محاسبات نرم

فصل نامه انجمن علمی دانشجویی رایانش امن دانشگاه تبریز

سال اول | شماره دوم | زمستان ۱۴۰۲



بسم الله الرحمن الرحیم

به نام آنکه جان را فکرت آموخت چراغ دل، به نور جان برافروخت

صاحب امتیاز:

انجمن علمی-دانشجویی رایانش امن دانشگاه تبریز

سردبیر:

سینا صمدی

مدیر مسئول:

کیمیا شیرینی

هیات تحریریه:

الهه دائی کوزه کنانی

(دانشجوی کارشناسی مهندسی کامپیوتر-نویسنده و طراح)

محمدرضا عبدالله زاده بینا

(دانشجوی کارشناسی مهندسی کامپیوتر)

ارتباط با ما :

https://t.me/secure_comp_tbz

آنچه در فصل نامه شماره اول خواندیم

ما در جلد اول نشریه محسابات نرم با مفهوم رایانش آشنا شدیم و همچنین روش های محساباتی (محاسبات نرم و محاسبات سخت) و به بررسی دقیق تر محاسبات نرم پرداختیم و همچنین آموختیم کاربرد های محاسبات نرم را من جمله شبکه عصبی فازی-سیستم های فازی و ... و همچنین اطلاعاتی در مورد دروس محاسبات نرم کسب کردیم.

مقایسه کردیم محاسبات نرم را با محاسبات سخت

نمونه کد شبکه عصبی را مشاهده کردیم

با سیستم های هوشمند و منطق فازی اشنا شدیم

در ادامه بر بررسی رایانش ابری و کاربرد ها و موارد استفاده آن و مزایا و ویژگی های مثبت و منفی آن آشنا شدیم

و در آخرین قسمت به برخی مفاهیم اینترنت اشیا پرداختیم و با تاریخچه رشد و تکامل اینترنت اشیا و معماری آن و به معرفی لایه های آن پرداختیم و در ادامه بیشتر با آن آشنا خواهیم شد.

آنچه در این فصل نامه خواهیم خواند

کاربردهای اینترنت اشیا

کاربردهای اینترنت اشیا

امنیت و حریم خصوصی در اینترنت اشیا

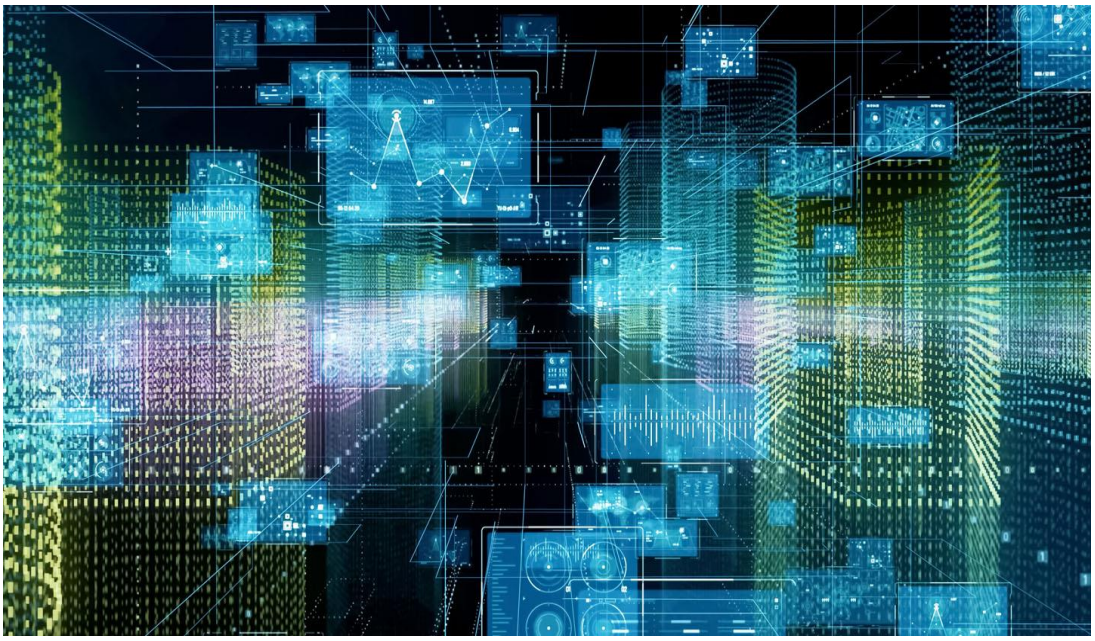
بلاکچین راه حل برقراری امنیت در اینترنت اشیا

رمز نگاری

- تکنیک های رمزنگاری
- انواع رمزنگاری ها
- تاریخچه رمز نگاری
- کاربرد های رمز نگاری در امنیت اطلاعات
- مفاهیم مرتبط با محاسبات نرم
- رمز نگاری همگن
- رمز نگاری کلید عمومی و خصوصی
- استفاده از هش در رمزنگاری

Map of computer science

کاربردهای اینترنت اشیا



کاربرد اینترنت اشیا بسیار گسترده است و محدود به یکی یا دو مورد نیست. به هر حوزه‌ای باعث بهبود IOT ورود عملکرد، انجام کارها به صورت خودکار و تسهیل کنترل فرایندهای مختلف می‌شود. که به برخی از کاربردهای مهم اینترنت اشیا اشاره می‌کنیم

کاربرد IOT در صنعت

اینترنت صنعتی اشیا (Industrial internet of things) به استفاده از فناوری اینترنت اشیا در یک محیط صنعتی اطلاق می‌شود. اینترنت اشیا در صنعت ترکیبی از حسگرها، شبکه‌های بی‌سیم، داده‌های بزرگ، هوش مصنوعی و تجزیه و تحلیل برای بهینه‌سازی فرآیندهای صنعتی است. افزایش بهره‌وری نیروی کار و صرفه جویی در هزینه دو هدف بالقوه به کارگیری اینترنت اشیا در صنعت است IOT .به شرکت‌ها و صنایع مختلف کمک می‌کند تا خدمات و محصولات خود را از راه دور به صورت آنلاین کنترل کنند و با جمع‌آوری داده‌های مورد نیاز، برای کنترل و بهبود فرآیندها تصمیماتی را اتخاذ کنند.

کاربرد IOT در محیط زیست

آی او تی در محیط زیست و حفظ زمین نقش بسیار مهمی دارد. امروزه درجوامع پیشرفته شاهد آن هستیم که گام‌های رو به جلویی برای استفاده هرچه بیشتر از این فناوری برداشته می‌شود زیرا نه تنها باعث سهولت زندگی انسان می‌شود بلکه به حفاظت از محیط زیست کمک می‌کند. برخی از کاربردهای اینترنت اشیا در محیط زیست به شرح زیر است: :مدیریت منابع آبی: یکی از چالش‌های اصلی که اغلب کشورها با آن دست و پنجه نرم می‌کنند، مشکل کم آبی است. به همین دلیل مدیریت منابع آب بسیار حائز اهمیت است. این موضوع در حوزه کشاورزی که بخش مهمی از کل آب مصرفی را به خود اختصاص می‌دهد از اهمیت بیشتری برخوردار است IOT .به کشاورزان کمک می‌کند تا به کمک سنسورهای اینترنت اشیا و محرک‌های ایجاد شده در زمین، آب مصرفی را تا حد بسیار زیادی کاهش دهند. جلوگیری از نابودی جنگل: قطع بی رویه و بدون مجوز درختان باعث نابودی جنگل‌ها می‌شود. یکی از روش‌های کارآمد برای پیشگیری از بروز چنین اتفاق ناخوشایندی حفاظت بیشتر از درختان از طریق اینترنت اشیا است. می‌توان روی تنه درختان سنسورهای حساس به صدای اره یا عبور وسایل نقلیه بزرگ (که برای حمل درختان قطع شده استفاده می‌شوند) نصب کرد. جنگل‌بانان در صورت دریافت علامت هشدار از سنسورها سریعا وارد عمل خواهند شد و از فعالیت بیشتر خرابکاران جلوگیری می‌کنند.



کاربرد IOT در کشاورزی

یکی از اصطلاحات جدیدی که اخیرا در صنعت کشاورزی می‌شنویم، مزارع هوشمند است. مزارع هوشمند دستگاه‌هایی هستند که به اینترنت متصل می‌شوند و انواع داده‌های آنلاین مربوط به محصولات را ارائه می‌دهند. این اطلاعات شامل بافت خاک، تعادل رطوبت، سطح آفت‌کش‌ها، سطح آب و سلامت محصولات است. ورود اینترنت اشیا در صنعت کشاورزی باعث افزایش کیفیت و کمیت محصولات شده است و از طرف دیگر نیروی کار لازم و مصرف انرژی به میزان قابل توجهی کاهش پیدا می‌کند. از نظر متخصصان این حوزه اینترنت اشیا در کشاورزی، موج دوم انقلاب سبز در جهان است که مزایای بسیار زیادی با خود دارد و مهمترین آن این است که کشاورزان در زمان کمتری کارها را انجام می‌دهند.



