌توان شش جفت را به هم وصل کرد؟ پاسخ این پرسش را می‌توان با بهره‌گیری از شاخه‌ای از ریاضی به نام حساب ترکیب‌ها (combinatorics) یافت. حساب ترکیب‌ها در واقع دانش شمردن چیزها است! اگر می‌پندارید شمردن چیزها آسان است، بکوشید پاسخ مسئله بالا را حدس بزنید. پاسخ عدد 100391791500 است. اگر این عدد را در شمار کلیدهای رمز انیگمای سه دیسکی (بدون صفحه پیوندها) ضرب کنیم، عددی بزرگ‌تر از ده هزار میلیون میلیون (ده به توان شانزده) به دست می‌آید.
رمزگشایی متنی که با چنین دستگاهی رمزگذاری شده‌باشد چه قدر زمان می‌برد؟ اگر آدم سمجی پیدا شود که بتواند در هر دقیقه یک کلید ممکن را بیازماید، آزمودن این شمار کلید رمز بیش از عمر کنونی جهان به طول خواهد انجامید. این مهندسی آلمانی به نظر بی‌نقص می‌رسید و در واقع هم در خلال چند هفته با به‌کارگیری انیگما در مخابرات نظامی آلمان، همه کشورهایی که تا پیش از این شنودکننده آن بودند، بهت‌زده شدند و از رمزگشایی پیام‌ها درماندند. این بهت‌زدگی چند سالی به طول انجامید، اما سرانجام به پایان رسید.

مطلب پیشنهادی

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

رمزگشایی از انیگما

مقام نظامی مسئولی که تصمیم به خریدن و به‌کارگیری انیگما گرفت، رودولف تیلوشمیت نام داشت. وی در دوران جنگ نخست در ارتش جنگیده بود و پس از جنگ نیز در ارتش مانده و پله‌پله بالا رفته بود. رودولف برادری به نام هانس داشت، که کمتر از او در ارتش موفق بود و پس از جنگ به مشکل مالی برخورده بود. رودولف برای هانس، کاری در اداره رمزنگاری یافت، اما گذران زندگی همچنان برای هانس دشوار بود، در حالی که مدارک سری ارزشمندی در دسترس داشت. هانس در بلژیک با یک جاسوس فرانسوی آشنا شد و موافقت کرد که در ازای دریافت ده هزار مارک (تقریباً معادل سی هزار دلار امروزی) دو سند را به وی نشان دهد و بگذارد از آن‌ها عکس‌برداری کند. این دو سند اهمیت فنی فراوانی داشتند، چراکه از آن‌ها می‌شد سازوکار درونی انیگما و همچنین سیم‌کشی درونی چرخ‌دنده‌ها را دریافت. بخش رمزگشایی سیستم امنیتی فرانسه ارزش این سندها را ندانست، اما به خاطر پیمان امنیتی میان انگلیس، فرانسه و لهستان، این سندها در اختیار دو کشور دیگر نیز قرار گرفت. انگلیسی‌ها هم در این زمان ارزش این سندها را درک نکردند، اما لهستان با جدیت پیگیر استفاده از آن شد. تیمی از ریاضی‌پیشگان لهستانی به کار کردن روی این مسئله پرداختند.
در گام نخست، آن‌ها با استفاده از سندها توانستند نمونه‌ای از انیگما با همان نقشه مدار درونی آلمانی‌ها را برای خود بسازند. اما حتی با در اختیار داشتن انیگما هم رمزگشایی از پیام‌ها دشوار است و انگلیسی‌ها و فرانسوی‌ها به همین دلیل زحمت بازسازی انیگما را به خود نداده بودند، چرا که در عمل رمزگشایی از انیگما را ناممکن می‌دانستند. اما لهستان بیش از فرانسه و انگلیس احساس خطر می‌کرد، چرا که زمان زیادی از استقلالش از آلمان نگذشته بود و همسایه شرقی‌اش هم به تازگی دارای حکومتی کمونیستی شده بود و برای گسترش آن چشم طمع به لهستان داشت.

