



# فصل اول: مقدمات درس

امنیت سیستم‌های کامپیوتری

ابوالفضل دیانت

آخرین ویرایش: ۲۵ بهمن ۱۴۰۱ در ساعت ۱۱ و ۲۲ دقیقه - نسخه ۱.۲.۱

# یک صفحه Login



Lovebirds

Welcome to Lovebirds

Users name or Email

David Brooks

Password

\*\*\*\*\*

[Forgot password?](#)

Sign in

or

Sign in with Google

New Lovebirds? [Create Account](#)

```
SELECT * FROM `accounts` WHERE `username`='?' AND password='?';
```



اوپرای خوب بود تا زمانی که هکرها آمدند. او فهمید چه Query اجرا می‌شود (حدس زدن ساختار پایگاه داده یا استفاده از اشتباہ پیاده‌ساز).

در ادامه کافی است که به جای Username مقدار ' or 1=1 LIMIT 1;-- ' را وارد کنیم.

```
1 SELECT * FROM `accounts` WHERE `username`=' or 1=1 LIMIT 1; --' AND  
password='Sa';
```

معمولًا اولین Username برای admin است.

یک حمله SQL Injection بسیار ساده، روش‌های مقابله با آن را می‌دانیم و یا حداقل توصیه می‌شود ....

# تعريف غیررسمی امنیت

نکته ۱

حافظت از هر آن‌چه برای ما مهم و ارزشمند است؟!



# هکرها



Michael Calce



Steve Wozniak and Steve Jobs



Gary McKinnon



Anonymous



Richard Matthew Stallman



من خیلی از این مطالب را از سایت‌هایی که در اینترنت بوده جستجو کردم و برداشتمن.

Gary McKinnon (گری مک‌کینون) هماهنگی بزرگترین هک نظامی دنیا را مدیریت کرده است، و توانسته بین سال‌های ۲۰۰۱ تا ۲۰۰۲ به صورت غیرمجاز به ۹۷ کامپیوتر متعلق به ناسا و ارتش آمریکا حمله کند. او ادعا کرده که هدف وی تنها دسترسی به اطلاعاتی بوده که دولت از آدمهای فضایی و دسترسی به انرژی آزاد از مردم مخفی نگه داشته است. گرچه ظاهرا او فایل‌های مهم زیادی را پاک کرده و ۳۰۰ کامپیوتر را از کار انداخته و در حدود ۷۰۰ هزار دلار خسارت وارد کرده است. فعلاً در انگلیس است.

Steve Jobs (استیو وازنیک) و Steve Wozniak که هر دو از بنیانگذاران شرکت اپل بودند. اما در روزگار جوانی کارهای هکری نیز می‌کردند. آن‌ها موفق شدند وسیله‌ای به نام Blue Box طراحی کنند که به مردم اجازه می‌داد بدون هزینه به مدت ۷ دقیقه و ۴۳ ثانیه مکالمه رایگان داشته باشند. بیشتر مشتریان آن‌ها دانشجویانی بودند که برای تحصیل به آمریکا می‌رفتند و قصد داشتند برای ارتباط برقرارکردن با خانواده خود هزینه کمتری

بپردازند. اما این سیستم چگونه کار می‌کرد؟ در گذشته، شرکت‌های مخابراتی برای برقراری تماس و اطلاع از وضع آن مجبور بودند از همان کانالی که صوت منتقل می‌شود، اطلاعات کنترلی خود را نیز ارسال کنند. برای اینکار از فرکانس‌های متنوع صوتی برای مخابره اطلاعات تماس استفاده می‌شد. این اصوات که مانند یک زبان برنامه‌نویسی سوییچ‌های بین راه را تنظیم می‌کردند. مثلاً با ایجاد فرکانس 2600 هرتز می‌توانند ارتباط را ریست کنند و این ویژگی به آن‌ها اجازه می‌داد بدون پرداخت پول، تلفن بزنند چرا که مخابرات با شنیدن فرکانس 2600، تصور می‌کرد که ارتباط از طریق گذاشتن گوشی قطع شده. در یک هک مشهور، استیو وزنیاک از طریق یک جعبه آبی به کشور واتیکان که مقر مرکزی کلیسای کاتولیک است زنگ زد و با تقلید لهجه آلمانی هنری کسینجر درخواست کرد تا فوراً با پاپ صحبت کند (که البته به خاطر خواب بودن پاپ، تماس برقرار نشد).

در فوریه ۲۰۰۰ فردی به نام Michael Calce (میشاپل کاسه) با نفوذ به شبکه دانشگاه و با استفاده از منابع DDoS (Denial Of Service)، موتور جستجوی شماره یک در آن زمان (یا هو) را هک کرد. در عرض یک هفته او با استفاده از

tributed Denial Of Service) وبسایت‌های شرکت‌های Amazon، CNN، eBay، Dell و tributed Denial Of Service)

تخرب و بسایت‌های آن‌ها شد. این پرسش در ذهن خیلی‌ها در آن زمان شکل گرفت که اگر بزرگ‌ترین وب‌سایت‌های جهان، می‌توانستند به این سادگی توسط هکرها به حاشیه رانده شوند، آیا دیگری امنیتی در دنیای اینترنت باقی می‌ماند؟ اغراق نیست اگر بگوییم توسعه قانون جرایم اینترنتی به لطف او ناگهان به یک اولویت اصلی دولت تبدیل شد.

در دنیای مجازی به عنوان هکر شناخته نمی‌شود بلکه اورا به عنوان Richard Matthew Stallman رهبر مبلغان نرم افزارهای آزاد می‌شناسند. اما همین رهبر به علت قدرتی که در برنامه نویسی دارد هکر ماهری هم هست. در ضمن او از دشمنان سرسرخ مایکروسافت است. در دسته بندی هکرها یک هکر کلاه سفید است و در دنیای مجازی تا به حال خرابکاری نکرده ولی مانند هر هکری به حریم شخصی اعتقاد ندارد و می‌گوید تمام اطلاعات دنیا باید به اشتراک گذاشته شود. این هکر آمریکایی کنفرانس‌های بسیاری درباره هک و هکرها برگزار کرده و چهره هکرهای واقعی را به دنیا نشان داده است. یکی از کارهای معروف او هک کردن قوی‌ترین سیستم امنیتی مایکروسافت است. استالمن درحالی که نماینده مایکروسافت در کنفرانس و در حال توضیح دادن همین مثلا

قوی ترین سیستم امنیتی بود به شبکه نفوذ کرد و در مقابل همه حضار و تنها در مدت ۸ دقیقه، نرم افزار را هک کرد و در فهرست سیاه مایکروسافت قرار گرفت.

در حقیقت یک جنبش است که به طور ناشناس فعالیت می‌کند. بیشترین معروفیت آن، حملات سایبری علیه دولت‌ها و شرکت‌های بزرگ است. هر کسی می‌تواند عضو این جنبش بشود، پس بهتر است گفته شود که این گروه ناشناس، از تعدادی هکر متعلق به کشورهای مختلف جهان تشکیل شده است. عملاً رهبر واحدی ندارند و حتی بسیاری از اعضایشان همدیگر را نمی‌شناسند.

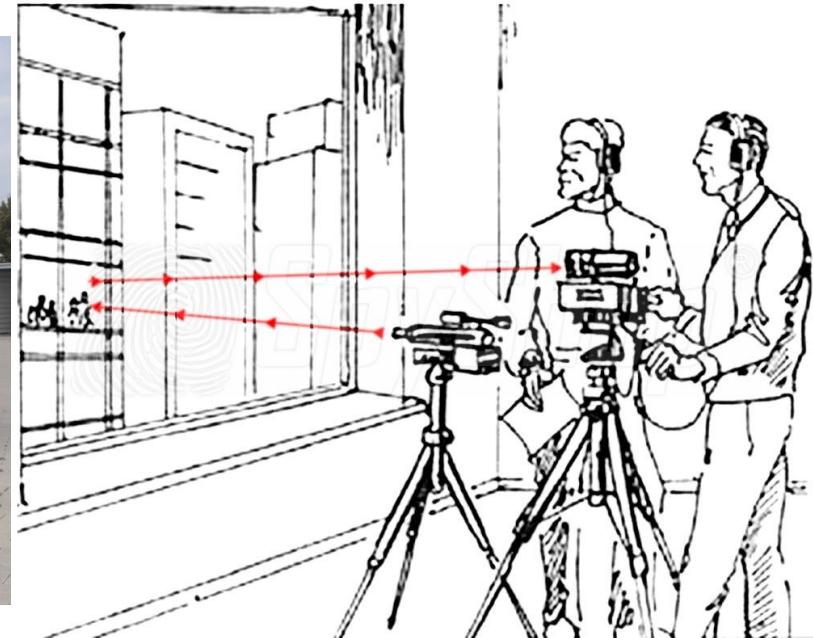
هکرهای بر حسب میزان دانش و هدف‌شان به چندین دسته تقسیم‌بندی می‌شوند. سعی می‌کنیم برخی از این دسته‌ها را در اینجا تشریح کنیم:

- **کلاه سفید:** این دسته از هکرهای، به صورت قانونی (با گرفتن اجازه) با هدف بالابردن ضریب امنیتی سامانه‌های یک سازمان، اقدام به نفوذ به این سامانه‌ها می‌کنند. دانش بسیار زیادی در این حوزه دارند، و به نوعی یک هک اخلاقی یا یک متخصص امنیتی محسوب می‌شوند.