کاربرد IOT در حوزه درمان

یکی از مهم‌ترین کاربردهای اینترنت اشیا در حیطه سلامتی است. استفاده از گجت‌های پوشیدنی یا حسگرهایی که به بیمار وصل می‌شود این امکان را به کادر درمان می‌دهد تا وضعیت بیمار را به صورت لحظه‌ای و حتی از راه دور کنترل کنند و در صورت لزوم اقدامات پیشگیرانه را اتخاذ کنند. نتایج تحقیقات نشان می‌دهد که کاربرد IOT در حوزه درمان، حوادث مرگبار بیماران را به میزان قابل توجهی کاهش می‌دهد. زیرا به دلیل نظارت مداوم، هرگونه علائم خطر سریعا تشخیص داده می‌شود و برای حفظ علائم حیاتی، حتی ممکن است به صورت خودکار از طریق دستگاه‌های هوشمند به بیمار دارو تزریق شود.



کاربرد IOT در خودروسازی

اتومبیل‌های خودران یکی از بهترین محصولات اینترنت اشیا است که رانندگی را بسیار جذاب و لذت‌بخش کرده است. این خودروها از از سنسورها و حسگرهای خاصی استفاده می‌کنند که وظیفه جمع‌آوری داده و ارسال آن به اپلیکیشن‌های کاربردی را بر عهده دارند. این برنامه‌ها با تحلیل داده‌ها، هشدارها و مشکلات احتمالی مانند معیوب شدن قطعات را به راننده اطلاع می‌دهند. در صورتی که راننده نسبت به رفع این مشکلات سریعا اقدام کند سطح کارایی و ایمنی خودرو را بالا می‌برد.

این خودروها به راننده کمک می کنند تا بتواند زمان خود را هم مدیریت کند. تصور کنید در حال رانندگی با ماشین هوشمند خود به مقصد خاصی هستید. خودروهای هوشمند این قابلیت را دارند که کوتاه‌ترین مسیر به مقصد را پیشنهاد دهند و همچنین با توجه به ترافیک، زمان تخمینی رسیدن به مقصد را نیز محاسبه کنند. با توجه به اینکه اینترنت اشیاء توانسته است در صنعت خودرو تغییرات مثبتی تا به امروز ایجاد کند. انتظار می‌رود که در آینده هم از طراحی تا تولید خودرو نقش بیشتری داشته



کاربرد IOT در ساختمان سازی

بدون تردید مهم‌ترین کاربرد آی او تی در هوشمندسازی ساختمان بوده است. اینترنت اشیا به شما کمک می کند تا تجهیزات و وسایل منزل یا محل کار خود را به کمک برنامه‌های مبتنی بر وب، کنترل کنید. برای مثال یخچال‌های هوشمند می‌توانند اطلاعات مختلفی مانند محتویات یخچال، مقدار یا تعداد مواد غذایی و حتی تاریخ انقضای آن‌ها را در اختیار کاربران قرار دهد. هدف از بکارگیری IOTدر ساختمان سازی، کنترل وسایل و ایجاد راحتی و آسایش و تامین امنیت برای کاربران است.

امروزه خانه‌های هوشمند طرفداران زیادی دارد و حتی در ایران، اگرچه هنور خانه‌های تمام هوشمند به اجرا درنیامده است اما خانه‌های نیمه هوشمند زیادی وجود دارد. بنابراین می‌توان گفت سرعت پذیرش IOT در حوزه ساختمان‌سازی توسط مردم نسبت به سایر حوزه‌ها بیشتر است.



کاربرد IOT در مدیریت مصرف انرژی

کاهش مصرف انرژی و جلوگیری از اتلاف انرژی‌های پایان پذیر یکی از چالش‌های اصلی انسان معاصر است. به همین دلیل راهکارهایی که برای صرفه جویی و بهینه سازی مصرف انرژی معرفی می‌شوند بسیار حائز اهمیت هستند. این در حالی است که خودکارسازی فرآیندها و سازماندهی مناسب برای کنترل و نظارت از راه دور به کمک اینترنت اشیا می‌تواند باعث کاهش مصرف انرژی شود.

به عنوان مثال می‌توان با قرار دادن حسگرها درنقاط مختلف یک ساختمان، داده‌های مربوط به دما را جمع آوری کرد و دمای هر قسمت را متناسب با شرایط تغییر داد. این کار علاوه بر بهینه کردن مصرف انرژی، باعث خواهد شد تا دستگاه‌های تهویه مطبوع دما را بهتر و هوشمندتر کنترل کنند و کاربران احساس راحتی بیشتری داشته باشند.





امنیت و حریم خصوصی در IOT

سیستم عامل‌های دستگاه‌های IOT مانند سیستم عامل‌های کامپیوتر نیستند و فقط برای دستگاه‌های اینترنت اشیا طراحی شده است. به دلیل برخی حفره‌های امنیتی که در این سیستم عامل‌ها وجود دارد، احتمال هک شدن توسط افراد مخرب، افزایش پیدا می‌کند.

هکرها به طور مرتب دستگاه‌های آی او تی مانند روترها و وب‌کم‌ها را مورد هدف قرار می‌دهند. برخی از گجت‌های پوشیدنی هوشمند حاوی حفره‌ها و خلاهای امنیتی هستند که به هکرها اجازه می‌دهد مکان کاربر را ردیابی کنند، مکالمات را استراق سمع کنند یا حتی با کاربر ارتباط برقرار کنند. توانایی دستگاه‌های IOT برای ردیابی موقعیت مکانی کاربر یک نگرانی خاص در خصوص حریم خصوصی است. داده‌های مکان در تئوری ناشناس هستند، اما داده‌هایی که مربوط به ردیابی حرکات افراد هستند می‌تواند باعث شناسایی هویت آن‌ها شود.

این در حالی است که نداشتن امنیت کافی و عدم حفظ حریم خصوصی موجب عدم پذیرش سرویس‌های اینترنت اشیا در بین مردم خواهد شد. اما با تنظیم یک چارچوب مشخص برای حفظ حریم خصوصی و ثبت قوانین آن، آموزش همگانی در ارتباط با نحوه استفاده از این دستگاه‌ها و پرورش نیروی کارآمد در این حوزه می‌توان بسیاری از حملات و تهدیدات سایبری را دفع کرد.

بلاکچین راه حل برقراری امنیت در اینترنت اشیا



ترکیب فناوری بلاکچین با IOT می‌تواند نگرانی‌های امنیتی زیادی که در رابطه با فناوری اینترنت اشیا مطرح است را رفع کند. در بلاکچین، داده‌ها در زنجیره‌ای از بلاک‌ها ذخیره می‌شوند که هر بلاک به بلاک قبلی متصل است. اطلاعات روی بلاک از طریق سیستم رمزنگاری دائمی ذخیره می‌شوند و به هیچ‌عنوان قابل تغییر یا حذف نیستند. این ویژگی بلاکچین می‌تواند IOTرا به شدت امن و قابل اعتماد بکند.

ترکیب اینترنت اشیا با فناوری دفتر کل توزیع شده از طریق سایر روش‌ها هم می‌تواند نگرانی‌های مربوط به امنیت IOT را کاهش دهد که به تعدادی از آن‌ها در ادامه اشاره می‌کنیم:

•بلاکچین یک شبکه همتا به همتا توزیع شده است و هیچ سازمان خاصی برای مدیریت و نگهداری داده‌های عظیم فراهم آمده توسط شبکه اینترنت اشیا وجود ندارد.

•رمزنگاری داده‌ها در بلاکچین به عنوان یک لایه امنیتی در IOT به شمار می‌رود و از داده‌ها در برابر هکرها محافظت می‌کند.

•یکی از مهم‌ترین ویژگی‌های زنجیره بلاک، ایجاد شفافیت است. تمام کاربران اجازه مشاهده فعالیت‌های انجام شده را دارند؛ به همین دلیل در صورت بروز هرگونه حمله مخرب، منبع نشت شده فورا مشخص می‌شود و می‌توان سریعا اقدامات لازم را در جهت دفع آن انجام داد.

رمز نگاری

رمز نگاری که با عنوان cryptography شناخته میشود،روشی برای محافظت از اطلاعات و ارتباطات به وسیله کدها است.بدین وسیله تنها کسی قادر به خواندن و پردازش کردن این اطلاعات می باشند که اطلاعات برای آنها در نظر گرفته شده است.



در علوم کامپیوتر،رمز نگاری به اطلاعات ایمن و تکنیک های ارتباطی ای اشاره دارد که از مباحث ریاضی و محاسباتی مشتق شده اند که به آن الگوریتم می گویند و به وسیله این الگوریتم ها،پیام ها تبدیل به متونی می شوند که رمزگشایی آنها برای افراد خربکار،کار دشواری است.

از این الگوریتم ها برای تولید کلید های رمزنگاری،امضای دیجیتال،تایید هویت برای محافظت از حریم خصوصی داده ها،مرور وب در اینترنت و ارتباط محرمانه مانند تراکنش های کارت های بانکی و ایمیل ها استفاده می شود.

تکنیک های رمزنگاری

رمزنگاری،ارتباط نزدیکی با رمزشناسی (cryptology)و تحلیل رمزی (Cryptanalysis)دارد که شامل تکنیک هایی از جمله ریز نقطه ها(Microdots) ادغام متن و تصویر سایر روش های پنهان سازی اطلاعات جهت ذخیره یا انتقال آن هاست.البته در دنیای کامپیوتری امروزی،واژه ی رمزنگاری بیشتر به درهم ریخته کردن متن های ساده (Plaintext) اشاره می کند.

به این صورت که متون معمولی و ساده را از طریق فرایندهای رمزنگاری،به یک متن رمزی یا Cipher text(بخوانید سایفرتکست) تبدیل می کند.این متن های رمزشده یا سایفر تکست ها،به وسیله فرایند رمزگشایی،دوباره به متن عادی تبدیل میشوند.به افراد فعال در این حوزه،

به اصطلاح رمزنگار یاCryptographer می گویند

.