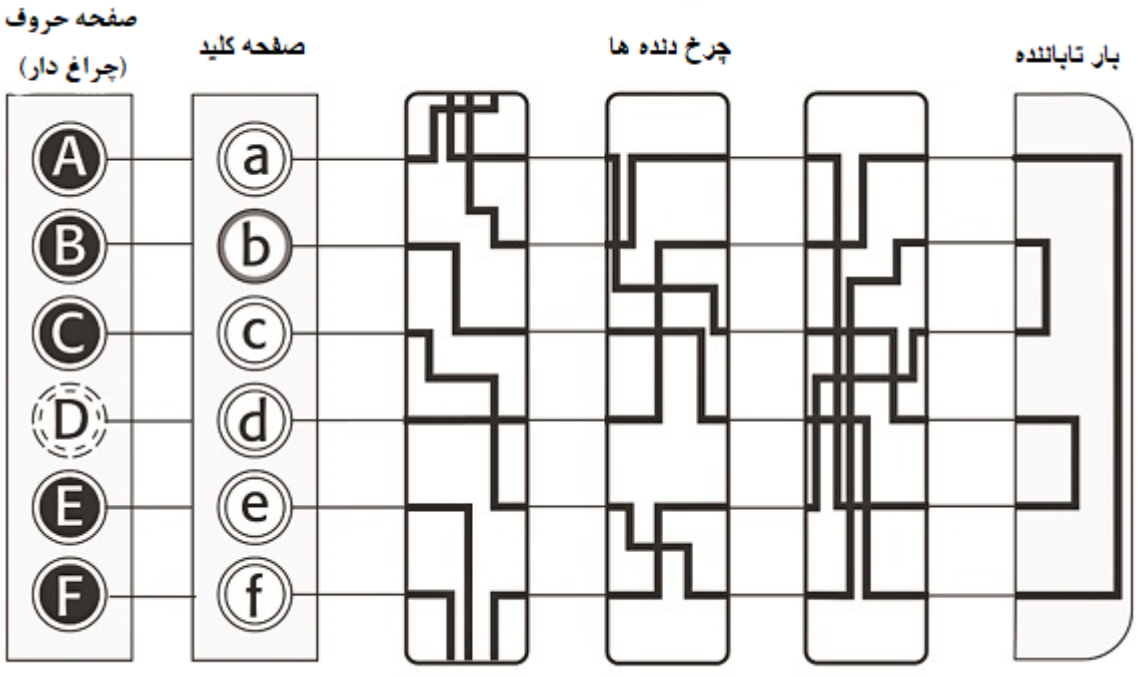
اگر آدم سمجی پیدا می‌شد که بتواند در هردقیقه یکی از کلیدهای انگیما را آزمایش کند، آزمودن کل کلیدهای آن بیش از عمر کنونی جهان به طول می‌انجامید!

گرچه لهستان در نهایت از هر دو سو مورد تعرض قرار گرفت (در جنگ دوم به اشغال آلمان درآمد و پس از آن به حیاط خلوت شوروی تبدیل شد)، اما همین هراس از موقعیت خطرناکش باعث شد رمزگشایی از انیگما را دنبال کند. در پروژه‌ای که لهستان به این منظور آغاز کرد، شاید نخستین‌بار در تاریخ بود که ریاضی‌دانان برای رمزگشایی نظامی به کار گماشته شدند. از این گروه، ریاضی‌دان جوانی به نام ماریان ریفسکی (Marjan Rejevski)توانست در چند مرحله تا سال 1932 روشی برای رمزگشایی از انیگما پیدا کند. وی دریافت که اثر صفحه پیوندها را می‌توان به کلی از کار چرخ‌دنده‌ها جدا کرد و مسئله را به این ترتیب به دو مسئله ساده‌تر (اگرچه هنوز بسیار پیچیده) فروکاست. اما کلید واقعی رمزگشایی از انیگما را خود آلمانی‌ها به دست لهستانی‌ها دادند.

برای امنیت بیشتر، آلمان ها مرحله تازه‌ای را به رمزگردانی انیگما افزوده‌بودند: هر پیام با کلیدی سه‌حرفی آغاز می‌شد که آرایش چرخ‌دنده‌ها را برای آن پیام مشخص می‌کرد. این کلید سه‌حرفی توسط فرستنده و به شکل تصادفی انتخاب می‌شد. برای نمونه، یک فرستنده ممکن بود پس از تنظیم کردن فرستنده خود با کلید روز، سه حرف KHW را در آغاز پیام خود بفرستد. این به آن مفهوم بود که این فرستنده، پس از فرستادن آن حرف‌ها با کلید روز، چرخ‌دنده‌هایش را روی KHW قرار می‌داد و متن پیام اصلی را می‌فرستاد. گیرنده که خود کلید روز را داشت، می‌توانست این کلید را رمزگشایی کرده و با تنظیم کردن دستگاه انیگمای خود با این سه حرف (KHW)، ادامه پیام را رمزگشایی کند. اما برای آن که گیرنده حتماً بتواند کلید تصادفی را درست دریافت کند، فرستنده باید کلید تصادفی را دو بار پشت سر هم می‌فرستاد.

