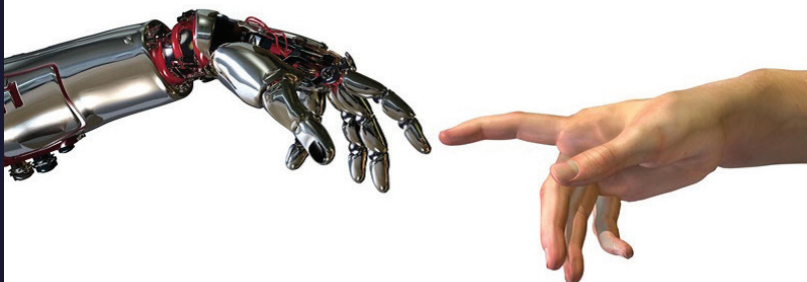




با پردازش همراه باشید...

- جوایز بزرگ دنیای کامپیوتر
- دیپ فیک چیست؟
- آشنایی با زبان Ruby
- آشنایی با تورینگ
- اینترنت اشیا Internet of Things
- Encryption چیست؟
- هکرهای کلاه سیاه
- Silicon Valley
- همه چیز درباره "cookies"
- دانشمند کامپیوتر Dijkstra
- کامپیوترهای کوانتومی

سخن سردبیر / پریناز میرباقری	۲
Encryption چیست؟ / دلارام درودگریان	۴
هکرهای کلاه سیاه / نواز بهشتی	۸
Silicon Valley / مریم عتباتی	۱۲
همه چیز درباره "cookies" / روشنگر حسینزاده عطار	۱۴
Dijkstra دانشمند کامپیوتر / پریناز میرباقری	۱۷
کامپیوترهای کوانتومی / مهدیه غروی	۲۰
جوایز بزرگ دنیای کامپیوتر / مریم احمدلو	۲۲
دیپ فیک چیست؟ / روشنگر حسینزاده عطار	۲۶
آشنایی با زبان Ruby / مریم عتباتی	۲۸
آشنایی با تورینگ / دلارام درودگریان	۳۰
اینترنت اشیا / Internet of Things / مهدیه کوکبی	۳۴



فصل نام‌ه علمی
دانشجویی پردازش
پاییز ۹۹ / شماره هجدهم

صاحب امتیاز انجمن
علمی کامپیوتر
دانشگاه الزهراء (س)

مدیر مسئول: نازنین عباسی
کارشناس نشریه: زهرا وزیری
سردبیر: پریناز میرباقری
طراح جلد: مائده رادفر
صفحه‌آرایی: مائده رادفر

تحریریه

دلارام درودگریان، نواز بهشتی،
مریم عتباتی، روشنگر حسینزاده
عطار، پریناز میرباقری، مهدیه
غروی / مریم احمدلو، مهدیه کوکبی

ویراستاری

پریناز میرباقری، رژین سولقانی،
پرستو جعفری، فاطمه اسدیار،
مریم عتباتی، سارا جواهریان،
دلارام درودگریان

امور چاپ
چاپخانه دانشگاه الزهراء (س)

سخن سردبیر

پاییزی دیگر آغاز شد و با نشریه‌ی پردازش همراه شما عزیزان هستیم. پیش از شروع هر چیز به دانشجویان ورودی جدید تبریک می‌گوییم که در یک دانشگاه سطح بالا و در یکی از بهترین رشته‌های مهندسی در کشور پذیرفته شده‌اند. امیدوارم این شروعی بر مسیری باشد که انتهای آن موفقیت‌های پی‌درپی به انتظار نشسته است.

با اینکه اولین شماره‌ی نشریه در زمستان سال ۱۳۹۱ منتشر شده است، اما تا پیش از آن تحت عنوان نام کلیک فعالیت خود را آغاز کرده بود. یعنی چیزی حدود ۱۰ سال از شکل‌گیری ایده‌ی نشریه می‌گذرد. طی سال‌هایی که در نشریه مشغول به کار بودم، این را وظیفه‌ی خود می‌دانستم تا ورودی‌های جدیدتر را با این سنت قدیمی آشنا کنم. پردازش میراث کسانی است که روزی تصمیم گرفتند در محیط افراد خود تغییری ایجاد کنند. کسانی که انجمن و نشریه را تاسیس کردند تا امروز ما بتوانیم به وسیله‌ی آن‌ها رشد کنیم. چراکه هدف نشریه یادگیری است. امیدوارم که راه آن‌ها همچنان ادامه یابد و دانشجویهای جدیدالورود هم بتوانند از این امکانی که فراهم شده است، نهایت استفاده را ببرند. هدف پردازش تنها یادگیری علمی نیست، بلکه همدلی و صمیمیت هم از ارکان مهم آن هستند. روند تولید یک نشریه به دست تنها یک نفر ممکن نیست. بلکه چندین و چند نفر در آن دخیل هستند و همین است که ارزش آن را بالا می‌برد. همین همدلی و صمیمیتی که طی تولید نشریه بین بچه‌ها شکل می‌گیرد.

ارزش برخی لحظه‌ها در زندگی حد و حصری ندارد. لحظاتی مانند بخشش یکدیگر هنگام کار گروهی، تکمیل راه دیگران و از همه مهمتر جبران کردن اشتباهات هم‌گروهی‌هایمان و... این‌ها بخشی از لحظاتی بود که من در پردازش تجربه کردم و از آن‌ها چیزهایی آموختم که هرگز در این چهار سال تحصیلی کسی به من یاد نداد.

این سه سال برای من فرصت بی‌ظری بود که توانستم عضوی کوچک از خانواده‌ی بزرگ پردازش باشم. امیدوارم که توانسته باشم نهایت تلاش خود را برای پیشرفت نشریه به کار برده باشم و امیدوارم که پردازش تا سال‌های سال به پیشرفت‌های خود به همین شکل ادامه دهد.

امیدوارم که در این روزهای سخت بیماری، تک‌تک شما عزیزان و خانواده‌هایتان در صحت و سلامت باشید که سلامتی بزرگترین هدیه است.

پریناز میرباقری

با **بیردازتر** همراه بماند...



Encryption چیست؟

دلارام درودگریبان



مفهوم Cryptography چیست؟

قبل از پرداختن به مبحث encryption لازم است ابتدا نگاهی کلی به مفهوم «cryptography» بیندازیم. بخش اول آن یعنی «crypto» از واژه یونانی «kryptos» که برای بیان و تجسم چیزهای مخفی به کار می‌رود و بخش دوم آن، «graph» از «graphim» که به معنای نوشتن است، گرفته شده است؛ و ترکیب این دو واژه به معنای «هنر رمز نگاری» می‌باشد.

Cryptography یا به اصطلاح مطالعات رمز نگاری، فهم تکنیک‌های ریاضی می‌باشد و بر پایه مقدمات بسیاری از قبیل نظریه اعداد و آمار بنا شده است که در مفاهیم امنیت اطلاعات مانند محرمانگی، یکپارچگی داده، احراز

به این موضوعات علاقه مندید توصیه میکنم فیلم "The Imitation Game (۲۰۱۴)" را از دست ندید!



ماشین انیگما

Encryption چیست؟

حال به موضوع اصلی مقاله مان میپردازیم. Encrypt در لغت به معنای پنهان کردن می باشد و به عملیات رمز نگاری اطلاق می شود و موجب می شود محتوای پیام ما از دید دیگران پنهان بماند. در واقع عمل encryption داده ها را به قالبی که فقط افراد مجاز می توانند آن را مشاهده کنند (و اصطلاحاً cipher-text می نامند) تبدیل می کند. Encryption دارای قدمت چند هزار ساله می باشد و همانطور که قبلاً اشاره کردیم، از زیر مجموعه های cryptography می باشد. این نوع از رمز نگاری بر خلاف فرایند «hashing» یک طرفه نیست و قابلیت «decrypt» (رمز گشایی) و دسترسی به پیام اصلی را دارد. به این صورت که هر رمز نگاری ای الگوی مخصوصی داشته و برای دستیابی به آن الگو باید کلید آن را داشته باشیم. الگوریتم های زیادی برای رمز نگاری وجود دارد و به انواع و اقسام سخت تا آسان طبقه بندی می شوند. الگوریتم رمز نگاری ای قوی تر است که بدون داشتن کلید آن، به هیچ وجه نتوان به داده هایش دسترسی پیدا کرد. سازمان های اطلاعاتی از encryption های خاصی برای تبادل اطلاعات مهم استفاده می کنند. برای مثال ما عبارت زیر را با الگوریتم «AES» رمز گذاری میکنیم:

سلام به کاربران سایت ناحیه هکرها این پیام هنوز رمز نشده است.

پس از رمز نگاری پیام فوق، عبارت رمز شده به صورت زیر است:

ZUXLW49jZIDOLVINUwe/FC9mIPvPrKUdo+jGUuc3p4p1+6ZDJ9jbKyHHBRM53clP6mjeoSeOMHLq5vBkweOK2Xh02VfISZR911DfwPJufzCj4c4vPGxeavoK0ve9TKMq1mB4VmRLbkamO2VA==

کلیدی که برای رمز فوق استفاده شده، عبارت رو به رو می باشد: **V#%\$%#5v353v#**

که با استفاده از این کلید، رمز فوق را به راحتی میتوانیم به حالت اولیه خود برگردانیم.

یادتان باشد الگوریتم های رمز نگاری علاوه بر پیامها برای فایلها هم قابل استفاده می باشند. مانند کاری که باج افزارها

هویت موجودیت و اصل داده آمیخته شده است. علم Cryptography پیام های رمز نشده را به کمک مفهوم رمز نگاری، به صورت رمز شده درمی آورد و امروزه در واقع فرایندی برای تامین امنیت اپلیکیشن ها و محافظت از داده های مربوط به آنها در برابر حملات می باشد؛ به طوریکه در فرایند ارسال و دریافت داده، صرفاً افراد مورد نظر، توانایی رمزگشایی داده های رمزنگاری شده را داشته باشند. همچنین یک حوزه وسیع محرمانگی می باشد که فرآیندهایی همچون encryption، hashing و ... زیر مجموعه های آن محسوب می شوند. در این بخش ما می خواهیم فرایند encryption را مورد مطالعه و بررسی قرار می دهیم.

تاریخچه رمزنگاری:

هنر رمزنگاری همراه با هنر نوشتن متولد شده است. رمز نگاری یک شیوه باستانی محافظت از اطلاعات سری است که سابقه آن حدوداً به ۴۰۰۰ سال پیش برمی گردد. اولین رمز نگاری حدود ۱۹۰۰ سال پیش از میلاد مسیح و توسط مصریان صورت گرفته است که به وسیله تکنیک «هیرئوگلیف» با نوشتن پیام هایی حیرت انگیز با یکدیگر ارتباط برقرار می کردند. در واقع در آن زمان که به جای کلمات از تصویر استفاده می شده، از تصاویری استفاده می کردند که متداول نبوده و به صورت رمزگونه بوده است. سپس در بین النهرین، یونان، هند و بسیاری دیگر از نقاط جهان از این شیوه تبادل اطلاعات استفاده هایی صورت گرفت تا به شکل امروزی خود درآمد.



همتون هیرئوگلیف

سابقه سیستم های اولیه رمز نگاری که گاهی به آنها کد (code) یا رمز (cipher) نیز گفته می شود، به مصر باستان و حدوداً ۲۰۰۰ سال پیش برمی گردد. یکی از موارد استفاده از رمز نگاری، در طول جنگها بوده است. به طور مثال، در دهه ۱۹۲۰ و اواخر جنگ جهانی اول، مهندس آلمانی آرتور شربیوس ماشین «انیگما» را اختراع کرد و ارتش آلمان نازی مدل ویژه ای از این ماشین به نام «انیگمای ورماخت» را تولید نمود و به منظور رمز نگاری و رمز گشایی پیام های نظامی در طول جنگ جهانی دوم به کار می برد. لازم به ذکر است که پیام های رمز گذاری شده ارتش آلمان به وسیله انیگما، اولین بار به دست بریتانیایی ها شکسته شد.

این پیروزی حاصل تلاش های چهار ریاضیدان لهستانی به نام های ماریان ریفسکی، یژی روژیٹسکی، آلن تورینگ و هنری زیگالسکی بود. همین امر در نهایت باعث پی بردن به نقاط ضعف نازی ها و شکست آنان در جنگ شد. (اگر

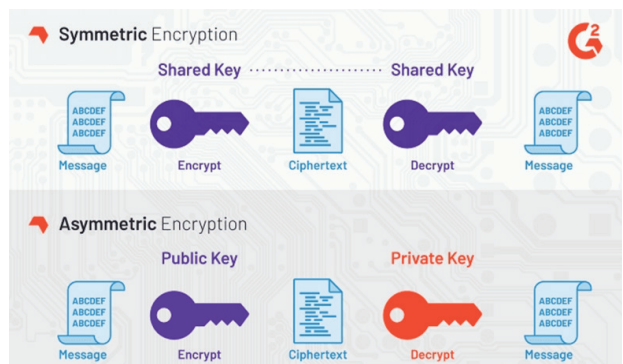
با فایل های قربانیان انجام می دهند؛ آن ها در واقع فایل افراد را encrypt کرده و در قبال دریافت مبلغ مشخصی، فایل ها را رمز گشایی می کنند و در اختیار صاحبان اصلی قرار می دهند. (پس مراقب باشید در دام این باج گیر ها گرفتار نشوید.)

الگوریتم متقارن و نامتقارن

یکی از مهم ترین الگوریتم های رمز نگاری، الگوریتم های متقارن (symmetric) و نامتقارن (asymmetric) هستند. در الگوریتم متقارن تنها یک کلید مشترک وجود دارد؛ به این صورت که از همان کلیدی که برای رمز نگاری استفاده شده است، برای رمز گشایی هم استفاده می شود. اما در الگوریتم نامتقارن یا «PKI» از دو کلید عمومی (public key) و کلید خصوصی (private key) برای رمز نگاری و رمز گشایی استفاده می شود. به این صورت که کد رمز گذاری عمومی است و هر کسی می تواند پیغام خود را رمز گذاری کند اما کد رمز گشایی خصوصی است و تنها گیرنده می تواند آن را از حالت encrypt خارج کند؛ بنابراین روش نامتقارن از امنیت بالاتری نسبت به روش متقارن برخوردار بوده اما سرعت پایین تری از آن دارد. روش نامتقارن در اکثر شبکه های کامپیوتری رایج است. گاهی اوقات هم از ترکیب هر دو این الگوریتم ها استفاده می کنند که به آن «hibrid» گفته می شود.

الگوریتم های متقارن و نامتقارن خود شامل انواع گوناگونی می باشند که از جمله انواع الگوریتم های متقارن می توان به Blowfish ، RC ، CAST ، 3DES ، AES ، DES ، و IDEA و

انواع الگوریتم های نامتقارن به ECC ، RSA ، و EL Gamal اشاره کرد.



نحوه عملکرد الگوریتم رمزنگاری متقارن و نامتقارن

کاربرد Encryption:

رمز نگاری سابقه دیرینه ای در دولت ها و نیروهای نظامی دارد که از آن به منظور برقراری ارتباط امن و یا مخفی استفاده می شود. اما در حال حاضر دامنه استفاده از آن وسیع تر شده و به طور معمول در راستای حفاظت از اطلاعات در انواع مختلفی از سیستم های غیر نظامی هم کاربرد دارد.

به گزارش موسسه امنیت کامپیوتری (CSI) در سال ۲۰۰۷، حدود ۷۱٪ از اطلاعات منتقل شده و ۵۳٪ از

Encrypt کردن گوشی های اندروید:

شاید با خود فکر کنید که اطلاعات خیلی خاص و سری در گوشی همراه خود ندارید و نیازی به انجام این قبیل کارها برای امن نمودن آن نیست. اما آیا برای شما مهم نیست که اگر گوشتان به سرقت رفت، فرد سارق به ایمیل شما دسترسی پیدا نکند؟ یا اینکه به فضاهای مجازی که شما در آنها فعالیت دارید رفته و در قالب شما، از دوستان و آشناهایتان سواستفاده کند؟ برای جلوگیری از این دست اتفاقات، اندروید از همان نسخه های اولیه خود، قابلیت encryption را در دسترس کاربران قرار داده است تا از این روش بتوانند اطلاعات تلفن همراه خود را رمزنگاری کنند.

با رعایت چند نکات ساده و در عین حال مهم، می توانید به راحتی دستگاه خود را encrypt کنید و اطلاعات خصوصی خود را در بستری امن نگهداری کنید.

قبل از encrypt کردن گوشی خود لازم است به چند نکته توجه داشته باشید که عبارتند از :

- عملکرد گوشی شما ضعیف تر خواهد شد و گوشی کند عمل خواهد کرد و این به خاطر خارج شدن از حالت رمزگذاری است چون هر بار که وارد گوشی می شوید دستگاه اقدام به خارج شدن از رمزگذاری می کند و این باعث کند شدن گوشی خواهد شد که البته اگر مشخصات گوشی شما بالا باشد چندان احساس نخواهید کرد.

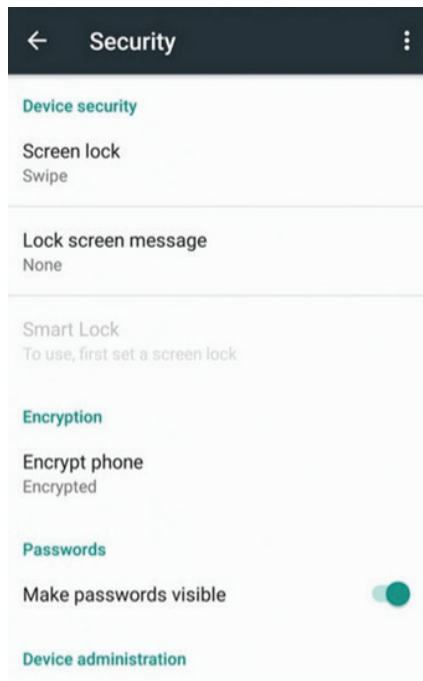
- حواستان باشد که هنگام فعالسازی Encrypt تنها یک روش برای بازگشت دارید و آن «ریست فکتوری» است؛ یعنی اگر رمزگذاری کردید و خواستید لغو کنید تنها گزینه این است که به تنظیمات کارخانه برگردانید.