هدف از رمزنگاری های مدرن،برقراری چهارمورد زیر است:

1.محرمانگی:

اطلاعات باید برای کسانی که به عنوان هدف آن اطلاعات در نظر گرفته نشده است،قابل خواندن و فهمیدن نباشد.

به عنوان مثال اگر فرد الف قصد ارسال پیامی را به فرد ب داشته باشد،به وسیله الگوریتم های رمزنگاری،تنها فرد ب قادر به رمزگشایی و خواندن این پیام است و هیچ شخص دیگری نباید قادر به خواندن آن پیام باشد.

2.یکپارچگی:

اطلاعات،قادر به تغییر در مسیر بین فرستنده وگیرنده نمی باشد و هر تغییری که بر روی این اطلاعات انجام شود،قابل شناسایی است.

3.عدم انکار:

فرستنده یا گیرنده اطلاعات،در مراحل بعد از ارسال،نمیتوانند ساختن یا انتقال این اطلاعات را انکار کنند

(فرآیند ارسال یک نامه را در نظر بگیرید)

4. احراز هویت:

فرستنده و گیرنده اطلاعات،می توانند هویت همدیگر و همچینین مبدا و مقصد این اطلاعات را تایید کنند.

•پروتکل ها و مراحلی که چهار قاعده ی ذکر شده ی فوق را رعایت کرده باشند،به عنوان سیستم های رمزنگاری یا Cryptosystems شناخته میشوند.اغلب اوقات از رمزنگاری،تنها به عنوان عملیات های ریاضی یاد می شود،اما با این حال رفتار های انسانی نیز در مراحل رمزنگاری دخیل است.به عنوان مثال انتخاب یک کلمه عبور (Password) که حدس زدن آن سخت باشد.یا مثلا خارج شدن از سیستم هایی که استفاده نمیشوند و عدم گفتگو با افراد ناشناس در مورد اطلاعات حساس.



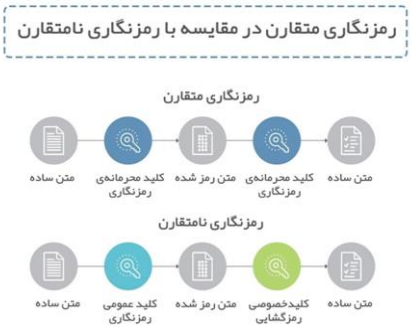
انواع رمزنگاری ها

الگوریتم های رمزنگاری تک کلید(simple-key)یا همان رمزنگاری کلید-متقارن،یک رشته ای از بیت ها را با طول یکسان تولید می کند که به آن یک بلاک رمز شده یا بلاک سایفر میگویند.در این نوع الگوریتم رمزنگاری،فرستنده و گیرنده اطلاعات، از یک کلید رمزی (secret key) برای رمزنگاری و رمزگشایی اطلاعات استفاده میکنند. یکی از نمونه های مهم رمزنگاری کلید-متقارن، AES یا advanced Encryption Standard می باشد AES .الگویی است که در نوامبر سال 2001 توسط موسسه ملی استانداردها و تکنولوژیک (NIST) به عنوان یک استاندارد پردازش اطلاعات فدرال (FIPS 197) تایید شد تااز اطلاعات حساس و محرمانه،محافظت کند. این استاندارد توسط دولت ایالات متحده آمریکا اجباری شده است و به طور گسترده ای در بخشهای خصوصی مورد استفاده قرار میگیرد.

در ژوین سال 2003 AES توسط دولت ایالات متحده آمریکا برای اطلاعات طبقه بندی شده تایید شد.همچنین برای استفاده و پیاده سازی AES یک جایگزین برای Data Encryption Standardیا DES و همچنین DES3 میباشد و از کلیدهای با طول بیشتر یعنی 128 بیتی،192 بیتی و 256 بیتی استفاده میکند تا از حملات Brute forceو دیگر حملات بتوان جلوگیری کرد.

کلید عمومی یا رمزنگاری کلید-نامتقارن یک الگوریتمی است که از جفت کلیدهایی برای رمزنگاری استفاده میکند.کلید عمومی که دست تولیدکنندگان و فرستندگان پیام است و از آن برای رمزنگاری استفاده میشود و یک کلید خصوصی که تنها دست مالک اصلی گیرنده پیام است و برای رمزگشایی پیام ها استفاده میشود(کلید خصوصی می تواند توسط مالک آن به اشتراک گذاشته شود و همچنین میتواند ناخواسته لو برود).

نمونه هایی از رمزنگاری کلید-نامتقارن



RSAکه به طور گسترده ای در اینترنت استفاده میشود.

الگوریتم امضای دیجیتال منحنی بیضوی یا Elliptic Curve Digital Signature Algorithm (ECDSA)که توسط بیت کوین مورد استفاده قرار گرفته است.

الگوریتم Digital Signature Algorithm یا DSA که به عنوان یک استاندارد پردازش اطلاعات فدرال برای امضای دیجیتال توسط NIST در FIPS 186-4پذیرفته شده است.

الگوریتم تعویض کلید دیفی هلمن یا Diffie-Hellman key exchangeکه یک الگوریتم ساده برای تبادل کلید می باشد.

برای تحقق یکپارچگی در رمزنگاری،از تابع های هش (Hash Functions)استفاده می شود که ورودی های متفاوت را به خروجی با طول یکسان تبدیل میکند و برای نگاشت داده ها به یک داده ای با سایز یکسان مورد استفاده قرار میگیرد.انواع متخلفی از توابع هش وجود دارد،

به عنوان مثال SHA-1 (Secure Hash Algorithm 1)و همچنین MD5، SHA-3، SHA-2

.

تاریخچه رمز نگاری

واژه رمزنگاری یا Cryptography ،از واژه یونانی kryptos به معنای مخفی مشتق شده است.پیشوند "crypto"به معنی مخفی میباشد و پسوند "graphy"به معنای نوشتن است.منشا رمزنگاری معمولا به 2 هزار سال قبل از میلاد مسیح برمیگردد در آن زمان مصریان از هیروگلیف استفاده میکردند.هیروگلیف شامل تعدادی تصاویر پیچیده از حیوانات و اشیا که معنای کامل آن را تعداد کمی از نخبگان میدانند.

اولین استفاده از رمزنگاری مدرن رت به ژولیوس سزار نسبت می دهند(100 سال تا 44 سال قبل از میلاد مسیح)وژولیوس به پیام رسان های خود هنگام برقراری ارتباط با فرمانداران و افسران،اعتماد نداشت.به همین دلیل او یک سیستمی درست کرد که در آن هر کاراکتر داخا متن پیام،با سه کاراکتر جلوتر در جایگاه الفبای رومی جایگزین شد.

در زمان های اخیر،رمزنگاری به یک میدان نبرد برای برخی از بهترین ریاضیدان ها و دانشمندان کامپیوتر در جهان تبدیل شده است.توانایی ذخیره و انتقال امن اطلاعات حساس و محرمانه به یک عامل مهم در کسب موفقیت در جنگ و تجارت تبدیل شده است.

از آنجایی که دولت ها نمیخواهند تا نهادهای خاص،چه در داخل چه در خارج از کشورشان به راه هایی برای دریافت و ارسال اطلاعات سری که ممکن است تهدیدی برای منافع ملی باشد،دسترسی داشته باشند.رمزنگاری در بسیاری از کشورها با محدودیت های مختلفی روبه رو شده است.از جمله محدودیت در استفاده و یا صادرات نرم افزارها و عمومی کردن مفاهیم ریاضیات که میتواند منجر به توسعه سیستم های رمزنگاری میشود.

با این حال،اینترنت امکان گسترش برنامه های قدرتمند و مهمتر از آن،تکنیک های اساسی و ساختاری رمزنگاری را فراهم کرده است. به طوری که امروزه پیشرفته ترین سیستم های رمزنگاری و ایده ها،در دسترس عموم قرار دارند.

کاربرد های رمزنگاری در امنیت اطلاعات

رمزنگاری در امنیت اطلاعات برای محافظت از اطلاعات محرمانه از جمله رمزنگاری داده ها وامضای دیجیتال وتاثیر هویت استفاده میشود.این کاربرد برای حفاظت اطلاعات در انتقال داده ها و همچنین ذخیره آنها مورد استفاده قرار میگیرد .



مفاهیم مرتبط با محاسبات نرم

این عنوان شامل مفاهیمی مانند شبکه های عصبی مصنوعی و الگوریتم های ژنتیک و سیستم های کنترل فازی و سایر مفاهیمی که در حل مسائل پیچیده و نیازمند قطعیت مطلوب استفاده میشود.

قوانین رمزنگاری هنوز هم مورد استفاده دانشمندان رمزنگاری پیشرفته است:

سامانه رمزنگاری نه فقط از دید تئوری بلکه درعمل هم باید غیر قابل شکستن باشد.سامانه رمزنگاری نباید هیچ نکته پنهان محرمانه ای داشته باشد بلکه تنها چیزی که سری است کلید رمز است.کلید رمز باید به گونه ای انتخاب پذیر باشد که

1) بتوان به سادگی آن را عوض کردو

2) بتوان آن را به یاد آورد .

متون رمزنگاری باید از طریق خطوط تلگراف مخابره پذیر باشند.

رمزنگاری همگن

در این نوع از رمزنگاری یک کلید مشترک برای رمزنگاری و رمزگشایی استفاده میشود.این امر به معنای این است که هر دو فرآیند رمزنگاری و رمزگشایی از یک کلید استفاده میشود.

