پردازش

فصل نامه علمی
دانشجویی پردازش
پاییز ۹۹ / شماره هجدهم

صاحب امتیاز انجمن
علمی کامپیوتر
دانشگاه الزهرا(س)

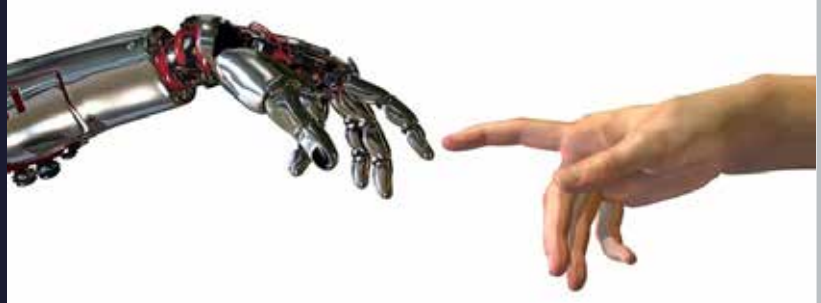
مدیر مسئول: نازنین عباسی
کارشناس نشریه: زهرا وزیری
سردبیر: پریناز میرباقری
طراح جلد: ملیکا صباغیان
صفحه‌آرایی: مائده رادفر

تحریریه
سارا حسین جانی، اسما رشیدیان،
مهدیه غروی، مریم عتباتی،
نازنین احمدپور، پریناز میرباقری

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

امور چاپ
چاپخانه دانشگاه الزهرا(س)

فهرست



سخن سـردبیر

پاییزی دیگر آغاز شد و با نشریه‌ی پردازش همراه شما عزیزان هستیم.
پیـش از شـروع هـر چیـز بـه دانشـجویان ورودی جدیـد تبریـک می‌گویـم کـه در یـک دانشـگاه سـطح بـالا و در یکـی از بهتریـن رشـته‌های مهندسـی در کشـور پذیرفتـه شـده‌اند. امیـدوارم ایـن شـروعی بـر مسـیری باشـد کـه انتهـای آن موفقیت‌هـای پی‌درپـی بـه انتظـار نشسـته اسـت.
بـا اینکـه اولیـن شـماره‌ی نشـریه در زمسـتان سـال ۱۳۹۱ منتشـر شـده اسـت، امـا تـا پیـش از آن تحـت عنـوان نـام کلیـک فعالیـت خـود را آغـاز کـرده بـود. یعنـی چیـزی حـدود ۱۰ سـال از شـکل‌گیری ایـده‌ی نشـریه می‌گـذرد. طـی سـال‌هایی کـه در نشـریه مشـغول بـه کار بـودم، ایـن را وظیفـه‌ی خـود می‌دانسـتم تـا ورودی‌هـای جدیدتـر را بـا ایـن سـنت قدیمـی آشـنا کنـم.
پـردازش میـراث کسـانی اسـت کـه روزی تصمیـم گرفتنـد در محیـط افـراد خـود تغییـری ایجـاد کننـد. کسـانی کـه انجمـن و نشـریه را تاسـیس کردنـد تـا امـروز مـا بتوانیـم بـه وسـیله‌ی آن‌هـا رشـد کنیـم. چراکـه هـدف نشـریه یادگیـری اسـت. امیـدوارم کـه راه آن‌هـا همچنـان ادامـه یابـد و دانشـجوهای جدیدالـورود هـم بتواننـد از ایـن امکانـی کـه فراهـم شـده اسـت، نهایـت اسـتفاده را ببرنـد.
هـدف پـردازش تنهـا یادگیـری علمـی نیسـت، بلکـه همدلـی و صمیمیـت هـم از ارکان مهـم آن هسـتند. رونـد تولیـد یـک نشـریه بـه دسـت تنهـا یـک نفـر ممکـن نیسـت. بلکـه چندیـن و چنـد نفـر در آن دخیـل هسـتند و همیـن اسـت کـه ارزش آن را بـالا می‌بـرد. همیـن همدلـی و صمیمیتـی کـه طـی تولیـد نشـریه بیـن بچه‌هـا شـکل می‌گیـرد.
ارزش برخـی لحظه‌هـا در زندگـی حـد و حصـری نـدارد. لحظاتـی ماننـد بخشـش یکدیگـر هنـگام کار گروهـی، تکمیـل راه دیگـران و از همـه مهمتـر جبـران کـردن اشـتباهات هم‌گروهی‌هایمـان و... این‌هـا بخشـی از لحظاتـی بـود کـه مـن در پـردازش تجربـه کـردم و از آن‌هـا چیزهایـی آموختـم کـه هرگـز در ایـن چهـار سـال تحصیلـی کسـی بـه مـن یـاد نـداد.
ایـن سـه سـال بـرای مـن فرصـت بی‌نظـری بـود کـه توانسـتم عضـوی کوچـک از خانـواده‌ی بـزرگ پـردازش باشـم. امیـدوارم کـه توانسـته باشـم نهایـت تـلاش خـود را بـرای پیشـرفت نشـریه بـه کار بـرده باشـم و امیـدوارم کـه پـردازش تـا سـال‌های سـال بـه پیشـرفت‌های خـود بـه همیـن شـکل ادامـه دهـد.
امیـدوارم کـه در ایـن روزهـای سـخت بیمـاری، تک‌تـک شـما عزیـزان و خانواده‌هایتـان در صحـت و سـلامت باشـید کـه سـلامتی بزرگتریـن هدیـه اسـت.

پریناز میرباقری

با بیردازتر همراه باشید...

padazesh_magazine

process.magazine1391@gmail.com

@padazesh_magazine

Encryption چیـــست؟

دلارام درودگریان

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 هویت موجودیت و اصل داده آمیخته شده است. علم Cryptography پیام‌های رمز نشده را به کمک مفهوم رمز نگاری، به صورت رمز شده درمی‌آورد و امروزه در واقع فرایندی برای تامین امنیت اپلیکیشن‌ها و محافظت از داده‌های مربوط به آن‌ها در برابر حملات می‌باشد؛ به طوریکه در فرایند ارسال و دریافت داده، صرفاً افراد مورد نظر، توانایی رمزگشایی داده‌های رمزنگاری شده را داشته باشند. همچنین یک حوزه وسیع محرمانگی می‌باشد که فرآیندهایی همچون encryption، hashing و ... زیر مجموعه‌های آن محسوب می‌شوند.

در این بخش ما می‌خواهیم فرایندencryption را مورد مطالعه و بررسی قرار می‌دهیم.

تاریخچه رمزنگاری:

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

همتون هیرئوگلیف

سابقه سیستم‌های اولیه رمز نگاری که گاهی به آن‌ها کد (code) یا رمز (cipher) نیز گفته می‌شود، به مصر باستان و حدودا ۲۰۰۰ سال پیش برمی‌گردد. 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 ویژه‌ای از این ماشین به نام «انیگمای ورماخت» را تولید نمود و به منظور رمز نگاری و رمز گشایی پیام‌های نظامی در طول جنگ جهانی دوم به کار می‌برد. لازم به ذکر است که پیام‌های رمزگذاری شده ارتش آلمان به وسیله انیگما، اولین بار به دست بریتانیایی‌ها شکسته شد.

این پیروزی حاصل تلاش‌های چهار ریاضیدان لهستانی به نام های ماریان ریفسکی، یژی روژیتسکی، آلن تورینگ و هنری زیگالسکی بود. همین امر در نهایت باعث پی بردن به نقاط ضعف نازی‌ها و شکست آنان در جنگ شد.(اگر 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 می‌باشد و به عملیات رمز نگاری اطلاق می‌شود و موجب می‌شود محتوای پیام ما از دید دیگران پنهان بماند. در واقع عمل encryption داده ها را به قالبی که فقط افراد مجاز می‌توانند آن را مشاهده کنند (و اصطلاحاً cipher-text می‌نامند) تبدیل می‌کند. Encryption دارای قدمت چند هزار ساله می‌باشد و همانطور که قبلا اشاره کردیم، از زیر مجموعه‌های cryptography می‌باشد. این نوع از رمز نگاری بر خلاف فرایند «hashing» یک‌طرفه نیست و قابلیت «decrypt»(رمز گشایی) و دسترسی به پیام اصلی را دارد. به این صورت که هر رمز نگاری‌ای الگوی مخصوصی داشته و برای دستیابی به آن الگو باید کلید آن را داشته باشیم. الگوریتم‌های زیادی برای رمز نگاری وجود دارد و به انواع و اقسام سخت تا آسان طبقه بندی می‌شوند. الگوریتم رمز نگاری‌ای قوی تر است که بدون داشتن کلید آن، به هیچ وجه نتوان به داده هایش دسترسی پیدا کرد. سازمان‌های اطلاعاتی از encryption های خاصی برای تبادل اطلاعات مهم استفاده می‌کنند. 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:

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

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

یادتان باشد الگوریتم‌های رمز نگاری علاوه بر پیام‌ها برای فایل‌ها هم قابل استفاده می‌باشند. مانند کاری که باج افزارها

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

الگوریتم متقارن و نامتقارن

یکی از مهم‌ترین الگوریتم‌های رمز نگاری، الگوریتم‌های 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 می‌شود. اما در الگوریتم نامتقارن یا «PKI» از دو کلید عمومی (public key) و کلید خصوصی (private key) برای رمز نگاری و رمز گشایی استفاده می‌شود. به این صورت که کد رمزگذاری عمومی است و هر کسی می‌تواند پیغام خود را رمز گذاری کند اما کد رمزگشایی خصوصی است و تنها گیرنده می‌تواند 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 شبکه‌های کامپیوتری رایج است. گاهی اوقات هم از ترکیب هردوی این الگوریتم‌ها استفاده می‌کنند که به آن «hibrid» گفته می‌شود.