- **کلاه سیاه:** این دسته از هکرها، به صورت غیر قانونی با هدف تخریب و سرقت اطلاعات، اقدام به نفوذ به سامانه‌های یک سازمان می‌کنند. دانش بسیار زیادی در این حوزه دارند، ولی به نوعی یک هکر غیراخلاقی محسوب می‌شوند (Cracker).
- **کلاه خاکستری:** گاهی نقش یک هکر کلاه سفید را دارند و گاه کلاه سیاه. مثلاً بدون اجازه به سامانه نفوذ می‌کنند، ولی تلاش می‌کنند باگ پیدا شده را در اختیار قربانی قرار دهند. این هکرها عموماً با اهداف تفریحی دست به این کار می‌زنند.
- **کلاه قرمز:** به نوعی شبیه هکرهاي کلاه خاکستری یا حتی کلاه سفید هستند. آنها به نوعی به مبارزه با هکرهاي کلاه سیاه می‌پردازند، ولی در این مبارزه هیچ مرز اخلاقی را رعایت نمی‌کنند. آنها بیرحمانه به هکرهاي کلاه سیاه حمله می‌کنند و به نوعی قصد نابودی آنها را دارند.
- **کلاه سبز:** عموماً دانش کمی در این حوزه دارند و به تازگی وارد حوزه هک شدند. گرچه آنها در تلاش هستند که سطح دانشی خود را در این حوزه بالا ببرند و به یک هکر حرفه‌ای تبدیل شوند.

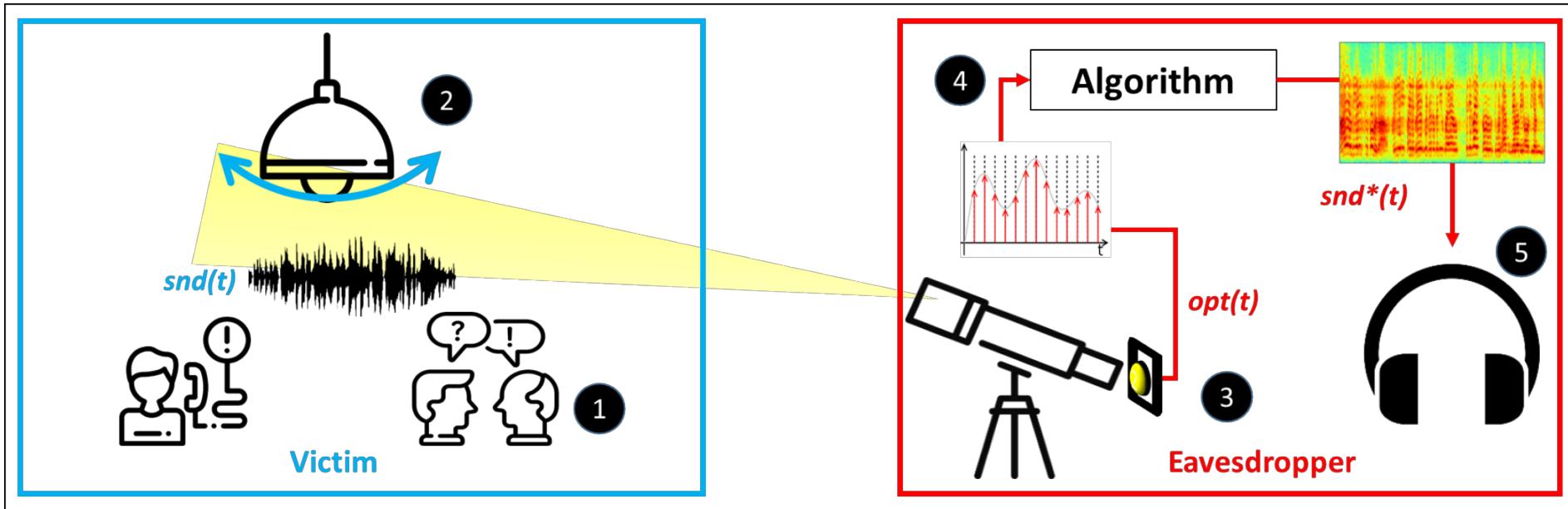
- کلاه صورتی: معمولاً دانش چندانی در این حوزه ندارند، و فقط به منظور جلب توجه و یا آزار و اذیت دیگران دست به هک می‌زنند.
- جوجه هکر یا Script Kiddie: به نوعی یک هکر آماتور است که لزوماً توانایی برنامه‌نویسی و دانش کافی برای یک حمله را ندارد. آن‌ها معمولاً از برنامه‌های خرابکارانه موجود استفاده می‌کنند و یا حتی ممکن است با پرداخت پول آن را تهییه کنند. سپس با استفاده از آن حمله هکی را بدون هیچ هدفی اجرا کنند. علی‌رغم دانش پایین این افراد، می‌توانند آسیب جدی به قربانیان خود وارد کنند.

# تلایشی برای شنود ...



- صوت یک موج مکانیکی است که برای انتشارش نیاز به ماده دارد (نوسان مولکول‌های هوا)
- می‌توان از انعکاس پرتو لیزری این ارتعاش را بازیابی کرد.

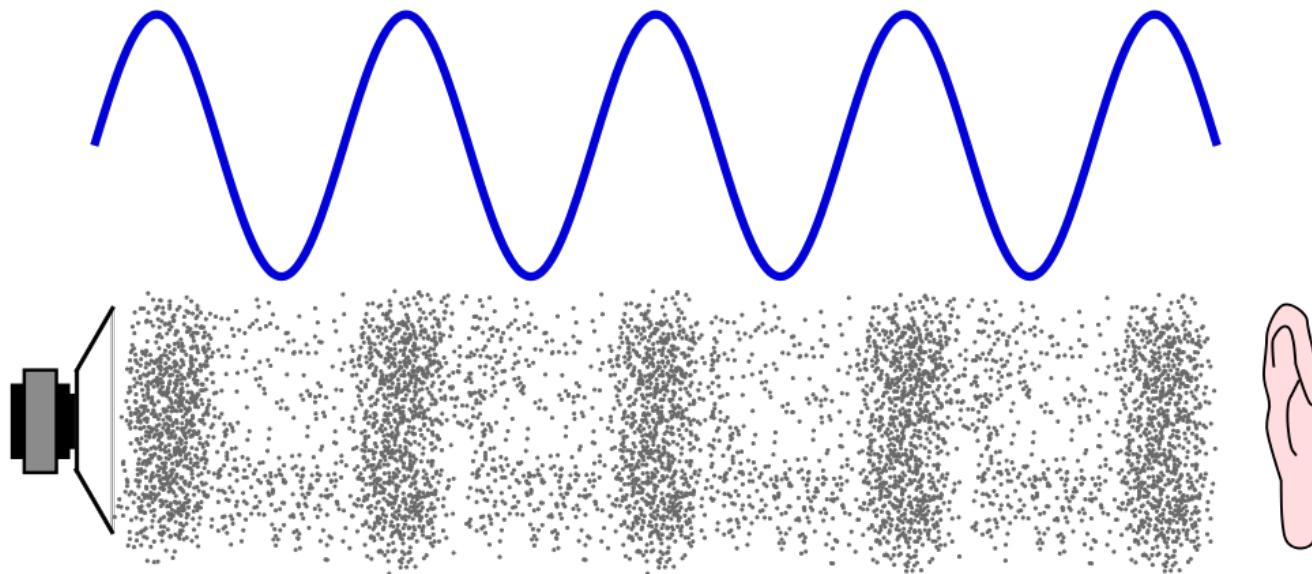
# تلاشی برای شنود ... (ادامه)



☞ این ایده برای سال ۱۹۴۷ بود، اما می‌توان با یک تشخیص‌دهنده به سادگی پی به حمله برد.

(BlackHat 2020) Lamphone تا Visual Microphone از ☞

نکته ۲ امنیت حوزه بسیار گستردگی است.



می دانیم که صوت یک موج مکانیکی است، یعنی برای انتشار نیاز به محیط مادی دارد. در حقیقت وقتی شما صحبت می کنید، به مولکول های هوای که در اطراف دهان شما هست فشار وارد می کنید و این فشار موجب نوسان این مولکول ها می شود. این نوسانات ادامه می یابد تا این که به سطح برخورد کند. دقیقاً به مانند نحوه کار کرد میکروفون، این نوسانات می توانند سطوح را تحت تاثیر خود قرار دهد. اگر ما بتوانیم به نحوی این تاثیر را تشخیص دهیم و آشکار کنیم، می توانیم یک میکروفون بسازیم.

در یک میکروفون لیزری (Laser microphone)، با استفاده از پرتوهای لیزر می توان ارتعاشات صدا در جسمی

که در فاصله دوری قرار گرفته است، مورد ارزیابی و آشکارسازی قرار داد. پرواضح است که این ابزار در درجه نخست با اهدافی نظیر شنود (Eavesdropping) بکار گرفته می‌شود. گرچه شاید این فناوری برای ما بسیار جذاب باشد، اما جالب است بدانید که این ایده، با Leon Theremin از اتحاد جماهیر شوروی در سال ۱۹۴۷ آغاز شد. او سیستم استراق سمع Buran را به طور خاص با این تکنیک توسعه داد. در داخل اتاقی که مکالمه در آن در حال انجام است و ما قصد شنود آن را داریم، یک جسم با قابلیت ارتعاش و ترجیحاً با سطحی صاف (تا پرتو لیزر را به خوبی منعکس کند) انتخاب می‌شود. پرتو لیزر از طریق یک پنجره به داخل اتاق فرستاده می‌شود. سپس این پرتو از جسم به گیرنده منعکس می‌شود، و در نهایت به سیگنال صوتی تبدیل می‌گردد.

با کمی دقیقت می‌توان دریافت که با یک آشکارساز پرتوهای لیزری، فرد قربانی به راحتی می‌تواند دریابد که مورد حمله شنود قرار گرفته است. برای جلوگیری از آشکار شدن این حمله، بعدها ایده‌ای با عنوان Visual Microphone داده شد. در این روش با استفاده از یک دوربین فوق سریع با قابلیت ثبت چندین هزار تصویر در ثانیه، سعی در ثبت ارتعاش اجسام در محیط می‌کنند. گرچه به دلیل حجم بسیار سنگین پردازشی، برای شنود

پنج ثانیه از مکالمه، نیاز هست چیزی در حدود دو تا سه ساعت عملیات پردازشی انجام شود.