- اگر گوشی خود را روت کردید به طور موقت unroot کنید، چون اگر رمزگذاری را روی گوشی روت شده انجام دهید با مشکلاتی مواجه خواهید شد. بنابراین اول unroot کرده و سپس اقدام به Encrypt نمایید و بعد از آن یک بار دیگر روت کنید.

همچنین هنگام رمز نگاری گوشی اندروید خود، نکات زیر را حتما در نظر بگیرید:

- رمز گذاری گاهی ۱ ساعت یا بیشتر زمان می برد.
- شارژ گوشی از ۸۰ درصد کمتر نباشد چون در اینصورت عملیات رمز گذاری انجام نمی شود.

روی گوشی خود رمز قرار نداده‌اید، در همین مسیری که آمدید، گزینه screen lock را انتخاب کنید و برای گوشی خود یک رمز یا الگو برای باز شدن قرار دهید. (تصویر ۲)



تصویر ۲

در صورتی که قصد لغو رمزگذاری را داشته باشید باید گوشی خود را factory کنید (البته دقت داشته باشید که در این صورت ممکن است همه اطلاعات گوشی از دست برود). اما اگر رمزگذاری به طور پیش فرض روی گوشی فعال باشد، نمی‌توان آن را لغو کرد.

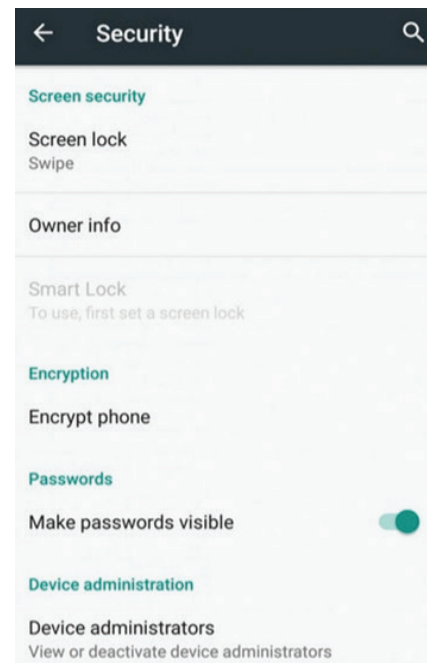
سخن آخر

رمزنگاری از گذشته‌های دور با بشر همراه بوده و با گذشت زمان پیشرفت‌های چشمگیری داشته است و همچنان به رشد و تکامل خود ادامه خواهد داد؛ چرا که انسان از همان ابتدا به اهمیت بسیاری از اطلاعات پی برده و در تلاش بوده تا آنها را از دست افراد سودجو و به روش‌های گوناگون در امان نگه دارد. در عصر حاضر و با پیشرفت تکنولوژی، بیش از پیش به این موضوع پرداخته می‌شود و در تمام ارگان‌های مختلف اعم از دولتی و غیر دولتی، ایجاد بستری امن توسط امنیت کاران حرفه‌ای برای انجام فعالیت‌های مختلف، در وهله اول قرار دارد. بنابراین داشتن حداقل دانشی در این زمینه حتی برای کسانی که از لحاظ کاری و حرفه ارتباط کمی با این قبیل موضوعات دارند، توصیه می‌شود.

۵ طی فرایند رمزگذاری، گوشی حتماً به شارژر متصل باشد.
۵ تا انتهای این عملیات، گوشی باید در حالت unroot باشد.

چگونگی رمزنگاری :

۱. ابتدا به قسمت setting گوشی رفته و از آنجا به قسمت security وارد شوید. اگر قبلاً رمزنگاری انجام شده باشد، مشخص خواهد بود و در غیر اینصورت باید گزینه encrypt phone را انتخاب کنید. (تصویر ۱)



تصویر ۱

۲. سپس صفحه‌ای از هشدارها باز می‌شود و از اتفاق‌هایی که ممکن است رخ دهد، خبر می‌دهد (که قبل‌تر به آن‌ها اشاره کردیم). در صورت موافق بودن، بر روی en-crypt phone کلیک کنید.

۳. هشدار دیگری باز می‌شود که در واقع می‌خواهد بداند شما از چگونگی روند این عملیات مطمئن هستید و اینکه در هر صورت نباید متوقف شوید. در صورت موافق بودن، بار دیگر بر روی encrypt phone کلیک کنید.

۴. سپس گوشی اقدام به راه‌اندازی کرده و ری‌استارت می‌شود و پیامی روی گوشی ظاهر می‌شود با این مضمون که این پروسه کمی زمان‌بر بوده و در این مدت نباید گوشی را دستکاری کرد.

۵. در پایان عملیات، گوشی بار دیگر ری‌استارت شده و اکنون آماده استفاده می‌باشد. اگر می‌خواهید مطمئن شوید که عملیات رمزگذاری با موفقیت به اتمام رسیده است، به قسمت setting و سپس security بروید و در آنجا می‌توانید کلمه encrypted را ببینید به این معنا که رمزگذاری با موفقیت انجام شده است. همچنین اگر

هکرهای کلاه سیاه

نواز بهشتی

علیرغم اینکه در کارهایی که انجام می دهند بهترین هستند ، می توانند صدمات زیادی وارد کنند.در ادامه اطلاعاتی چند ، از بدنام ترین و شرورترین «کلاهبرداران سیاه» آورده شده است.



بود) دستگیر کرد.

میتنیک به wire fraud (۱۴ فقره)، در اختیار داشتن وسایل دسترسی غیرمجاز (۸ فقره)، رهگیری سیم یا ارتباطات الکترونیکی، دسترسی غیرمجاز به یک کامپیوتر فدرال و ایجاد خسارت به یک کامپیوتر متهم شد.

میتنیک پنج سال در زندان (چهار و نیم سال قبل از محاکمه و هشت ماه در انفرادی) خدمت کرده است؛ زیرا، به گفته میتنیک، مأموران اجرای قانون، یک قاضی را قانع کردند که وی توانایی «شروع جنگ هسته‌ای» را با یک تلفن دارد چون می‌تواند از طریق تلفن زندان، مودم NORAD را شماره‌گیری کرده و با سوت زدن برای پرتاب موشک‌های هسته‌ای، با مودم ارتباط برقرار کند. علاوه بر این، تعدادی از رسانه‌ها از عدم دسترسی وعده‌های غذایی در زندانی که در آن حبس شده بود، خبر دادند.

وی در تاریخ ۲۱ ژانویه ۲۰۰۰ آزاد شد. در طول آزادی تحت نظر، که در ۲۱ ژانویه ۲۰۰۳ به پایان رسید، ابتدا به او ممنوعیت استفاده از هر فناوری ارتباطی به غیر از تلفن ثابت داده شد. میتنیک با این تصمیم در دادگاه مبارزه کرد و سرانجام و به او اجازه دسترسی به اینترنت را دادند. طبق توافق نامه دعوی، میتنیک به دلیل فعالیت‌های جنایی خود به مدت هفت سال، از استفاده کردن از فیلم یا کتاب منع شد.

● تناقض

فعالیت‌های جنایی، دستگیری و محاکمه میتنیک، همراه با روزنامه‌نگاری مرتبط، همه بحث برانگیز بود. گرچه میتنیک به دلیل غیرقانونی کپی کردن نرم افزار محکوم شده بود، هواداران وی معتقد بودند که مجازات وی بیش از حد بوده است و بسیاری از اتهامات علیه وی، درست نبوده است.

میتنیک در کتاب ۲۰۰۲ خود با عنوان «هنر فریب» اظهار داشت که او کامپیوترها را فقط با استفاده از رمزهای عبور و کدهایی که توسط مهندسی اجتماعی به دست آورده بود، هک کرده است. وی ادعا می‌کند که از برنامه‌های نرم افزاری و یا ابزارهای هک کردن برای رمز عبور یا استفاده از امنیت رایانه یا تلفن استفاده نکرده است.

● مشاوره

از سال ۲۰۰۰، میتنیک مشاور امنیتی پولی، سخنران عمومی و نویسنده شده است. او مشاوره امنیتی را برای شرکت‌های Fortune ۵۰۰ و FBI، خدمات آزمایش نفوذ برای بزرگترین شرکت‌های جهان و کلاس‌های مهندسی اجتماعی را به ده‌ها شرکت و آژانس‌های دولتی آموزش می‌دهد.

کارت ویزیت‌های فلزی سفارشی او به عنوان کیت‌های جمع‌آوری قفل، استفاده می‌شود.

Kevin David Mitnick - ۱

(متولد ۶ آگوست ۱۹۶۳) هکر، مشاور، نویسنده و محکوم به پنج سال زندان به دلیل جرایم مختلف رایانه‌ای است که به واسطه‌ی دستگیری‌اش در سال ۱۹۹۵ شناخته شد. وی اکنون شرکت امنیتی Mitnick Security Consulting LLC، را اداره می‌کند و همچنین مدیر ارشد هکینگ، سهامدار شرکت آموزش آگاهی از امنیت KnowBe4 و همچنین عضو فعال مشاوره‌ای در Zimperium، شرکتی است که یک سیستم پیشگیری از نفوذ موبایل را توسعه می‌دهد، است.

● زندگی

میتنیک در ۶ آگوست ۱۹۶۳ در ون‌نویز، کالیفرنیا، متولد شد. وی در لس‌آنجلس بزرگ شد و در دبیرستان جیمز مونرو در لس‌آنجلس، کالیفرنیا، شرکت کرد که در این مدت یک اپراتور رادیویی آماتور شد. او بعدها در کالج لس‌آنجلس پیرس و USC ثبت نام کرد. مدتی در بخش پذیرش معبد خردمند استنفان اس. کار کرد.

● هک کامپیوتر

میتنیک اولین بار در سال ۱۹۷۹، یعنی در ۱۶ سالگی، هنگامی که یکی از دوستانش شماره تلفن Ark را به او داد (Ark سیستم کامپیوتری است که شرکت تجهیزات دیجیتال (DEC) برای توسعه نرم افزار سیستم عامل RSTS / E از آن استفاده کرده است) توانست دسترسی غیرمجاز به شبکه رایانه‌ای بدست آورد. وی وارد شبکه رایانه‌ای DEC شد و نرم افزار شرکت را کپی کرد؛ جرمی که در سال ۱۹۸۸ به خاطر آن به ۱۲ ماه زندان محکوم شد و به دنبال آن سه سال تحت نظر بود. میتنیک نزدیک به پایان محکومیتش، رایانه‌های پست صوتی Pacific Bell را هک کرد که به واسطه آن به مدت دو سال و نیم فراری شد.

به گفته وزارت دادگستری ایالات متحده، میتنیک در حالی که فراری بود، به ده‌ها شبکه رایانه‌ای دسترسی غیرمجاز داشت. وی برای مخفی کردن موقعیت مکانی خود، از تلفن‌های همراه کلون شده استفاده می‌کرد و نرم افزارهای ارزشمند اختصاصی را از برخی از بزرگترین شرکت‌های تلفن همراه و رایانه در کشور کپی می‌کرد. همچنین رمزهای رایانه را رهگیری و به سرقت می‌برد، شبکه‌های رایانه‌ای را تغییر می‌داد و نامه‌های الکترونیکی خصوصی را بدست می‌آورد و می‌خواند.

● دستگیری، محکومیت و حبس

پس از پیگیری‌های تبلیغاتی، FBI، میتنیک را در ۱۵ فوریه ۱۹۹۵ در آپارتمان خود در رالی، کارولینای شمالی، به جرائم فدرال مربوط به یک دوره دو نیم ساله از هک رایانه (که شامل کلاهبرداری در کامپیوتر و wire fraud

وی در ۳۰ نوامبر ۱۹۶۵ در پاسادنا، کالیفرنیا متولد شد.

هک کلاه سیاه

در اول ژوئن سال ۱۹۹۰، پولسن تمام خطوط تلفن ایستگاه رادیویی KIIS-FM را در لس آنجلس به دست گرفت و تضمین کرد که صدودومین تماس گیرنده خواهد بود و جایزه ۹۴۴ دلار را به دست خواهد آورد.

در ژوئن ۱۹۹۴، پولسون به پنج سال حبس در زندان های فدرال و ممنوعیت استفاده از رایانه یا اینترنت به مدت ۳ سال پس از آزادی، محکوم شد. او اولین آمریکایی بود که با حکم دادگاه آزاد شد و از استفاده از رایانه و اینترنت منع شد. اگرچه کریس لمپرکت برای اولین بار به ممنوعیت استفاده از اینترنت در ۵ مه ۱۹۹۵ محکوم شده بود، اما پولسن قبل از لمپرکت از زندان آزاد شد و پیش از او نیز اجرای حکم ممنوعیت خود را آغاز کرد. (بعدها، مامور زندان پولسن با استفاده از محدودیت های نظارت خاصی، به او اجازه استفاده از اینترنت در سال ۲۰۰۴ را داد).

● روزنامه نگاری

پولسن بعد از آزادی از زندان، به عنوان روزنامه نگار از گذشته جنایتکارانه خود فاصله گرفت. پولسن در موسسه تحقیقاتی امنیتی SecurityFocus، به عنوان روزنامه نگار، مشغول خدمت بود و همان جا، شروع به نوشتن اخبار امنیتی و موضوعاتی در حیطه ی هک (در اوایل سال ۲۰۰۰) کرد. اخبار دنیای فناوری در دوره ی پولسن با این شرکت و توسط Symantec به دست آمد. علاوه بر این، گزارش های تحقیقاتی اولیه او، اغلب توسط مطبوعات اصلی تهیه می شد. پولسون در سال ۲۰۰۵، SecurityFocus را ترک کرد. در ژوئن ۲۰۰۵، وی سردبیر ارشد Wired News شد.

در اکتبر ۲۰۰۶، پولسن اطلاعاتی را در رابطه با جستجوی موفقیت آمیز مجرمان جنسی، با استفاده از MySpace برای وکالت جنسی از کودکان منتشر کرد در نتیجه ۷۴۴ نفر را با پروفایل های MySpace شناسایی کرد و منجر به دستگیری شخصی به نام اندرو لوبرانو شد.

SecureDrop

James Dolan SecureDrop و Aaron Swartz، Poulsen

یک بستر نرم افزاری منبع باز برای برقراری ارتباط امن بین روزنامه نگاران و منابع را طراحی و توسعه دادند. در ابتدا با نام DeadDrop توسعه یافت. پس از مرگ Swartz، پولسن اولین نمونه آن را در نیویورکر، در ۱۵ مه ۲۰۱۳، راه اندازی کرد. بعداً پولسن توسعه SecureDrop را به بنیاد آزادی مطبوعات تغییر داد و به هیئت مشاوره فنی بنیاد پیوست.

۳- ALBERT GONZALEZ

آلبرت گونزالز (متولد ۱۹۸۱) یک هکر کامپیوتر و از مجرمان رایانه ای آمریکایی است که متهم به سرقت از کارت های اعتباری ترکیبی و فروش بیش از ۱۷۰ میلیون کارت و ... کرد یعنی؛ بزرگترین کلاهبرداری در تاریخ! گونزالز اولین کامپیوتر خود را در سن ۱۲ سالگی خریداری کرد و در ۱۴ سالگی موفق به هک کردن ناسا شد. وی در دبیرستان جنوبی میامی، فلوریدا، شرکت کرد در سال ۲۰۰۰ به نیویورک سیتی نقل مکان کرد، جایی که قبل از عزیمت به کرنی نیوجرسی سه ماه زندگی کرد.

● حرفه ی هک

ShadowCrew

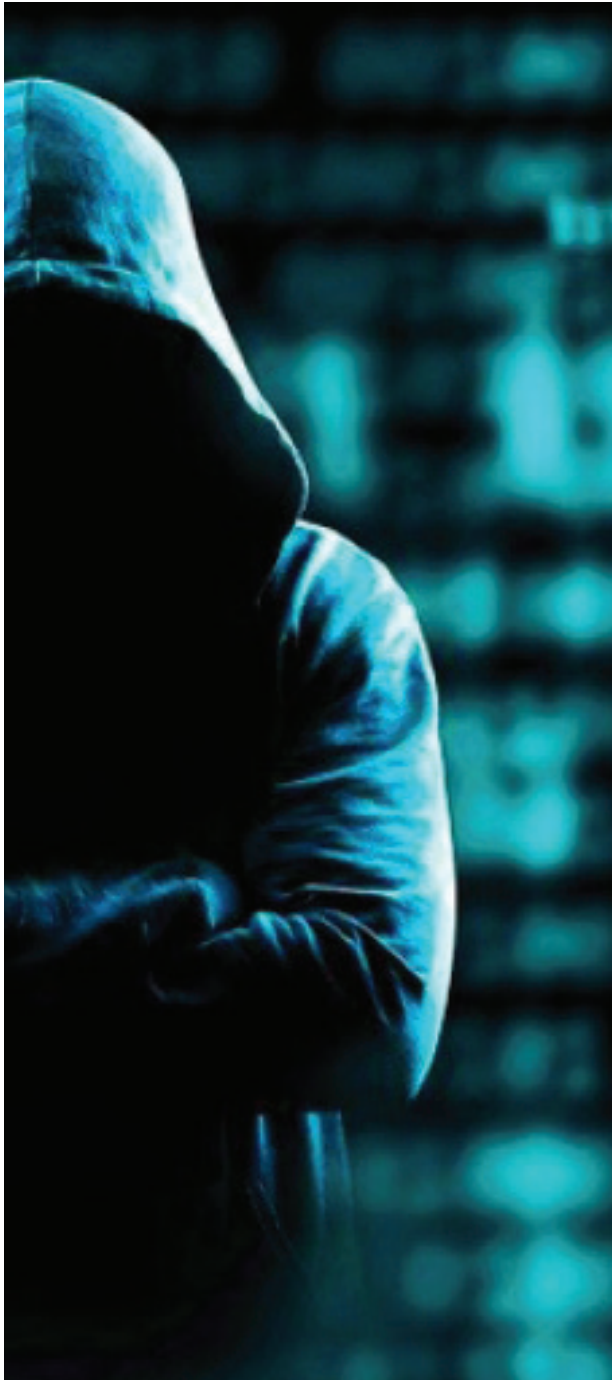
در حالی که در کرنی حضور داشت، متهم شد که مغز متفکر گروهی از هکرها، به نام گروه «ShadowCrew» است که در سرقت ۱,۵ میلیون کارت اعتباری و کارتهای خودپرداز، دست داشته است. اگرچه او مغز متفکر این طرح (عملیاتی در سایت «CumbaJohnny») در نظر گرفته شد، اما واقعا متهم نبود. طبق مدارک، ۴۰۰۰ نفر بودند که در وب سایت Shadowcrew.com ثبت نام کرده بودند. پس از ثبت نام، آنها می توانستند شماره های حساب سرقت شده یا اسناد تقلبی را در حراج بخرند یا آموزشها و نحوه کار را (یعنی نحوه استفاده از رمزنگاری در نوارهای مغناطیسی در کارت های اعتباری و کارت های خودپرداز) بخوانند تا بتوانند از این شماره ها استفاده کنند. ناظران وب سایت، اعضای را که قوانین سایت را رعایت نمی کردند، مجازات کردند؛ مثلا، ارائه بازپرداخت به خریداران در صورت عدم معتبر بودن شماره کارت های سرقت شده.