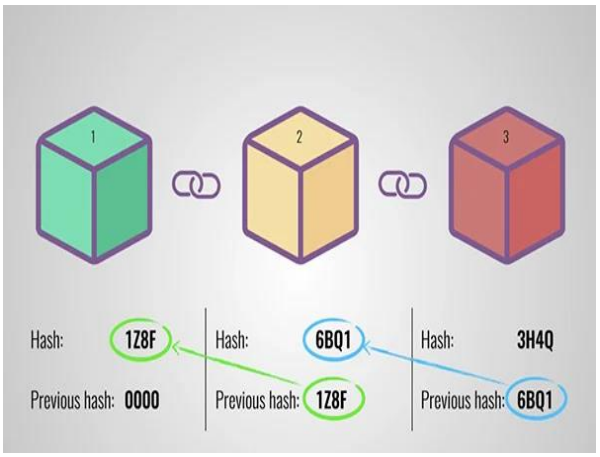




رمز نگاری کلید عمومی و خصوصی

در رمزنگاری عمومی از دو کلید متمایز استفاده میشود وهر کس میتواند از آن استفاده کنداما رمزگشایی تنها با استفاده از کلید خصوصی ممکن است . در رمزنگاری خصوصی کلید تنها به افراد خاص خاص دارنده کلید رمزگشایی ارسال میشود.

استفاده از هش در رمزنگاری



هش ها(HASH) در رمزنگاری برای تایید یک داده به کار میروند . آنها یک نشانه منحصر به فرد از یک داده هستند میتوانند استفاده شوند تا از تغییرات در داده ها اطمینان حاصل کند .

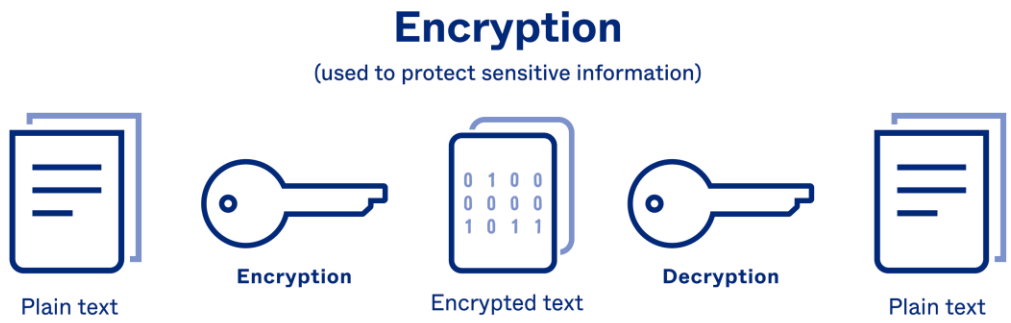
هر تابع هش باید شامل ویژگی های خاص باشد

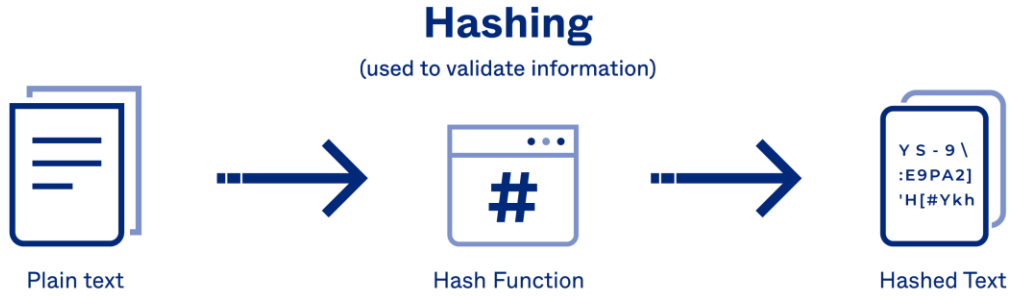
طول خروجی تابع هش یا مقدار هش همیشه ثابت است

تا زمانی که ورودی تغییر نکند خروجی ثابت میماند

مقدار هش معمولا کوچکتر از ورودی است به همین خاطر به تابع هش فشرده ساز نیز میگویند

عملکرد تابع هش با رمزنگاری متفاوت است

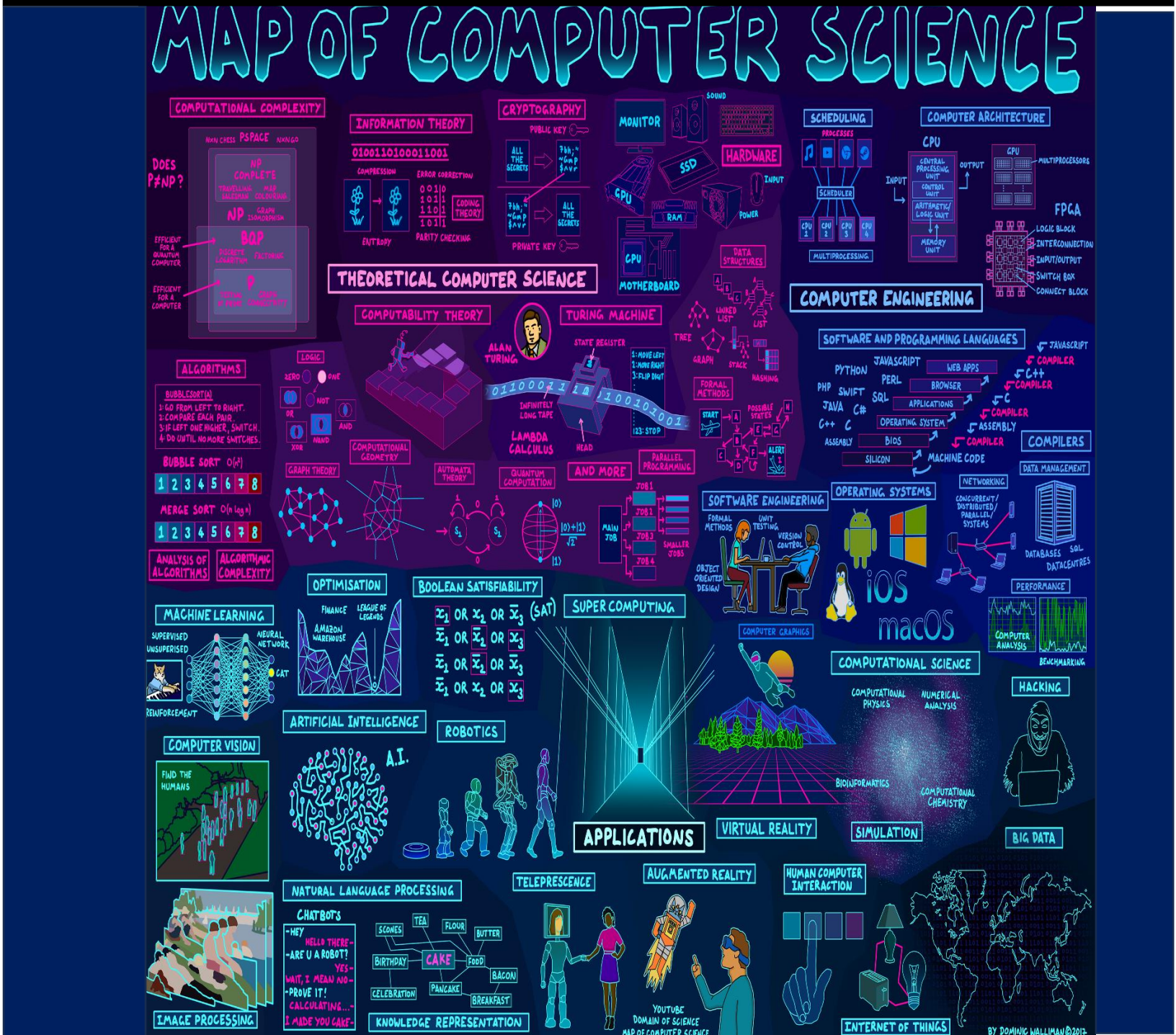




MAP OF COMPUTER SCIENCE

Elahe Daei KouzehKonani

Computer engineering student

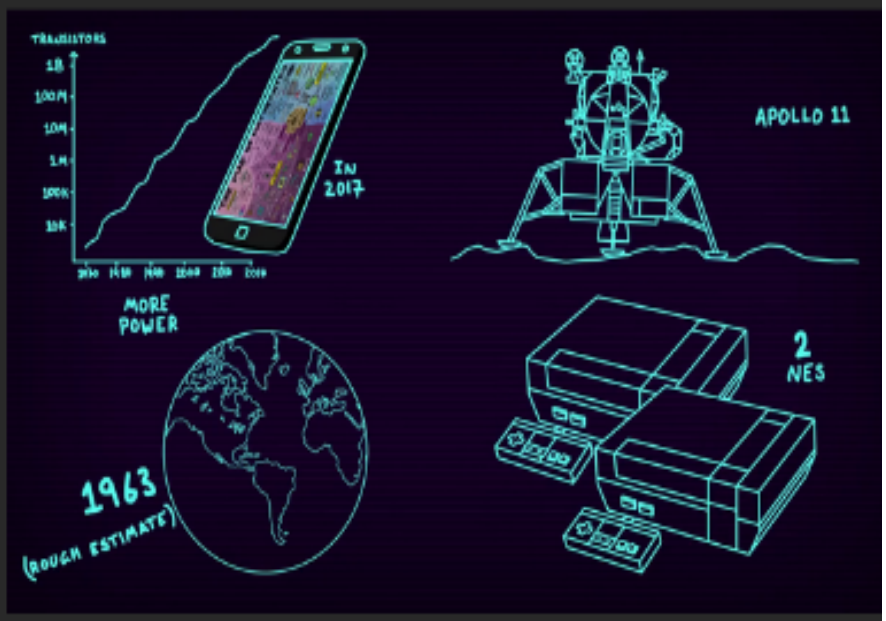


MAP OF COMPUTER SCIENCE



We built computers to expand our brains originally scientists build computers to solve arithmetic, but they turned out to be incredibly useful for many other things as well:
running the entire internet, lifelike, graphics,artificial brains or simulating the
universe, but amazingly all of it boils down to just flipping zeros and ones.
Computers have become smaller and more powerful at an incredible rate.