ایده Lamphone در کنفرانس Blackhat 2020 برای نخستین بار مطرح گشت. سعی شده است که ایده‌ای مطرح شود که بتوان به صورت بی‌درنگ (Realtime) و بدون آشکارشدن حمله، حمله شنود را انجام داد. در این ایده که مطالعه جزئیات آن را به عهده خواننده گذاشته می‌شود، از تاثیر ارتعاش لامپ‌های نصب شده در اتاق قربانی، و همچنین واکنش نور لامپ به این ارتعاش، بهره گرفته شده تا بتوان یک حمله شنود موفق را انجام داد.

# چند کنفرانس مشهور



Jeff Moss (DefCon & BlackHat)



Def Con (CTF)



Hope



Positive Hack Days (The Standoff)

Jeff Moss در سال ۱۹۹۳ یک مهمانی خداحافظی برای یکی از دوستانش ترتیب داده بود. گرچه به خاطر بروز مشکلی، مهمانی برگزار نشد، ولی او تصمیم گرفت که صد نفر از دوستانش که همگی هکر بودند را به لاس و گاس دعوت کند تا یک مهمانی جایگزین تشکیل دهند. این رویداد برای بسیاری از شرکت‌کنندگان بسیار جذاب و جالب بود. تقاضای برگزاری این مهمانی سال‌های بعد نیز تکرار شد، و از همین نقطه بود که Def Con بوجود آمد. Def Con سبک و سیاق کنفرانس‌های رسمی را ندارد، و عملاً یک دورهمی بین هکرهای سرتاسر دنیا محسوب می‌شود. این دورهمی هر سال گستردگی از سال پیش شد، تا جایی که در سال ۲۰۱۹ و پیش از شیوع ویروس کورونا، تعداد شرکت‌کنندگان این رویداد به حدود ۳۰ هزار نفر رسید.

برنامه‌های Def Con در نوع خود بسیار جالب است. فتح پرچم که با عنوان CTF نیز شناخته می‌شود، شاید معرو فترین موضوعات مطرح شده در این کنفرانس باشد. این رقابت هکری بدین صورت است که تیم‌های هکرها با بهره‌گیری از نرم‌افزارها و ساختارهای شبکه، اقدام به حمله و دفاع از رایانه‌ها و شبکه‌ها می‌نمایند. تقریباً هیچ‌کس و هیچ‌چیز در این کنفرانس از دست هکرها در امان نیست. تا جایی که برگزارکنندگان برای

شرکت‌کنندگان هشدار صادر نموده و موارد پیش‌گیری از هک شدن و نقض به سیستم آنان را به شرح ذیل گوش زد نمودند.

- نیاوردن تلفن همراه و یا در صورتی که تلفن همراه در اختیار دارید اصلاً به شبکه متصل نشوید.
- به شبکه کابلی و وای‌فای موجود در محل کنفرانس یا شارژر فرد دیگری متصل نشوید.
- پول نقد به همراه داشته باشید و گرنه کارت اعتباری شما هک می‌شود.
- لپ‌تاب خود را اگر کار ندارید، خاموش کنید چرا که هکرها می‌توانند آن را در حالت Sleep نیز هک کنند.

# در مسیر دستیابی به محرمانگی (Confidentiality)

LmxvgsvivdzhzgivvzmwhsvolevwzorggovylbZmwvevib-wzbgsvylbdlfowxlnvzmwsdlfowtzgsvisviovezhzmwn-zpgsvnrmglxildmhzmwkozbprmtlugsvulivhgSvdlfowx-ornyfksvigifmpzmwhdrmtuilnsviyizmxsvhzmwvzgzkk-ovhZmwgsvbdlfowkozbsrwzwmwlhvvpZmwdsvmsvdzhgrivw,svdlfowhovvkrmsvihszwvZmwgsvylbolevwgsvgi-vvevibnfxsZmwgsvgivvdzhzsckbYfggrnvdmgybZmw-gsvylbtivdlowviZmwgsvgivvdzhlugvmzolmvGsvmlmvwzbgsvylbxznglgsvgivvzmwgsvgivvhzrwXlnvYlbxlnvzmw-xornyfknbgifmpzmwhdrmtuilnnbyizmxsvhzmwvzgzkk-kovhzmwkozbrmnbhsszwzwmwyvszkkbRzngllrtglxorn-yzmwkozbhzrwsyvylRdzmgglyfbgsrmthzmwszevufm-RdzmghlnvnlmvbRnhliib,hzrwsyvgivvyfgRszevmlnlmvb-RszevmlmobovzevhzmwzkkovahGzpvnbzkkovahYlbzmwh-voogsvnrmgsvxrgbGsvmblfdrooszevnlmvbzmwblfdro-oyvszkkbZmwhlgsvylbxornywfwkgsgvgivvzmwtzgsvivw-sviakkovhzmwzkkovhZmwiwszvnlvwdzhszkkh-

- کلید چیست؟
- بزرگی فضای کلید؟
- رمزشکنی غیرهوشمندانه
- رمزشکنی هوشمندانه
- قصه چه بود؟

بالاخره باید پذیرفت که امنیت در حالت کلاسیک آن تا سال‌ها با مفهوم رسیدن به هدف محربانگی شناخته می‌شد. در اینجا ما از یک الگوریتم رمزگذاری (Encryption) ساده استفاده کردیم. در این الگوریتم هر حرف را با یک حرف دیگر از الفبای زبان انگلیسی جایگزین می‌کنیم. برای این الگوریتم، کلید را می‌توان به صورت یک رشته به مانند

*QWERTYUIOPASDFGHJKLZXCVBNM*

در نظر گرفت. این بدان معنا است که حرف A به Q نگاشت می‌شود و حرف B به W و ... . پس طول کلید در این الگوریتم برابر با ۲۶ کاراکتر است، و فضای کلید برابر با:

$$|\mathcal{K}| = 26! \approx 4 \times 10^{26}$$

یک روش غیرهوشمندانه برای تحلیل رمز (Cryptanalysis)، روش Brute-force است. در این روش تمامی حالت‌های موجود در فضای کلید با هدف رسیدن به یک متن با معنا، ارزیابی می‌شود. اگر یک کامپیوتر با قدرت ۱۰ petaFLOPS (هر یک petaFLOPS یعنی  $10^{15}$  محاسبه در ثانیه) در اختیار داشته باشیم، حدود ۱۲۶۸ سال

باید برای رمزشکنی این متن منتظر بمانیم.

$$\text{Time} = \frac{4 \times 10^{26}}{10^{16}} = 4 \times 10^{10} \text{ [Sec]} \approx 1268 \text{ [Year]} \odot \odot$$

اما اگر کمی هوشمندانه‌تر عمل کنیم، اوضاع خیلی بهتر می‌شود. به عنوان مثال ببینیم که کدام حرف‌ها در متن رمز (Ciphertext) فرکانس تکرار بیشتری دارند. حرف‌های یاد شده احتمالاً حروف پرتکراری مثل ...T,E,A... است. حتی می‌توان پارا فراتر گذاشت و دو حرفی‌های پرتکرار را در نظر گرفت. این دو حرفی‌های پرتکرار احتمالاً TH خواهد بود. با حدس برخی از حروف و جایگذاری آن‌ها در متن می‌توان برخی کلمات را حدس زد و از روی آن برخی حروف دیگر را بدست آورد. اگر ما تنها پنج حرف را بتوانیم حدس بزنیم، خواهیم داشت:

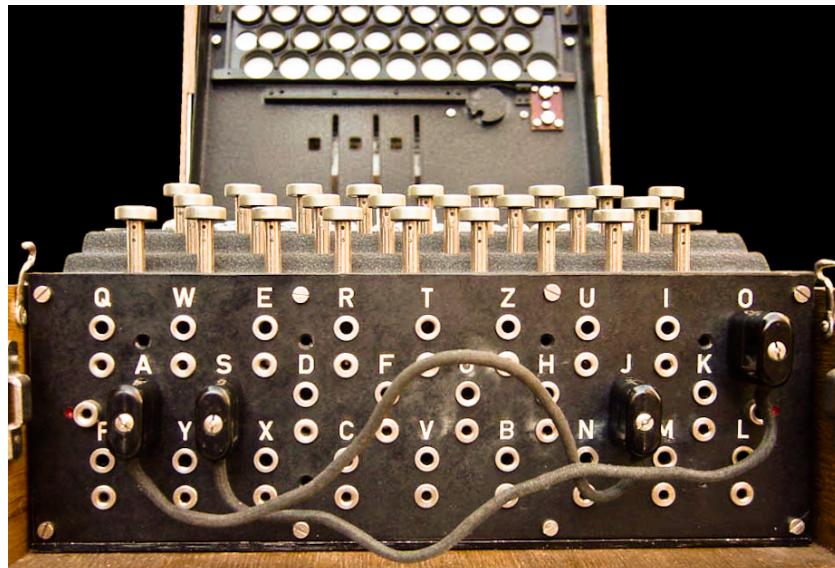
$$|\mathcal{K}| = 21! \approx 5 \times 10^{19}$$

$$\text{Time} = \frac{5 \times 10^{19}}{10^{16}} = 5 \times 10^3 \text{ [Sec]} \approx 83 \text{ [Min]} \odot \odot$$

آیا شما می‌توانید نوشته من را رمزگشایی کنید؟ قطعاً محتوای آن برای شما جذاب خواهد بود.

ofrugltqOfrcitfitcolmaktritcgwsrlstthafitkliortOfrmitzgbsgxtrmitmkttxtkbdweiOfrmitmktt  
coliohhbZwmmadtctfmzbOfrmitzgbuktcgsrtkOfrmitmkttcolgymtfosgftMitfgftrobmitzgbeo  
dtmgmitmkttofrmitmkttloarEgdtZgbegdofresadzwhdbmkwfqofrlcafuykgddbzkofeitlofrtom  
ohhstlofrhsobafdbliortofrztiohhbAodmgzaumgesadzofrhsobloarmitzgbAcofmmgzwbmiaful  
ofrioxtywfAcofmlgdtdgftbAdlgkkbloarmitmktzwmAioxtfgdgftbAioxtgfsbstoxtlofrohhstlM  
oqtdbohhstlZgbofrltssmitdafmiteambMitfbgwcassioxtdgftbofrbgwcassztiohhbOfrlgmitzgbes  
adztrwhmitmkttofruomitktritkohhstlofreokkatrmitdocobOfrmitmkttcoliohhbZwmmitzgbl  
mobtrocobygkosgfumadtofrmitmktcollorOfrmitfgftrobmitzgbeodtzoeqofrmitmktliggqca  
mipgbofrlitloarEgdtZgbesadzwhdbmkwfqofrlcafuykgddbzkofeitlofrztiohhbAodmggzwlbm  
gesadzmkttlloarmitzgbAcofmoigwlmgqtthdtcokditloarAcofmocaytofrAcofmeiasrktfofrlgA  
fttroigwltEofbgwuaxtdtoigwltAioxtfgigwlloarmitmktMitygktmladbigrwtzwmbgwdoe