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

انواع الگوریتم های نامتقارن به RSA ، ECC 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 می‌شود. اما در حال حاضر دامنه استفاده از آن وسیع تر شده و به طور معمول در راستای حفاظت از اطلاعات در انواع مختلفی از سیستم‌های غیر نظامی هم کاربرد دارد.

به گزارش موسسه امنیت کامپیوتری (CSI) در سال ۲۰۰۷، حدود ۷۱٪ از اطلاعات منتقل شده و ۵۳٪ از اطلاعات ذخیره شده بر روی حافظه های کامپیوتری رمزگذاری شده بودند. رمز نگاری می‌تواند برای حفاظت از اطلاعات ذخیره شده بر روی انواع حافظه کامپیوتری از جمله حافظه‌های فلش مورد استفاده قرار گیرد. امروزه رمز گذاری برای محافظت از اطلاعات در حمل و نقل استفاده می‌شود. به عنوان مثال در داده‌هایی که از طریق شبکه‌های مختلفی همچون اینترنت، تلفن همراه، میکروفون بی‌سیم، دستگاه مخابره داخل ساختمان و دستگاه‌های بلوتوث منتقل می‌شوند نیز کاربرد دارند.

Encrypt کردن گوشی‌های 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 گوشیتان 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، می‌توانید 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 می‌شوید دستگاه اقدام به خارج شدن از رمزگذاری می‌کند 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 بهEncrypt نمایید و بعد از آن یک بار دیگر روت کنید.

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

o رمزگذاری گاهی ۱ ساعت یا بیشتر زمان می‌برد.

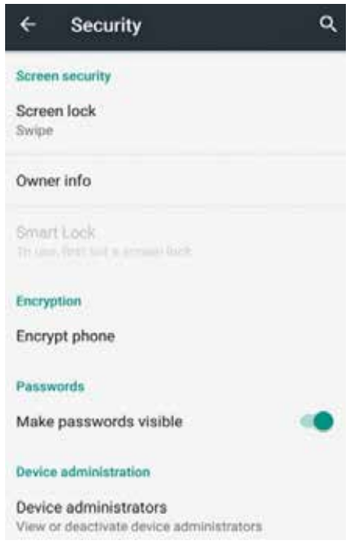
o شارژ گوشی از ۸۰ درصد کمتر نباشد چون در اینصورت عملیات رمزگذاری انجام نمی‌شود.

o طی فرایند رمزگذاری، گوشی حتما به شارژر متصل باشد.

o 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 قبلا رمزنگاری انجام شده باشد، مشخص خواهد بود و در غیر اینصورت باید گزینه encrypt phone را انتخاب کنید. (تصویر ۱)



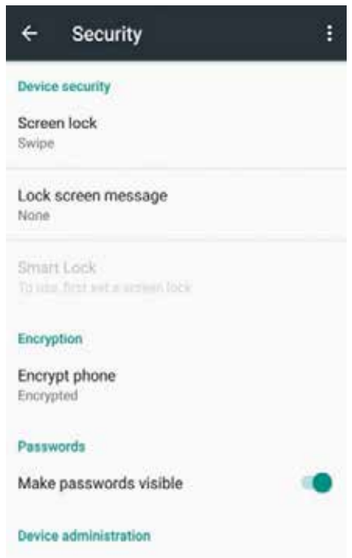
تصویر۱

۲. سپس صفحه ای 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 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)



تصویر۲

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 گذشته های دور با بشر همراه بوده و با گذشت زمان پیشرفت‌های چشمگیری داشته است وهمچنان 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 روش های 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 حرفه ای برای انجام فعالیت های 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.

هـــــکرهای کـــلاه سیـــاه

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.

۱- Kevin David Mitnick

(متولد ۶ آگوست ۱۹۶۳) هکر، مشاور، نویسنده و محکوم به پنج سال زندان به دلیل جرایم مختلف رایانه ای است که به واسطه ی دستگیری اش در سال ۱۹۹۵ شناخته شد. وی اکنون شرکت امنیتی Mitnick Security Consulting LLC ، را اداره می کند وهمچنین مدیر ارشد هکینگ ، سهامدار شرکت آموزش آگاهی از امنیت KnowBe۴ و همچنین عضو فعال مشاوره ای در Zimperium ،شرکتی است که یک سیستم پیشگیری از نفوذ موبایل را توسعه می دهد، است.

●زندگی

میتنیک در ۶ اگوست ۱۹۶۳ در ون نویز،کالیفرنیا، متولد شد.وی در لس آنجلس بزرگ شد و در دبیرستان جیمز مونرو در لس آنجلس ، کالیفرنیا ، شرکت کرد که در این مدت یک اپراتور رادیویی آماتور شد. او بعدها در کالج لس آنجلس پیرس و USC ثبت نام کرد. مدتی در بخش پذیرش معبد خردمند استفان 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 رایانه ای بدست آورد.وی وارد شبکه رایانه ای DEC شد و نرم افزار شرکت را کپی کرد ؛ جرمی که در سال ۱۹۸۸ به خاطرآن به ۱۲ ماه زندان محکوم شد و به دنبال آن سه سال تحت نظر بود. میتنیک نزدیک به پایان محکومیتش ، رایانه های 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 رایانه ای دسترسی غیرمجاز داشت. وی برای مخفی کردن موقعیت مکانی خود ، از تلفن های همراه کلون شده استفاده میکرد و نرم افزارهای ارزشمند اختصاصی را از برخی از بزرگترین شرکتهای تلفن همراه و رایانه در کشور کپی می کرد. همچنین رمزهای رایانه را رهگیری و به سرقت می برد ، شبکه های رایانه ای را تغییر می داد و نامه های الکترونیکی خصوصی را بدست می اورد و می خواند.

●دستگیری ، محکومیت و حبس

پس از پیگیری های تبلیغاتی ، FBI ، میتنیک را در ۱۵ فوریه ۱۹۹۵ در آپارتمان خود در رالی ، کارولینای شمالی ، به جرائم فدرال مربوط به یک دوره دونیم ساله از هک رایانه(که شامل کلاهبرداری در کامپیوتر و wire fraud بود) دستگیرکرد.

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 هسته ای» را با یک تلفن دارد چون می تواند از طریق تلفن زندان ،مودم NORAD را شماره گیری کرده و با سوت زدن برای پرتاب موشک های هسته ای ،با مودم ارتباط برقرار کند. علاوه بر این ، تعدادی از رسانه ها از عدم دسترسی وعده های 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

فعالیت های جنایی ، دستگیری و محاکمه میتنیک ، همراه با روزنامه نگاری مرتبط ، همه بحث برانگیز بود. گرچه میتنیک به دلیل غیرقانونی کپی کردن نرم افزار محکوم شده بود ، هواداران وی معتقدبودند 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 می کند که از برنامه های 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 شرکت های Fortune ۵۰۰ و FBI ، خدمات آزمایش نفوذ برای بزرگترین شرکت های جهان و کلاس های مهندسی اجتماعی را به ده ها شرکت و آژانس های دولتی آموزش می دهد.

کارت ویزیت های فلزی سفارشی او به عنوان کیت های جمع آوری قفل ،استفاده می شود.

KEVIN POULSEN-۲

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 ی پورشه ۹۴۴ S2 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 درحیطه 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 درنتیجه ۷۴۴ نفررا با پروفایل های MySpace شناسایی کرد و منجر به دستگیری شخصی به نام اندرو لوبرانو شد.

SecureDrop

James Dolan SecureDrop،Aaron Swartz ، Poulsen
یک بستر نرم‌افزاری 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.

