**به نام خدا**

**مبهم سازی**

اگر مبتدی هستید پایتون بهترین زبان جهت شروع می باشد. و این همان چیزی است که آن را تا این حد محبوب می سازد. شما می توانید کد قدرتمندی را صرفا با نوشتن چند خط کد ایجاد کنید. مهم تر از آن اینکه می توانید به طور دلخواه اعداد صحیح بزرگ با دقت بسیار را دستکاری کنید.

این کتاب مفاهیم اساسی رمزنگاری را پوشش می دهد. موارد کلاسیکی مانند Caesar cipher و یا XOR و همچنین پیچیده و پراکنده سازی که مشخص کننده نحوه عملکرد یک سیستم پیچیده می باشند، مخفی نمودن داده ها توسط مبهم سازی، هش نموده( درهم سازی) کلمه های عبور و داده های حساس و روش های قدرتمند رمز نگاری و حملاتی مانند padding oracle که جهت شکستن این روش ها به کار می رود. برای یادگیری این موارد نیاز به تجربه در زمینه برنامه نویسی یا داشتن یک کامپیوتر با امکانات منحصر به فرد ندارید. هر کامپیوتری که بتواند پایتون را اجرا کند می تواند تمام این ها را نیز پیاده سازی نماید.

قرار نیست در این کتاب روش جدیدی را برای رمز نگاری ابداع کنیم، ما فقط می خواهیم یاد بگیریم که چگونه از موارد موجود استفاده کنیم. و این موضوع به چیزی جز یک جبر پایه ( در ریاضیات) نیاز ندارد.

در ابتدا درباره مبهم سازی داده ها صحبت خواهیم کرد که ایده ی پایه و ابتدایی جهت آشنایی با فرآیند رمز نگاری می باشد. این موضوع( مبهم سازی) یک روش قدیمی بوده که در آن داده با دستکاری به گونه ای تغییر می کند که خواندن آن دشوار تر شود. مورد گفته شده یکی از کارهای پایه ای بوده که روش های رمز نگاری انجام می دهد و روش های مدرن به این فرآیند قدرت بیشتری می بخشند.

در این فصل موارد زیر را پوشش می دهیم:

* صحبت درباره رمزنگاری
* نصب و راه اندازی پایتون
* Caesar cipher و ROT13
* کد گشایی base64
* XOR

**رمزنگاری(Cryptography)**

واژه crypto اخیرا با ایجاد ارز های مجازی همانند بیتکوین، اتریوم و لایتکوین بسیار شنیده می شود. وقتی که به واژه crypto از منظر شکلی از ایمن سازی نگاه می کنیم، در واقع منظور کاربرد رمزنگاری(Cryptography) در مواردی مانند شبکه های ارتباطی، فضاهای ذخیره سازی، نرم افزار ها و پیام های استفاده شده در یک سیستم می باشد. رمزنگاری دارای یک تاریخچه بسیار طویل و مهم در محافظت از سیستم های حیاتی و اطلاعات حساس می باشد.

در خلال جنگ جهانی دوم آلمان ها از ماشین های رمزنگاری جهت کد گذاری ارتباطات خود استفاده می کردند. و متحدان(رقبای آن ها) مسیر طولانی را جهت کدگشایی این ارتباطات پیمودند. ماشین های رمزنگاری از چرخ دنده هایی در خود استفاده می کردند تا متن ساده(plain text) را به متن رمزنگاری(cipher text) شده تبدیل کنند. با درک این موضوع که چرخ دنده ها در چه موقعیتی قرار دارند متحدین می تواستند متن رمزنگاری شده را به متن ساده تبدیل کنند. این یک پیشرفت قابل توجه بود ولی به نیروی انسانی و منابع عظیمی نیاز داشت. امروزه هنوز می توانیم برخی روش های رمز نگاری را شکست و داده ها را کدگشایی کرد. اغلب حمله به جنبه هایی از رمزنگاری سیستم ها مانند پروتکل ها، نقاط اتصال و حتی کتابخانه های ساخته شده حهت پیاده سازی رمزنگاری عملی تر است.