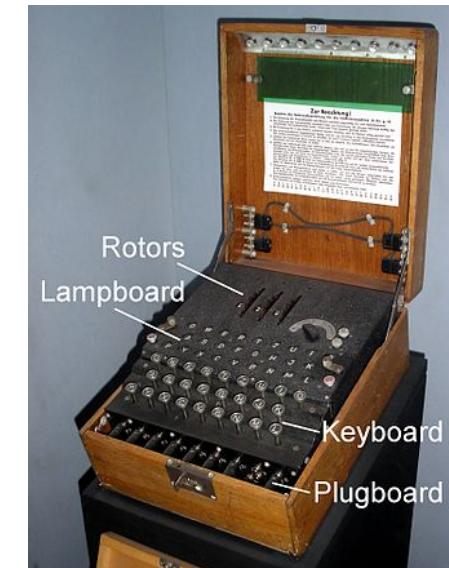
# Enigma



Bombe



Alan Turing

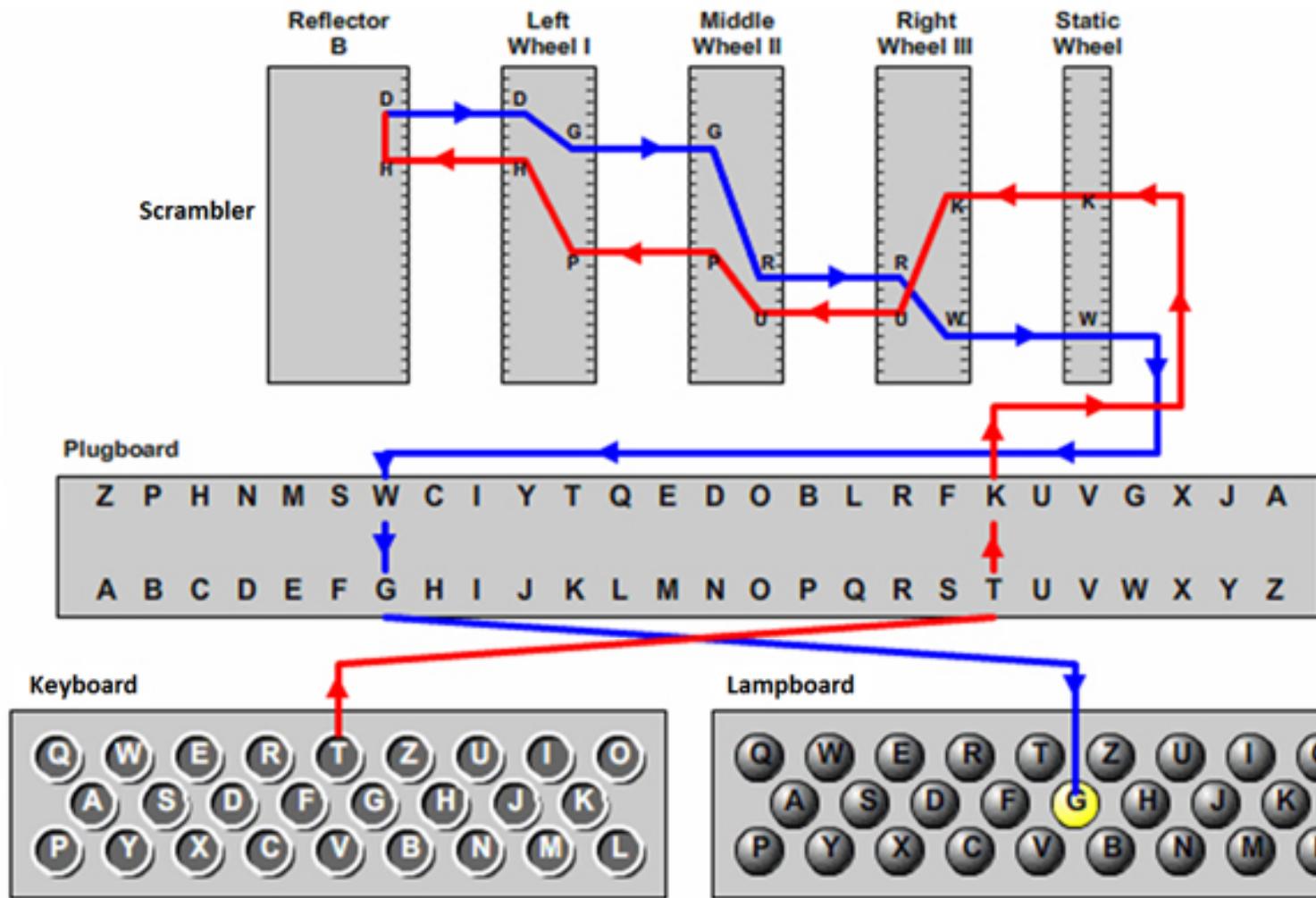


Enigma Machine

ماشین انیگما، یک دستگاه الکترومکانیکی رمزنگاری بود که به ویژه توسط آلمان‌ها در جنگ جهانی دوم بکار گرفته شد.

فشردن کلید (۲۶ حرف) + عملیات جانشینی در Plugboard (تا حداقل ۱۳ سیم) + هفت بار عملیات جانشینی در Rotorها + روشن شدن لامپ (خروجی)

## Enigma Encipherment Stages



© 2006, by Louise Dade

یک فیلم خوب جهت آشنایی با این دستگاه

ماشین Enigma، بعد از پایان جنگ جهانی اول، توسط یک فرد آلمانی به نام Arthur Scherbius اختراع شد. یک سیستم الکترومکانیکی بسیار جذاب، به عنوان یک ماشین رمزگذاری. البته بعدها توسعه‌های زیادی بر روی این ماشین انجام شد. Enigma از چهار بخش کلی تشکیل شده بود:

• Keyboard ❶

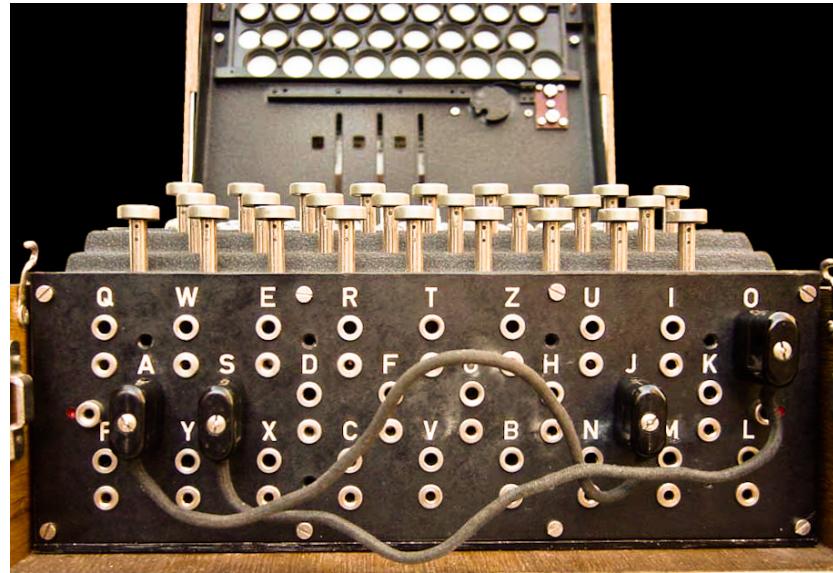
• Plugboard ❷

• Rotors ❸

• Lampboard ❹

کاربر می‌بایست حروف متن اصلی (Plaintext) را تک به تک توسط Keyboard وارد کند. با فشردن هر حرف، عملیات رمزگذاری (Encryption) آغاز شده و در نهایت یک حرف در بخش Lampboard روشن می‌شود. کاربر حرف روشن شده را باید بر روی کاغذی به عنوان متن رمز (Ciphertext) بنویسد و سپس برود سراغ رمزکردن حرف بعدی. برای رمزگشایی (Decryption) نیز دقیقاً عکس این عمل رخ می‌دهد. الگوریتم موجود در Enigma را

می‌توان در دو مرحله تشریح کرد:



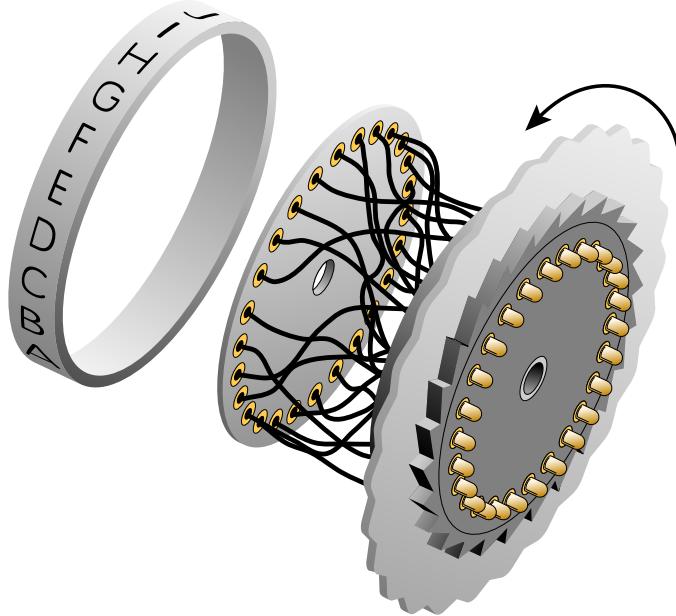
شکل ۴: Enigma Plugboard

مرحله اول: در Plugboard ما تعداد حداقل ۱۳ سیم داریم. کاربر می‌تواند بین صفر تا ۱۳ سیم را انتخاب کند. به عنوان مثال همان طور که در شکل ۴ نشان داده شده است کاربر فقط دو سیم را انتخاب کرده است. Plugboard در حقیقت یک نگاشت بین حروف ایجاد می‌کند. همان‌طور که در شکل مشاهده می‌کنید حرف A به J متصل شده. این بدان معنا است که اگر کاربر حرف A را وارد کند این حرف به J تبدیل می‌شود و بالعکس.