There is more computing power in your cellphone then there was in the entire world in the mid 60s.and the entire Apollo moon landing could have been run and couple of Nintendo computer science is the subject that studies what computers can do. It is diverse and over lapping field but I'm going to split it into three parts. The fundamental theory of computer science, computer engineering , and applications.





WE'LL START WITH THE FATHER OF THEORETICAL COMPUTER SCIENCE: ALAN TURING

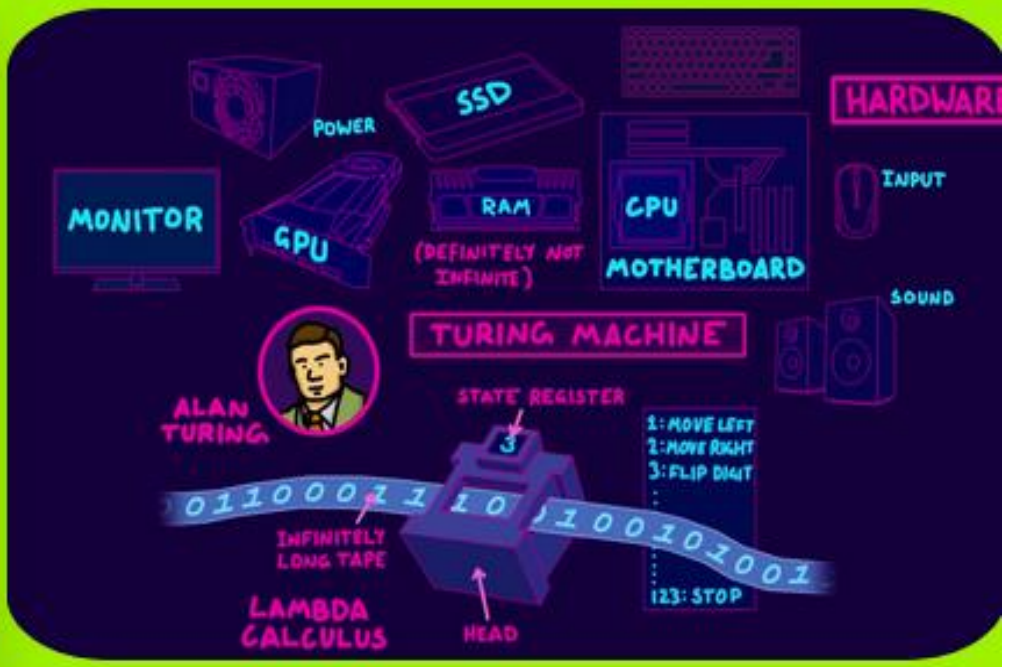
who formalized the concept of a Turing machine which is a simple description of a general purpose computer.

People came up with other designs for computing machines but they are all equivalent to a Turing machines which makes it the foundation of computer science.

Turing machine

A Turing machine
contains several parts: An infinitely long tape that is split into cells there is also a head that can read and write symbols to the tape, a state register that containing symbols. Stores that state of the head and a list of possible instructions.

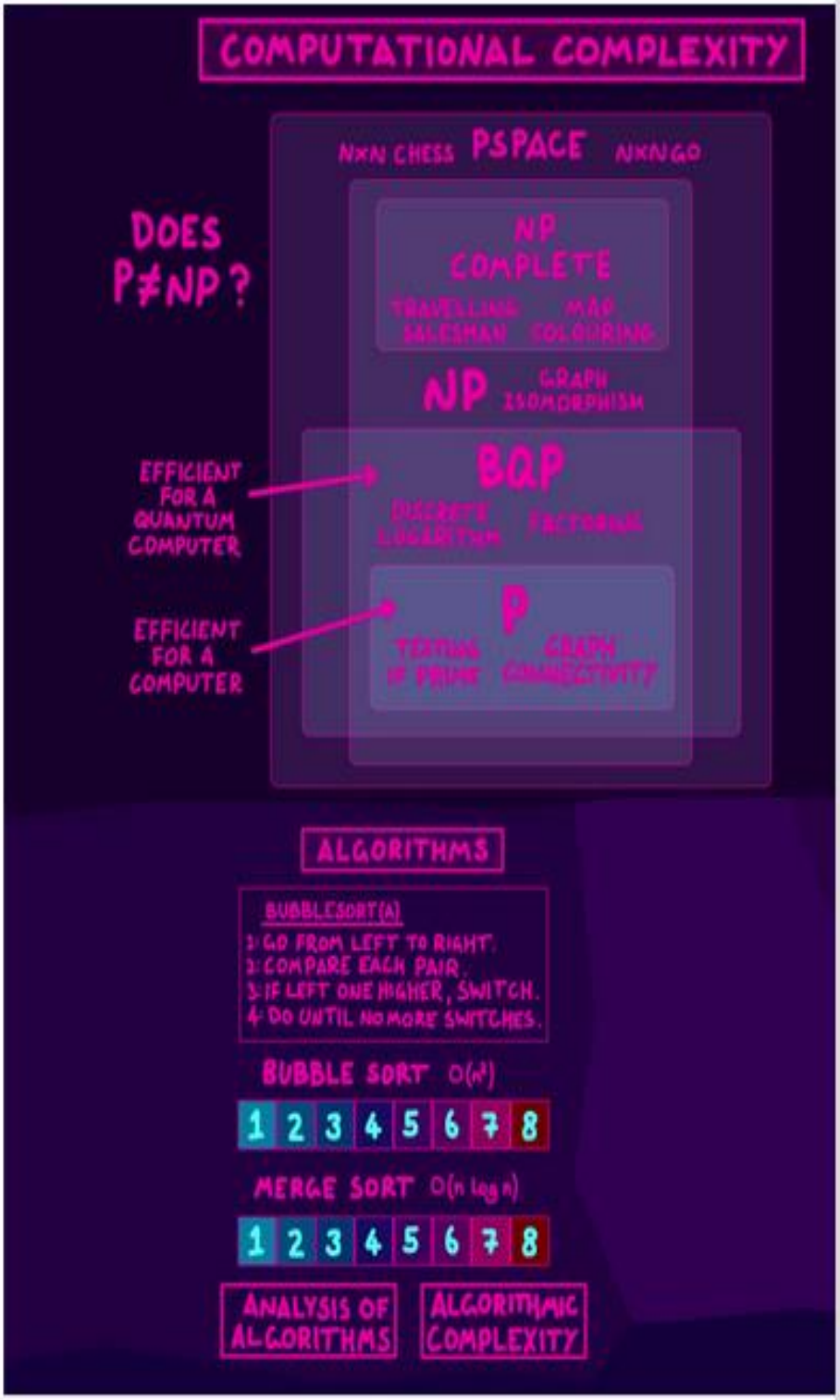
In todays computers
the tape is like the working memory or RAM, the head is the central processing unit and the list of instructions is held in the computer's memory.
Even thought
a Turing machine is a simple set of rules, it's incredibly powerful, and this is essentially what all computers do nowadays
Although our computers obviously
have a few more parts like permanent storage and all the other components



Every problem that is computable by
a Turing machine is computable using Lambda calculus which is the basis of research in programming languages.

COMPUTABILITY THEORY
ATTEMPTS TO CLASSIFY WHAT IS AND ISN'T COMPUTABLE. THERE ARE SOME PROBLEMS THAT DUE TO THEIR VERY NATURE, CAN NEVER BE SOLVED BY A COMPUTER, A FAMOUS EXAMPLE IS THE HALTING PROBLEM WHERE YOU TRY TO PREDICT WHETHER A PROGRAM WILL STOP RUNNING OR CARRY ON FOREVER. THERE ARE PROGRAMS WHERE THIS IS IMPOSSIBLE TO ANSWER BY A COMPUTER OR A HUMAN. MANY PROBLEMS ARE THEORETICALLY SOLVABLE BUT IN PRACTICE TAKE TOO MUCH MEMORY OR MORE STEPS THAN LIFETIME OF THE UNIVERSE TO SOLVE,