ALBERT GONZALEZ -۳

آلبرت گونزالز(متولد ۱۹۸۱)یک هکر کامپیوتر و از مجرمان رایانه ای آمریکایی است که متهم به سرقت از کارت‌های 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 می‌توانستند شماره‌های 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 کارت‌های اعتباری و کارت‌های خودپرداز) بخوانند تا بتوانند از این شماره‌ها استفاده کنند. ناظران وب سایت، اعضایی را که قوانین سایت را رعایت نمی‌کردند، مجازات کردند؛ مثلا، ارائه بازپرداخت به خریداران در صورت عدم معتبر بودن شماره کارت‌های سرقت شده.
علاوه بر شماره کارت، اشیایی همچون: گذرنامه‌های جعلی، گواهینامه‌های رانندگی، کارت‌های تأمین اجتماعی، کارت‌های اعتباری، شناسنامه، کارت‌های شناسایی دانشجویی کالج و کارت‌های بیمه درمانی به حراج گذاشته شده بود.بیشتر متهم‌هایی که عضو بودند، کالاهای غیرقانونی را می فروختند؛ مثلا، یک عضو، ۱۸ میلیون حساب پست الکترونیکی با نام‌های کاربری مرتبط، گذرواژه‌ها، تاریخ تولد و سایر اطلاعات شخصی که شخصاً شناسایی کرده بود را فروخت. اعضایی 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.
سرویس 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 گروه‌های دیگر با نام‌های Carderplanet و Darkprofits به اشتراک گذاشته است. در این تحقیق واحدهایی از ایالات متحده، بلغارستان، بلاروس، کانادا، لهستان، سوئد، هلند و اوکراین درگیر شدند. گونزالز در ابتدا به اتهام داشتنِ 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 شرکت های 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 جمع آوری 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 کیسه های پلاستیکی در حیاط خلوت خانه ی والدینش) ،لپ تاپ وی و یک تپانچه جمع و جورGlock 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.

JEANSON JAMES ANCHETA-۴

در ۹ مه ۲۰۰۶ ، جینسون جیمز آنچتا (متولد ۱۹۸۵) اولین فردی شد که به دلیل کنترل تعداد زیادی رایانه ربوده شده یا بات نت‌ها دستگیرشد.
آنچتا، تا سال ۲۰۰۱ (وقتی مدرسه را ترک کرد)به دبیرستان داونی، کالیفرنیا، می رفت. وی در یک کافه اینترنتی کار می‌کرد و به گفته خانواده، می‌خواست به ذخایر نظامی بپیوندد. در حدود ژوئن ۲۰۰۴، وی پس از کشف rxbot، کرم رایانه ای رایج که می‌تواند شبکه رایانه‌های آلوده‌اش را گسترش دهد، شروع به کار با بات نت کرد.

●بات‌نت

Botnet یک اصطلاح برای مجموعه ای از روبات‌های نرم‌افزاری است که به طور خود مختار 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.

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 فعالیت های مرتبط رایانه‌ها متهم شد ونهایتا مکلف شد که علاوه بر ۶۰ ماه حبس، یک دستگاه BMW و بیش از ۵۸۰۰۰ دلار سود را به عنوان جریمه پرداخت کند.

Silicon Valley

مریم عتباتی

دره سیلیکون منطقه ای در قسمت جنوبی منطقه خلیج سان فرانسیسکو در کالیفرنیای 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؟

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 مهندسین بیش 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 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. بیایید 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.

درهٔ سیلیکون، سن‌خوزه، کالیفرنیا

همـــه چیـــــز درباره "cookies"

روشنک حسین‌زاده‌عطار

اگـر دقـت کـرده باشـید بـا ورود بـه اکثـر سـایت‌ها پیامـی مبنـی براینکـه «ایـن سـایت از cookies اسـتفاده می‌کنـد آیـا موافـق هسـتید؟» در زیـر صفحـه ظاهـر می‌شـود:

کـه خـب اکثـرا خوانـده نخوانـده گزینـه موافقـم را می‌زنیـم تـا سـریع‌تر بـه کارمـان برسـیم و بی‌تفـاوت از کنـار ایـن پیغـام می‌گذریـم، غافـل از اینکـه در بسـیاری از مواقـع در حـال اسـتفاده از کوکی‌هـا هسـتیم بـدون اینکـه خودمـان بدانیـم.
سوال اول که مطرح می‌شود این است که:

cookies چیست؟

کوکی‌هـا ماهیتـا فایل‌هایـی حـاوی متـن و یـا بـه زبـان عامیانـه text file هسـتند، ایـن فایـل حـاوی اطلاعاتـی اسـت کـه دسترسـی دوبـاره بـه سـایت را بـرای کاربـر و البتـه سـرور سـایت راحت‌تـر می‌کنـد.
وقتـی کاربـر وارد سـایت می‌شـود و اعـلام می‌کنـد مشـکلی بـا کوکی‌هـا نـدارد فایـل متنـی را سیسـتم کاربـر سـاخته می‌شـود و اطلاعـات کاربـر اعـم از خریدهایـی کـه بـه سـبدش اضافـه کـرده، موقعیـت مکانـی کاربـر، نـام کاربـری و ... و هـر اطلاعاتـی کـه کاربـر وارد کنـد را ذخیـره می‌کنـد. البتـه امـکان ذخیره‌سـازی رمـز عبـور هـم وجـود دارد امـا بـه دلایـل امنیتـی مجـددا سـوال می‌پرسـید کـه « آیـا می‌خواهیـد رمـز عبـور هـم ذخیـره شـود؟» .
اینجـا مرورگـر واسـط بیـن کامپیوتـر کاربـر و سـایتی اسـت کـه بـه آن وارد شـده ، وقتـی بـرای بـار بعـدی کاربـر وارد همـان سـایت می‌شـود مرورگـر فایـل سـاخته شـده روی سیسـتم کاربـر را می‌خوانـد و بـه سـایت انتقـال می‌دهـد.
رایج‌تریـن نـوع کوکی‌هـا همیـن کوکی‌هـای احـراز هویـت(authentication cookies (هسـتند کـه نـام کاربـری و رمـز عبـور را ذخیـره می‌کننـد ، اگـر قـرار بـه ایـن باشـد کـه هـر سـایت در حافظـه خـودش اطلاعـات تمـام کاربـران را ذخیـره کنـد و کل پروسـه احـراز هویـت را خـودش انجـام بدهـد رونـد سـایت کنـد می‌شـود! امـا الان بـا اسـتفاده از کوکی‌هـا بخشـی از پروسـه بـه عهـده سیسـتم هـر کاربـر اسـت و ایـن رونـد بازیابـی اطلاعـات را تسـریع می‌بخشـد.
حـالا کـه بـا مفهـوم ایـن موجـود پرکابـرد اشـنا شـدیم سـوالی کـه پیـش می‌آیـد ایـن اسـت کـه:

آیـا بایـد بـه خاطـر کوکی‌هـا نگـران امنیـت اطلاعـات خود باشـــیم؟

خـب خبـر خـوب ایـن اسـت کـه کوکی‌هـا بـه لحـاظ ماهیـت نمیتواننـد عامـل انتقـال ویـروس یـا بـد افـزار (malware) بـه سیسـتم شـما باشـند تنهـا بدیشـان ایـن اسـت کـه ممکـن اسـت یـک سـری تبلیـغ روی سیسـتم ایجـاد کننـد کـه خـب آن هـم بـا یـک گزینـه « نـه ممنـون « مـی‌رود و کار مـا را مختـل نمی‌کنـد. امـا آیـا صددرصـد امـن هسـتیم؟ دوسـت عزیـزم بایـد بگویـم تـوی دنیـای اینترنتـی چیـزی بـه اسـم امنیـت صدرصـد وجـود خارجـی نـدارد اساسـا، فقـط یـک مدل از کوکی‌هـا وجـود دارنـد کـه ممکـن اسـت دردسـاز شـوند آن هـم «tracking cookie» خـب کاربـرد ایـن کوکی‌هـا می‌تواننـد بـا بقیـه مدل‌هـا متفـاوت باشـد و اصـلا قصـد آسـان کـردن دسترسـی بـه اطلاعـات را نداشـته باشـند. ایـن کوکی‌هـا می‌تواننـد بفهمنـد بـه چـه سـایت‌هایی مراجعـه کردیـد و چـه اطلاعاتـی نظیر ایمیـل یـا نـام خانوادگـی یـا اسـم دوسـتانتان و ... را وارد کردیـد و آنهـا را ذخیـره کنند و ممکـن اسـت بشـود از ایـن اطلاعـات سـو اسـتفاده کـرد البتـه شـما بـه راحتـی بـه صـورت دسـتی هـر کوکـی را کـه می‌خواهیـد غیرفعـال کنیـد یـا حتـی حافظشـان را پـاک کنیـد. البتـه حواسـتان باشـد کـه اگـر کوکی‌هـای احـراز هویـت فیسـبوک را پـاک کنیـد دیگـر بـه صـورت اتومـات وارد اکانتتـان نمی‌شـوید و بایـد خودتـان نـام کاربـری و رمـز را دسـتی وارد کنیـد.