يعنى اگر حرف J وارد شود، به حرف A تبدیل می‌شود. این اتفاق در مورد حروف O و S نيز رخ داده است. لازم به ذکر است مابقی حروف تغییری نخواهد کرد. مثلا عبارت YELLOWJACKETS در همین مرحله اول (يعنى بعد از گذر از Plugboard) به عبارت زیر مبدل می‌شود:

YELLOWJACKETS       $\Rightarrow$       YELLSWAJCKETO

پرواضح است اين که کاربر چند سيم را انتخاب کند و اين نگاشت را چگونه انجام دهد، بخشی از عبارت کلید را برای ما تشکیل می‌دهد.



Enigma Rotors

**مرحله دوم:** در ماشین انیگما، تعداد پنج چرخ دنده وجود داشت که می‌بایست سه چرخ از میان انتخاب می‌شد و در جایگاه مورد نظر قرار می‌گرفت. هر چرخ دنده، در حقیقت یک نگاشت‌دهنده بین حروف بود. پر واضح است که هر چرخ دنده نگاشت متفاوتی را برای ما به ارمغان می‌آورد. در نهایت نیز یک چرخ دنده ثابت به نام Reflector که هر چرخ دنده نگاشت متفاوتی را برای ما به ارمغان می‌آورد. در نهایت نیز یک چرخ دنده ثابت به نام Reflector قرار داشت. هر حرف که وارد چرخ دنده اول می‌شد بعد از نگاشت به یک حرف دیگر، وارد چرخ دنده دوم می‌شد.

این روند ادامه می‌یافت تا حرف خروجی چرخدنده سوم وارد Reflector شود. در آن‌جا نیز یک نگاشت دیگر بین حروف انجام می‌شد و عملیات بازگشت آغاز می‌گشت. یعنی دوباره خروجی Reflector وارد چرخدنده سوم می‌شد و سپس از چرخدنده سوم وارد چرخدنده دوم و همین طور وارد چرخدنده اول. در نهایت نیز خروجی چرخدنده اول به Lampboard منتقل شد. با کمی دقیق می‌توان دریافت که در این مرحله تا هفت مرتبه عملیات نگاشت یک حرف با حرف دیگر انجام می‌شود.

نکته جالب در این مرحله، حرکت سه چرخدنده بود. در واقع با وارد شدن هر حرف، چرخدنده اول یک گام حرکت می‌کرد. وقتی چرخدنده اول یک دور کامل می‌زد، چرخدنده دوم یک گام حرکت می‌کرد، و به طور مشابه وقتی چرخدنده دوم یک دور کامل می‌زد، چرخدنده سوم یک گام به جلو می‌رفت. دقیقاً به مانند عقربه‌های ثانیه‌شمار، دقیقه‌شمار و ساعت‌شمار در یک ساعت. حالت اولیه سه چرخدنده را باید به عنوان بخشی از کلید محسوب کرد، چراکه بر حسب این حالت اولیه، خروجی این هفت مرحله نگاشت قطعاً متفاوت می‌شد. پس کاربر برای رمزگشایی، می‌بایست، سه چرخدنده درست را در جایگاه صحیحش قرار دهد (ترتیب قرار گرفتن مهم

است)، و سپس وضعیت اولیه آن‌ها را به درستی تنظیم کند. بدیهی است که برای هر چرخدنده مامی توانیم ۲۶ حالت مختلف برای وضعیت اولیه داشته باشیم.

در ادامه اجازه دهید فضای کلید را برای ماشین Enigma محاسبه کنیم. برای راحتی، ما کار را از چرخدنده‌ها شروع می‌کنیم. در ماشین انیگما، تعداد پنج چرخدنده وجود داشت که می‌بایست سه چرخ از میان انتخاب می‌شد و در جایگاه مورد نظر قرار می‌گرفت. به دلیل این که ترتیب چرخدنده‌ها مهم است، خواهیم داشت:

$$P_3^5 = 60$$

هنگامی که چرخدنده‌ها در جال خود قرار می‌گرفت، فرد مورد نظر می‌توانست آن را در یکی از ۲۶ حالت ممکن قرار دهد. در حقیقت سه مقدار حالت اولیه برای سه چرخدنده داشتیم. بدین‌سان خواهیم داشت:

$$26^3 = 26 \times 26 \times 26 = 17576$$

می‌توانست تا حدود زیادی می‌توانست فضای کلید را گسترش دهد. همان‌طور که بیان شد، روش Plugboard

کار این گونه بود که تعدادی سیم وجود داشت که توسط هر سیم می‌توانستیم یک جفت حرف را به یکدیگر نگاشت کنیم. بین صفر تا ۱۳ سیم برای این کار در نظر گرفته شده است. گرچه آلمان‌ها معمولاً ۵ سیم را انتخاب می‌کردند، و کمی جلوتر ما علت این کار را به خوبی درک خواهیم کرد. اجازه دهید برای این‌که مساله ۲۶ را براحتی بتوانیم درک کنیم فرض کنیم به عنوان یک مثال عددی، ۵ سیم رنگی با رنگ‌های متمایز داریم. جایگاه برای حروف نیز داریم. پر واضح است که  $\binom{26}{2}$  حالت مختلف وجود دارد که بتوان دو تا از این ۲۶ جایگاه را برای سیم اول (مثلاً سیم با رنگ قرمز)، انتخاب کرد. برای سیم دوم با توجه به اشغال دو جایگاه، ۲۴ جایگاه دیگر باقی می‌ماند و تعداد حالت‌ها نیز برابر با  $\binom{24}{2}$  خواهد شد. این کار را می‌توان ادامه داد، و در نهایت تعداد کل حالت‌ها را برای ۵ سیم به صورت زیر نوشت:

$$\binom{26}{2} \times \binom{24}{2} \times \dots \times \binom{8}{2} = \frac{26!}{(26 - 2 \times 10)! 2^{10}} = \frac{26!}{6! 2^{10}}$$

ولی ما می‌دانیم که در این جاترتیب بسته شدن سیم‌ها اهمیتی ندارد، در واقع ما با ده سیم یکسان مواجه هستیم.

پس خواهیم داشت:

$$\frac{26!}{6!2^{10}10!}$$

برای  $p$  سیم این رابطه را می‌توان به صورت کلی به صورت زیر نوشت:

$$\frac{26!}{(26 - 2p)!} \cdot \frac{1}{2^p p!}$$

در رابطه فوق این که چند سیم از مجموع ۱۳ سیم انتخاب شود، وارد بازی نشد. بالاخره کاربر یا سیمی انتخاب نمی‌کند یا یک سیم یا دو سیم یا .... . به دلیل این که واقعاً آلمان‌ها معمولاً از ده سیم استفاده می‌کردند و از محاسبه این موضوع صرف نظر می‌کنیم. آیا می‌توانید بگویید که چرا آلمان‌ها ده سیم را انتخاب کردند؟ چرا مثلاً از هر ۱۳ سیم یعنی یک نگاشت کامل استفاده نمی‌کردند؟ به طور مجموع برای هر دو مرحله خواهیم داشت:

$$|\mathcal{K}| = 158,962,555,217,826,360,000 \approx 1.6 \times 10^{20}$$

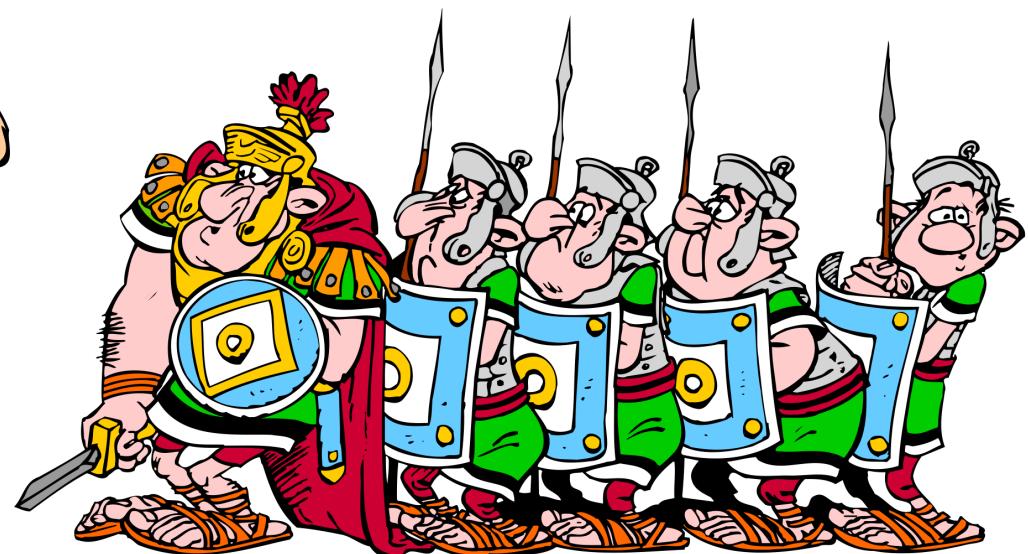
# (ادامه) Enigma



فیلم بازی تقلید (The Imitation Game)

هیچ‌گاه نباید امنیت را به لونرفتن خود الگوریتم گره زد.