علاوه بر شماره کارت، اشیایی همچون: گذرنامه های جعلی، گواهینامه های رانندگی، کارت های تأمین اجتماعی، کارت های اعتباری، شناسنامه، کارت های شناسایی دانشجویی کالج و کارت های بیمه درمانی به حراج گذاشته شده بود. بیشتر متهم هایی که عضو بودند، کالاهای غیرقانونی را می فروختند؛ مثلا، یک عضو، ۱۸ میلیون حساب پست الکترونیکی با نام های کاربری مرتبط، گذرنامه ها، تاریخ تولد و سایر اطلاعات شخصی که شخصا شناسایی کرده بود را فروخت. اعضای که خود وب سایت را حفظ یا تعدیل کرده بودند نیز محاکمه شدند؛ از جمله کسی که اقدام به ثبت نام دامنه cc Shadowcrew.cc کرد.

سرورس مخفی، تحقیقات خود را «عملیات فایروال» لقب داد و اعتقاد داشت که تا حدود ۴,۳ میلیون دلار به سرقت رفته است؛ زیرا، ShadowCrew اطلاعات خود را با گروه های دیگر با نام های Carderplanet و Darkprofits به اشتراک گذاشته است. در این تحقیق واحدهایی از ایالات متحده، بلغارستان، بلاروس، کانادا،

در نوامبر ۲۰۰۵، وی هنگامی که مأمورین اف بی آی به بهانه جمع‌آوری تجهیزات رایانه‌ای، او را به دفتر محلی خود دعوت کردند، او را دستگیر کردند.

در ۹ مه ۲۰۰۶، آنچتا، به نقض قوانین ایالات متحده، کلاهبرداری و فعالیت‌های مرتبط رایانه‌ها متهم شد و نهایتاً مکلف شد که علاوه بر ۶۰ ماه حبس، یک دستگاه BMW و بیش از ۵۸۰۰۰ دلار سود را به عنوان جریمه پرداخت کند.



لهستان، سوئد، هلند و اوکراین درگیر شدند. گونزالز در ابتدا به اتهام داشتن ۱۵ کارت اعتباری و جعلی در نیویورک و نیوجرسی متهم شد؛ اگرچه او با ارائه مدارکی به سرویس مخفی ایالات متحده، در برابر همکاران خود، از زندان رفتن خودداری کرد.

● هک شرکت‌های TJX

گفته می‌شود که وی هنگام همکاری با مقامات، هک شرکت‌های TJX را انجام می‌داد که در مدت زمان ۱۸ ماه، ۴۵٫۶ میلیون شماره کارت اعتباری به سرقت رفت و در صدر تخلف سال ۲۰۰۵، از ۴۰ میلیون پرونده در CardSystems Solutions بود.

آلبرت گونزالز بیش از ۱۷۰ میلیون کارت اعتباری و شماره کارت‌های خودپرداز را در مدت زمان دو سال جمع‌آوری کرد. سپس پایگاه داده‌های شرکت‌های TJX و سیستم‌های پرداخت Heartland را هک کرد تا تمام شماره کارت‌های اعتباری ذخیره شده آنها را نیز سرقت کند.

● دستگیری

گونزالز در اتاق ۱۵۰۸ در هتل ملی، در ساحل میامی، دستگیر شد. مقامات، ۱٫۶ میلیون دلار پول نقد (از جمله ۱٫۱ میلیون دلار دفن شده در کیسه‌های پلاستیکی در حیاط خلوت خانه ی والدینش)، لپ‌تاپ وی و یک تپانچه جمع و جور Glock یافتند. وی به بازداشتگاه متروپولیتن در بروکلین، منتقل شد.

گونزالز به ۲۰ سال زندان محکوم شد (دو حکم ۲۰ ساله همزمان) و قرار است در سال ۲۰۲۵ آزاد شود.

۴- JEANSON JAMES ANCHETA

در ۹ مه ۲۰۰۶، جینسون جیمز آنچتا (متولد ۱۹۸۵) اولین فردی شد که به دلیل کنترل تعداد زیادی رایانه ربوده شده یا بات‌ها دستگیر شد.

آنچتا، تا سال ۲۰۰۱ (وقتی مدرسه را ترک کرد) به دبیرستان داوونی، کالیفرنیا، می‌رفت. وی در یک کافه اینترنتی کار می‌کرد و به گفته خانواده، می‌خواست به ذخیره نظامی بپیوندد. در حدود ژوئن ۲۰۰۴، وی پس از کشف rxbot، کرم رایانه‌ای رایج که می‌تواند شبکه رایانه‌های آلوده‌اش را گسترش دهد، شروع به کار با بات‌نت کرد.

● باتنت

Botnet یک اصطلاح برای مجموعه‌ای از روبات‌های نرم‌افزاری است که به طور خودمختار و خودکار اجرا می‌شوند.

او در جایی از منطقه، نیم میلیون سیستم رایانه‌ای ربود. این نه تنها بر رایانه‌هایی مانند خانه شما تأثیر گذاشت بلکه به او و دیگران این امکان را داد که حملات در مقیاس بزرگ را برپا کنند.

Silicon Valley

مریم عتباتی

دره سیلیکون منطقه ای در قسمت جنوبی منطقه خلیج سان فرانسیسکو در کالیفرنیا شمالی است که به عنوان یک مرکز جهانی برای فناوری های پیشرفته، نوآوری، سرمایه گذاری و رسانه های اجتماعی خدمت می کند. کلمه "سیلیکون" در ابتدای نام این دره به تعداد زیادی از مبتکران و تولید کنندگان در منطقه که متخصص در ترانزیستورهای مبتنی بر سیلیکون هستند، اشاره دارد.

این منطقه در حال حاضر شامل دفتر مرکزی بزرگترین شرکتهای برتر فناوری و همچنین بیش از هزاران شرکت نوپا است. از همین روست که دره سیلیکون یک سوم از کل سرمایه گذاری ها را در ایالات متحده به خود اختصاص داده است، که به آن کمک کرده تا تبدیل به یک اکوسیستم پیشرو و نوآورانه برای نوآوری با تکنولوژی بالا و توسعه علمی شود.

تاریخچه:

چه چیزی باعث شده Silicon Valley یک مرکز اصلی برای کارآفرینان باشد؟ و چرا این مسئله به یک مزیت تبدیل شده است؟



در یک کافی شاپ بنشینید و یک تیم تشکیل دهید، مقداری پول جمع کنید و شروع به کار کنید. شتاب دهنده های زیادی مانند Y Combinator شروع به کار را آسان می کند و به دلیل خدمات وب آمازون (زیرساخت های مبتنی بر ابر) و ابزارهای توسعه نرم افزار و چارچوب های مشخص، هزینه راه اندازی یک شرکت به میزان قابل توجهی کاهش یافته است.

با این حال، ما به جایی رسیده ایم که نژاد پرستی، تبعیضهای جنسیتی و سنی، سوء مصرف مواد مخدر و الکل، خودکشی و افسردگی به مشکلات شدید دره سیلیکون تبدیل شده اند.

ناگفته نماند که هم اکنون می توان یک شرکت را در هر نقطه و به ویژه در نزدیکی دانشگاه راه اندازی کرد. بیا بیا برای ایجاد فرهنگ کارآفرینی، که واقعاً یک فرهنگ تاب آوری است، به Silicon Valley اعتبار بدهیم و سپس بدانیم که برای رسانه های دیجیتال، بهشت نیست.

ترانزیستور در سیلیکون دره اختراع و ساخته شد، که به صنایع منطقه رادیو و تلگراف می دهد. تا سال ۱۹۵۷، روسیه با Sputnik یک رقابت بزرگ فضایی را آغاز کرد و دولت ایالات متحده ناسا را تأسیس کرد. در زمان افتتاح ناسا تنها شرکتی که قادر به ساخت الکترونیک برای کپسول فضایی بود Fairchild Semiconductor بود. افسانه دره سیلیکون از ابتدای صنعت ترانزیستور با مستندهای نوشته شده کاملاً مشهور است. بیشتر موفقیت های اولیه دره از دو مولفه تراشه های سیلیکون و سخت افزاری که تراشه ها در آن قرار گرفته اند ناشی شده است. تراشه های سیلیکون الهام دهنده اسم دره نیز هستند.

خواندن تاریخ دره از این جهت سرگرم کننده است که متوجه میشویم موسسین آن مهندسانی بودند که هدفشان عملی کردن ایده هایشان در مورد توانایی های علم و فناوری بوده است.

مانند طرح یک کتاب که رادیویی پوشیدنی را تصویر میکرد و در آن دوران به عنوان طنز کشیده شده بود و اکنون ما آن را به نام اپل واچ میشناسیم و استفاده میکنیم!

در آن زمان که مهندسين بيش از پول به دنبال ممکن کردن ناممکنها بودند. این مسئله باعث شد که دره هم از کمکهای دولت و هم سرمایه گذاری را پذیرا باشد.

اگر به تاریخچه دره سیلیکون علاقه مند هستید، ممکن است بخواهید نمایش Silicon Valley از شبکه HBO را که با لحن طنز خودش به شما همه چیزهایی را که باید در مورد دره بدانید میگوید را تماشا کنید. همچنین فصل چهارم AMC's Halt and Catch Fire که می تواند شما را از دهه ۱۹۸۰ به ظهور شبکه جهانی وب ببرد.

اکنون به جایی رسیده ایم که سیلیکون ولی یک اکوسیستم غنی است که در نهایت همه افراد با ایده خود را نشان می دهند زیرا این امکان وجود دارد که

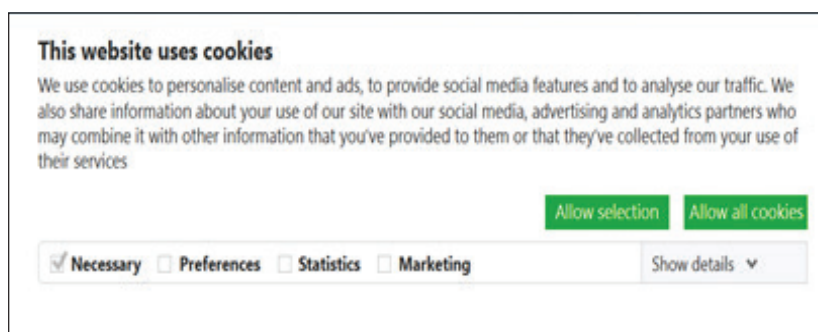
دره سیلیکون، سن خوزه، کالیفرنیا



همه چیز درباره "cookies"

روشنک حسین زاده عطار

اگر دقت کرده باشید با ورود به اکثر سایت‌ها پیامی مبنی بر اینکه «این سایت از cookies استفاده می‌کند آیا موافق هستید؟» در زیر صفحه ظاهر می‌شود:



که خب اکثرا خواننده نخوانده گزینه موافقم را می‌زنیم تا سریع‌تر به کارمان برسیم و بی تفاوت از کنار این پیغام می‌گذریم، غافل از اینکه در بسیاری از مواقع در حال استفاده از کوکی‌ها هستیم بدون اینکه خودمان بدانیم. سوال اول که مطرح می‌شود این است که:

cookies چیست؟

کوکی‌ها ماهیتاً فایل‌هایی حاوی متن و یا به زبان عامیانه text file هستند، این فایل حاوی اطلاعاتی است که دسترسی دوباره به سایت را برای کاربر و البته سرور سایت راحت‌تر می‌کند. وقتی کاربر وارد سایت می‌شود و اعلام می‌کند مشکلی با کوکی‌ها ندارد فایل متنی را سیستم کاربر ساخته می‌شود و اطلاعات کاربر اعم از خریدهایی که به سبدش اضافه کرده، موقعیت مکانی کاربر، نام کاربری و ... و هر اطلاعاتی که کاربر وارد کند را ذخیره می‌کند. البته امکان ذخیره‌سازی رمز عبور هم وجود دارد اما به دلایل امنیتی مجدداً سوال می‌پرسید که «آیا می‌خواهید رمز عبور هم ذخیره شود؟».

اینجا مرورگر واسط بین کامپیوتر کاربر و سایتی است که به آن وارد شده، وقتی برای بار بعدی کاربر وارد همان سایت می‌شود مرورگر فایل ساخته شده روی سیستم کاربر را می‌خواند و به سایت انتقال می‌دهد. رایج‌ترین نوع کوکی‌ها همین کوکی‌های احراز هویت (authentication cookies) هستند که نام کاربری و رمز عبور را ذخیره می‌کنند، اگر قرار به این باشد که هر سایت در حافظه خودش اطلاعات تمام کاربران را ذخیره کند و کل

آن کوکی را حذف می‌کنید. خب برای تکمیل بحث امنیت کوکی‌ها می‌خواهم چند مورد از امن‌ترین مرورگرها را معرفی کنم. طبق گفته‌های سایت «restoreprivacy.com» بهترین مرورگرها از نظر امنیت:

۱. Firefox

۲. Iridium browser

۳. GNU IceCat browser

شما می‌توانید با مراجعه به این سایت با مزیت‌های این مرورگرها و چند مرورگر خوب و امن دیگر هم آشنا شوید.

اما یک سوال دیگر هم اینجا مطرح می‌شود و آن اینکه:

خب ما قبلا هم وقتی از یک سایت خرید می‌کردیم در سبد خرید همه اجناس ذخیره می‌شد و حتی نام کاربری و بقیه‌ی اطلاعات به صورت اتومات وارد سیستم می‌شدند از طرفی به تازگی این پیغام کوکی را روی سایت‌ها مشاهده می‌کنیم پس قبلا به چه صورت بوده است؟!

خب قضیه این است که ما مدت زیادی - تقریبا از سال ۱۹۹۶- هست که از مزایای کوکی‌ها استفاده می‌کنیم فقط خودمان نمی‌دانیم! قبلا کوکی‌ها به صورت پیش فرض اجازه‌ی دسترس‌داشتند اما به تازگی استانداردها عوض شده و به خاطر امنیت بیشتر سایت موظف هستند برای استفاده از کوکی‌ها از کابر تایید بگیرند.

آیا ما برای هر سایتی که راه اندازی می‌کنیم به کوکی احتیاج داریم؟ نه! اگر شما وبلاگی را راه اندازی کردید تا صرفا دلنوشته‌هایتان را منتشر کنید و سایت قسمتی برای عضو شدن هم نداره نیازی به کوکی نیست اما اگر سایت شما سایت فروشگاه هست و باید افراد وارد اکانت خودتون بشوند و باید برای ذخیره‌ی نام کاربری، رمز عبور، سبد خرید، موجودی کیف پول و ... از کوکی‌ها استفاده کنید تا سرور سایت مجبور به پیدا کردن اطلاعات نباشد و سایت دچار کندی نشود. می‌خوام چند تا از کوکی‌های مرسوم را به طور خلاصه معرفی کنم، البته کوکی‌ها به چند مدل قابل دسته‌بندی هستند این دسته‌بندی بر اساس روش کار آنهاست:

۱. **Session cookies**: این کوکی‌ها دارای حافظه‌های موقت و تقریبا کم هستند و برای نشان دادن آیتم‌های موقت هستند و با بسته شدن مرورگر بلاک می‌شوند و تقریبا می‌شود گفت هیچ خطری ندارند اولاً چون موقت هستند و خودکار بلاک می‌شوند و دوماً هیچ اطلاعاتی از کاربر نمی‌گیرند.