امنیـت اطلاعـات شـما در سـایت‌هایی کـه بـه آن‌هـا مراجعـه می‌کنیـد بسـتگی دارد و البتـه بـه مرورگرتـان اینکـه مرورگـر شـما بـا چـه روشـی اطلاعـات شـما را رمـز گـذاری یـا بـه اصطـلاح encrypt می‌کنـد و اگـه مرورگـر شـما امنیـت قابـل قبولـی داشـته باشـد دیگـر نیـازی بـه نگرانـی نیسـت و بـا خیـال راحـت می‌توانیـد بـه سـایت‌ها اجـازه‌ی اسـتفاده از کوکی‌هـا را بدهیـد و مطمئـن باشـید بـه احتمـال زیـادی کسـی نمی‌توانـد بـه راحتـی اطلاعـات شـما را رمـز گشـایی کنـد و بخوانـد، یادتـان باشـد فقـط یـک تعـداد سـایت محـدود هسـتند کـه اگـر بـه کوکی‌هایشـان اجـازه‌ی دسترسـی ندهیـد همچنـان قابـل اسـتفاده هسـتند، بنابرایـن توصیـه ایـن اسـت کـه تـا حـد امـکان بـه کوکی‌هـا دسترسـی بدهیـد نهایتـا بعـد از اسـتفاده از سـایت مـورد نظـر در قسـمت تنظیمـات مرورگـر آن کوکـی را حـذف می‌کنیـد.
خـب بـرای تکمیـل بحـث امنیـت کوکی‌هـا می‌خواهـم چنـد مـورد از امن‌تریـن مرورگرهـا را معرفـی کنـم. طبـق گفته‌هـای سـایت «restoreprivacy.com» بهتریـن مرورگرهـا از نظـر امنیـت:

۱. **Firefox**

۲. **Iridium browser**

۳. **GNU IceCat browser**

شـما می‌توانیـد بـا مراجعـه بـه ایـن سـایت بـا مزیت‌هـای ایـن مرورگرهـا و چنـد مرورگـر خـوب و امـن دیگـر هـم اشـنا شـوید.
اما یک سوال دیگر هم اینجا مطرح می‌شود و آن اینکه:
خـب مـا قبـلا هـم وقتـی از یـک سـایت خریـد می‌کردیـم در سـبد خریـد همـه اجنـاس ذخیـره می‌شـد و حتـی نـام کاربـری و بقیـه‌ی اطلاعـات بـه صـورت اتومـات وارد سیسـتم می‌شـدند از طرفـی بـه تازگـی ایـن پیغـام کوکـی را روی سـایت‌ها مشـاهده می‌کنیـم پـس قبـلا بـه چـه صـورت بـوده اسـت؟!
خـب قضیـه ایـن اسـت کـه مـا مـدت زیـادی- تقریبـا از سـال ۱۹۹۶- هسـت کـه از مزایـای کوکی‌هـا اسـتفاده می‌کنیـم فقـط خودمـان نمی‌دانیـم! قبـلا کوکی‌هـا بـه صـورت پیـش فـرض اجـازه‌ی دسترسیداشـتند امـا بـه تازگـی اسـتاندارها عـوض شـده و بـه خاطـر امنیـت بیشـتر سـایت موظف هسـتند بـرای اسـتفاده از کوکی‌هـا از کاربـر تاییـد بگیرنـد.
آیـا مـا بـرای هـر سـایتی کـه راه انـدازی می‌کنیـم بـه کوکـی احتیـاج داریـم؟ نـه! اگـر شـما وبلاگـی را راه انـدازی کردیـد تـا صرفـا دلنوشـته‌هایتان را منتشـر کنیـد و سـایت قسـمتی بـرای عضـو شـدند هـم نـداره نیـازی بـه کوکـی نیسـت امـا اگـر سـایت شـما سـایت فروشـگاهی هسـت و بایـد افـراد وارد اکانـت خودشـون بشـوند و بایـد بـرای ذخیـره‌ی نـام کاربـری، رمـز عبـور، سـبد خریـد، موجـودی کیـف پـول و ... از کوکی‌هـا اسـتفاده کنیـد تـا سـرور سـایت مجبـور بـه پیـدا کـردن اطلاعـات نباشـد و سـایت دچـار کنـدی نشـود.
می‌خـوام چنـد تـا از کوکی‌هـای مرسـوم را بـه طـور خلاصـه معرفـی کنـم، البتـه کوکی‌هـا بـه چنـد مـدل قابـل دسـته‌بندی هسـتند ایـن دسـته‌بندی بـر اسـاس روش کار آن‌هاسـت:

۱. **Session cookies:** ایـن کوکی‌هـا دارای حافظه‌هـای موقـت و تقریبـا کـم هسـتند و بـرای نشـان دادن آیتم‌هـای موقـت هسـتند و بـا بسـته شـدن مرورگـر بـلاک می‌شـوند و تقریبـا می‌شـود گفـت هیـچ خطـری نـدارن اولا چـون موقـت هسـتند و خـودکار بـلاک می‌شـوند و دومـا هیـچ اطلاعاتـی از کاربـر نمی‌گیرنـد.

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 خطرساز باشند.

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.

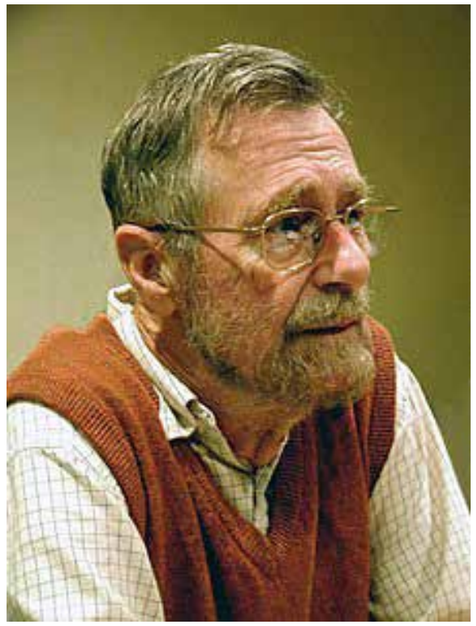
۴. Third-party cookies: این کوکی‌ها به کوکی اصلی اضافه می‌شوند یکی از مهم‌ترین کاربردهای آن‌ها در کوکی‌هایی است که حاوی تبلیغات هستند وقتی کاربر روی تبلیغ کلیک می‌کند از این کوکی‌ها برای ارتباط شما با سایتی که تبلیغش بالا آمده استفاده می‌شود.
و اما اخرین نکته اسم این موجودات هست! همگی میدونیم که کوکی 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[1] الهام گرفته، اون برنامه نویس از عبارت "magic cookie" برای یکی از برنامه‌های یونیکس استفاده کرده بود.

۱_ سیتم 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 امریکا و برخی سیستم‌ها دانشگاهی بود و الان به عنوان مجموعه ای از سیستم عامل‌ها شناخته می‌شود.

Dijkstra دانشمند کامپیوتر

پریناز میرباقری

شایسته است که مهندسین 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، مخصوصا 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 ــ 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) کردند. ALGOL ۶۰ باعث شد تا زبان‌های B، BCPL، Simula، Pascal و C به وجود بیایند. همچنین ALGOL ۶۰ جزو اولین کامپایلرهایی 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.

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 توزیع‌شده

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.

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

کامپیوترهـــــای کوانتـــــومی

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 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 رمزگذاری‌شده‌ای 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 n/۲ تلاش به نتیجه می‌رسیم؛ یعنی اگر چندین بار این کار را با کامپیوترهای الکترونیکی انجام دهیم، میانگین تعداد تلاش‌های موفق به n/۲ 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 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 پسوردهای 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.

جوایز بزرگ دنیـــای کامپیوتر

مریم احمدلو

خیلی از ماها موقع انتخاب‌رشته 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 وسوسه انگیزی که خیلی از ماها رو به سوی این علوم سوق میده.
در ادامه می‌خوام شما رو با بعضی از این جوائز آشنا کنم. پس اگه انگیزتونو توی این راه ازدست 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 آلن‌تورینگ ، 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.

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 استعدادهای 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.

Facebook hacker cup

این مسابقات رقابت‌های بین المللی برنامه‌نویسی است که توسط فیسبوک برگزار می‌شود.
این رقابت‌ها در سال ۲۰۱۱ با هدف شناسایی استعدادهای مهندسی برای کار در فیسبوک راه اندازی 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 برنامه نویسی است که در حال تبدیل شدن به لیگ اصلی مسابقات برنامه نویسی 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، برنامه نویسان تمام عیاری برای مسابقه دادن هستند که به طور مرتب در اکثر مسابقات برنامه نویسی شرکت می‌کنند.

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 به‌صورت 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# ، Java و در مواردی Python قابل استفاده هستند.

ICFP

ICFP یک کنفراس بین المللی برنامه نویسی کاربردی است که سالیانه 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 . شرکت‌کنندگان می‌توانند تیم تشکیل داده و به صورت تیم‌های چند نفره با هم رقابت کنند .