امنیت حوزه‌ای است پویا و زنده. چرا؟! دشمن داریم، مهم است هم سیاسی و هم مالی



در ابتدا گفته می‌شد که هیچ‌کس نمی‌تواند رمز Enigma را بشکند. دقت کنید ما در زمانی هستیم که اصلاً خبری از کامپیوترها و محاسبات سریع ماشین وجود ندارد. لهستانی‌ها قبل‌کارهای بسیار خوبی بر روی ماشین Enigma انجام داده بودند، اما آلمان‌ها سعی کردند که این ماشین را بیش از پیش پیچیده کنند. وینستون چرچیل نخست وزیر بریتانیا دستور داد چندین جوان نابغه را دور هم جمع کنند، و هر جور که شده این مشکل (رمزنگی Enigma) حل شود. یکی از این افراد، نابغه‌ای به نام آلن تورینگ (Alan Turing) بود. آن‌ها در مقر فوق محترمانه‌ای به نام (Bletchley Park) گرد هم جمع شدند و هر روز بر روی پیام‌های شنود شده از آلمان‌ها کار می‌کردند، اما تا مدتی هیچ موفقیتی در این زمینه کسب نکردند.

تورینگ خیلی زود متوجه شد که اگر بتوان ماشینی ساخت که حالات مختلف را سریع‌تر بررسی کند، آن وقت می‌توان تعداد حالات بیشتری را در یک ثانیه مورد تحلیل قرار داد (یعنی کار انسان را ماشین انجام دهد). ماشین الکترومکانیکی به نام بامب (Bombe) حاصل این تفکر بود. البته در این میان ضعفی که خود الگوریتم Enigma داشت، اشتباه و تنبیه اپراتورهای آلمانی دستگاه رانیز نمی‌توان نادیده گرفت. این رخداد باعث شد که چرچیل

بتواند از پیام‌های نظامی آلمان‌ها با خبر بشود و از آن لحظه به بعد برای حملات و نقشه‌های آلمان‌ها آماده شود. جالب است بدانید که برای این‌که آلمان‌ها شک نکنند، عمدتاً در یکی دو حمله آلمان‌ها که چندان مهم نبود واکنشی نشان ندادند.

آلن ماتیسون تورینگ (Alan Mathison Turing) دانشمند علوم کامپیوتر، فیلسوف و ریاضیدان نابغه انگلیسی بود که امروزه به عنوان پدر علم کامپیوتر و هوش مصنوعی شناخته می‌شود (۱۹۱۲-۱۹۵۴ میلادی). در طول جنگ جهانی دوم، او به یکی از بهترین کارشناسان رمزشکنی مبدل گشت. وی در دسامبر ۱۹۴۰، با همکاری اعضای گروهش موفق به شکستن رمز Enigma نیروی دریایی آلمان شد، که از نظر ریاضیاتی بسیار پیچیده‌تر از ماشین Enigma مورد استفاده دیگر نیروها بود. فیلم The Imitation Game روایتی از همین قصه است.

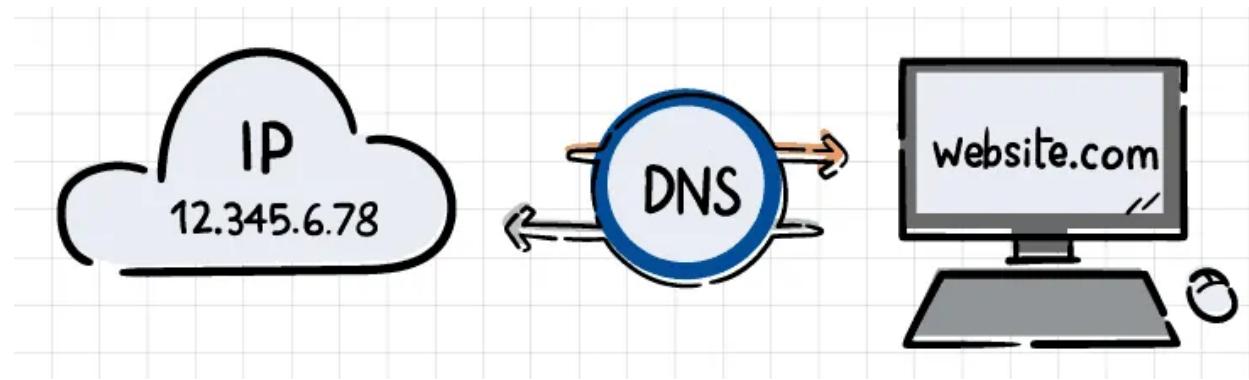
تست تورینگ که آن را با نام بازی تقلید می‌شناسیم، از جمله از کارهای دیگر او بود. در این بازی سه شرکت‌کننده داشتیم: یک مرد، یک زن و نفر سومی که می‌تواند مرد یا زن باشد و تورینگ از او به عنوان بازجو یاد می‌کند.

هدف بازی تقلید این بود که بازجو که به صورت جداگانه و از طریق سیستم با این افراد در ارتباط است، تشخیص دهد که کدام یک از کسانی که با او صحبت می‌کنند، مرد است و کدام یک زن! اگر شرکت کننده زن به گونه‌ای صحبت می‌کرد که داور او را مرد تشخیص می‌داد، داوطلب زن برنده می‌شد، اما این موضوع چه ارتباطی با هوش مصنوعی و ارزیابی آن دارد؟

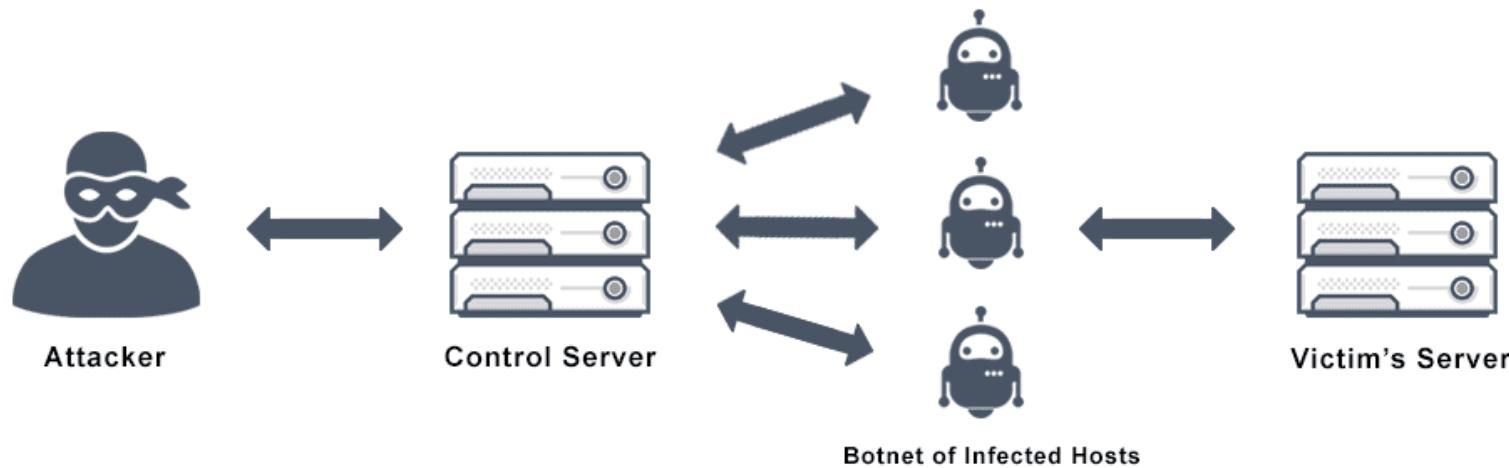
اکنون فرض کنید که جای شرکت کننده زن با رایانه (هوش مصنوعی) عوض می‌شود، به نحوی که در این زمان داور باید تشخیص دهد که کدام شرکت کننده انسان و کدام یک ربات است! در این شیوه ارزیابی اگر هوش مصنوعی قادر باشد که در بیش از نیمی از سوالات داور را فریب دهد و باعث شود که قضاوت اشتباهی انجام دهد، رایانه بر ذهن انسان پیشی می‌گیرد و برنده رقابت خواهد شد.

جایزه ACM A.M. Turing Award، سالانه از سوی ACM به اشخاصی که سهم بسزایی در زمینه کامپیوتر دارند، اعطای می‌شود. از آن جایی که جایزه نوبل برای علوم کامپیوتر وجود ندارد، از این جایزه به عنوان جایزه نوبل در کامپیوتر یاد می‌شود.

## DoS (Denial Of Service) و DNS (Domain Name System)



خدمت‌گزاران DNS به مانند دفترچه تلفنی در دنیای اینترنت



DoS حمله‌ای بر علیه دسترسی‌پذیری (Availability)

سه حمله DDoS پیچیده، هماهنگ و وسیع (۱.۲ ترابایت در ثانیه) به Dyn با استفاده از باتنت Mirai  یک بدافزار (Malware) Mirai  است که در فضای اینترنت به دنبال تجهیزات IoT می‌گردد که Username و Password پیش‌فرض آن‌ها تغییر نکرده باشد.

Please resolve [4565djfn3.tabnak.ir](http://4565djfn3.tabnak.ir)

منع خدمات برای حدود ۱۷۵۰۰۰ وبسایت نظیر Github, Netflix, Amazon, Twitter, Paypal در سال ۲۰۲۰ از تعداد صدهزار وبسایت آدم عاقل از یک سوراخ دوبار گزیده نمی‌شود! بطبق تحقیقات در سال ۲۰۲۰ فقط ۸۴.۸٪  مورد بررسی، یک خدمت‌گزار DNS تنظیم کردند [۱].