رمزنگاری تاریخچه غنی دارد، امروزه در سراسر مفاهیم جدید مانند بلاکچین که می تواند به عنوان ابزاری جهت کمک به ایمن سازی اینترنت اشیا استفاده می شود، کاربرد دارد.

بلاکچین بر اساس مجموعه ای از روش های شناخته شده رمزنگاری پایه ایجاد شده، یک مورد دیگر الگوریتم های قدرتمند رمزنگاری کوانتومی می باشد. که در شاخه ی کامپیوتر های کوانتومی و کلید کوانتومی توزیع شده کاربرد دارد. این موارد از پروتکل هایی مانندBB84 و BB92 استفاده می کنند تا از کوانتوم محض به روش هایی بسیار پرقدرت برای رمزنگاری کلاسیک( کامپیوتر های معمولی) دست پیدا کنند.

نصب و راه اندازی پایتون

نصب پایتون هیچ گاه کار آسانی نبوده است( مترجم: با این جمله مخالفم!) برای ادامه کار بیایید اطمینان پیدا کنیم که پایتون را به درستی بر روی سیستم خود تنظیم کرده ایم. در ادامه خواهیم دید که چگونه در لینوکس و مک پایتون را بکار گیریم و همچنین چگونه آن را در ویندوز نصب کنیم.

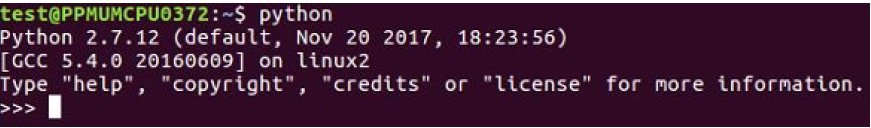
استفاه از پایتون در لینوکس یا مک

در سیستم عامل لینوکس یا macOS نیازی به نصب پایتون نیست زیرا آن ها به خودی خود شامل پایتون می شوند. فقط کافیست یک پنجره terminal باز کرده و دستور python را وارد نمایید. این موضوع شما را در یک حالت تعاملی قرار می دهد به این معنا که شما می توانید یکی یکی دستورات را وارد کرده و همان هنگام نتیجه را ملاحظه کنید. همچنین می توانید با استفاده از دستور exit() از این حالت تعاملی خارج شوید.

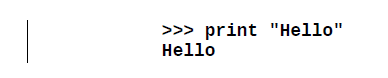
در حالت بسیار ساده و ابتدایی برای ساخت یک اسکریپت از ویرایشگر nano به همراه نام مورد نظر استفاده می کنیم.

بیایید ببینیم چگونه باید از پایتون در لینوکس یا مک استفاده کنیم:

1. یک terminal بر روی مک یا لینوکس باز کرده و دستور python را اجرا نمایید. این موضوع همانطور که در زیر می بینید، منجر به اجرای پایتون در حالت تعاملی می گردد:



1. هنگامی که از دستور print استفاده می کنید، پایتون به سرعت Hello را بر روی صفجه نمایش می دهد:



1. و در نهایت به این حالت تعاملی با اجرای دستورexit() خاتمه می بخشیم:



1. همانطور که قبلا گفته شد، برای اجرای حالت تعاملی پایتون دستور زیر را وارد می کنیم:



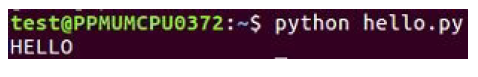
1. در فایل hello.py دستوری مانند زیر را وارد کنیم:



1. فایل را با زدن Ctrl + X و بعد از آن y ذخیره کنید و چنانچه فقط فایل را تعییر داده اید کلید Enter را فشار دهید.
2. حال بیاید دستورpython را به همراه نام اسکریپت مربوطه بنویسیم:



هنگامی که آن را اجرا کنید خروجی زیر را دریافت خواهید کرد:



دستور بالا اسکریپت را اجرا کرده و Hello را در خروجی چاپ می کند. اگر از لینوکس یا مک استفاده می کنید، این موارد همه آن چیزی بود که شما باید انجام می دادید!

نصب پایتون بر روی ویندوز

اگر کاربر ویندوز می باشید ناگزیر از دانلود پایتون می باشید!( خودمانی: باید پایتون را دانلود نمایید ☺!!)