مسابقه Codewars شرکت اچ‌پی

Codewars (HP) Hewlett Packard از سال ۱۹۹۹ همه ساله برای رقابت دانش آموزان دبیرستانی برگزار می‌شود. شرکت‌کنندگان 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 محیط این مسابقه برای شرکت کنندگان هیجان انگیز، تحریک کننده و رقابتی شود.

مسابقه حل مسئله اینترنت IPSC

مسابقه Internet Problem Solving Contest یا IPSC 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 ، شرکت‌کنندگان باید داده‌های خروجی صحیح را برای داده‌های ورودی محاسبه کنند. در این رویداد، شرکت‌کنندگان آزاد هستند که از هر زبان برنامه‌نویسی که خروجی صحیحی می‌دهد، استفاده کنند.

IEEEXtreme

IEEEXtreme 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 . شرکت‌کنندگان 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 کنفراس‌های IEEE در هرکجای 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 بیش از ۴۰ زبان برنامه نویسی، 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 برنامه نویسی 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 شرکت کنندگان 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، علم‌وصنعت، خواجه‌نصیر و شهیدبهشتی نیز همه ساله با چندین تیم در این مسابقه شرکت کرده و به رقابت با جمعی از زبده‌ترین برنامه نویسان ایران می‌پردازند.

مسابقه برنامه نویسی جاواکاپ

جاواکاپ یک مسابقه برنامه‌نویسی است که با هدف ارزیابی زبان جاوا و مهارت‌های برنامه نویسی طراحی شده است. این مسابقه در دو بخش کتبی و عملی به سنجش دانش و مهارت‌های برنامه نویسی 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 سامانه‌ی 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 جوائز 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 فکرکردن 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.

دیپ فیک چیست؟

روشنک حسین‌زاده‌عطار

”ببین 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 سیاست مداران پخش شده در حال گفتن حرف هایی که هرگز نزده‌اند!

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 ؟ ایا 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 میخوایم 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 مراحلی که تو این تعویض اتفاق افتاده:

راه دیگه ای که وجود داره استفاده از الگوریتم شبکه مولد تخاصمی (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 بده اون چهره حقیقیه 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 ایا 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 سودجو 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 تشخصیه 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 کارامد 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 دیگر ابزار های متکی بر دیتا بیس 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 اونا سخت تر میشه.

اگر ما نتونیم تشخیص بدیم چیزی که میبینیم واقعیه یا نه باید به هر چیزی که میبینیم شک کنیم این روی جنبه های زیادی از زندگیمون تاثیر میزاره 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!

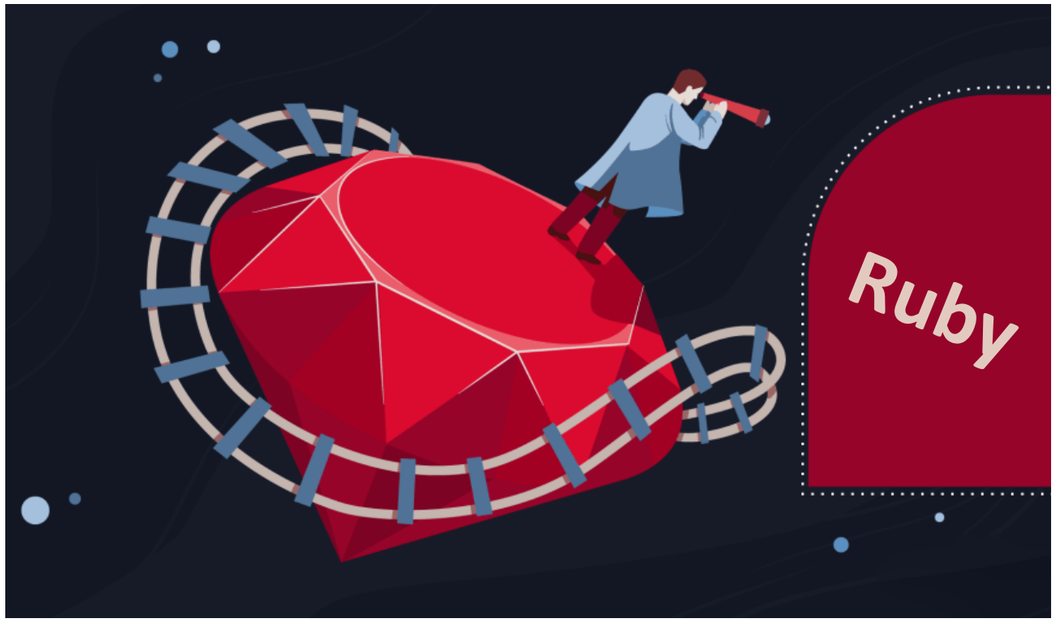
خوشبختانه دیپ فیک در حوزه هایی هم مفید و سرگرم کننده واقع شده و اینجور نیست که همیشه برای فریب دادن افراد باشه! در بسیاری از موزه ها و گالری ها از این تکنولوژی استفاده شده مثلا یک نقاش تاریخی درباره هنرش و اثارش در یک ویدیو صحبت میکنه یا حتی موفق شدن از بازیگر های فوت شده در فیلم ها استفاده کنند!

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 دیگر 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 اموزش ببینید چطور خودتون یک ویدیو جعلی با استفاده از هنر دیپ فیک درست کنید.

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 میخواهیم یکی از این زبان ها که شاید اسمش را زیاد شنیده اید اما با آن آشنا نیستید را به شما معرفی کنیم.
زبان روبی (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 میبینند که در عین کارآمدی ساده است. روبی قابل حمل بوده و به مانند زبان های پایتون و جاوا توانایی مدیریت استثناها را داراست.