**نکته ۳** دانش شبکه خیلی خیلی مهم است + خیلی از چالش‌ها در حوزه امنیت، اشتباهات فردی است.

Mirai در حقیقت یک بدافزار است که سعی در تاثیر بر روی اشیاء هوشمند با پردازنده ARC (خانواده‌ای از IoT پردازنده‌های ۳۲ بیتی) و سیستم‌عامل Linux می‌کند. این بدافزار در فضای اینترنت به دنبال ابزارهای (Internet of Things) به مانند دوربین‌های نظارتی، تلویزیون‌های هوشمند، چاپگرهای و حتی مانیتورها می‌گردد که درگاه Telnet آن‌ها باز باشد (درگاه 23 و یا 2323)، و از سوی دیگر Username و Password پیش‌فرض آن‌ها تغییر نکرده باشد. بدین‌منظور مجموعه‌ای در حدود ۶۰ نام کاربری و رمزعبور پیش‌فرض کارخانه‌های سازنده این ابزارها مورد تست قرار می‌گیرد و در صورت عدم تغییر، Mirai به سیستم‌عامل Login کرده و وارد ابزار مورد نظر IoT می‌شود. در ادامه از سمت خدمت‌گزار خود، فایل‌های Binary لازم را بارگیری می‌کند. اکنون دستگاه مورد نظر می‌تواند بسان یک قربانی در اختیار اهداف هکرها قرار گیرد. عملاً Mirai زمانی ارزش واقعی خود را نشان می‌دهد که در تعداد زیادی دستگاه IoT پخش شود، که در این صورت شبکه‌ای از Bot‌ها تشکیل خواهد شد. در ادامه کنترل کننده Mirai می‌تواند از این Bot net ایجاد شده برای یک حمله هماهنگ و وسیع استفاده کند. Mirai نخستین بار به صورت متن‌باز بر روی وب سایت [HackForums.net](https://HackForums.net) منتشر شد. همین اتفاق منجر

شد که افراد دیگر این کد را توسعه دهند و در حملات بسیاری از آن استفاده کنند. این بدافزار، متهم اصلی چندین حمله DDoS، از جمله حمله به Dyn، در سال‌های گذشته است. شاید اگر موارد زیر اجرا می‌شد، Mirai

آسیب‌پذیری کمتری داشت:

- تغییر کلمه عبور پیش‌فرض
- استفاده از VPN به عنوان یک شبکه امن برای دسترسی امن به ابزارهای هوشمند.

• غیرفعال‌سازی خدمات غیرضروری بر روی دستگاه نظیر Telnet

ماتاکنون ضربات بسیار مهلكی از بدافزارها خورده‌یم. قصه‌های بسیار جذابی در این زمینه وجود دارد که در ادامه درس به آن‌ها خواهیم پرداخت، اما صرفاً جهت اطلاع:

• **ویروس ILOVEYOU** (که ضمیمه یک ایمیل عاشقانه در قالب یک فایل به ظاهر txt.. (اما یک اسکریپت به زبان ویژوال بیسیک) در سال ۲۰۰۰ شناسایی شد و حدود ۱۰ درصد کل کامپیوترهای دنیا را الوده کرد و ۱۰ میلیارد دلار ضرر مالی بر جای گذاشت.

ویروس Stuxnet که ادعا شده است توسط آمریکا و اسراییل با همکاری دستگاه‌های اطلاعاتی هلند، فرانسه

و آلمان در عملیات موسوم به "بازی‌های المپیک" برای ضربه زدن به سیستم‌های کنترل‌کننده سانتریفوژها.

باج‌گیر WannaCry در روز اول بیش از ۹۰۰۰ کامپیوتر را در ۹۹ کشور مورد حمله قرار داد. تقریباً یک

چهارم از کل حملات باج افزارهای رمزگذاری که در سال ۲۰۱۹ روی داد، با WannaCry انجام شدند.

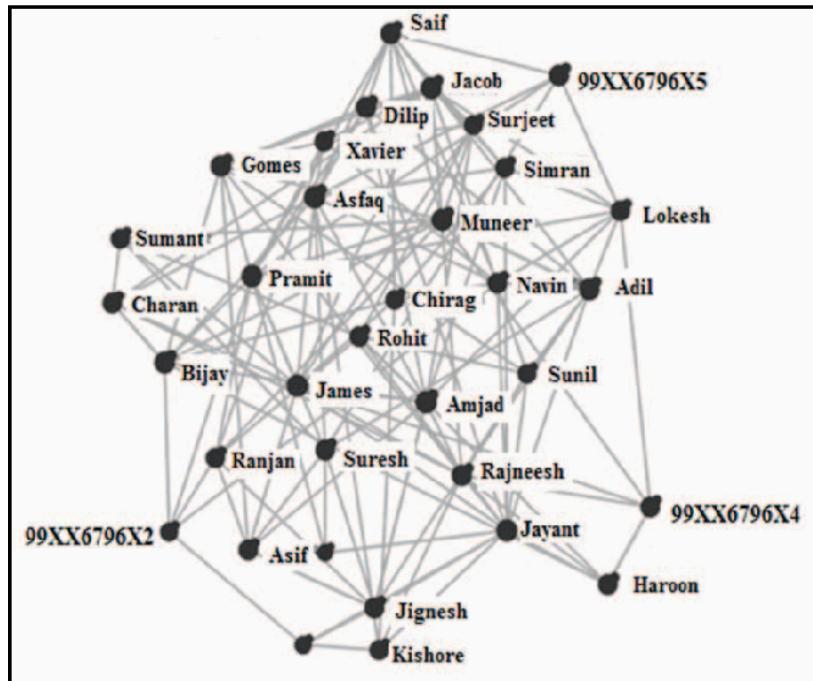
به جرات می‌توان گفت که نفوذ و سرقت اطلاعات شرکت Equifax در حوالی سال ۲۰۱۷ یکی از مهم‌ترین

و خبرسازترین رخدادها در حوزه امنیت بوده. این شرکت ارائه دهده خدمات مالی و اعتباری در سپتامبر

۲۰۱۷ اعلام کرد تمامی اطلاعات سوابق خرید و هزینه‌های مشتریان به دست هکرها افتاده است. در این

حادثه، اطلاعات مالی محترمانه بیش از ۱۴۵ میلیون نفر در آمریکا و چند میلیون نفر در انگلستان به سرقت رفت.

# ترور رفیق حریری و تحلیل CDR (Call Detail Record)



CDR Graph



Rafic Hariri

فایل‌های CDR با هدف مدیریت هزینه (Charging) شبکه ولی ...  
آنچه که برای ما مهم است: (Where, When, Who, ...) داده Context است.

در ۱۴ فوریه ۲۰۰۵ (۲۶ بهمن ۱۳۸۳)، نخست وزیر لبنان رفیق حریری، به همراه ۲۱ نفر دیگر در اثر انفجار کامیونی که در مسیر حرکت خودروهای حامل او بود، در نزدیکی هتل سنت جورج در بیروت کشته شدند. این موضوع موجب کشمکش‌های سیاسی بسیاری در لبنان و در سطح جهان شد. آمریکا و اسرائیل از یک سو، حزب الله لبنان و سوریه از سوی دیگر، دو سر این کشمکش بودند.

# هدیه شوروی به آمریکا



یکی از قشنگ‌ترین ابزار جاسوسی تاریخ، این نشان عقاب امریکاییه که سال ۱۹۴۵ روس‌ها به نشانه صلح و دوستی به امریکایی‌ها قالب کردن و امریکایی‌ها هم برداشتن بردنش تو سفارت خودشون تو مسکو!

این متن را از توئیتر برداشتمن:

یکی از قشنگ‌ترین ابزار جاسوسی تاریخ این تابلو بدقيافه با نشان عقاب امریکاییه که سال ۱۹۴۵ روسها به نشانه صلح و دوستی به امریکایی‌ها قالب کردن و امریکایی‌ها هم برداشتن بردنش تو سفارت خودشون تو مسکو! داخل تابلو یه غشای خازنی متصل به یه آنتن غیر فعال جاسازی شده بود دستگاه هیچ منبع تغذیه‌ای نداشت و قشنگی اون هم همین غیرفعال بودنش بود. چون امریکایی‌ها هیچ‌جوره شک نکردن که همچین چیزی می‌تونه ابزار جاسوسی باشه! غشای خازنی به عنوان میکروفون عمل می‌کرد و وقتی امواج صوتی به غشا برخورد می‌کرد ظرفیت خازن تغییر می‌کرد. روسها برای گوش دادن به صوت از یه ساختمان نزدیک سفارت یه موج الکترومغناطیس با طول موج مشخص (۴ برابر طول آنتن) می‌فرستادن و امواج بازگشتی رو با یه گیرنده رادیویی گوش می‌دادن!

امریکایی‌ها تا سفیر تو روسیه عوض کردن و این تابلو هم به مدت هفت سال تو اتاق سفیر امریکا تو روسیه نصب بود تا این که یه روز اپراتور سفارت انگلیس که داشت سعی می‌کرد مکالمات نیروی هوایی روسیه رو گوش

بده دید که عه! اینا چه قدر واضح و شفاف و قشنگ انگلیسی حرف می‌زنن :))

خلاصه امریکایی‌ها هر چی می‌گردن میکروفونی پیدانمی‌کنن تا این که دو تا کارشناس از امریکا می‌فرستن با یه وسیله اسکن جدید موقعی که روس‌ها داشتن سیگنال الکترومغناطیس رو می‌فرستادن بالاخره کشفش می‌کنن!

بعد امریکایی‌ها با کمک دانشمندانه ای انگلیسی کلی زور می‌زنن تا دستگاه رو کار بندازن و خودشون از روش کپی کنن. به غیر از انگلیس و امریکا، کانادا و استرالیا هم بعدها از این وسیله برای جاسوسی استفاده می‌کردن.

جالبه که تا ۱۹۶۰ امریکایی‌ها صداشو در نمیارن تا این که یه هواپیمای U۲ جاسوسی امریکا تو آسمان روسیه هدف حمله موشک ضد هوایی روس‌ها قرار می‌گیره. خلبان با چتر بیرون می‌پره و دستگیر می‌شه. امریکایی‌ها اول می‌گن این هواپیما برای تحقیقات آب و هوایی بوده ولی چند روز بعد روس‌ها قطعات هواپیما و عکسایی که از مراکز نظامی روسیه گرفته بوده رو رو می‌کنن و امریکایی‌ها مجبور به پذیرش موضوع می‌شن. تو جلسه شورای امنیت که به درخواست شوروی برای بررسی موضوع جاسوسی امریکا تشکیل می‌شه، امریکایی‌ها تابلو رو بر می‌دارن می‌برن می‌گن روس‌ها هم از ما جاسوسی می‌کردن :))

### امنیت رایانه‌ای (Cybersecurity)

به معنای محافظت از اطلاعات ذخیره شده، منتقل شده و یا مورد پردازش قرار گرفته در شبکه‌ای از سامانه‌های رایانه‌ای، تجهیزات شبکه، ابزارهای دیجیتالی و خطوط انتقال است. این حفاظت شامل موارد زیر است:

- محترمانگی (Confidentiality): داده از افشای غیرمجاز محافظت شود.
- یکپارچگی (Integrity): عدم تغییر داده و عملکرد سامانه به صورت غیرمجاز
- دسترسی‌پذیری (Availability): اطمینان از عملکرد بی‌درنگ سامانه و عدم رد خدمات برای کاربران مجذوب
- سندیت (Authenticity): از منبعی که ادعا می‌شود واقعاً رسیده باشد.
- مسئولیت‌پذیری (Accountability): عملیات کاربر قابل رهگیری باشد.