پروسه احراز هویت را خودش انجام بدهد روند سایت کند می‌شود! اما الان با استفاده از کوکی‌ها بخشی از پروسه به عهده سیستم هر کاربر است و این روند بازبایی اطلاعات را تسریع می‌بخشد. حالا که با مفهوم این موجود پرکاربرد آشنا شدیم سوالی که پیش می‌آید این است که:

آیا باید به خاطر کوکی‌ها نگران امنیت اطلاعات خود باشیم؟

خب خبر خوب این است که کوکی‌ها به لحاظ ماهیت نمیتوانند عامل انتقال ویروس یا بد افزار (malware) به سیستم شما باشند تنها بدیشان این است که ممکن است یک سری تبلیغ روی سیستم ایجاد کنند که خب آن هم با یک گزینه «نه ممنون» می‌رود و کار ما را مختل نمی‌کند. اما آیا صددرصد امن هستیم؟ دوست عزیزم باید بگویم توی دنیای اینترنتی چیزی به اسم امنیت صددرصد وجود خارجی ندارد اساسا، فقط یک مدل از کوکی‌ها وجود دارند که ممکن است دردساز شوند آن هم «tracking cookie» خب کاربرد این کوکی‌ها می‌تواند با بقیه مدل‌ها متفاوت باشد و اصلا قصد آسان کردن دسترسی به اطلاعات را نداشته باشند. این کوکی‌ها می‌توانند بفهمند به چه سایت‌هایی مراجعه

کردید و چه اطلاعاتی نظیر ایمیل یا نام خانوادگی یا اسم دوستانتان و ... را وارد کردید و آنها را ذخیره کنند و ممکن است بشود از این اطلاعات سو استفاده کرد البته شما به راحتی به صورت دستی هر کوکی را که می‌خواهید غیرفعال

کنید یا حتی حافظشان را پاک کنید. البته حواستان باشد که اگر کوکی‌های احراز هویت فیسبوک را پاک کنید دیگر به صورت اتومات وارد اکانتتان نمی‌شوید و باید خودتان نام کاربری و رمز را دستی وارد کنید.

امنیت اطلاعات شما در سایت‌هایی که به آنها مراجعه می‌کنید بستگی دارد و البته به مرورگرتان اینکه مرورگر شما با چه روشی اطلاعات شما را رمز گذاری یا به اصطلاح encrypt می‌کند و اگه مرورگر شما امنیت قابل قبولی داشته باشد دیگر نیازی به نگرانی نیست و با خیال راحت می‌توانید به سایت‌ها اجازه‌ی استفاده از کوکی‌ها را بدهید و مطمئن باشید به احتمال زیادی کسی نمی‌تواند به راحتی اطلاعات شما را رمز گشایی کند و بخواند، یادتان باشد فقط یک تعداد سایت محدود هستند که اگر به کوکی‌هایشان اجازه‌ی دسترسی ندهید همچنان قابل استفاده هستند، بنابراین توصیه این است که تا حد امکان به کوکی‌ها دسترسی بدهید نهایتا بعد از استفاده از سایت مورد نظر در قسمت تنظیمات مرورگر



Scan me

۲. **Peristent cookies**: این کوکی‌ها می‌توانند برای مدت طولانی اطلاعات را ذخیره کنند، این نوع کوکی‌ها همان‌هایی هستند که وقتی گزینه‌ی "مرا به یاد بسپار" را تیک می‌زنیم دست به کار میشوند. جذابیت این کوکی‌ها این است که مهم نیست در چه سایتی ساخته شوند، می‌توان در تمامی سایت‌های مرتبط از آن‌ها استفاده کرد، برای مثال اگر در یک سایت به اکانت گوگل یا فیس بوک خودتان متصل شوید در هر سایت دیگری لازم باشد به طور خودکار اتصال برقرار می‌شود. این کوکی‌ها می‌توانند خطرناک باشند.



۱- سیستم عامل یونیکس (UNIX) در سال ۱۹۷۰ توسط شرکت AT&T به عنوان اولین سیستم عامل دنیا تولید شد اما به دلیل اینکه open source نبود و قیمت بالایی هم داشت (حدود ۱۰۰,۰۰۰ دلار) تنها مورد استفاده برخی شرکت‌های نظامی آمریکا و برخی سیستم‌ها دانشگاهی بود و الان به عنوان مجموعه‌ای از سیستم عامل‌ها شناخته می‌شود.

۳. **First-party cookies**: این کوکی‌ها منحصر به هر سایت هستند و فقط در سایتی قابل استفاده هستند که ساخته شده‌اند و حاوی اطلاعات کاربر مرتبط با همون سایت به خصوص هستند.

۴. **Third-party cookies**: این کوکی‌ها به کوکی اصلی اضافه می‌شوند یکی از مهم‌ترین کاربردهای آن‌ها در کوکی‌هایی است که حاوی تبلیغات هستند وقتی کاربر روی تبلیغ کلیک می‌کند از این کوکی‌ها برای ارتباط شما با سایتی که تبلیغش بالا آمده استفاده می‌شود. و اما آخرین نکته اسم این موجودات هست! همگی میدونیم که کوکی واقعی-شیرینی-هیچ ربطی به این قضیه نداره! ولی اسمشون توسط برنامه‌نویس شبکه‌های وب "Lou Montulli" شده که البته لو هم این اسم را از یکی از برنامه‌نویس‌های سیستم عامل یونیکس^۱ الهام گرفته، اون برنامه نویس از عبارت "magic cookie" برای یکی از برنامه‌های یونیکس استفاده کرده بود.

Dijkstra دانشمند کامپیوتر

پریناز میرباقری

شایسته است که مهندسين کامپیوتر دانشمندان حوزه‌ی خود را بیشتر بشناسند، از این رو شما را به مطالعه‌ی مطلب پیش رو دعوت می‌کنم. ادسخر دکسترا، دانشمند هلندی، در سال ۱۹۳۰ به دنیا آمد و در سال ۲۰۰۲ از دنیا رفت. دکسترا یک برنامه‌نویس، مهندس نرم‌افزار و یک پیشرو در علم کامپیوتر بود. شاید شما دکسترا را بیشتر با الگوریتم کوتاه‌ترین مسیر در درخت به یاد بیاورید اما بهتر است بدانید که این فرد الگوریتم‌های بسیار بیشتری را به دنیای کامپیوتر ارائه و مسائل گوناگون بسیاری را حل کرده است.



بیوگرافی

پدر دکسترا شیمی‌دان و مادرش ریاضی‌دان بود. جالب است بدانید دکسترا ابتدا علاقه به مسائل حقوقی داشت و آرزوی وی معرفی هلند به جامعه‌ی بین‌الملل بود. با این حال پس از اتمام دبیرستان در سال ۱۹۴۸ با هدایت پدر و مادرش، در زمینه‌ی ریاضی و فیزیک و سپس تئوری فیزیک در دانشگاه لیدن تحصیلات خود را ادامه داد. در سال ۱۹۵۰ کامپیوترها پدیده‌ی نوینی بودند و دکسترا به صورت اتفاقی از طریق یکی از استادان سرپرست خود به مرکز ریاضیات در آمستردام معرفی شد و در سال ۱۹۵۲ به اولین برنامه‌نویس در هلند تبدیل شد. در سال ۱۹۵۹ دکسترا با اتمام پایان‌نامه‌ی خود با عنوان ارتباط با یک کامپیوتر خودکار که به توصیف زبان اسمبلی اختصاص داده شده بود، PHD خود را دریافت کرد.

در مرکز ریاضیات آمستردام، دکسترا به همراه دو عضو دیگر مسئول ساخت یک کامپیوتر بودند. اهداف آن‌ها طراحی رابط کاربری بین سخت‌افزار و نرم‌افزار و طراحی سخت‌افزار بود و دکسترا به عنوان برنامه‌نویس برای قسمت نرم‌افزاری کد می‌نوشت. دکسترا الگوریتم کوتاه‌ترین مسیر را در ساخت کامپیوترهای ARMAC در سال ۱۹۵۶ پیدا کرد اما تا سال ۱۹۵۹ آن را منتشر نکرد.

مشارکت‌ها و تاثیرات علمی

دکسترا به عنوان یکی از اولین پیشروها در زمینه‌ی علوم کامپیوتر توانست مفاهیم زیادی را به دیدگاه‌های مهندسی و آکادمی اضافه کند. مفاهیمی که هم اکنون جزو استانداردهای علوم کامپیوتر به شمار می‌روند. بسیاری از مسائل مهم توسط دکسترا مطرح و حل شده است. همچنین خوب است بدانیم در سال ۱۹۹۴ هزاران نفر از اساتید علوم کامپیوتر گرد هم آمدند و ۳۸ مقاله‌ی تاثیرگذار در این رشته را انتخاب کردند که از بین آن‌ها، ۵ مقاله توسط دکسترا نوشته شده است.

تلاش‌های دکسترا در حوزه‌ی الگوریتم، مخصوصاً الگوریتم‌های گراف، هم‌زمانی (Concurrent) و توزیع‌شده (Distributed) نقش بسیار مهمی در اکثر حوزه‌های علوم کامپیوتر دارد. الگوریتم کوتاه‌ترین مسیر (SPF) که اکنون با عنوان الگوریتم دکسترا شناخته می‌شود، همچنان مورد استفاده قرار می‌گیرد و دانشمندان تنها تلاش کردند با استفاده از جستجو بر حسب تجربه (heuristics) مرتبه زمانی این الگوریتم را کاهش دهند.

پس از الگوریتم SPF دکسترا با یک مشکل سخت‌افزاری روبرو شد: کاهش دادن ورودی‌های پشت پنل ماشین. برای حل این مسئله، دکسترا الگوریتم کاهش‌یافته‌ی Prime را ارائه داد.

در سال ۱۹۶۱ دکسترا الگوریتم shunting yard را برای pars کردن عبارات ریاضی در فرمت infix را ارائه داد. این الگوریتم برای تولید عبارات با فرمت معکوس لهستانی (NPR) یا abstract syntax tree (AST) به کار می‌رود. در سال ۱۹۶۲ یا ۱۹۶۳ دکسترا مکانیسم سمافور را برای حل مشکل انحصار متقابل (Mutual Exclusion) پیشنهاد داد که تعمیمی برای الگوریتم Dekker است. همچنین دکسترا پدیده‌ی بن‌بست را شناسایی و الگوریتم بانکدار را برای پیشگیری از بن‌بست ارائه داد.

در سال ۱۹۷۴ دکسترا سه الگوریتم خود تثبیت‌کننده برای راه حل انحصار متقابل در یک حلقه ارائه داد. در اواسط دهه‌ی ۱۹۷۰ دکسترا دو مفهوم انتزاعی (mutator و collector) در زمینه‌ی garbage collection (فرمی برای مدیریت حافظه) ارائه داد.

در سال ۱۹۸۰ دکسترا به همراه شولتن الگوریتم دکسترا - شولتن را برای تشخیص خاتمه در سیستم‌های توزیع‌شده ارائه دادند. در سال ۱۹۸۱ دکسترا الگوریتم smoothsort را که مبتنی بر مقایسه است را به همراه تغییری در الگوریتم heapsort ارائه داد.

ساختار کامپایلر و تحقیقات درباره‌ی زبان‌های برنامه‌نویسی

دکسترا به علاقه داشتن به زبان ALGOL مشهور بود. وی به همراه تیم خود سعی بر اجرای اولین کامپایلر بر روی زبان ALGOL ۶۰ (ALGOrithmic Language) (۱۹۶۰) کرد.

کردند. ALGOL ۶۰ باعث شد تا زبان‌های BCPL، B، Pascal، Simula و C به وجود بیایند. همچنین ALGOL ۶۰ جزو اولین کامپایلرهای بود که از ویژگی بازگشتی بودن زبان‌ها حمایت می‌کرد. کتاب کوتاه دکسترا با عنوان مقدمه‌ای بر برنامه‌نویسی زبان ALGOL ۶۰ تا سال‌ها مرجعی برای این زبان بود.

الگوهای برنامه‌نویسی و متدولوژی

در سال‌های ۱۹۵۰ تا ۱۹۶۰، برنامه‌نویسی یک حوزه‌ی آکادمیک نبود و هیچ مفاهیم تئوری یا سیستم کدنویسی نداشت بلکه صرفاً یک فعالیت حرفه‌ای به حساب می‌آمد که عده‌ی بسیار کمی درک درستی از آن داشتند.

در اواخر ۱۹۶۰ برنامه‌نویسی دچار بحران شده بود. بحران نرم‌افزار (نوشتن کد قابل استفاده، مفید و کافی در زمان معین) از همان سال‌های ابتدایی در علوم کامپیوتر وجود داشت. این بحران به دلیل پیشرفت کامپیوترها و پیچیده‌تر شدن مشکلات به وجود آمد. با افزایش پیچیدگی نرم‌افزارها، بسیاری از مشکلات نرم‌افزاری به دلیل روش‌های ناکارآمد به وجود آمد.

دکسترا با مطالعه درباره‌ی زبان‌های سطح بالا که از دستور GOTO استفاده می‌کنند، متوجه شد که این زبان‌ها ساختار بسیار ضعیفی دارند و در سال ۱۹۶۸ مقاله‌ای با عنوان پرونده‌ای علیه دستور GOTO را منتشر کرد. وی معتقد بود که ریشه‌ی اصلی تمام خطاها همین دستور است و باید حذف شود. در حال حاضر عده‌ای کمی از این دستور برای برنامه‌نویسی استفاده می‌کنند. دکسترا عقیده داشت که با استفاده از if then else و حلقه‌ی while می‌توانیم مشکلات مذکور را رفع کنیم. این متدولوژی در کتابی که با عنوان جنبش برنامه‌نویسی ساختاریافته در سال ۱۹۷۲ توسط دکسترا و دو تن دیگر منتشر شد، به عنوان اولین حرکت به سمت برنامه‌نویسی ساختاریافته در تاریخ ثبت شد.

تحقیقات درباره‌ی نرم‌افزار

تلاش‌های دکسترا برای برنامه‌نویسی ساختاریافته منجر به ایجاد پایه‌هایی برای مهندسی نرم‌افزار شد و به برنامه‌نویسان اجازه داد تا بتوانند مشکلات پیچیده‌ی نرم‌افزاری را سازماندهی و مدیریت کنند.

تکنیک‌های آنالیز و طراحی ساختاریافته نیز از مفاهیم و تکنیک‌های برنامه‌نویسی ساختاریافته ایجاد شده است و ابتدایی‌ترین ایده‌ها درباره‌ی طراحی ماژولار بوده است.

تحقیقات درباره‌ی سیستم‌های عامل

در سال ۱۹۶۰ دکسترا سیستم‌عامل THE (Technische Hogeschool Eindhoven) را طراحی کرد که از لایه‌های انتزاعی سازمان‌یافته تشکیل شده بود. مقاله‌ی وی در سال ۱۹۶۸ باعث شد تا طراحی‌های بعدی برای سیستم‌های عامل به وجود آید.

افتخارات دکسترا

- عضو آکادمی سلطنتی هنر و علوم هلند (۱۹۷۱)
- همکار برجسته‌ی جامعه‌ی کامپیوتر بریتانیا (۱۹۷۱)
- انجمن ماشین‌های محاسباتی A.M. جایزه تورینگ (۱۹۷۲)
- جایزه یادبود هری اچ. گود از انجمن کامپیوتر IEEE (۱۹۷۴)
- عضو افتخاری آکادمی هنر و علوم آمریکا (۱۹۷۵)
- دکتر دانش هونوریس کوزا از دانشگاه ملکه بلفاست (۱۹۷۶)
- دریافت کننده منشور رایانه در رایانه از انجمن کامپیوتر IEEE (۱۹۸۲)
- جایزه ACM / SIGCSE برای کمک‌های برجسته در آموزش علوم کامپیوتر (۱۹۸۹)
- عضو انجمن ماشین آلات رایانه‌ای (۱۹۹۴)
- دکترای افتخاری از دانشگاه اقتصاد و تجارت آتن، یونان

همواره از مشکلات برنامه‌نویسان چگونگی سازماندهی نرم‌افزار بوده است و همواره پیچیده‌ترین کدها در همین زمینه نوشته شده است. دکسترا در سال ۱۹۶۷ در مقاله‌ی خود سازماندهی نرم‌افزار با استفاده از لایه‌ها را توضیح می‌دهد و یک سیستم‌عامل با ۵ لایه را مثال می‌زند. هم‌اکنون ایده‌ی استفاده از لایه‌ها برای کنترل پیچیدگی به یکی از اصل‌های مهم در معماری نرم‌افزار تبدیل شده است.

برنامه‌نویسی هم‌زمانی

در سال ۱۹۶۵ دکسترا در یک مقاله مسئله‌ی انحصار متقابل را معرفی کرد و برای آن راه‌حلی ارائه داد. این راه‌حل به عنوان اولین الگوریتم هم‌زمانی شناخته می‌شود. همچنین در این مقاله مسئله‌ی ناحیه‌ی بحرانی نیز معرفی شد. راه‌حل Dekker به عنوان اولین راه‌حل صحیح برای مسئله‌ی انحصار متقابل برای دو فرآیند معرفی شده است و دکسترا این راه‌حل را به n فرآیند تعمیم داده است.

همچنین دکسترا یک مکانیسم همگام‌سازی برای فرآیندهای هم‌زمان ارائه داد. این مکانیسم همان سمافور است که شامل P و V است. همچنین برای مسئله‌ی بن‌بست الگوریتم بانکدار که یک الگوریتم پیشگیری است را ارائه داد.

دو مسئله‌ی غذا خوردن فیلسوف‌ها و آرایشگر خوابیده نیز توسط دکسترا به عنوان مثالی برای مسائل همگام‌سازی ارائه شد.

مسائل همگام‌سازی دارای مفاهیم، مکانیسم‌ها و تکنیک‌های منحصر به خود هستند. این مسائل را می‌توان در تمام فیلدهای مرتبط با علوم کامپیوتر مشاهده کرد. از اینرو مطالعه و تحقیق درباره‌ی مسائل همگام‌سازی از ارزش بسیار زیادی برخوردار است.

دکسترا در سال ۱۹۶۸ مسئله‌ی برنامه‌نویسی هم‌زمانی را برای نوشتن کدهای موازی بدون آنکه سخت‌افزار لحظه‌ای توقف داشته باشد، را معرفی کرد.

منظور دکسترا از برنامه‌نویسی هم‌زمان، برنامه‌نویسی با نمادهای استاندارد و تکنیک‌هایی برای بیان حالت‌های موازی و حل مسائل همگام‌سازی بوده است. برنامه‌نویسی هم‌زمان از این نظر مهم است که می‌توانیم حالت‌های موازی را مورد مطالعه قرار دهیم بدون آنکه در محیط نصب به مشکل بخوریم.