برای اولین بار این زبان در ۲۱ دسامبر سال ۱۹۹۵ تحت عنوان روبی ۰.۹۵ عرضه شد و تا به حال به ورژن ۲.۳.۳ رسیده است.
زبان روبی شیوه های متفاوت برنامه نویسی را از جمله شی گرا، تابعی و بازتابی را به شکلی متعادل پشتیبانی میکند.
سازنده روبی 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 روبی را طبیعی بسازد. نه ساده. و مثالی که همراه این مطلب آورده این است که «روبی همچون بدن انسان در ظاهر ساده و از داخل پیچیده است.»
یوکیهیرو 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 روبی، روبی 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 روبی می پردازند.
تا به حال از روبی گونه های مختلفی توسعه یافته که میتوان از آنها به جی روبی، روبینیوس، ترافل روبی، مروبی، آیرون روبی، مگلو و کاردینال اشاره کرد.
با اینکه کمی از محبوبیت روبی در طی زمان کاسته شد اما طبق سایت indeed روبی 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]
```

آشـــنایی با تورینـــــگ

دلارام درودگریان

تولد و تحصیلات

آلـن ماتیسـون تورینـگ ریاضـی دان، دانشـمند رایانـه، منطـق دان، فیلسـوف، زیسـت - ریاضیـدان، و رمزنـگار بریتانیایـی بـود. تورینـگ بـه عنـوان پـدر علـم محاسـبه نویـن و هـوش مصنوعـی شـناخته شـده اسـت و مهـم تریـن جایـزه علمـی رایانـه بـه افتخـار وی جایـزه تورینـگ نـام گرفتـه اسـت. همچنیـن دارای نشـان سـلطنتی و عضـو کالـج سـلطنتی بـود.

از همـان کودکـی علایـم نبـوغ در وی هویـدا بـود. آلـن تورینـگ در سـن ۱۴ سـالگی توانسـت بـه مدرسـه دولتـی و پرهزینـه «شـربورن» در شـهر دورسـت راه پیـدا کنـد امـا تمایـل ذاتـی او بـه سـمت ریاضیـات و علـم نـزد اسـاتید ایـن مدرسـه اهمیتـی نداشـت زیـرا در آن دوره تاکیـد بیشـتر روی مسـایل و مباحـث کلاسـیک بـود. در همـان سـال مدیـر مدرسـه بـرای والدیـن او نامـه نوشـت کـه اگـر او مـی خواهـد دانشـمند شـود وقـت خـود را در یـک مدرسـه دولتـی هـدر مـی دهـد.

بـا ایـن حـال تورینـگ توانایـی قابـل توجـه خـود را در زمینـه هـای مـورد علاقـه اش، بـا حـل مسـایل پیچیـده در سـال ۱۹۲۷ بـدون اینکـه حتـی حسـاب دیفرانسـیل مقدماتـی خوانـده باشـد بـه نمایـش گذاشـت. در سـال ۱۹۲۸ بـا کریسـتوفر مرکـوم کـه از دانشـجویان سـال بالایـی او بـود، رابطـه دوسـتی عمیقـی پیـدا کـرد کـه ایـن دوسـتی در سـال ۱۹۳۰ بـا مـرگ مرکـوم پایـان یافـت.

آلـن تورینـگ

کریسـتوفر اولیـن کسـی بـود کـه پیلـه تنهایـی او را سـوراخ کـرده بـود و بـا مـرگ او تورینـگ درهـم شکسـت و ایمـان مذهبـی خـود را از دسـت داد.

آلـن تورینـگ در سـال هـای ۱۹۳۱ تـا ۱۹۳۴ مشـغول تحصیـل در دانشـگاه کینگـس کالـج بـود و بـه خاطـر مقالـه اش در رابطـه بـا قضیـه محدودیـت مرکـزی در سـال ۱۹۳۵ بـه عنـوان عضـو آنجـا انتخـاب شـد.

فعالیت‌هـای اصلـی تورینـگ در زمینـه‌ی رمزنـگاری بـه دوران جنـگ جهانـی دوم مربـوط اسـت. در طـول ایـن جنـگ، تورینـگ در بلچلـی پـارک (Bletchley Prk) بـه تحقیـق و سـاخت دسـتگاه‌های رمزنـگاری مشـغول و بـرای مدتـی مسـئول بخـش مربـوط بـه تحلیـل نوشـته‌های رمـزی نیـروی دریایـی آلمـان بـود. او چنـد روش بـرای شکسـتن رمزهـای آلمان‌هـا ابـداع کـرد، از جملـه روش ماشـینی الکترومکانیکـی کـه می‌توانسـت ویژگی‌هـای ماشـین انیگمـا را پیـدا کنـد.

حـالا توضیـح مختصـری دربـاره ماشـین انیگمـا میدهیـم تـا یـک آشـنایی کلـی بـا آن پیـدا کنیـد:

آرتـور شـربیوس مختـرع و مهنـدس آلمانـی، ماشـین رمزنـگاری انیگمـا را اختـراع کـرد. انیگمـا یـک وسـیله الکترومکانیکـی بـود و زمانـی کـه کلیـد یـک حـرف بـر روی ایـن دسـتگاه فشـار داده می‌شـد، درون آن یـک جریـان الکتریکـی بوجـود مـی آمـد و قطعـات مکانیکـی متحـرک، مسـیر ایـن جریـان رو تغییـر میدادنـد تـا در نهایـت یـک حـرف دیگـر تولیـد شـود. وظیفـه ماشـین انیگمـا تبدیـل پیغـام هـای خوانـا بـه ناخوانـا یـا همـان عمـل رمزنـگاری بـود. ارتـش نـازی در طـول جنـگ جهانـی دوم بـه منظـور رمزنـگاری و رمـز گشـایی پیـام هـای نظامـی، مـدل خاصـی از ایـن ماشـین بـه نـام انیگمـای ورماخـت را تولیـد نمـود . ایـن دسـتگاه مـی توانسـت رمزهایـی غیرقابـل حـل را بـه شـکل یـک سـری اعـداد و حـروف بـدون معنـی تولیـد کنـد.

یـک ویژگـی انیگمـا این اسـت کـه در آن هیـچ گاه هیـچ حرفی بـه خـودش رمزنـگاری نمی‌شـود، مثـلاً T بـه T رمـز نمی‌شـود، بلکـه همیشـه بـه حـرف دیگـری برگردانـده می‌شـود. پـس از تایـپ کـردن هـر حـرف، چرخ‌دنـده‌ای کـه در جایـگاه نخسـت اسـت، یـک حـرف جابه‌جـا می‌شـود، مثـلاً اگـر روی حـرف U اسـت، بـه حـرف V مـی‌رود. اگـر چرخ‌دنـده نخسـت روی حـرف Z باشـد، بـا تایـپ کـردن یـک حـرف، بـه حـرف A مـی‌رود و سـپس چرخ‌دنـده دوم نیـز یـک حـرف جلـو مـی‌رود، درسـت ماننـد نشـانگرهای یـکان و دهـگان در کیلومترشـمار مکانیکـی خودروهـا. بـه همیـن ترتیـب، اگـر چرخ‌دنـده دوم بـه حـرف Z برسـد، بـه حـرف A مـی‌رود و چرخ‌دنـده سـوم هـم یـک حـرف جلـو مـی‌رود (ماننـد نشـان‌گرهای دهـگان و صـدگان). چیـزی کـه بـرای شـروع کار مهـم اسـت، آرایـش نخسـتین چرخ‌دنده‌هـا اسـت و ایـن آرایـش در طـول فرآینـد تایـپ کـردن، تغییـر خواهـد کـرد.

ماشین انیگما

برمیگردیم به موضوع اصلی:

از سـپتامبر سـال ۱۹۳۸، آلـن تورینـگ در سـازمان رمزنـگاری بریتانیـا بـه نـام GC&CS بـه فعالیـت پاره‌وقـت مشـغول بـود. ایـن سـازمان امـروزه بـا نـام سـتاد ارتباطـات دولـت بریتانیـا شـناخته می‌شـود. تمرکـز اصلـی فعالیت‌هـای تورینـگ در ایـن سـازمان، رمزگشـایی دسـتگاه انیگمـا بـود. آلـن تورینـگ رمزنـگاری ایـن دسـتگاه‌ها را بـه همـراه همـکار ارشـدش دیلـی ناکـس و همـکاری کاشناسـان دیگـر انجـام مـی‌داد؛ مسـاله‌ای کـه بـه آنهـا کمـک کـرد تـا سرنوشـت جنـگ را تغییـر دهند(بـا ایـن حـال بـاز هـم بسـیاری از رمـز هـای انیگمـا هرگـز شکسـته نشـد).

رمزگشایی ماشین انیگما

آلـن تورینـگ چنـد هفتـه پـس از ورود بـه بلچلـی پـارک، دسـتگاه الکترومکانیکـی Bombe را بـرای رمزگشـایی پیام‌هـای دسـتگاه انیگمـا تولیـد کـرد. دسـتگاه او بـا بهبـود فرآیندهـای دسـتگاه لهسـتانی Bomba تولیـد شـده بـود. ایـن دسـتگاه بـه جسـتجو میـان تنظیمـات احتمالـی بـرای رمزگشـایی انیگمـا می‌پرداخـت. اولیـن دسـتگاه Bombe در ۱۸ مـارس سـال ۱۹۴۰ شـروع بـه کار کـرد. نابغـه‌ی هـوش مصنوعـی در خـلال فعالیت‌هایـش در طـول جنـگ جهانـی دوم، دسـتگاه‌های رمزگشـایی متعـددی تولیـد کـرد. یکـی از ایـن دسـتگاه‌ها Hut ۸ نـام داشـت کـه بـرای رمزگشـایی دسـتگاه مخصـوص نیـروی دریایـی نازی‌هـا سـاخته شـده بـود. دسـتگاه انیگمـای نیـروی دریایـی ارتـش نـازی، بسـیار حرفه‌ای‌تـر از دیگـر دسـتگاه‌های انیگمـا بـود و تورینـگ بـا رمزگشـایی تنظیمـات آن، کمـک بزرگـی بـه پایـان جنـگ جهانـی دوم کـرد.