ریفسکی از همین تکرار برای رمزگشایی از انیگما سود جست: هر روز صدها کلید تصادفی با استفاده از کلید آن روز فرستاده می‌شد که در هر کدام یک تکرار وجود داشت. ریفسکی به کمک همکارانش آرشیو عظیمی از کلیدها تهیه کرد که می‌شد آن را با کلیدهای تصادفی فرستاده شده در هر پیام مقایسه کرد و کلید اصلی را دریافت.

وی برای این کار ماشین رمزگشای بزرگی به نام Bomba (همان بمب در زبان لهستانی) ساخت که الهام‌بخش نمونه بعدی آن در انگلیس شد. اکنون لهستان می‌توانست پیام‌های آلمانی‌ها را رمزگشایی کند و از هر کشور دیگری در این زمینه ده سال جلوتر بود. اما چنان که می‌دانیم، این دستاورد برای خود لهستان چندان فایده‌ای نداشت. کمی پیش از آغاز جنگ، آلمانی‌ها شمار چرخ‌دنده‌های انیگما را به پنج افزایش دادند.



شکل۴: نمونه ساده شده دستگاه انیگما که یک «صفحه پیوند» هم به آن افزوده شده است.

همه آرشیو ریفسکی بی‌فایده شد و در ضمن سیم‌کشی درون چرخ‌دنده‌های تازه نیز مورد نیاز بود. برای رمزگشایی از انیگمای تازه، ماشین بمب بزرگتری (ده برابر نمونه موجود) لازم بود که لهستانی‌ها بودجه کافی برای ساختنش را نداشتند. اما آن‌ها در نهایت توانستند دست‌کم سیم‌کشی درونی این چرخ‌دنده‌های تازه را نیز بیابند. رئیس اداره رمزگشایی لهستان، سرگرد لنگِر (Langer)، نقش عجیبی در این میان داشت. وی تقریباً هر ماه کلیدهای رمز را از طریق همان رابط نخست، یعنی هانس تیلوشمیت، دریافت می‌کرد، اما ریفسکی و دیگران را از این موضوع آگاه نمی‌کرد. او پیش‌بینی می‌کرد که اگر جنگی درگیرد، گرفتن کلیدهای رمز از تیلوشمیت ممکن نخواهد بود، پس

ریفسکی و دیگران باید در شکستن کد ورزیده می‌شدند!

مطلب پیشنهادی

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

در روز سی‌ام ژوئن 1939، لنگر به همتایان انگلیسی و فرانسوی خود تلگراف زد و آنان را به لهستان فراخواند. در لهستان، آنان با دستاوردهای شگرفی روبه‌رو شدند که به راستی فراتر از پندارشان بود. فرانسوی‌ها شاید با آمیزه‌ای از شادی و شرم ماشین بزرگ کدشکن لهستانی‌ها را نگریستند، زیرا همه کار لهستانی‌ها بر پایه اطلاعاتی بود که جاسوس فرانسوی (با نام رمزی رکس) از تیلوشمیت گرفته بود و خود فرانسوی‌ها آن را دارای ارزش بررسی جدی ندانسته بودند! لنگر مصمم بود دستاوردهای گروهش به متحدان لهستان انتقال یابد تا در صورت سقوط لهستان به دنبال حمله احتمالی آلمانی‌ها، این فناوری و تلاش‌هایی که برای به دست آوردنش شده بود، تباه نشود.
اگرچه دوراندیشی لنگر در ورزیده کردن تیمش برای زمان جنگ چندان به کار نیامد، درایت او در این زمان باعث شد همه دستاوردهای لهستانی‌ها (از جمله دو دستگاه انیگمای کامل) به فرانسه و انگلیس داده شود. اگر غیر از این بود، شاید هرگز انگیزه کافی برای شکستن کد انیگما در انگلیسی‌ها ایجاد نمی‌شد.

برای مطالعه قسمت بعد 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 سوم و آخر)

تاریخ انتشار:

19 دی 1396

نشانی منبع:
https://www.shabakeh-mag.com/are-network/11363/%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%AF%D9%88%D9%85