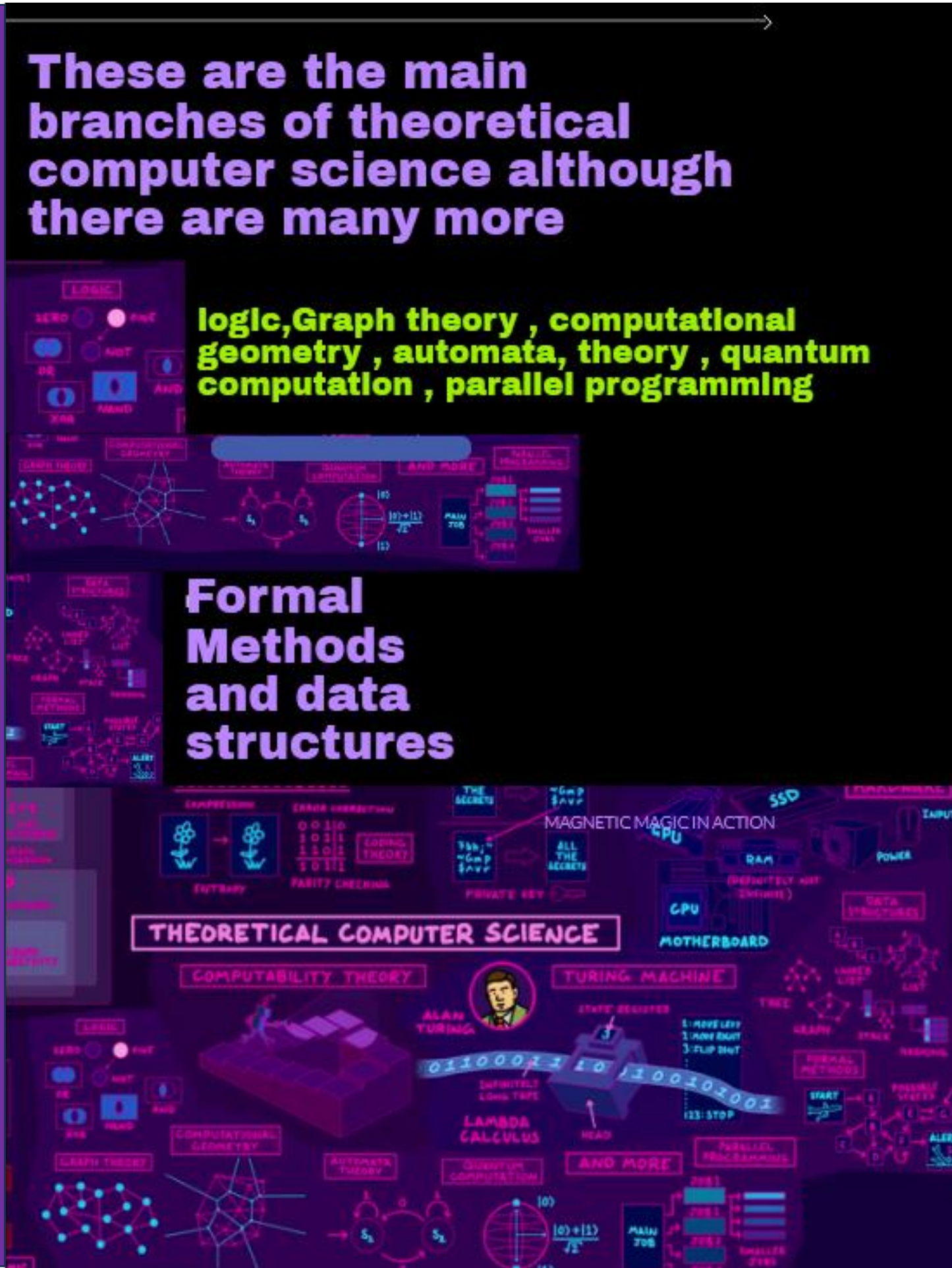
, and computational complexity attempts to categories these problems according to how they scale. There are many different classes of problem that fall into each type. There are a lot of real world problems that fall into these impossible to solve categories, but fortunately computer scientists have a bunch of sneaky tricks where you can fudge things and get pretty good answers but you'll never know if they are the best answer.



An algorithm is a setoff instructions independent of the hardware or programming language designed to solve a particular problem. It is kind of like a recipe of how to build a program and a lot of work is put into developing algorithms to get the best out of computers. Different algorithms can get to the same final result, like sorting a random set of numbers into order, but some algorithms are much more efficient that others,this is studied in algorithmic complexity

. information theory studies properties of information and how it can be measured, stored and communicated. One application of this is how well you can compress data , making it take up less memory while preserving all or most of the information but there are lots of other applications. Related to information theory is coding theory. And cryptography is obviously very important for keeping information sent over the internet secret. There are many different encryption schemes which scramble data and usually rely on some very complex mathematical problem to keep the information locked up.



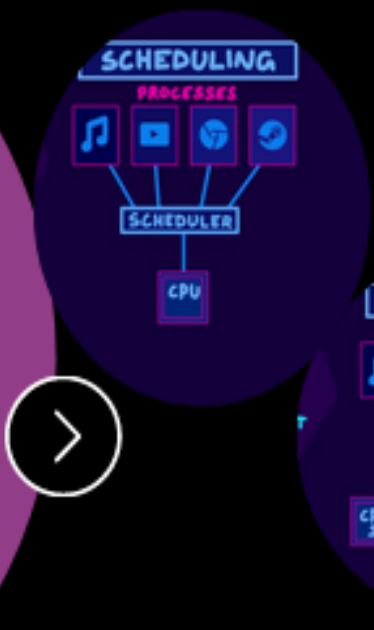

These are the main branches of theoretical computer science although there are many more
logic,Graph theory , computational geometry , automata, theory , quantum computation , parallel programming
Formal Methods and data structures
MAGNETIC MAGIC IN ACTION
THEORETICAL COMPUTER SCIENCE
COMPUTABILITY THEORY
TURING MACHINE
ALAN TURING
LAMBDA CALCULUS
AND MORE
CPU
MOTHERBOARD
RAM
SSD
POWER

lets move on to computer Engineering

Designing computers is difficult because they have to do so many different things. Designers need to try and make sure they are capable of solving many different kinds of problem as optimally as possible. Every single task that is run on the computer goes through the core of the computer :

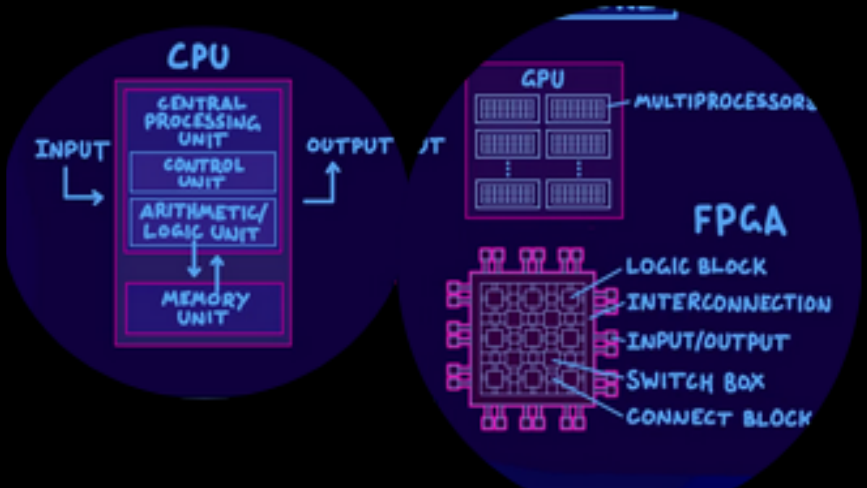
the CPU

When you are doing lots f different things at the same time , the CPU needs to switch back and forth between these jobs to make sure everything gets done in a reasonable time. This is controlled buy a scheduler , which chooses what to do when and tries to get through the tasks in the most efficient way , which can be very difficult problem. Multiprocessing helps speed things up because the CPU has several cores that can execute multiple jobs in parallel. But this makes the job of the scheduler even more complex..



Computer architecture

architecture is how a processor is designed to perform tasks and different architectures are good different things. CPU are general purpose , GPUs are optimized for graphics and FPGAs can be programmed to be very fast at very narrow range of tasks.

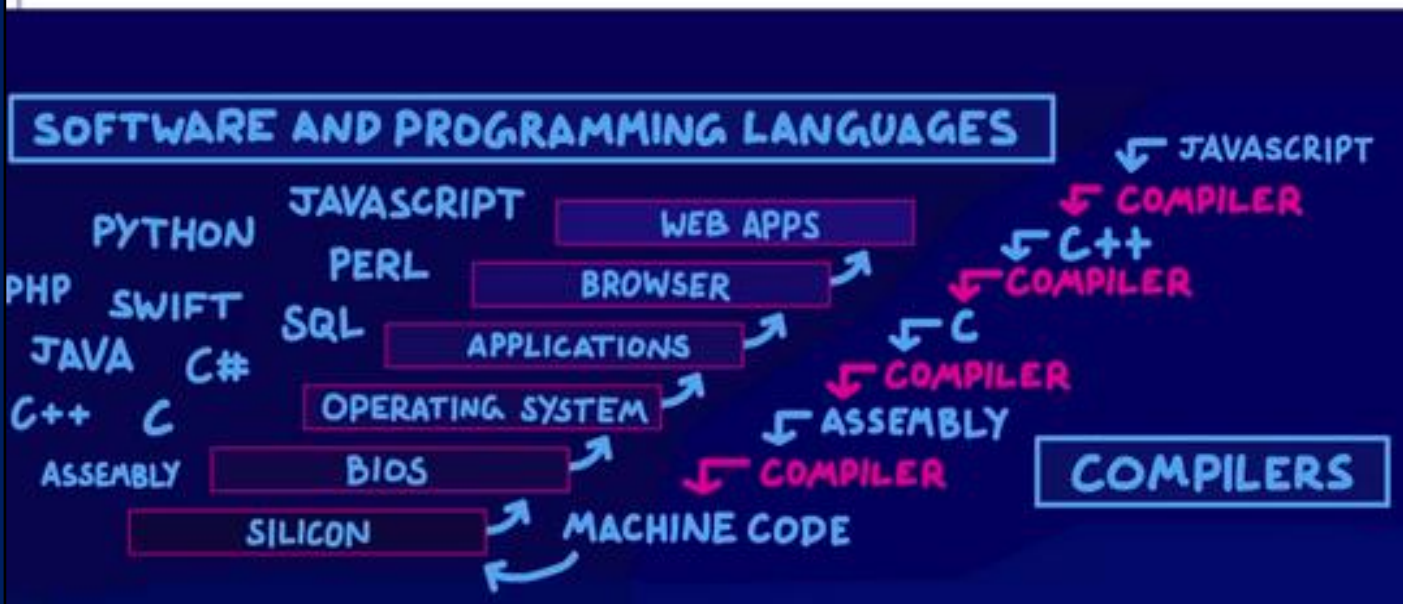


ON TOP OF THE RAW HARDWARE THERE ARE MANY LAYERS OF SOFTWARE

WRITTEN BY PROGRAMMERS USING MANY DIFFERENT PROGRAMMING LANGUAGES.
A PROGRAMMING LANGUAGE IS HOW HUMANS TELL A COMPUTER WHAT TO DO AND THEY VARY GREATLY DEPENDING ON THE JOB AT HAND FROM :