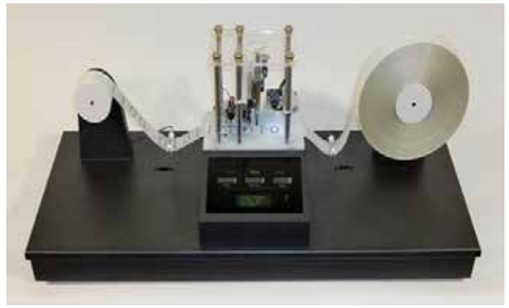
دستگاه bombe

و امـا ماشـین تورینـگ کـه بـه نـام خـود تورینـگ نامگـذاری شـده، چیسـت؟

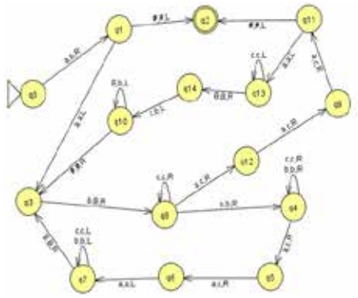
آلـن در سـال ۱۹۳۷ مقالـه ای را بـا عنـوان «دربـاره اعـداد محاسـبه پذیـر» منتشـر کـرد کـه به انـدازه هـر رویـداد منحصر بـه فـرد دیگـری مـی توانـد آغـاز عصـر جدیـد کامپیوتـر تلقـی شـود. ایـن مقالـه بـه اختصـار طرحـی از آنچـه را شـرح مـی دهـد کـه بـه آن ماشـین تورینـگ مـی گوینـد و آن کامپیوتـری بـود کـه شـالوده اش در قلـب کامپیوترهـای دیجیتـال بعـدی قـرار دارد.

ایـن موضـوع بـه تمـام جنبـه هـای کامپیوترهـای ابتدایـی تـا مـدرن، همچـون توانایـی خوانـدن، نوشـتن و پـاک کـردن داده هـا، حافظـه ای بـرای ذخیـره سـازی داده هـا، یـک واحـد پـردازش مرکـزی و بـه معنـای یـک برنامـه بـه واسـطه مجموعه ای از دسـتورالعمل هـای ریاضیاتـی سـاخته شـده، شـکل داد. ماشـین تورینـگ در واقـع یـک وسـیله تخیلـی اسـت کـه دارای

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 دستورالعمل‌ها 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 زمان های 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 پویش کرده، محتوای این مربع را با دستورالعمل‌های 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 دستورالعمل 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 مقاله های مرتبط را نمایش دهد.



ماشین تورینگ

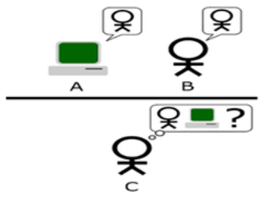


ماشین تورینگ {n)a^۱۸۲ :n≤}

آزمایش تورینگ

آلن تورینگ شکی نداشت که کامپیوترها نه تنها نقش فزاینده ای در زندگی نسل های بعدی ایفا خواهندکرد بلکه متقاعد شده بود که آنها ترجیحا به سطحی از مهارت خواهند رسید که می توانند همانند انسان ها فکر کنند. برای اندازه گیری زمانی که در آینده این امر در اختیار قرار می گیرد، 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، این‌ست 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 می گیرد.



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 شرکت کنندگان 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 میتسوکو (Mitsuku) است. شخصیت تعریف شده برای این چت‌بات، یک دختر ۱۸ ساله اهل شهر لیدز است. میتسوکو از توانایی اولیه‌ای برای تصمیم‌گیری‌های منطقی برخوردار است. برای مثال، اگر از او بپرسید «می‌توانی یک خانه را بخوری؟»، این ربات مولفه‌ی «ماده‌ی سازنده» را جستجو می‌کند و با توجه به این که ماده‌ی سازنده‌ی تعریف شده برای خانه «آجر» است و آجر نیز در دسته‌ی مولفه‌های غیرخوردنی قرار می‌گیرد، پاسخ این ربات به سوال فوق منفی خواهد بود.

اگر دوست دارید چت کردن با میتسوکو را امتحان کنید، می‌توانید 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، پیشنهادهای مختلفی برای بهبود و جایگزینی این آزمون ارائه شده‌اند.

(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 می‌توانید به سایت‌هایی همچون:

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

https://daneshyari.com/isi/articles/roboticsمراجعه کنید.)

زندگی و مرگ تورینگ

آلن تورینگ یک نامزدی کوتاه مدت با همکارش در پروژه‌ی Hut ۸ یعنی Joan Clarke داشت. نامزدی آنها به دلیل تمایلات جنسی خاص تورینگ به ازدواج نینجامید. این نابغه‌ی ریاضی به خاطر همین تمایلات در ۲۷ فوریه‌ی سال ۱۹۵۲ محاکمه شد. او از میان زندان و درمان هورمونی، دومی را انتخاب کرد. اتهامات و محاکمه‌ی تورینگ، حفاظت اطلاعاتی و امنیتی و همکاری او با دولت انگلستان را لغو کرد. البته شغل‌های دانشگاهی تورینگ تا زمان مرگش برقرار بودند. او پس از اتفاقات سال ۱۹۵۲ از ورود به خاک ایالات متحده‌ی آمریکا منع شد اما اجازه داشت در کشورهای اروپایی سفر کند. تورینگ هیچ‌گاه در طول زندگی به جاسوسی متهم نشد. او و تمام همکارانش در بلچلی تا پایان عمر از صحبت در مورد فعالیت‌های 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 دقتیش در نگهداری از مواد شیمیایی رخ داده است. کالبد شکافی علت مرگ را مسمومیت با سیانور یافت و پلیس مرگ را خودکشی اعلام کرد.

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 کامپیوترمعروف است؛ همچنین خیابان و پل آلن تورینگ در شهر منچستر و ... . در سال ۱۹۹۹، مجله‌ی تایمز تورینگ را در میان ۱۰۰ فرد مهم قرن بیستم قرار داد. جمله‌ی یادبود این مجله برای تورینگ به این صورت بود: «هر فردی که دکمه‌ای را روی صفحه‌کلید می‌فشارد یا یک نرم‌افزار را باز می‌کند، 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.

اینتـــــرنت اشـــــیاء Internet of Things

مژده کوکبی

تهیـــه کننـــده: مـــژده کوکبـــی،
دانشـــجوی رشته مهندسی کامپـیوتر
Prepared by: MOZHDEH Kokabi,
Computer Engineering Student

۱-مفاهیم پایه اینترنت اشیاء

امـروزه نوآوری‌هـا و ارتباطـات بـا سـرعت چشـمگیری در حـال رشـد هسـتند. اینترنـت بـه عنـوان یکـی از بدیع‌تریـن ابزارهـای ارتباطـی در حـال تکامـل و رشـد اسـت و هـر روزه دسـتگاه‌های بیشـتری در حـال اتصـال بـه شـبکه هسـتند و شـبکه‌ها در حـال گسـترش می‌باشـند. گسـترش ارتباطـات و فناوری‌هـای مرتبـط و همچنیـن وجـود دسـتگاه‌هایی بـا قابلیـت اتصـال بـه شـبکه اینترنـت منجـر بـه ایجـاد شـبکه بسـیار گسـترده‌ای از دسـتگاه‌ها و اتصال‌هـا شـده، کـه مفهومـی بـه نـام اینترنـت اشـیاء را شـکل داده اسـت.[۱]

اینترنـت اشـیا مفهومـی اسـت کـه بـه شـرایطی اطـلاق مـی شـود کـه وسـایل موجـود در محیـط بتواننـد بـه شـبکه اینترنـت متصـل و توسـط برنامـه هـای کاربـردی مدیریـت شـوند. اینترنـت اشـیاء بـه زبـان سـاده، ارتبـاط سنسـورها و دسـتگاه‌ها بـا شـبکه‌ای اسـت کـه از طریـق آن می‌تواننـد بـا یکدیگـر و بـا کاربرانشـان تعامـل کننـد. ایـن مفهـوم می‌توانـد به‌سـادگی ارتبـاط یـک گوشـی هوشـمند بـا تلویزیـون باشـد و یـا بـه پیچیدگـی نظـارت بـر زیرسـاخت‌های شـهری و ترافیـک. از ماشـین لباسشـویی و یخچـال گرفتـه تـا پوشـاک، ایـن شـبکه بسـیاری از دسـتگاه‌های اطـراف مـا را در برمی‌گیـرد.