در پایین مراحلی که باید انجام دهید را مشاهده می کنید:

1. پایتون را از [www.python.org/downloads/](http://www.python.org/downloads/) دانلود کنید.
2. آن را از طریق خط فرمان ویندوز اجرا نمایید.
3. حالت تعاملی پایتون را به اجرا در آورید.
4. با دستور exit() از آن خارج شوید.

شما برای ساخت یک اسکریپت، فقط نیاز به notepad دارید. یک متن را نوشته و با فشردن کلید های ترکیبی Ctrl + S آن را ذخیره کنید. سپس با نوشتن نام فایل پس از دستور python آن را اجرا نمایید. با نصب پایتون شروع می کنیم.

صفحه پایتون را با لینکی که قبلا داده شده باز کنید و آن را دانلود نمایید. نسخه های مختلفی به شما پیشنهاد می شود، در این کتاب ما از پایتون 2.7.12 استفاده کرده ایم.

گاهی اوغات نمی توانید پایتون را به سرعت نصب کنید زیرا ویندوز نصب کننده را نا ایمن ارزیابی می کند:

1. شما باید آن را از فهرست برنامه های ناایمن خارج کنید و سپس نصب کننده را اجرا کنید.
2. در مراحل نصب پایتون یک گزینه اختیاری تحت عنوان Add python.exe to path را مشاهده می کنید، که می بایست آن را اتخاب نمایید.

هدف از انتخاب این گزینه آن است که بتوان پایتون را مستقیما در ترمینال ویندوز که خط و فرمان نامیده می شود اجرا کرد.( یعنی صرفا با نوشتن دستور python آن را فراخوانی کنیم.)

به ادامه بحث می پردازیم:

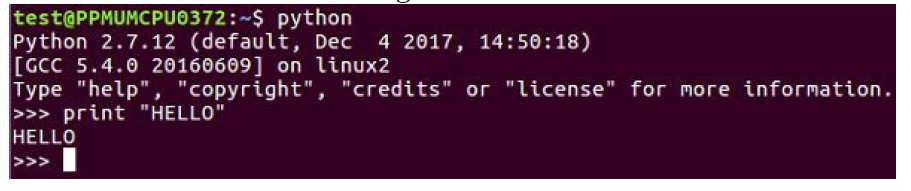
1. ترمینال را باز کرده و دستور زیر را وارد کنید:



1. وقتی که دستور را اجرا کنید، می بینید که پایتون کار می کند. حال می توانیم یک دستور وارد کنیم.



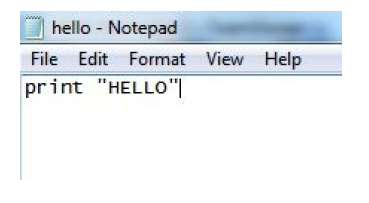
صفحه پایین را مشاهده کنید:



1. می توانیم با استفاده از دستور exit() که قبلا گفته شده از برنامه خارج شویم.
2. حال اگر بخواهیم یک اسکریپت ایجاد کنیم، دستور زیر را اجرا می کنیم:



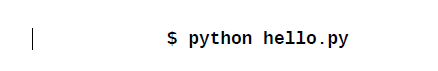
1. این دستور NotePad را اجرا می کند.



1. می خواهیم یک فایل متنی ایجاد کرده و داخل آن دستور زیر را بنویسید:

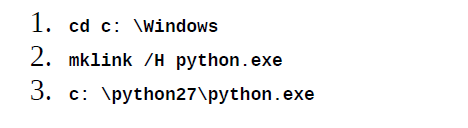


1. اکنون فایل را ذخیره کرده و از notepad خارج شوید. برای اجرای این فایل باید دستور زیر را اجرا کنیم:



این فایل اجرا شده و Hello را بر روی صفحه نمایش می دهد.

معمولا هنگام نصب پایتون مسیر آن درست مشخص نمی شود، بنابراین می بایست دستورات زیر را اجرا کرده تا یک لینک نمادین از پایتون را در خط فرمان داشته باشید در غیر این صورت احتمالا پایتون در خط فرمان به درستی کار نخواهد کرد:



در قسمت بعدی، نگاهی بر Caesar chipher و ROT13 خواهیم انداخت.