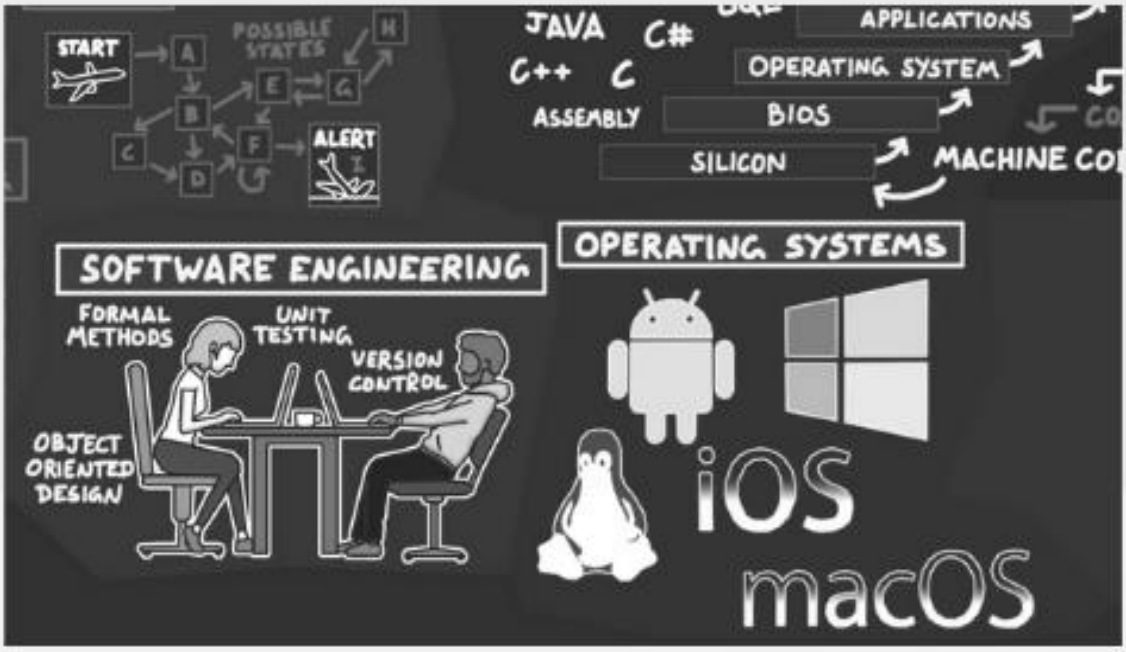
low level languages	high level languages
like assembly	ike python or JavaScript for coding website and apps

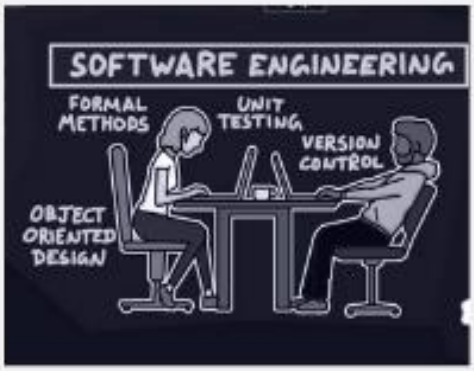
In general, the closer a language is to the hardware, the more difficult it is for humans to use. At all stages of this hierarchy the code that programmers write needs to be turned into raw CPU instructions and this is done by one or several programs called compilers. Designing programming language and compilers is a big deal , because they are the tool that software engineers use to make everything and so they need to be as easy to use as possible but also be versatile enough to allow the programmers to build their crazy ideas.



The operating system is the most important piece of software on the computer as it is what we interact with and it controls how all of the other programs are run on the hardware, and engineering a good operating system is a huge challenge.

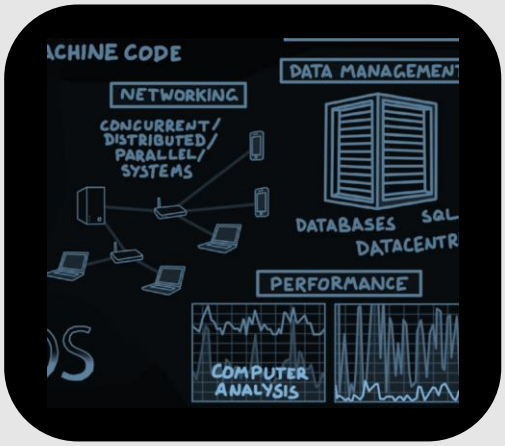


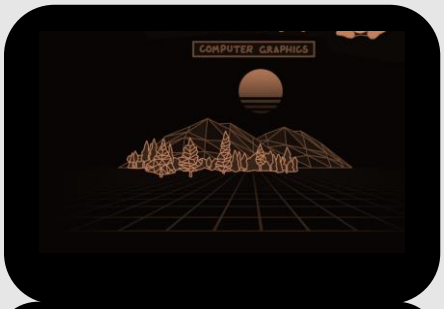




This brings us to software engineering: writing bundles of instructions telling the computer what to do. Into logical instructions in a specific language, make it as efficient as possible to run and as free of error as you can. So there are many best practices and design philosophies that people follow.

Some other important areas are getting many computers to communicate and work together to solve problems. Storing and retrieving large amounts of data. Determining how well computer systems are performing at specific tasks , and creating highly detailed and realistic graphics. Now we get to a really cool part of computer science, getting computers to solve real world problems. These technologies underline a lot of the programs, apps and websites we use.

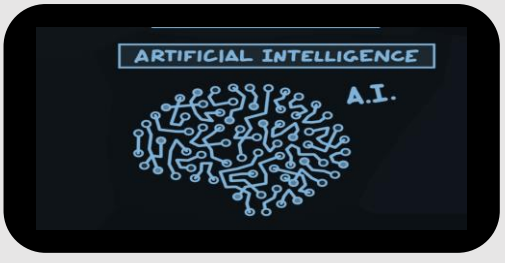


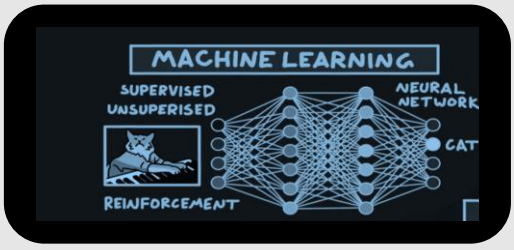




Optimization problems appear everywhere and finding the best path or most efficient combination of parts can save businesses millions of dollars. This is related Boolean satisfiability where you attempt to work out if a logic formula can be satisfied or not. This was the first problem proved to be NP-complete and so widely considered to be impossible to solve, but amazing development of news SAT solvers means that huge SAT problems are solved routinely today especially in artificial intelligence.

Computers extend our brains multiply our cognitive abilities. The forefront of computer science research is developing computer systems that can think for themselves: artificial intelligence. There are many avenues that AI research takes, the most prominent of which is machine learning which aims to develop algorithms and techniques to enable computers to learn from large amounts of data and then use what they've learned to do something useful like make decisions or classify things. And there are many different types of machine learning.

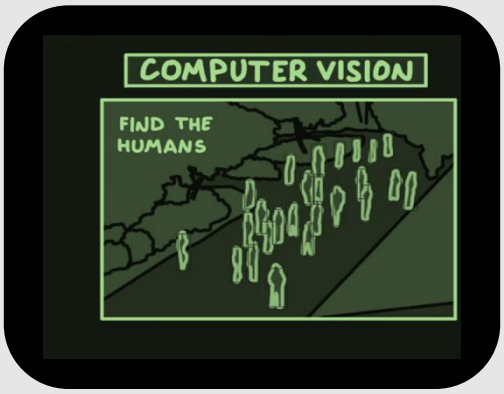


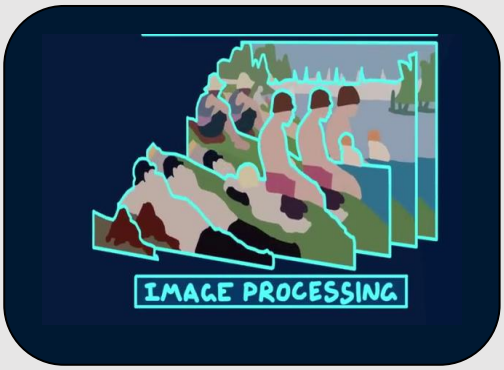


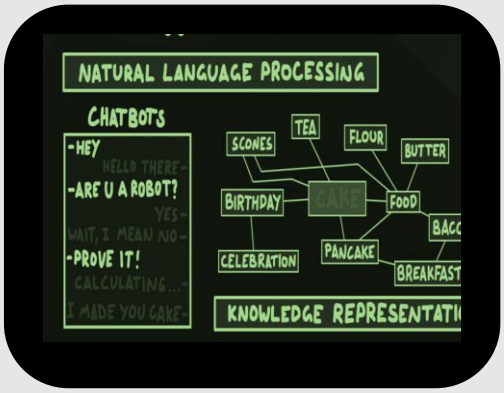
Closely related are fields like computer vision trying to make computers able to see objects in image like we do , which image uses image processing techniques. Natural language processing aims to get computers to understand and communicate using human language , or to process large amounts of data in the form of words for analysis.