در سـال ۲۰۱۳، طـرح اسـتانداردهای جهانـی اینترنـت اشـیاء(IOT-GSI) مطـرح شـد و ایـن اسـتانداردها بـه عنـوان زیرسـاخت جامعـه اطلاعاتـی معرفـی گردیـد. بـرای ایـن اهـداف یـک "چیـز " در واقـع یـک شـی از جهـان فیزیکـی (چیزهـای فیزیکـی) یـا جهـان اطلاعـات (چیزهـای مجـازی) اسـت کـه قـادر بـه شناسـایی و یکپارچه¬سـازی شـبکه‌های ارتباطـی می‌باشـد. اینترنـت اشـیاء اجـازه می‌دهـد تـا اشـیاء در سراسـر زیرسـاخت‌های شـبکه موجـود، از راه دور کنتـرل شـوند. اینترنـت اشـیاء همچنیـن فرصتـی بـرای ادغـام مسـتقیم جهـان فیزیکـی بـه سیسـتم‌های مبتنـی بـر کامپیوتـر ایجـاد کـرده اسـت و بـه بهبـود بهـره‌وری، دقـت و سـود اقتصـادی عـلاوه بـر کاهـش دخالـت انسـان، منجـر شـده اسـت. هنگامـی کـه اینترنـت اشـیاء بـا سنسـورها و محرک‌هـا تکمیـل می‌شـود، تکنولـوژی آن بـه یـک نمونـه جامـع از سیسـتم‌های سـایبری فیزیکـی کـه شـامل شـبکه‌های هوشـمند، خانه‌هـای هوشـمند، حمـل و نقـل هوشـمند و شـهرهای هوشـمند اسـت، تبدیـل می‌شـود. هـر چیـز منحصـر بـه فـردی از طریـق سیسـتم‌های محاسـباتی جاسـازی شـده قابـل شناسـایی و در زیرسـاخت اینترنـت موجـود اسـت.

بـه طـور معمـول، انتظـار مـی‌رود کـه اینترنـت اشـیاء اتصالـی پیشـرفته از دسـتگاه‌ها، سیسـتم‌ها و خدمـات کـه فراتـر از ارتباطـات ماشـین بـه ماشـین اسـت، ارائـه کنـد و انـواع پروتکل‌هـا، دامنه‌هـا و برنامه‌هـای کاربـردی را پوشـش دهـد. انتظـار مـی‌رود کـه اتصـال ایـن دسـتگاه‌های تعبیـه شـده (از جملـه اشـیای هوشـمند) بـه اتوماسـیون در تقریبـا تمامـی زمینه‌هـا کمـک کنـد. اشـیاء می‌تواننـد بـه طیـف گسـترده¬ای از دسـتگاه‌ها ماننـد ایمپلنـت نظـارت بـر قلـب، فرسـتنده زیسـت تراشـه در حیوانـات در معـرض انقـراض، حلزون‌هـای الکتریکـی در آب‌هـای سـاحلی، خودروهـا بـا سنسـورهای مختلـف، دسـتگاه‌های تجزیـه و تحلیـل دی¬ان¬ای ، نظـارت بـر محیـط زیسـت و نیـز مـواد غذایـی و یـا دسـتگاه‌های عملیـات میدانـی اطـلاق شـود. حقوق¬دانـان «چیزهـا» را بـه عنـوان یـک «ترکیبـی از سـخت‌افزار، نرم‌افـزار، اطلاعـات و خدمـات» قلمـداد می‌کننـد.

ایـن دسـتگاه‌ها اطلاعـات مفیـد را بـا کمـک فناوری‌هـای مختلـف موجـود جمـع‌آوری می‌کننـد، سـپس به‌صـورت خـودکار داده‌هـا را بیـن دسـتگاه‌های دیگـر بـه جریـان می‌اندازنـد. نمونه‌هـای موجـود آن عبارتنـد از: اتوماسـیون خانگـی ماننـد کنتـرل و اتوماسـیون روشـنایی، گرمایشـی (ماننـد ترموسـتات هوشـمند)، تهویـه و لـوازم خانگـی از قبیـل ماشـین لباسشـویی، جاروبرقـی روباتیـک، تصفیـه هـوا، اجـاق¬گاز و یخچـال کـه می‌تـوان بـا اسـتفاده از اینترنـت اشـیاء از راه دور آن‌هـا را کنتـرل نمـود. اینترنـت اشـیا یکـی از سیسـتم عامل‌هـای شـهرهای هوشـمند امـروزی و مدیریـت انـرژی اسـت.

فنـاوری اینترنـت اشـیاء نقـش بسـیار مهمـی در دنیـای کارآفرینـان بـازی می‌کنـد. کسـب و کارهـای متعـددی بـر محـور ایـن فنـاوری راه‌انـدازی شـده‌اند، در حالی‌کـه ایـن مفهـوم و ایـن فنـاوری در ابتـدای راه خـود قـرار دارد و هـر روز بیـش از پیـش تغییـرات و تحـولات جدیـدی در آن رخ می‌دهـد. اسـتفاده از ایـن فنـاوری بـرای کارآفرینـان و محققیـن خـلاق ایرانـی یـک فرصـت گران‌بهـا بـه شـمار مـی‌رود کـه می‌توانـد بـه بهبـود فضـای کسـب و کار و اشـتغال‌زایی در کشـور کمـک شـایانی نمایـد.

کویـن اشـتون بـا مطـرح کـردن مفهـوم اینترنـت اشـیاء جهانـی را بـه تصویـر کشـید کـه در آن هـر چیـزی، از جملـه اشـیاء بـرای خـود هویـت دیجیتـال داشـته باشـند و بـه رایانه‌هـای مرکـزی کـه بـه آنهـا متصلنـد، اجـازه دهنـد کـه آن‌هـا را سـازماندهی و مدیریـت کننـد.[۲] اینترنـت اشـیاء سیسـتمی بهـم پیوسـته از دسـتگاه‌های محاسـباتی، مکانیکـی و ماشـین‌های دیجیتالـی اسـت کـه هـر یـک از ایـن اشـیاء دارای یـک شناسـه واحـد می‌باشـند و توانایـی انتقـال داده در بسـتر شـبکه بـدون نیـاز بـه دخالـت انسـان را دارنـد، در واقـع ایـن تعریـف اشـیاء در مفهـوم اینترنـت اشـیاء اسـت.[۳]

اینترنـت در واقـع شـبکه‌ای از شـبکه هاسـت. هرکـدام از مـا بـه اینترنـت بـا اسـتفاده از یـک کابـل فیزیکـی یـا یـک ابـزار بـی سـیم متصـل مـی شـویم. در زیرسـاخت ایـن شـبکه، یـک سـتون فقـرات واقعـی از اتصـالات کـه دنیـا را بـه رایانه-هـای مـا متصـل می‌کننـد، وجـود دارد.

۲- کاربردهای اینترنت اشیاء

اینترنـت اشـیاء در حوزه‌هـای متعـدد و گسـترده‌ای کاربـرد دارد امـا یکـی از سـاده‌ترین و قابـل درک‌تریـن نمونه‌هایـی کـه می‌تـوان مثـال زد، دسـتگاه‌های تهویـه مطبـوع واقـع در یـک فضـا ماننـد منـزل اسـت. نمونـه‌ای از ایـن دسـتگاه سـاخته شـده، ترموسـتات نسـت اسـت. ایـن دسـتگاه نوعـی ترموسـتات هوشـمند اسـت کـه می‌توانـد زمـان خـواب و کلیـه عـادات شـما را یـاد گرفتـه، زمانـی کـه شـما خـواب هسـتید دمـا را بـا توجـه بـه دمایـی کـه شـما دوسـت داریـد تنظیـم کنـد. در ایـن حالـت شـما دیگـر لازم نیسـت نگـران گـرم یـا سـرد شـدن محیـط زندگی‌تـان در طـول شـب باشـید. نمونـه دیگـر محصـولات شـرکت اسـمارت تینگـز اسـت. ایـن شـرکت حس¬گرهـای مختلفـی را بـرای ایجـاد خانـه هوشـمند در اختیـار شـما قـرار می‌دهـد. بـا اسـتفاده از ایـن حس¬گرهـا می‌توانیـد متوجـه شـوید چـه شـخصی وارد منـزل شـده یـا از آن خـارج می‌شـود. همچنیـن ایـن حس‌گرهـا قابلیـت ایـن را دارنـد کـه در صـورت هـدر رفتـن آب نیـز گزارشـی مربـوط بـه نشـتی سیسـتم آب بـه شـما بدهنـد (شـکل ۱).

شکل۱- خانه هوشمند[۳]

بـا گسـترش و ارتقـای ابزارهـای موجـود در ایـن اکوسیسـتم، بـه عنـوان مثـال دسـتبند هوشـمند مخصـوص فعالیت‌هـای بدنـی، می‌توانـد بـه محـض خوابیـدن شـما، تلویزیـون و چراغ‌هـا را خامـوش کنـد و یـا حتـی پیـش از سوارشـدن بـر خـودرو در زمانـی مشـخص، بهتریـن مسـیر بـرای رسـیدن شـما بـه مقصـد توسـط خـودرو انتخـاب و در صـورت دیـر رسـیدن بـه محـل قـرار، پیامکـی بـه شـخص مقابـل ارسـال شـود.

چشـم‌اندازی کـه بـرای اینترنـت اشـیاء می‌تـوان متصـور بـود، بسـیار گسـترده اسـت و همان‌طورکـه از نـام آن برمی‌آیـد شـامل اتصـال همـه چیزهـا در دنیـا بـه یکدیگـر می‌شـود.

پیش‌بینی اینترنت اشیاء:

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

شکل۲- چشم‌انداز اینترنت اشیاء[۴]

شکل ۲ چشم اندازی از اینترنت اشیاء 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 اشیاء وجود خواهد داشت.[۴]

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

مراجع:

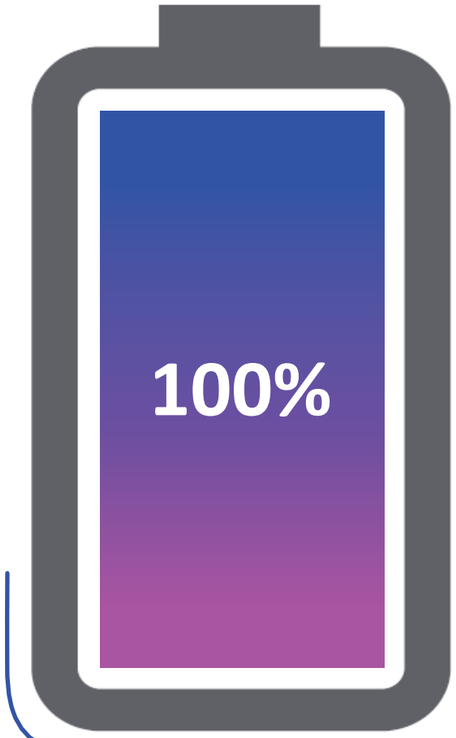
[۱] Ermesan, Ovidiu; Friess ,Peter , Internet of things: covering Technologies for smart Environments and Integrated Ecosystems, 2013

[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 August2016)



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