سیستم‌های توزیع شده

به جرئت می‌توان گفت که دکسترا بیشترین تاثیر را در زمینه‌ی سیستم‌های توزیع شده گذاشته است. حتی بعضی از مقالاتش را می‌توان به عنوان بنیان‌گذار این فیلد دانست.

کامپیوترهای کوانتومی

مهدیه غروی

سلام دوستان

در این بخش سعی دارم تا شما را با یکی از دستاوردهای جالب قرن ۲۱، یعنی کامپیوترهای کوانتومی آشنا کنم. طبق شایعاتی که درباره‌ی دستاورد گوگل منتشر شده است، برای اولین بار یک رایانه‌ی کوانتومی توانسته محاسبه‌ای را یک میلیارد بار سریع‌تر از قوی‌ترین ابررایانه‌ی کنونی جهان انجام دهد. حال می‌خواهم به ساختار جالب این نوع رایانه بپردازم که پژوهشگران در تلاشند آن را از ابزاری آزمایشگاهی به محصولی تجاری تبدیل کنند. کامپیوترهای کوانتومی با استفاده از قوانین فیزیک کوانتوم کار می‌کنند. دانشمندان هنگامی که روی ذرات بسیار ریز در حال مطالعه بودند، متوجه شدند رفتار آن‌ها تابع قوانین فیزیک کلاسیک (فیزیک نیوتونی) نیست. اینجا بود که فیزیک کوانتوم بیان شد تا رفتار آن‌ها را توجیه کند.



ویژگی کامپیوترهای کوانتومی

همان‌طور که می‌دانید کامپیوترهای امروزه با بیت‌ها سروکار دارند که یا صفر هستند یا یک. ولی کامپیوترهای کوانتومی با مفهومی به نام کیوبیت، (Qbit یا Qubit) کار می‌کنند که می‌توانند برخلاف بین‌ها سه مقدار بگیرند. (صفر، یک، صفر و یک به طور همزمان که به آن SuperPosition (برهم‌نهی) می‌گویند). برای درک بهتر آن این‌طور تصور کنید که مثلاً اگر یک اتم در راستای افقی نوسان کند یعنی مقدارش یک هست، اگر در راستای عمودی نوسان کند، یعنی مقدارش صفر هست و اگر در هر دو راستا نوسان کند، SuperPosition رخ

از ثانیه استانداردهای رمزنگاری فعلی را در هم بشکنند. از این رو اینترنت در شکل فعلی آن در برابر کامپیوترهای کوانتومی به شدت آسیب‌پذیر است و همین عامل باعث شده سازمان‌های دولتی به دنبال توسعه روش‌های رمزنگاری مقاوم در برابر آن‌ها باشد.

همان‌طور که گفته شد یک کاربرد هیجان‌انگیز این کامپیوترها در شبیه‌سازی‌ها است. شبیه‌سازی‌های دنیای کوانتوم بسیار عمیق است. در مواردی که با اتم‌ها و مولکول‌ها سروکار داشته باشیم، این کامپیوترها در این زمینه با قدرت بسیار زیادی عمل خواهند کرد و می‌توانند در آن واحد مدل‌های مختلفی را شبیه‌سازی کرده و کمک‌های بسیار زیادی به علم پزشکی و داروسازی کنند.

همان‌طور که گفتیم کامپیوترهای کوانتومی در یک لحظه تمام حالات یک مسئله را در خود دارند، حال فرض کنید از این قدرت برای شکستن رمزهای عبور و پروتکل‌های رمزنگاری استفاده شود؛ چراکه یک کامپیوتر کوانتومی در لحظه تمام رمزهای موجود را در خود دارد، تنها کافیست رمز صحیح در یک لحظه انتخاب شود!

به همین دلیل بسیاری از دولت‌ها در حال رقابت در این زمینه هستند. در حقیقت اولین کسی که بتواند به تکنولوژی رایانش کوانتومی دست پیدا کند قادر است تمام پسردهای جهان را یافته و از هر قفلی عبور کند. از سوی دیگر استفاده از قابلیت‌های کامپیوترهای کوانتومی در هوش مصنوعی قدرت پردازش و تحلیل خارق‌العاده‌ای در اختیار ربات‌ها قرار می‌دهد. احتمالاً در آینده‌ای نه‌چندان دور شاهد به حقیقت پیوستن فیلم‌های علمی تخیلی خواهیم بود. دنیایی که در آن ربات‌های هوشمند با انسان همکاری می‌کنند یا شاید علیه انسان‌ها شورش کرده و ما را به عنوان برده‌های خود به کار گیرند.

حرف آخر!

رایانه‌های کوانتومی نمی‌توانند جایگزین رایانه‌های الکترونیکی شوند. قرار دادن کیوبیت‌ها در حالت‌های شکننده‌ی کوانتومی و نگهداری آن‌ها در این وضعیت، نیازمند شرایط بسیار دشوار و فوق‌العاده سردی (نزدیک به صفر مطلق) است.

همچنین رایانه‌های کوانتومی فقط برخی مسائل خاص را سریع‌تر از ابررایانه‌های الکترونیکی حل می‌کنند و ابررایانه‌ها همچنان بخش مهمی از سخت‌افزارهای نسل آینده را تشکیل خواهند داد. پیش‌بینی دقیق تاثیر رایانه‌های کوانتومی بر پیشرفت تمدن بشر و تاثیر آن بر زندگی روزمره کار سختی است و از عهده‌ی من خارج است.

می‌دهد.

و اما SuperPosition چه فایده‌ای دارد!

فرض کنید شما چهار بیت در اختیار دارید. در حالت عادی شما ۲ به توان ۴ یعنی ۱۶ حالت دارید که تنها یکی از آن‌ها را می‌توانید در یک زمان استفاده کنید ولی اگر ۴ کیوبیت داشته باشید شما همزمان همه‌ی ۱۶ حالت را می‌توانید داشته باشید و این ۱۶ حالت به صورت موازی ذخیره می‌شوند.

ویژگی عجیب دیگر کیوبیت‌ها، Entanglement (برهم‌تنیدگی) است که وقتی دو یا چند کیوبیت با هم در ارتباط هستند، مقدارشان با هم ارتباط دارد و بی‌تاثیر از هم نیست و حتی مهم نیست که چقدر از یکدیگر دور باشند. این یعنی وقتی یک کیوبیت درهم‌تنیده را اندازه‌گیری می‌کنید، می‌توانید بدون نگاه کردن به شریکش مستقیم از ویژگی‌هایش استفاده کنید. مثلاً اگر یکی از آن‌ها بعد از اندازه‌گیری مقدار یک را داشته باشد، ما بدون اندازه‌گیری می‌توانیم بگوییم دیگری مقدارش صفر است.

برای درک بهتر سرعت این رایانه‌ها براتون یک مثال می‌زنم:

فرض کنید می‌خواهیم پسورد فایل رمزگذاری‌شده‌ی را پیدا کنیم. تنها راه‌حل این مسئله آن است که گذرواژه را حدس بزنیم و آن را امتحان کنیم. N حالت ممکن برای پاسخ وجود دارد و زمان لازم برای حدس زدن و آزمایش گزینه‌ی احتمالی برای همه‌ی آن‌ها یکسان است. اگر برای انتخاب و آزمایش گذرواژه از کامپیوترهای الکترونیکی رایج استفاده کنیم، به طور متوسط پس از تعداد $2/N$ تلاش به نتیجه می‌رسیم؛ یعنی اگر چندین بار این کار را با کامپیوترهای الکترونیکی انجام دهیم، میانگین تعداد تلاش‌های موفق به $2/N$ نزدیک می‌شود. اگر از رایانه‌های کوانتومی برای حل این مسئله استفاده کنیم، زمان لازم برای دستیابی به گذرواژه‌ی درست با رادیکال n متناسب خواهد بود.

همان‌طور که می‌بینید کامپیوترهای کوانتومی به مراتب سریع‌تر و بهینه‌تر از رایانه‌های الکترونیکی امروز هستند و می‌توانند با حل مسائلی که پیشرفته‌ترین ابررایانه‌های الکترونیکی قادر به پردازش آن‌ها نیستند، انقلابی در پیشرفت تمدن بشر ایجاد کنند.

کاربرد کامپیوترهای کوانتومی

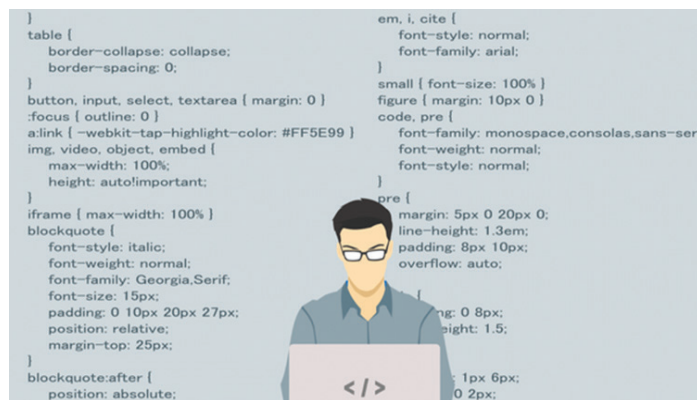
کامپیوترهای کوانتومی بیشتر در زمینه‌هایی نظیر هواشناسی، مدل‌سازی شیمی و فیزیک و رمزنگاری کاربرد دارند؛ چون این موارد شامل محاسبات پیچیده و تکراری هستند.

این کامپیوترها را می‌توان در هر لحظه در جایگشت‌های ریاضیاتی بسیار زیادی اجرا کرد که روی کاغذ (چون هنوز اجرایی نشده) به آن‌ها اجازه می‌دهد در کسری

جوایز بزرگ دنیای کامپیوتر

مریم احمدلو

خیلی از ماها موقع انتخاب رشته تمام اولویت‌های اولمون رو به مهندسی و علوم کامپیوتر اختصاص دادیم. عده‌ای هم در کنار رشته تحصیلیشون به یادگیری این علوم پرداختند. پیشرفت تکنولوژی و آینده‌ی شغلی در این حیطه موجب جذب شخص در این مسیر میشه. اما جایزه‌های بزرگ دنیای رایانه، در این باره بی‌تاثیر نیست. شاید تابه‌حال آوازه‌ی جایزه‌های بزرگ و خفن در علوم رایانه‌ای رو شنیده باشید. آوازه‌ی وسوسه‌انگیزی که خیلی از ماها رو به سوی این علوم سوق میده. در ادامه می‌خوام شما رو با بعضی از این جوایز آشنا کنم. پس اگه انگیزتونو توی این راه از دست دادید یا خدای نکرده خسته شدید این مطلب رو دنبال کنید.



جایزه تورینگ

جایزه تورینگ به صورت سالانه از سوی انجمن ماشین‌های محاسباتی به اشخاصی که سهم بسزایی در زمینه‌ی علوم کامپیوتر دارند، اعطا می‌شود. از این جایزه به عنوان نوبل کامپیوتر یاد می‌شود.

این جایزه به افتخار آلن تورینگ، ریاضیدان انگلیسی نام‌گذاری شده‌است که اغلب از وی با عنوان پدر علوم کامپیوتر نام می‌برند. شرکت‌های گوگل و اینتل حامیان مالی این جایزه ۲۵۰ هزار دلاری هستند.



Facebook hacker cup

این مسابقات رقابت‌های بین‌المللی برنامه‌نویسی است که توسط فیسبوک برگزار می‌شود. این رقابت‌ها در سال ۲۰۱۱ با هدف شناسایی استعداد های مهندسی برای کار در فیسبوک راه‌اندازی شدند که شامل مجموعه‌ی الگوریتم‌هایی است که باید در مدت زمان مشخصی حل شوند. برای حل مسائل، هیچ‌گونه محدودیتی وجود ندارد و از هر زبان و محیطی می‌توان استفاده کرد.



Top coder

TopCoder یکی از معروف‌ترین سایت‌های مسابقات برنامه‌نویسی است که در حال تبدیل شدن به لیگ اصلی مسابقات برنامه‌نویسی آنلاین است. TopCoder هر هفته اعضای خود را جمع می‌کند تا بصورت آنلاین با یکدیگر رقابت کنند و نفرات برتر دو بار در سال بصورت حضوری برای تعیین برنده‌ی نهایی، با هم به رقابت می‌پردازند.

در این سایت، کاربران رتبه‌بندی می‌شوند و کاربران برتر TopCoder، برنامه‌نویسان تمام‌عباری برای مسابقه دادن هستند که به طور مرتب در اکثر مسابقات برنامه‌نویسی شرکت می‌کنند.



جایزه هوپر

جایزه هوپر در سال ۱۹۷۱ و توسط انجمن ماشین‌سازی محاسباتی (Association of Computing Machinery) ایجاد شد. این جایزه به افتخار Grace Hooper ملکه‌ی برنامه‌نویسی نام‌گذاری شده است.



مسابقه‌ی برنامه‌نویسی گوگل

مسابقه‌ای است که گوگل هر ساله برگزار می‌کند. این مسابقات بیشتر با هدف شناسایی استعداد های بالقوه در زمینه‌ی برنامه‌نویسی و کامپیوتر انجام می‌شود و برنده مسابقه علاوه بر اینکه جایزه نقدی دریافت می‌کند، شانس استخدام در این شرکت را هم بدست می‌آورد. در این رقابت شرکت‌کنندگان ۲۷ ساعت فرصت دارند تا امتیاز لازم برای راه‌یابی به مرحله اول مسابقه را بدست آورند. نحوه‌ی برگزاری مسابقه نیز به جز مرحله پایانی که در ساختمان گوگل انجام می‌شود، بصورت آنلاین است.

محیط این مسابقه برای شرکت کنندگان هیجان انگیز، تحریک کننده و رقابتی شود.

مسابقه حل مسئله اینترنت IPSC

مسابقه IPSC یا Internet Problem Solving Contest یک مسابقه آنلاین سالانه است که در قالب تیم‌های سه نفره برگزار می‌شود. که هر تیم باید سوالات داده شده را در مدت زمان مشخصی پاسخ دهد. در این مسابقات ابتدا تعدادی مسئله بیان می‌شود که هر مسئله شامل توضیح مسئله و مجموعه داده‌های ورودی است. برای حل مسئله، شرکت کنندگان باید داده‌های خروجی صحیح را برای داده‌های ورودی محاسبه کنند. در این رویداد، شرکت کنندگان آزاد هستند که از هر زبان برنامه‌نویسی که خروجی صحیحی می‌دهد، استفاده کنند.



IEEEExtreme

IEEEExtreme که اغلب به اختصار Xtreme نام برده می‌شود، یک مسابقه‌ی برنامه‌نویسی سالانه است که در میان دانشجویان برق و کامپیوتر در سراسر جهان برگزار می‌شود. شرکت کنندگان در این مسابقه طی ۲۴ ساعت و به صورت آنلاین در گروه‌های ۲ یا ۳ نفره به حل مسائل برنامه‌نویسی می‌پردازند.

حل سوالات مسابقه در این رویداد با یکی از زبان‌های C، C++ و Java انجام می‌شود و برنده مسابقه هزینه کامل شرکت در یکی از کنفرانس‌های IEEE در هر کجای جهان را دریافت می‌کند.



SPOJ (Sphere Online Judge)

SPOJ یک سیستم داوری برنامه‌نویسی آنلاین است که ۶۴۰ هزار نفر کاربر در آن عضو هستند که می‌توانند با

ACM ICPC

ACM ICPC یک مسابقه سالانه‌ی برنامه‌نویسی دانشجویی است که در سراسر جهان برگزار می‌شود. این یک مسابقه از مهم‌ترین و معتبرترین مسابقات برنامه‌نویسی جهان است. حمایت مالی این مسابقات توسط IBM انجام می‌شود و تحت نظارت انجمن ماشین آلات رایانه‌ای (ACM) است.

ACM به صورت چند سطحی و در تیم‌های سه نفره برگزار می‌شود. هر گروه باید هشت سوال الگوریتمی را پاسخ دهد. هر تیمی که در کمترین زمان و با خطای کمتر به این سوالات پاسخ دهد، رتبه بهتری کسب می‌کند. در این مسابقات فقط زبان‌های C، C++، C#، و Java و در مواردی Python قابل استفاده هستند.



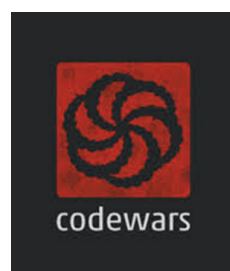
ICFP

ICFP یک کنفرانس بین‌المللی برنامه‌نویسی کاربردی است که سالانه برگزار می‌شود و هر سال، چند ماه قبل از برگزاری کنفرانس، یک مسابقه‌ی برنامه‌نویسی برگزار می‌کند. همه می‌توانند در این مسابقه حضور یابند و نیازی نیست هیچ هزینه‌ای برای ورودی پرداخت شود و نیاز به ثبت‌نام قبل از مسابقه هم نیست. شرکت کنندگان می‌توانند تیم تشکیل داده و به صورت تیم‌های چند نفره با هم رقابت کنند.



مسابقه Codewars شرکت اچ پی

Codewars (HP) Hewlett Packard از سال ۱۹۹۹ همه ساله برای رقابت دانش آموزان دبیرستانی برگزار



می‌شود. شرکت کنندگان در این رویداد از محیط پیشرفته HP، طیف گسترده‌ای از چالش‌های برنامه‌نویسی، موسیقی، پذیرایی با پیتزا و قهوه و از همه مهم‌تر جوایز متعدد برخوردار می‌شوند. همه این موارد باعث می‌شود

شرکت کرده و به رقابت با جمعی از زبده‌ترین برنامه‌نویسان ایران می‌پردازند.