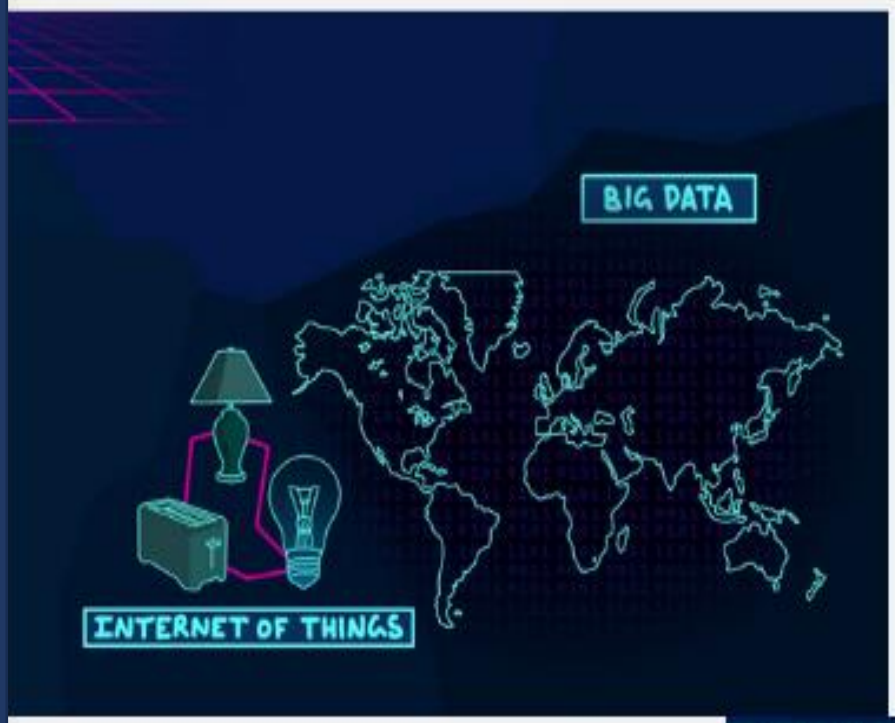
This commonly uses another field called knowledge representation where data is organized according to their relationships, like words with similar meanings are clustered together.

Machine learning algorithms have improved because of the large amount of data we give them.



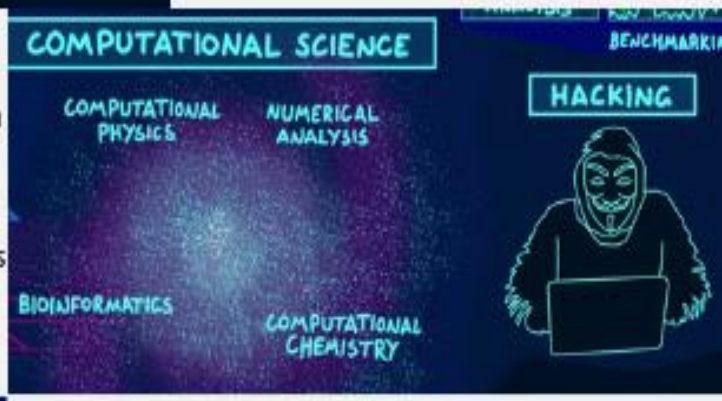


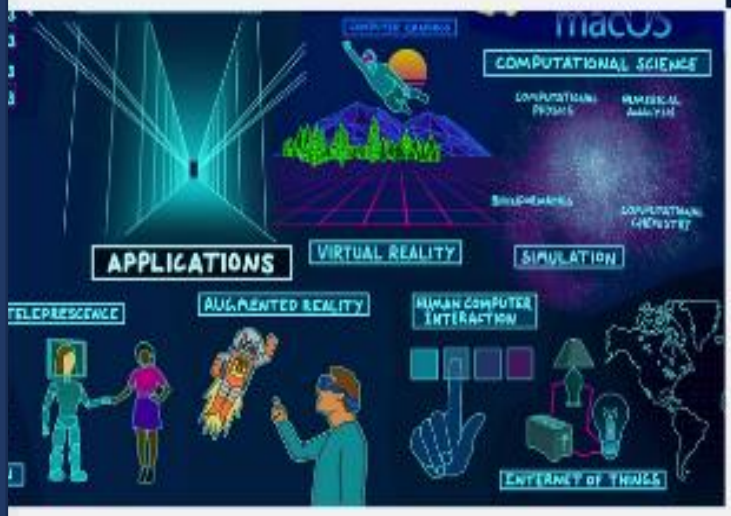




Big data looks at how to manage and analyze large amounts of data to get value from it. And will get even more data from the internet of things, adding data collection and communications to every objects

Hacking is not a traditional academic discipline but definitely worth mentioning. Trying to find weaknesses in computer systems, and take advantage of them without being noticed. Computational science uses computers to help answer scientific questions from fundamental physics to neuroscience...

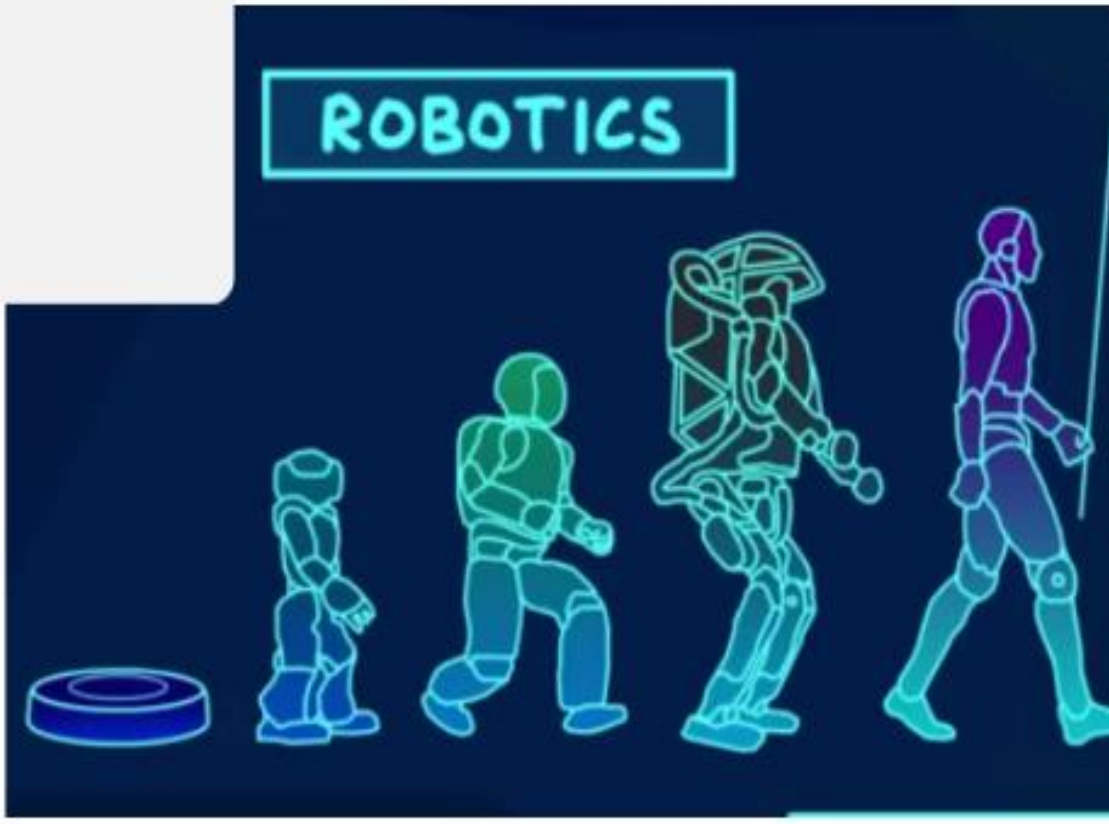




and often makes use of super computing which throws the weight of the worlds most powerful computers at very large problems, often in the area of simulation. Then there is human computer interaction which looks at how to design computer systems to be easy and intuitive to use. Virtual reality, Augmented Reality and Telepresence enhancing or replacing our experience of reality.

ROBOTICS

And finally Robotics which gives computers a physical embodiment , from a Roomba to trying to make intelligent human like machines.



So that is Map of computer science , a field that is still developing as fast as it ever has despite that fact that the underlying hardware is hitting some hard limits as we struggle to miniaturize transistors any more, so lots of people are working on other kinds of computers to try and overcome this problem. Computer have had an absolutely huge impact on human society and so it is going to be interesting to see where this technology goes in the next one hundred years.

Who knows, perhaps one day, we'll all be computers…