دو زیرمجموعه: امنیت اطلاعات (Information Security) و امنیت شبکه (Network Security) 

# اهداف امنیت - یکپارچگی (Integrity)



۱) **یکپارچگی داده:** اطمینان از قابل تغییر بودن اطلاعات و برنامه‌ها فقط به صورت مشخص و مجاز

۲) **یکپارچگی سامانه:** اطمینان از انجام عملیات سامانه به صورت عادی، عاری از دستکاری غیرعمدی یا

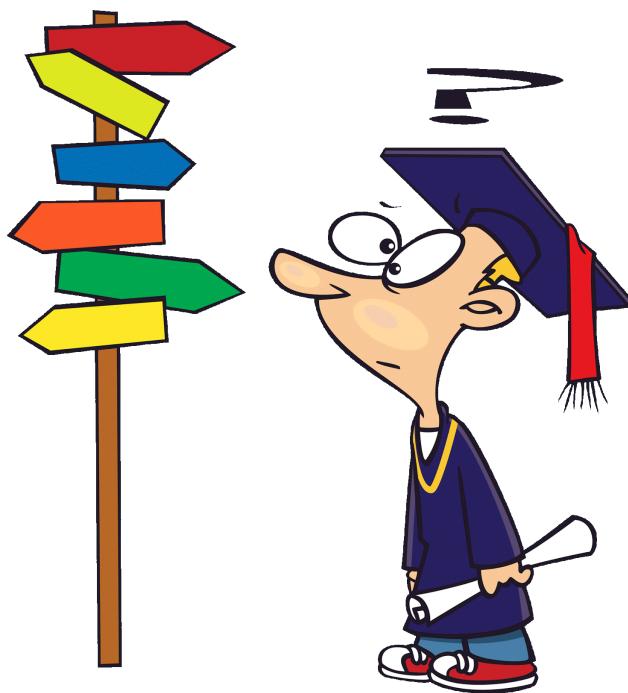
غیرمجاز

NIST (National Institute of Standards and Technology) یا همان موسسه ملی فناوری و استاندارد است

که در سال ۱۹۰۱ به عنوان یک موسسه دولتی در آمریکا تشکیل شد. این موسسه زیر نظر وزارت بازرگانی ایالات متحده آمریکا فعالیت می‌کند، و مسؤول وضع استانداردها و سازوکارهایی در حوزه امنیت اطلاعات. البته باید گفت که هدف غایی آن تشویق نوآوری و رقابت صنعتی توسط پیشبرد علوم سنجشی و فناوری در آمریکا، بگونه‌ای که امنیت اقتصادی را ارتقا بخشدیده، و سطح کیفیت زندگی را افزایش دهد.

چارچوب امنیت سایبری مجموعه‌ای از دستورالعمل‌ها برای شرکت‌های بخش خصوصی است که توسط NIST تهیه شده است، تا در شناسایی، کشف و پاسخگویی به حملات سایبری آمادگی بیشتری داشته باشند. هم‌چنین این برنامه شامل دستورالعمل‌هایی برای نحوه جلوگیری از حملات و ترمیم آثار ناشی از حملات است. به عبارت ساده‌تر، این چارچوب مجموعه‌ای از بهترین شیوه‌ها، استانداردها و توصیه‌هایی است که به یک سازمان در بهبود اقدامات خود در زمینه امنیت سایبری کمک می‌کند.

# سرفصل‌ها



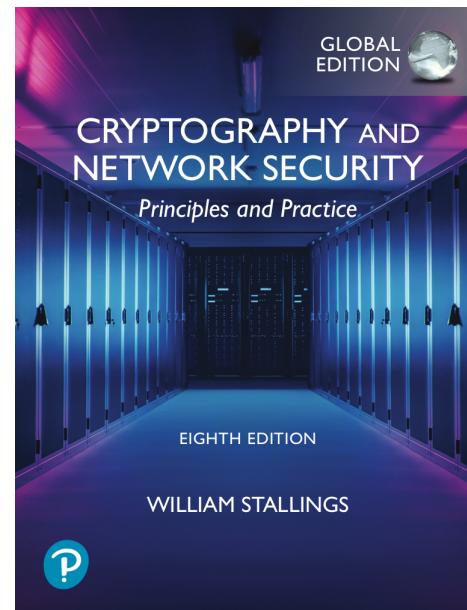
- ♠ فصل اول: گذری بر درس
- ♠ فصل دوم: گذشته رمزنگاری و رمزنگاری متقارن (Public Key)
- ♠ فصل سوم: رمزنگاری کلید عمومی (Public Key Infrastructure)
- ♠ فصل چهارم: زیرساخت کلید عمومی (IPSec و TLS)
- ♠ فصل پنجم: دیوار آتش (Firewall)
- ♠ فصل ششم: دیگر مباحث

# نحوه نمره‌دهی



- امتحان‌های کوتاه کلاسی (۱۲ نمره) - سه امتحان
  - پروژه به همراه ارایه (۵ نمره)
  - باقی موارد (۴ نمره)
- ✓ امتحان پایان ترم (2.0 نمره)
- ✓ فعالیت کلاسی (0.2 نمره)
- ✓ حضور در کلاس (جلسه‌ای 0.08 نمره)
- ✓ کتابنویسی و نوشتارها (2.0 نمره)

# مراجع درسی



یک کتاب خوب و کلاسیک در حوزه آشنایی با امنیت 

Stallings, William. Cryptography and Network Security: Principles and Practice, Global Edition. United Kingdom, Pearson, 2022.

# برخی نکات

تمرین‌ها، کوییزها و اطلاع‌رسانی‌ها به صورت متمرکز در [lms.iust.ac.ir](https://lms.iust.ac.ir) صورت می‌پذیرد.



تعیین نماینده برای کلاس



عضویت در کanal تلگرامی درس (لینک در [LMS](#) درس)



یک پروژه دارید که می‌بایست در گروه‌های حداکثر دو نفره اجرا شود. گزارش پروژه‌ها و تمامی نوشتارها باید با [LATEX](#) باشد.



یک امتحان را می‌توانید در پایان ترم جبران کنید.



لطفا کپی نکنید!! فریب و سوشهای ChatGPT و GitHub Copilot را نیز نخورید :)

- [1] A. Kashaf, V. Sekar, and Y. Agarwal, “Analyzing third party service dependencies in modern web services: Have we learned from the mirai-dyn incident?,” in *Proceedings of the ACM Internet Measurement Conference*, IMC ’20, (New York, NY, USA), p.634–647, Association for Computing Machinery, 2020.

# فهرست اختصارات

## C

CDR ..... Call Detail Record

## D

DDoS ..... Distributed Denial Of Service

DNS ..... Domain Name System

DoS ..... Denial Of Service

I

IoT ..... Internet of Things

N

NIST ..... National Institute of Standards and Technology

V

VPN ..... Virtual Private Network



# واژه‌نامه انگلیسی به فارسی

Charging ..... A هزینه

Ciphertext ..... متن رمز ..... Accountability ..... مسئولیت‌پذیری

Confidentiality ..... محرومگی ..... Authenticity ..... سندیت

Cryptanalysis ..... تحلیل رمز ..... Availability ..... دسترس‌پذیری

D ..... C

Database ..... پایگاه داده ..... Cybersecurity ..... امنیت رایانه‌ای

# I

Information Security ..... امنیت اطلاعات ..... Download ..... بارگیری ..

Integrity ..... یکپارچگی ..

# E

# K

Key Space ..... فضای کلید ..... Encryption ..... رمزگذاری ..

# M

Malware ..... بدافزار ..... Firewall ..... دیوار آتش ..

## P

Public Key ..... کلید عمومی N

Public Key Infrastructure ..... زیرساخت کلید عمومی . Network Security .. امنیت شبکه ..

Plaintext ..... متن اصلی ..

Port ..... درگاه O

Open Source ..... متن باز ..

## R

Operating System ..... سیستم عامل ..

Realtime ..... بی درنگ ..

S

خدمتگزار . . . . . Server

# واژه‌نامه فارسی به انگلیسی

Malware .....	بدافزار .....	۱
Realtime .....	بی‌درنگ .....	امنیت اطلاعات .....
	Information Security .....	امنیت رایانه‌ای .....
	Cybersecurity .....	امنیت شبکه .....
Database .....	پایگاه داده .....	۲
		Download .....
		بارگیری .....

ت

تحلیل رمز ..... Cryptanalysis

د

Encryption ..... رمزگذاری

خ

Decryption ..... رمزگشایی

خدمتگزار ..... Server

ز

Public Key Infrastructure ..... زیرساخت کلید عمومی

د

درگاه ..... Port

دسترس پذیری ..... Availability

دیوار آتش ..... Firewall

س

Public Key .....	کلید عمومی .....	Authenticity .....	سندیت .....
		Operating System .....	سیستم عامل .....

م

Plaintext .....	متن اصلی .....	ش
Ciphertext .....	متن رمز .....	شنود .....
Open Source .....	متن باز .....	
Confidentiality .....	محرمانگی .....	
Accountability .....	مسئولیت پذیری .....	ف
		فضای کلید .....
		Key Space .....

هزینه ..... Charging .....

ی

یکپارچگی ..... Integrity .....