مسابقه برنامه نویسی جاواکاپ

جاواکاپ یک مسابقه برنامه‌نویسی است که با هدف ارزیابی زبان جاوا و مهارت‌های برنامه‌نویسی طراحی شده است. این مسابقه در دو بخش کتبی و عملی به سنجش دانش و مهارت‌های برنامه‌نویسی شرکت‌کنندگان در حوزه جاوا می‌پردازد. به نفرات برتر در این رویداد در پایان گواهینامه و جایزه نقدی تعلق می‌گیرد.

سایت کوئرا

Quera یک سایت داوری برنامه‌نویسی آنلاین است که سالانه مسابقات برنامه‌نویسی متعددی برگزار می‌کند. کوئرا سامانه‌ای برگزاری تعدادی دیگر از مسابقات برنامه‌نویسی از جمله کدکاپ و جاواکاپ نیز است. کاربران این سایت رتبه‌بندی می‌شوند و کاربران برتر به شرکت‌های فعال در حوزه فناوری معرفی می‌شوند.



مسابقات دنیای کامپیوتر به همین جا ختم نمی‌شوند و همه ساله روند افزایشی دارند. بخاطر وجود جوایز ارزنده در این مسابقات و همچنین معرفی برندگان به جامعه‌ی برنامه‌نویسی و افزایش شانس استخدام در شرکت‌های برتر، متقاضیان زیادی نیز دارند.

اما بزرگترین جایزه‌ای که به همه شرکت‌کنندگان می‌رسد قدرت فکر کردن است.

به نقل از مرحوم استیو جابز:

”همه باید یاد بگیرند که چگونه برنامه‌نویسی کنند. زیرا به شما می‌آموزد چگونه فکر کنید.“

و اگر یاد بگیریم چگونه فکر کنیم، چگونه زیستن را خواهیم آموخت.

بیش از ۴۰ زبان برنامه‌نویسی، به سوالات پاسخ دهند. این سایت به کاربران حرفه‌ای اجازه می‌دهد تا مسابقاتی تحت قوانین خود برگزار کنند.

امتیازدهی در مسابقات این سایت به این صورت است که هر سوالی که شرکت‌کنندگان بیشتری پاسخ دهند، امتیاز کمتری دارد و به هر سوالی که کمتر حل شده باشد، امتیاز بیشتری تعلق می‌گیرد.

Sphere online judge

و در ادامه با برخی از مسابقات برنامه‌نویسی در ایران آشنا می‌شویم.

مسابقه برنامه نویسی کدکاپ

کدکاپ یک مسابقه برنامه‌نویسی است که در ایران برگزار می‌شود. برنامه‌نویسان با هر سطحی از تجربه می‌توانند در این مسابقه شرکت کنند. این مسابقه صرفاً یک رقابت فنی بین شرکت‌کنندگان نیست، بلکه قرار است مهارت برنامه‌نویسی افراد سنجیده شود و افراد برتر به شرکت‌های فعال در حوزه‌ی IT، توصیه و معرفی شوند. یکی از بخش‌های همیشگی کدکاپ، بخش الگوریتم است. مسابقات این بخش در دو مرحله‌ی آنلاین و حضوری برگزار می‌شود که شامل رقابت‌های الگوریتمی با ۱۴ زبان پرکاربرد است.

مسابقه برنامه نویسی بیان

مسابقه برنامه‌نویسی بیان یک رویداد سالانه می‌باشد که به صورت بین‌المللی برگزار می‌شود. انتخاب و استفاده از زبان برنامه‌نویسی در این مسابقه آزاد بوده و همچنین شرکت در این مسابقه به صورت انفرادی است. این مسابقه به دو بخش دانش‌آموزی و آزاد تقسیم می‌شود و اولین دوره‌ی آن در پاییز سال ۱۳۹۰ برگزار گردید.

در مسابقات بیان، برای استفاده از تکنولوژی‌ها و زبان‌های برنامه‌نویسی، هیچ محدودیتی وجود ندارد و مخاطب این رویداد تمامی کسانی هستند که توانایی برنامه‌نویسی دارند. این مسابقات بصورت انفرادی برگزار می‌شوند.

این مسابقه انتخابی کشور برای حضور در رقابت‌های ACM-ICPC جهانی است که هر ساله در دانشگاه صنعتی امیرکبیر و در قالب تیم‌های سه نفره، برگزار می‌شود. سالانه بیش از ۲۰۰ نفر برنامه‌نویس از دانشگاه‌های سراسر کشور در این مسابقه حضوری شرکت می‌کنند. این مسابقه از سال ۱۳۸۰ تاکنون در حال برگزاری است. کیفیت و اعتبار مسابقه سالانه برنامه‌نویسی دانشگاه صنعتی امیرکبیر به گونه‌ای است که علاوه بر تیم‌های این دانشگاه، دانشگاه‌های مطرح ایران از جمله دانشگاه‌های صنعتی شریف، تهران، علم و صنعت، خواجه‌نصیر و شهیدبهبشتی نیز همه ساله با چندین تیم در این مسابقه

دیپ فیک چیست؟

روشنک حسین زاده عطار



”بین و باور کن“ شعاری قدیمی که امروزه دیگر اعتباری ندارد! چرا که به کمک تکنولوژی دیپ فیک میشود برای اتفاقی که هرگز اتفاق نیفتادند ساخت. مثلا ویدیو هایی که از سیاستمداران پخش شده در حال گفتن حرف هایی که هرگز نکرده اند!

اینجا میخواهیم به یک سری از سوالات متداول در مورد دیپ فیک جواب بدیم اول اینکه اساسا دیپ فیک چی هست؟ به چه دردی میخوره؟ آیا اصلا میتونه مفید باشه یا فقط برای سواستفاده از افراد کاربرد داره؟ چه

کسانی به این تکنولوژی دسترسی دارن و اصلا چطور این کار رو میکنن؟ چطور میتونیم ویدیو های اصل رو از دیپ فیک تشخیص بدیم و اطلاعات مفید دیگه (:

اول میریم سراغ ماهیت این تکنولوژی، کلمه **deep fake** از ترکیب دو کلمه **deep learning** (که بخشی از هوش مصنوعی است) و **fake** (به معنای تقلبی) ساخته شده با کمک این تکنولوژی میتونیم جای شخصی در یک ویدیو یا عکس حضور داره رو با کسی که خودمون میخواهیم عوض کنیم.

قسمتی از دیپ فیک که شما رو وادار به باور چیزی میکنه که وجود نداره و میتونه تصاویر و صدا های تقلبی باور پذیر رو بسازه اتفاق زیاد جدیدی نیست و با استفاده از دانش یادگیری ماشین و هوش مصنوعی (نوعی که قادر باشه الگو پیدا کند) امکان پذیره.

گفتیم هوش مصنوعی که قادر باشه الگو پیدا کنه این دقیقا چه ارتباطی به دیپ فیک داره؟ برای اینکه بتونیم صورت یک نفر رو با کسی فرضا داره در یک ویدیو صحبت میکنه جا به جا کنیم باید دقیقا بدونیم صورت فرد جایگزین از تمامی زاویا چه شکلی هست و حتی در زوایای نوری مختلف صورتش چه حالتی داره.

یک از راه های عوض کردن چهره دو نفر اینکه بیاین تعداد زیادی عکس از هر دو چهره با کمک هوش مصنوعی -که اسمش اینکودر هست -رو در تهیه کنید، اینکودر شباهت های بین دو چهره رو پیدا میکنه و دو تا چهره رو روی هم میندازه (با توجه به شباهت ها) و بعد هوش مصنوعی دوم -دیکودر- وارد عمل میشه و چهره اصلی رو خارج میکنه از فریم و با این روند چهره ها جایگزین میشن.



دقیقا مرحله ای که تو این تعویض اتفاق افتاده:

راه دیگه ای که وجود داره استفاده از الگوریتم شبکه مولد تخصصی (Generative Adversarial Network)

یا به اختصار **GAN** میباشد. گن از دو الگوریتم مخالف هم تشکیل شده یکی بخش مولد و یکی بخش ممیز (generator discriminator)، به طور خلاصه و ساده بخش مولد دیتای تقلبی رو تولید میکنه و بخش ممیزی سعی میکنه تشخیص

های موجود هستند که عکس ها و ویدیو های واقعی رو در دسترس دارن میتونن بعضی اوقات ویدیو جعلی در مورد افراد معروف رو با مقایسه اون ویدیو با دیتا بیس ها تشخیص بدن.

امروزه برخی شرکت ها سرمایه گذاری های عظیمی کردن برای پیدا کردن راهی برای تشخیص ویدیو های حاصل از دیپ فیک کردن ولی خوده شرکت ها هم اقرار کردن که معلوم نیست راهی پیدا بشه یا نه چون اشاره کردیم که هر چقدر میگذره گن قوی تر و قوی تر میشه و ویدیو های طبیعی تری میسازه و تشخیص اون سخت تر میشه.

اگر ما نتونیم تشخیص بدیم چیزی که میبینیم واقعه یا نه باید به هر چیزی که میبینیم شک کنیم این روی جنبه های زیادی از زندگیمون تاثیر میزازه و کم کم میرسیم به عصر "پایانی بر حقیقت".

این ویدیو ها نه تنها بر اعقاید سیاسی ما میتونه تاثیر بزاره بلکه میتونه بسیار فرا تر بره. در حال حاضر بزرگ ترین محافظ ما در برابر این ویدیو های جعلی اینکه میدونیم ممکنه جعلی باشن!

خوشبختانه دیپ فیک در حوزه هایی هم مفید و سرگرم کننده واقع شده و اینجور نیست که همیشه برای فریب دادن افراد باشه! در بسیاری از موزه ها و گالری ها از این تکنولوژی استفاده شده مثلا یک نقاش تاریخی درباره هنرش و آثارش در یک ویدیو صحبت میکنه یا حتی موفق شدن از بازیگر های فوت شده در فیلم ها استفاده کنند!

اتفاق جالب این هست که امروزه همه میتونن به این تکنولوژی دسترسی داشته باشن و برای سرگرمی ازش استفاده کنند میتونید خودتون رو روی استیج کنار خواننده های معروف و یا کنار بازیگرانی که سال ها پیش فوت شده اند ببینید این اپلیکیشن ها که برای موبایل هم در دسترس هستند حاوی ویدیو های چند ثانیه ای هستند که میتونید بهشون عکس "خودتون" رو بدید تا صورت شما روی بدن کس دیگه ای قرار بگیره البته همونطور که میدونید به محض وصل شدن سیستم به اینترنت امنیت دیگه مفهومی ندارد پس مراقب باشید چه عکسی روی چه کلیپی قرار میگیره چون ممکنه برخی از اپلیکیشن ها حافظ اطلاعات شما نباشند! اپلیکیشن reface یکی از اپلیکیشن های سرگرم کننده در این زمینه هست که



به راحتی میتونید دانلود و استفاده کنید. اما اگر بخوایم روی هر ویدیو دلخواهی دیپ فیک رو انجام بدیم کافیه سیستمی که میخوایم ازش برای درست کردن دیپ فیک (صد البته در راه درست)

استفاده کنیم از نظر سخت افزاری قدرت کافی رو داشته باشه با اسکن کردن کردن زیر میتونید آموزش ببینید چطور خودتون یک ویدیو جعلی با استفاده از هنر دیپ فیک درست کنید.

بده اون چهره حقیقه یا نه، هر چقدر که مولد بهتر عمل کنه و پیشرفت کنه از اون طرف ممیز بیشتر یاد میگیره و پیشرفت میکنه در نهایت بالاخره یک تصویر جعلی با کیفیت بالا در این چرخه تولید میشه که توسط ممیز قابل تشخیص نیست.

حالا سوالی که مثل همیشه در این حوزه پیش میاد اینکه آیا این تکنولوژی میتونه خطرناک باشه؟

این تکنولوژی بعضی ها رو خیلی مضطرب کرده به طوری که مارکو روبیو سناتور جمهوری خواه امریکا و کاندیدای ریاست جمهوری سال ۲۰۱۶ این تکنولوژی رو سلاح هسته ای خطاب کرد و گفت: قبلا برای تهدید ایالات متحده به ده ها موشک و سلاح هسته ای احتیاج بود امروز فقط لازمه به اینترنت متصل شید و توانایی ویدیو جعلی رو داشته باشید که به حدی واقعی باشه



که کل انتخابات ما رو زیر سوال ببره! قانون های جدیدی با هدف جلوگیری افراد از ساختن ویدیو های جعلی و پخش اونها (مخصوصا در مورد افراد سیاسی مثل ویدیویی که از اوباما پخش

شد با اسکن کردن کد QR میتونید این ویدیو رو ببینید) داره در دنیا مجازی وضع میشه برای مثال توییتر و فیس بوک پخش ویدیو های جعلی یا همون دیپ فیک رو ممنوع کردن.

این ویدیو ها به بیان ساده میتونن قسمتی از مغز انسان رو هک کنند تا چیزی

که واقعی نیست رو باور کنه، و این به افراد سوذجو فرصت بسیار مناسبی داده چون همونطور که اول بحث گفتیم دیدن همون باور کردنه انسان به صورت غریزی تمایل داره چیزی که میبینه رو باور کنه و باقی توضیحات از جمله اینکه ممکنه چیزی که میبینه جعلی هست رو نادیده بگیره.

حالا چطور میتونیم ویدیو های واقعی رو از دیپ فیک تشخیص بدیم تا گرفتار اخبار دروغین نشیم؟

شاید خنده دار باشه اما باز هم جواب هوش مصنوعی هست! هوش مصنوعی ما رو گول میزنه و خودش ما رو کمک میکنه که گول نخوریم!

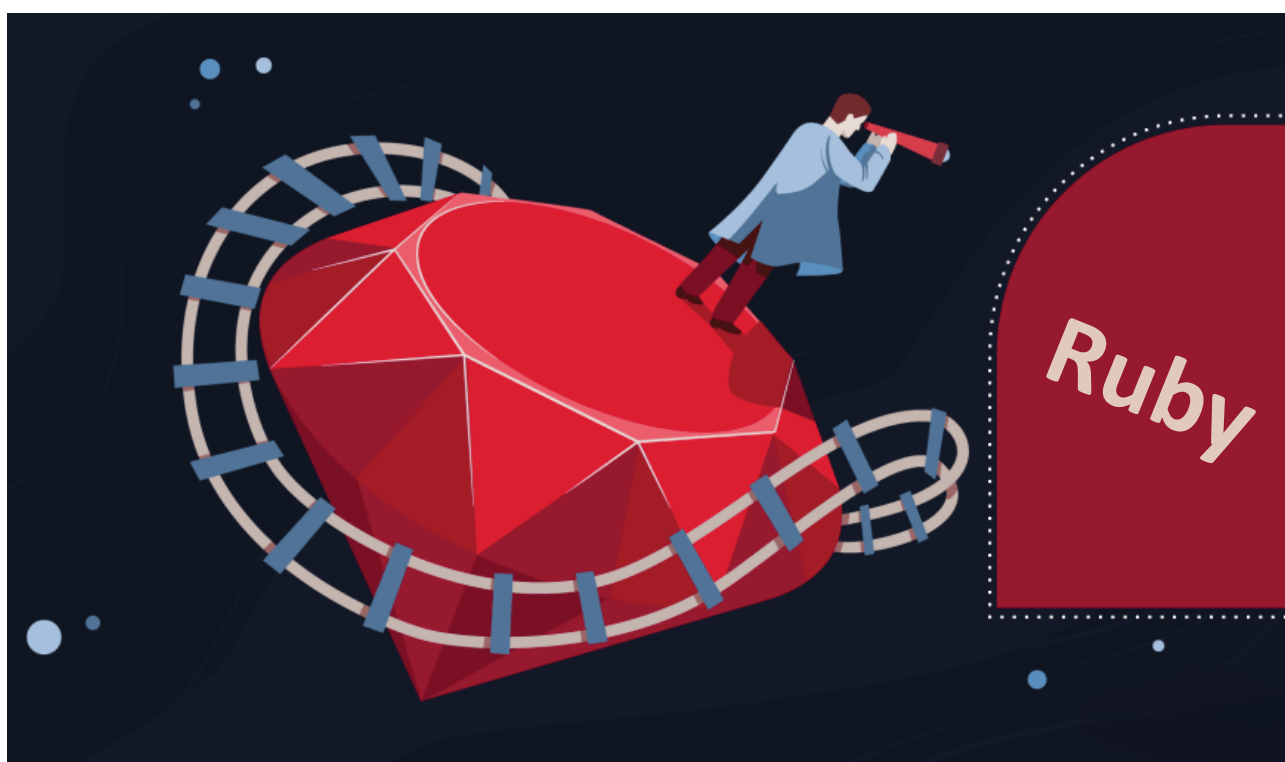
اگر ویدیو جعلی توسط یک اماتور تهیه شده باشه به راحتی با چشم غیر مسلح قابل تشخیصه و موردی نداره و اما ویدیو های حرفه ای، جعلی بودن اونها فقط توسط هوش مصنوعی میتونه اتفاق بیفته اونم اگر اشتباهی داخل ویدیو باشه اشتباهی سریعی قدر یک پلک زدن مثلا یک سایه اشتباهی.

بعضی از ابزار های تشخیص ویدیو جعلی فقط برای افراد معروف میتونن کارآمد باشن اونها فقط یک سری معیار های بسیار ساده رو در نظر میگیرن و اگر ویدیو تو یکی از اون معیار ها صدق نکنه اعلام میکنند که ویدیو جعلی هست.

یک روش تشخیص دیگه ابزار های متکی بر دیتا بیس

آشنایی با زبان Ruby

مریم عتباتی



در دنیای بی حد و مرز کامپیوتر، اگر به کار کد زنی بپردازید همیشه خوب است که نیم نگاهی به زبان های جدید داشته باشید. زبان هایی که شاید در ابتدا آنقدر بر سر زبان ها نباشند و ناشناخته به نظر برسند. امروز ما می خواهیم یکی از این زبان ها که شاید اسمش را زیاد شنیده اید اما با آن آشنا نیستید را به شما معرفی کنیم. زبان رویی (Ruby) در اصل از چند زبان الهام گرفته شده است. مخترع آن یعنی یوکیهیرو ماتسوموتو ژاپنی با تلفیق زبان های برنامه نویسی محبوب خود یعنی پرل، اسمالتاک، آیفل، آیدا و لیسپ به وجود آورده. طرفداران این زبان برنامه نویسی آن را زیبا و هنرمندانه می بینند که در عین کارآمدی ساده است. رویی قابل حمل بوده و به مانند زبان های پایتون و جاوا توانایی مدیریت استثناها را داراست.

```

function ['_CAPTCHA']['config'] = serialize($c
return array(
  'code' => $captcha_config['code'],
  'image_src' => $image_src
);

function_exists('hex2rgb') ) {
  on hex2rgb($hex_str, $return_string = false,
  ex_str = preg_replace("/[A0-9A-Fa-f]/", ' ');
  rgb_array = array();
  strlen($hex_str) == 6 ) {
    $color_val = hexdec($hex_str);
    $rgb_array['r'] = 0xFF & ($color_val >> 0x11);
    $rgb_array['g'] = 0xFF & ($color_val >> 0x08);
    $rgb_array['b'] = 0xFF & $color_val;
  } elseif ( strlen($hex_str) == 3 ) {
    $rgb_array['r'] = hexdec(str_repeat(substr($
    $rgb_array['g'] = hexdec(str_repeat(substr($
    $rgb_array['b'] = hexdec(str_repeat(substr($
  );
  return false;
}
$return_string ? implode('

```

برای اولین بار این زبان در ۲۱ دسامبر سال ۱۹۹۵ تحت عنوان روبي ۰.۹۵ عرضه شد و تا به حال به ورژن ۲.۳.۳ رسیده است.

زبان روبي شیوه های متفاوت برنامه نویسی را از جمله شی گرا، تابعی و بازتابی را به شکلی متعادل پشتیبانی میکند.

سازنده روبي در مورد زبانش می گوید که به دنبال زبانی بوده که از پایتون شی گرا تر و از پرل قوی تر باشد. و اینکه سعی کرده زبان روبي را طبیعی بسازد. نه ساده. و مثالی که همراه این مطلب آورده این است که «روبي همچون بدن انسان در ظاهر ساده و از داخل پیچیده است.»

یوکیه پرو در ادامه با فلسفی خودش تاکید زیادی دارد که در زبان های برنامه نویسی به رابط کاربری توجه زیادی نمی شود و بیشتر تمرکز روی ماشین است تا انسان.

فریمورک اصلی و محبوب زبان روبي، روبي آن ریلز است. این فریم ورک اینقدر محبوب است که خیلی از علاقه مندان به این زبان از روی شناختن آن به کد زنی به زبان روبي می پردازند.

تا به حال از روبي گونه های مختلفی توسعه یافته که میتوان از آنها به جی روبي، روبینوس، ترافل روبي، مروبی، آبرون روبي، مگلو و کاردینال اشاره کرد.

با اینکه کمی از محبوبیت روبي در طی زمان کاسته شد اما طبق سایت indeed روبي در رتبه پنجم بهترین زبان های برنامه نویسی برای یادگیری شناخته میشود و علت آن سادگی زبان ذکر شده و اینکه برای برنامه نویسی به این زبان به دانش عمیق دستورات برنامه نویسی نیست.

و در پایان طبق سنتی نانوشته شیوه چاپ کردن hello را در این زبان می آوریم:

```
puts "hello world!"
```

و چند کد مبتدی و مهم در این زبان:

```
-199.abs # 199
```

```
"ruby is cool".length # 12
```

```
"Rick".index("c") # 2
```

```
"Nice Day Isn't It?".split(/ /).uniq.sort.join # " ?DINaceinsty"
```

```
a = [1, 'hi', 3.14, 1, 2, [4, 5]]
```

```
a[2] # 3.14
```

```
a.reverse # [[4, 5], 2, 1, 3.14, 'hi', 1]
```

آشنایی با تورینگ

دلارام درودگریان

تولد و تحصیلات

آلن ماتیسون تورینگ ریاضی دان، دانشمند رایانه، منطق دان، فیلسوف، زیست - ریاضیدان، و رمزنگار بریتانیایی بود. تورینگ به عنوان پدر علم محاسبه نوین و هوش مصنوعی شناخته شده است و مهم ترین جایزه علمی رایانه به افتخار وی جایزه تورینگ نام گرفته است. همچنین دارای نشان سلطنتی و عضو کالج سلطنتی بود. از همان کودکی علایم نبوغ در وی هویدا بود. آلن تورینگ در سن ۱۴ سالگی توانست به مدرسه دولتی و پرهزینه «شربورن» در شهر دورست راه پیدا کند اما تمایل ذاتی او به سمت ریاضیات و علم نزد اساتید این مدرسه اهمیتی نداشت زیرا در آن دوره تاکید بیشتر روی مسایل و مباحث کلاسیک بود. در همان سال مدیر مدرسه برای والدین او نامه نوشت که اگر او می خواهد دانشمند شود وقت خود را در یک مدرسه دولتی هدر می دهد. با این حال تورینگ توانایی قابل توجه خود را در زمینه های مورد علاقه اش، با حل مسایل پیچیده در سال ۱۹۲۷ بدون اینکه حتی حساب دیفرانسیل مقدماتی خوانده باشد به نمایش گذاشت. در سال ۱۹۲۸ با کریستوفر مرکوم که از دانشجویان سال بالایی او بود، رابطه دوستی عمیقی پیدا کرد که این دوستی در سال ۱۹۳۰ با مرگ مرکوم پایان یافت.



آلن تورینگ

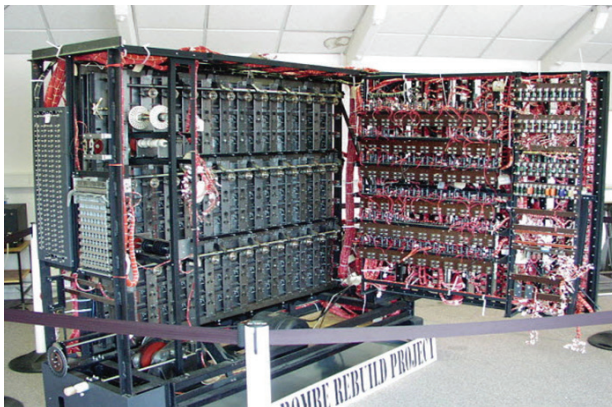
کریستوفر اولین کسی بود که پبله تنهایی او را سوراخ کرده بود و با مرگ او تورینگ در هم شکست و ایمان مذهبی خود را از دست داد.

آلن تورینگ در سال های ۱۹۳۱ تا ۱۹۳۴ مشغول تحصیل در دانشگاه کینگز کالج بود و به خاطر مقاله اش در رابطه با قضیه محدودیت مرکزی در سال ۱۹۳۵ به عنوان عضو آنجا انتخاب شد.

فعالیت های اصلی تورینگ در زمینه ی رمزنگاری به دوران جنگ جهانی دوم مربوط است. در طول این جنگ، تورینگ در بلچلی پارک (Bletchley Park) به تحقیق و ساخت دستگاه های رمزنگاری مشغول و برای مدتی مسئول بخش مربوط به تحلیل نوشته های رمزی نیروی دریایی آلمان بود. او چند روش برای شکستن رمزهای آلمان ها ابداع کرد، از جمله روش ماشینی الکترومکانیکی که می توانست ویژگی های ماشین انیگما را پیدا کند.

مساله‌ای که به آنها کمک کرد تا سرنوشت جنگ را تغییر دهند (با این حال باز هم بسیاری از رمزهای انیگما هرگز شکسته نشد).

رمزگشایی ماشین انیگما
آلن تورینگ چند هفته پس از ورود به بلجی پاریس، دستگاه الکترومکانیکی Bombe را برای رمزگشایی پیام‌های دستگاه انیگما تولید کرد. دستگاه او با بهبود فرآیندهای دستگاه لهستانی Bomba تولید شده بود. این دستگاه به جستجو میان تنظیمات احتمالی برای رمزگشایی انیگما می‌پرداخت. اولین دستگاه Bombe در ۱۸ مارس سال ۱۹۴۰ شروع به کار کرد. نابغه‌ی هوش مصنوعی در خلال فعالیت‌هایش در طول جنگ جهانی دوم، دستگاه‌های رمزگشایی متعددی تولید کرد. یکی از این دستگاه‌ها Hut ۸ نام داشت که برای رمزگشایی دستگاه مخصوص نیروی دریایی نازی‌ها ساخته شده بود. دستگاه انیگمای نیروی دریایی ارتش نازی، بسیار حرفه‌ای‌تر از دیگر دستگاه‌های انیگما بود و تورینگ با رمزگشایی تنظیمات آن، کمک بزرگی به پایان جنگ جهانی دوم کرد.



دستگاه bombe

و اما ماشین تورینگ که به نام خود تورینگ نامگذاری شده، چیست؟

آلن در سال ۱۹۳۷ مقاله‌ای را با عنوان «درباره اعداد محاسبه پذیر» منتشر کرد که به اندازه هر رویداد منحصر به فرد دیگری می‌تواند آغاز عصر جدید کامپیوتر تلقی شود. این مقاله به اختصار طرحی از آنچه را شرح می‌دهد که به آن ماشین تورینگ می‌گویند و آن کامپیوتری بود که شالوده‌اش در قلب کامپیوترهای دیجیتال بعدی قرار دارد.

این موضوع به تمام جنبه‌های کامپیوترهای ابتدایی تا مدرن، همچون توانایی خواندن، نوشتن و پاک کردن داده‌ها، حافظه‌ای برای ذخیره سازی داده‌ها، یک واحد پردازش مرکزی و به معنای یک برنامه به واسطه مجموعه‌ای از دستورالعمل‌های ریاضیاتی ساخته شده، شکل داد. ماشین تورینگ در واقع یک وسیله تخیلی است که دارای

حالا توضیح مختصری درباره ماشین انیگما می‌دهیم تا یک آشنایی کلی با آن پیدا کنید:

آرتور شریبوس مخترع و مهندس آلمانی، ماشین رمزنگاری انیگما را اختراع کرد. انیگما یک وسیله الکترومکانیکی بود و زمانی که کلید یک حرف بر روی این دستگاه فشار داده می‌شد، درون آن یک جریان الکتریکی بوجود می‌آمد و قطعات مکانیکی متحرک، مسیر این جریان رو تغییر میدادند تا در نهایت یک حرف دیگر تولید شود. وظیفه ماشین انیگما تبدیل پیغام‌های خوانا به ناخوانا یا همان عمل رمزنگاری بود. ارتش نازی در طول جنگ جهانی دوم به منظور رمزنگاری و رمزگشایی پیام‌های نظامی، مدل خاصی از این ماشین به نام انیگمای ورماخت را تولید نمود. این دستگاه می‌توانست رمزهایی غیرقابل حل را به شکل یک سری اعداد و حروف بدون معنی تولید کند.

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



ماشین انیگما

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 خواهد کرد.

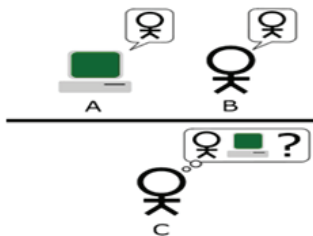
برمیگردیم به موضوع اصلی:

از سپتامبر سال ۱۹۳۸، آلن تورینگ در سازمان رمزنگاری بریتانیا به نام GC&CS به فعالیت پاره‌وقت مشغول بود. این سازمان امروزه با نام ستاد ارتباطات دولت بریتانیا شناخته می‌شود. تمرکز اصلی فعالیت‌های تورینگ در این سازمان، رمزگشایی دستگاه انیگما بود. آلن تورینگ رمزنگاری این دستگاه‌ها را به همراه همکار ارشدش دیلی ناکس و همکاری کاشناسان دیگر انجام می‌داد؛

آزمایش تورینگ

آلن تورینگ شکی نداشت که کامپیوترها نه تنها نقش فزاینده‌ای در زندگی نسل‌های بعدی ایفا خواهند کرد بلکه متقاعد شده بود که آنها ترجیحا به سطحی از مهارت خواهند رسید که می‌توانند همانند انسان‌ها فکر کنند. برای اندازه‌گیری زمانی که در آینده این امر در اختیار قرار می‌گیرد، او آزمایشی را که در مقاله سال ۱۹۵۰ با عنوان دستگاه محاسبه و نبوغ مختصرا شرح داده بود، اختراع کرد.

آلن در این مقاله معیاری را برای تعیین میزان هوشمندی رایانه پیشنهاد کرد که پس از نیز آن به آزمایش تورینگ معروف شد و از این قرار بود که: "سزاوارترین معیار برای هوشمند شمردن یک ماشین، این است که آن ماشین بتواند انسانی را توسط یک پایانه «تله تایپ» به گونه‌ای بفریبد که آن فرد متقاعد گردد با یک انسان روبروست." برای اینکه تمرکز آزمون بر روی هوشمندی ماشین باشد، و نه توانایی آن در تقلید صدای انسان، مکالمه تنها از طریق متن و صفحه کلید و نمایشگر کامپیوتر صورت می‌گیرد.

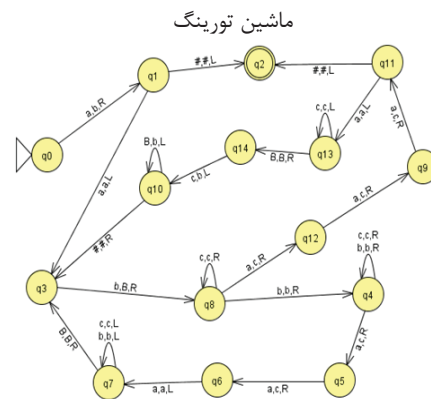
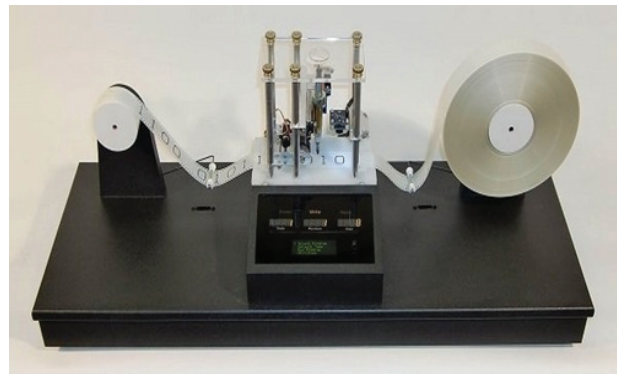


شمایی از آزمون تورینگ

جایزه لوبنر

جایزه‌ی لوبنر به‌طور سالانه به نرم‌افزارهایی اعطا می‌شود که توسط آزمون تورینگ موجب ارزیابی قرار می‌گیرند و تا حد زیادی به هوش انسانی نزدیک می‌شوند. قالب کلی رقابت لوبنر بر اساس آزمون تورینگ استاندارد است؛ اما تغییراتی نیز در آن اعمال شده است. برای مثال، در سال‌های اولیه‌ی برگزاری این رقابت، مدت زمان داده شده به داوران برای گفتگوی متنی با شرکت‌کنندگان و اعلام رأی تنها ۵ دقیقه بود؛ اما این زمان تدریجا افزایش پیدا کرده و از سال ۲۰۱۰ به ۲۵ دقیقه رسیده است. مدال نقره‌ی لوبنر به نرم‌افزاری اعطا می‌شود که توسط نیمی از داوران به عنوان انسان قلمداد شود و مدال طلای لوبنر به نرم‌افزاری تعلق می‌گیرد که بتواند اطلاعات را از طریق متن، تصویر و صدا دریافت کند و تمام داوران را نیز متقاعد کند که در حال گفتگو با یک انسان هستند. تا کنون هیچ نرم‌افزاری نتوانسته یکی از این دو جایزه را دریافت کند. بر اساس قوانین رقابت لوبنر، اگر نرم‌افزاری موفق شود مدال طلای لوبنر را به دست آورد، پس از آن رقابت لوبنر برای همیشه پایان خواهد یافت. آخرین برنده‌ی جایزه‌ی لوبنر، رباتی موسوم به

سه جزء اصلی می‌باشد. جزء اول، یک نوار بی‌نهایت طولانی که شامل ردیفی از مربع‌ها است؛ جزء دوم، یک هد خواندن / نوشتن است که می‌تواند در طول این نوار و در هر زمان یک مربع بالای آن به حرکت درآید و جزء سوم، مجموعه‌ای از دستورات عمل‌ها است. این ماشین قادر به خواندن و نوشتن تعدادی از نمادها است و می‌توان آن را از یک حالت به حالتی دیگر تغییر داد. هر آن‌چه این ماشین در زمان‌های مشخص انجام می‌دهد توسط حالتی که در آن قرار دارد، محتوای درون نوار و قوانینی که از آن پیروی می‌کند، تعیین می‌شود. در زمان حرکت، این ماشین مربع واقع در بالای هد خواندن / نوشتن خود را پوشش کرده، محتوای این مربع را با دستورات عمل‌های آن مقایسه کرده، عمل مرتبط (چون نوشتن، پاک کردن، خالی رها کردن) را انجام داده و به سمت راست یا چپ جهت آغاز مجدد فرایند به مربعی دیگر به حرکت در می‌آید. زمانی که ماشین به حالتی برسد که در آن هیچ دستورات عمل دیگری اجرا نشده باشد، متوقف می‌گردد. نشان‌های باقی مانده بر نوار، پاسخی را به وظیفه در دست اجرا نشان می‌دهد. این وسیله به شکلی که توصیف شده بود هرگز ساخته نشد ولی عملا به شکلی پیشرفته و اصلاح شده از دهه ۱۹۵۰ به تولید انبوه رسید. مطلب در اینباره بسیار است پس اگر علاقمند به کسب اطلاعات بیشتر در این زمینه هستید، می‌توانید به سایت <https://www.noormags.ir> رفته و کلید واژه "ماشین تورینگ" را در قسمت جستجو بنویسید تا مقاله‌های مرتبط را نمایش دهد.



ماشین تورینگ $\{2^n \mid a^n(n)\}$

نکته پایانی

یادبودها و سازه های زیادی به منظور گرامیداشت نام و خدمات پدر علم کامپیوتر در نظر گرفته شده اند مانند: جایزه تورینگ که به نوبل دنیای کامپیوتر معروف است؛ همچنین خیابان و پل آلن تورینگ در شهر منچستر و ... در سال ۱۹۹۹، مجله ای تایمز تورینگ را در میان ۱۰۰ فرد مهم قرن بیستم قرار داد. جمله ای یادبود این مجله برای تورینگ به این صورت بود: «هر فردی که دکمه ای را روی صفحه کلید می فشارد یا یک نرم افزار را باز می کند، در حال کار روی تجسمی از ماشین تورینگ است.»



جایزه تورینگ

توصیه مولف

اگر به این مقاله و زندگینامه این دانشمند علاقمند شدید پیشنهاد میکنم فیلم imitation game را از دست ندهید و همچنین کتاب آشنایی با تورینگ اثر پل استراسن.

شاد و پیروز باشید.

میتسوکو (Mitsuku) است. شخصیت تعریف شده برای این چت بات، یک دختر ۱۸ ساله اهل شهر لیدز است. میتسوکو از توانایی اولیه ای برای تصمیم گیری های منطقی برخوردار است. برای مثال، اگر از او پرسید «می توانی یک خانه را بخوری؟»، این ربات مولفه ای «ماده ی سازنده» را جستجو می کند و با توجه به این که ماده ی سازنده ی تعریف شده برای خانه «آجر» است و آجر نیز در دسته ی مولفه های غیرخورندگی قرار می گیرد، پاسخ این ربات به سوال فوق منفی خواهد بود.

اگر دوست دارید چت کردن با میتسوکو را امتحان کنید، می توانید به آدرس:

<https://www.pandorabots.com/mitsuku>

مراجعه کنید و پس از انتخاب پلتفرم مناسب، گفتگو را با میتسوکو شروع کنید.

گرچه بر اساس مشکلات ساختاری آزمون تورینگ، پیشنهاد های مختلفی برای بهبود و جایگزینی این آزمون ارائه شده اند.

(توصیه میکنم اگر علاقمند به این بخش هستید، فیلم x-machine را حتما ببینید. و همچنین برای اطلاعات بیشتر در زمینه رباتیک و هوش مصنوعی می توانید به سایت های همچون:

https://daneshyari.com/isi/articles/artificial_intelligence

<https://daneshyari.com/isi/articles/robotics> مراجعه کنید.)

زندگی و مرگ تورینگ

آلن تورینگ یک نامزدی کوتاه مدت با همکارش در پروژه ی Hut ۸ یعنی Joan Clarke داشت. نامزدی آنها به دلیل تمایلات جنسی خاص تورینگ به ازدواج نینجامید. این نابغه ی ریاضی به خاطر همین تمایلات در ۲۷ فوریه ی سال ۱۹۵۲ محاکمه شد. او از میان زندان و درمان هورمونی، دومی را انتخاب کرد. اتهامات و محاکمه ی تورینگ، حفاظت اطلاعاتی و امنیتی و همکاری او با دولت انگلستان را لغو کرد. البته شغل های دانشگاهی تورینگ تا زمان مرگش برقرار بودند. او پس از اتفاقات سال ۱۹۵۲ از ورود به خاک ایالات متحده ی آمریکا منع شد اما اجازه داشت در کشورهای اروپایی سفر کند. تورینگ هیچ گاه در طول زندگی به جاسوسی متهم نشد. او و تمام همکارانش در بلچلی تا پایان عمر از صحبت در مورد فعالیت های جنگی منع شده بودند.

در ۸ ژوئن ۱۹۵۴ کارگر خانه جسد او را پیدا کرد؛ روز قبل او در اثر خوردن سم سیانور جان سپرده بود؛ ظاهرا به خاطر سیب نیم خورده سیانوری که کنار تختش بود. بسیاری بر این باورند که مرگ او عمدی بوده، اما مادر او اعتقاد داشت که مرگ او حادثه ای بوده که به دلیل بی دقتی در نگهداری از مواد شیمیایی رخ داده است. کالبد شکافی علت مرگ را مسمومیت با سیانور یافت و پلیس مرگ را خودکشی اعلام کرد.

اینترنت اشیاء Internet of Things

مژده کوبی



تهیه کننده: مژده کوبی،
دانشجوی رشته مهندسی کامپیوتر
Prepared by: MOZHDEH Kokabi,
Computer Engineering Student



۱- مفاهیم پایه اینترنت اشیاء

امروزه نوآوری‌ها و ارتباطات با سرعت چشمگیری در حال رشد هستند. اینترنت به عنوان یکی از بدیع‌ترین ابزارهای ارتباطی در حال تکامل و رشد است و هر روزه دستگاه‌های بیشتری در حال اتصال به شبکه هستند و شبکه‌ها در حال گسترش می‌باشند. گسترش ارتباطات و فناوری‌های مرتبط و همچنین وجود دستگاه‌هایی با قابلیت اتصال به شبکه اینترنت منجر به ایجاد شبکه بسیار گسترده‌ای از دستگاه‌ها و اتصال‌ها شده، که مفهومی به نام اینترنت اشیاء را شکل داده است. [۱]

اینترنت اشیاء مفهومی است که به شرایطی اطلاق می‌شود که وسایل موجود در محیط بتوانند به شبکه اینترنت متصل و توسط برنامه‌های کاربردی مدیریت شوند. اینترنت اشیاء به زبان ساده، ارتباط سنسورها و دستگاه‌ها با شبکه‌ای است که از طریق آن می‌توانند با یکدیگر و با کاربرانشان تعامل کنند. این مفهوم می‌تواند به سادگی ارتباط یک گوشی هوشمند با تلویزیون باشد و یا به پیچیدگی نظارت بر زیرساخت‌های شهری و ترافیک. از ماشین لباسشویی و یخچال گرفته تا پوشاک، این شبکه بسیاری از دستگاه‌های اطراف ما را در برمی‌گیرد.

در سال ۲۰۱۳، طرح استانداردهای جهانی اینترنت اشیاء (IOT-GSI) مطرح شد و این استانداردها به عنوان زیرساخت جامعه اطلاعاتی معرفی گردید. برای این اهداف یک "چیز" در واقع یک شیء از جهان فیزیکی (چیزهای فیزیکی) یا جهان اطلاعات (چیزهای مجازی) است که قادر به شناسایی و یکپارچه‌سازی شبکه‌های ارتباطی می‌باشد. اینترنت اشیاء اجازه می‌دهد تا اشیاء در سراسر زیرساخت‌های شبکه موجود، از راه دور کنترل شوند. اینترنت اشیاء همچنین فرصتی برای ادغام مستقیم جهان فیزیکی به سیستم‌های مبتنی بر کامپیوتر ایجاد کرده است و به بهبود بهره‌وری، دقت و سود اقتصادی علاوه بر کاهش دخالت انسان، منجر شده است. هنگامی که اینترنت اشیاء با سنسورها و محرک‌ها تکمیل می‌شود، تکنولوژی آن به یک نمونه جامع از سیستم‌های سایبری فیزیکی که شامل شبکه‌های هوشمند، خانه‌های هوشمند، حمل و نقل هوشمند و شهرهای هوشمند است، تبدیل می‌شود. هر چیز منحصر به فردی از طریق

به اینترنت با استفاده از یک کابل فیزیکی یا یک ابزار بی سیم متصل می شویم. در زیرساخت این شبکه، یک ستون فقرات واقعی از اتصالات که دنیا را به رایانه‌های ما متصل می‌کنند، وجود دارد.

۲- کاربردهای اینترنت اشیاء

اینترنت اشیاء در حوزه‌های متعدد و گسترده‌ای کاربرد دارد اما یکی از ساده‌ترین و قابل درک‌ترین نمونه‌هایی که می‌توان مثال زد، دستگاه‌های تهویه مطبوع واقع در یک فضا مانند منزل است. نمونه‌ای از این دستگاه ساخته شده، ترموستات نست است. این دستگاه نوعی ترموستات هوشمند است که می‌تواند زمان خواب و کلیه عادات شما را یاد گرفته، زمانی که شما خواب هستید دما را با توجه به دمایی که شما دوست دارید تنظیم کند. در این حالت شما دیگر لازم نیست نگران گرم یا سرد شدن محیط زندگی‌تان در طول شب باشید. نمونه دیگر محصولات شرکت اسمارت تینگز است. این شرکت حسگرهای مختلفی را برای ایجاد خانه هوشمند در اختیار شما قرار می‌دهد. با استفاده از این حسگرها می‌توانید متوجه شوید چه شخصی وارد منزل شده یا از آن خارج می‌شود. همچنین این حسگرها قابلیت این را دارند که در صورت هدر رفتن آب نیز گزارشی مربوط به نشتی سیستم آب به شما بدهند (شکل ۱).



شکل ۱- خانه هوشمند [۳]

با گسترش و ارتقای ابزارهای موجود در این اکوسیستم، به عنوان مثال دستبند هوشمند مخصوص فعالیت‌های بدنی، می‌تواند به محض خوابیدن شما، تلویزیون و چراغ‌ها را خاموش کند و یا حتی پیش از سوار شدن بر خودرو در زمانی مشخص، بهترین مسیر برای رسیدن شما به مقصد توسط خودرو انتخاب و در صورت دیر رسیدن به محل قرار، پیامکی به شخص مقابل ارسال شود. چشم‌اندازی که برای اینترنت اشیاء می‌توان متصور بود، بسیار گسترده است و همان‌طور که از نام آن برمی‌آید شامل اتصال همه چیزها در دنیا به یکدیگر می‌شود.

سیستم‌های محاسباتی جاسازی شده قابل شناسایی و در زیرساخت اینترنت موجود است.

به طور معمول، انتظار می‌رود که اینترنت اشیاء اتصال پیشرفته از دستگاه‌ها، سیستم‌ها و خدمات که فراتر از ارتباطات ماشین به ماشین است، ارائه کند و انواع پروتکل‌ها، دامنه‌ها و برنامه‌های کاربردی را پوشش دهد. انتظار می‌رود که اتصال این دستگاه‌های تعبیه شده (از جمله اشیای هوشمند) به اتوماسیون در تقریباً تمامی زمینه‌ها کمک کند. اشیاء می‌تواند به طیف گسترده‌ای از دستگاه‌ها مانند ایمپلنت نظارت بر قلب، فرستنده زیست تراشه در حیوانات در معرض انقراض، حلزون‌های الکتریکی در آب‌های ساحلی، خودروها با سنسورهای مختلف، دستگاه‌های تجزیه و تحلیل دی‌ان‌ای، نظارت بر محیط زیست و نیز مواد غذایی و یا دستگاه‌های عملیات میدانی اطلاق شود. حقوق‌دانان «چیزها» را به عنوان یک «ترکیبی از سخت‌افزار، نرم‌افزار، اطلاعات و خدمات» قلمداد می‌کنند.

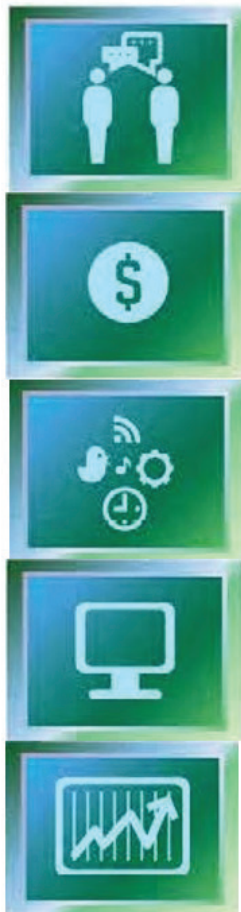
این دستگاه‌ها اطلاعات مفید را با کمک فناوری‌های مختلف موجود جمع‌آوری می‌کنند، سپس به صورت خودکار داده‌ها را بین دستگاه‌های دیگر به جریان می‌اندازند. نمونه‌های موجود آن عبارتند از: اتوماسیون خانگی مانند کنترل و اتوماسیون روشنایی، گرمایشی (مانند ترموستات هوشمند)، تهویه و لوازم خانگی از قبیل ماشین لباسشویی، جاروبرقی رباتیک، تصفیه هوا، اجاق‌گاز و یخچال که می‌توان با استفاده از اینترنت اشیاء از راه دور آن‌ها را کنترل نمود. اینترنت اشیاء یکی از سیستم عامل‌های شهرهای هوشمند امروزی و مدیریت انرژی است.

فناوری اینترنت اشیاء نقش بسیار مهمی در دنیای کارآفرینان بازی می‌کند. کسب و کارهای متعددی بر محور این فناوری راه‌اندازی شده‌اند، در حالی که این مفهوم و این فناوری در ابتدای راه خود قرار دارد و هر روز بیش از پیش تغییرات و تحولات جدیدی در آن رخ می‌دهد. استفاده از این فناوری برای کارآفرینان و محققین خلاق ایرانی یک فرصت گران‌بها به شمار می‌رود که می‌تواند به بهبود فضای کسب و کار و اشتغال‌زایی در کشور کمک شایانی نماید.

کوین اشتون با مطرح کردن مفهوم اینترنت اشیاء جهانی را به تصویر کشید که در آن هر چیزی، از جمله اشیاء برای خود هویت دیجیتال داشته باشند و به رایانه‌های مرکزی که به آنها متصلند، اجازه دهند که آن‌ها را سازماندهی و مدیریت کنند. [۲] اینترنت اشیاء سیستمی به هم پیوسته از دستگاه‌های محاسباتی، مکانیکی و ماشین‌های دیجیتالی است که هر یک از این اشیاء دارای یک شناسه واحد می‌باشند و توانایی انتقال داده در بستر شبکه بدون نیاز به دخالت انسان را دارند، در واقع این تعریف اشیاء در مفهوم اینترنت اشیاء است. [۳]

اینترنت در واقع شبکه‌ای از شبکه‌هاست. هر کدام از ما

پیش‌بینی اینترنت اشیا:



۴ میلیارد نفر افراد مرتبط با یکدیگر

۴ تریلیون دلار درآمد جدید

بیش از ۲۵ میلیون برنامه کاربردی جدید

بیش از ۲۵ میلیون سیستم‌های هوشمند و نهفته

تبادل اطلاعات ۵۰ تریلیون گیگابایت بر ثانیه

شکل ۲- چشم‌انداز اینترنت اشیا [۴]

- ۱- Things
- ۲- Machine to Machine (M2M)
- ۳- DNA
- ۴- Backbone
- ۵- Thermostat Nest
- ۶- Smart Things

شکل ۲ چشم‌اندازی از اینترنت اشیا نشان می‌دهد که در آن چهار میلیارد نفر متصل به شبکه، چهار تریلیون دلار فرصت درآمدی، بیش از ۲۵ میلیون اپلیکیشن موبایل، بیش از ۲۵ میلیارد سیستم هوشمند متصل و ۵۰ تریلیون گیگابایت حجم داده‌ها در فضای اینترنت اشیا وجود خواهد داشت. [۴]

مراجع:

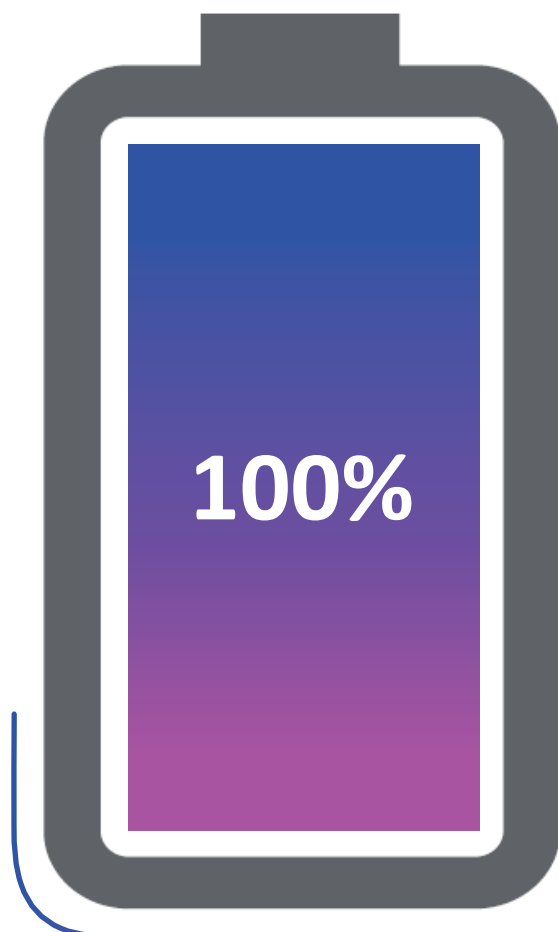
[۱] Ermesan, Ovidiu; Friess, Peter, Internet of things: covering Technologies for smart Environments and Integrated Ecosystems, 2013

[۲] Ashton, K., That 'Internet of Things' Thing, 22 June 2009, accessed 9 May 2017

[۳] Ben cole, The IoT business Model, 2017

[۸] «خانه هوشمند در اصفهان» دریافت از: خانه هوشمند در اصفهان
<http://sepasgroup.com/home>

[4] Nordrum, Amy «Popular Internet of Things Forecast of 50 Billion Devices by 2020 Is Outdated», (18 August 2016)



لطفا نظرات، پیشنهادات و انتقادات خود را از طریق راه‌های ارتباطی با ما در میان بگذارید.