

به نام پروردگار هدایت کننده به راه راست

دانشگاه اصفهان

ساختمان داده - دکتر رضانی

پاییز ۰۲-۰۱

پروژه پنجم - ماشین انیگما



طراحان پروژه : امیر علی گلی - علیرضا ساعی - محمد توکلی

مبحث : نگاشت (مپ)

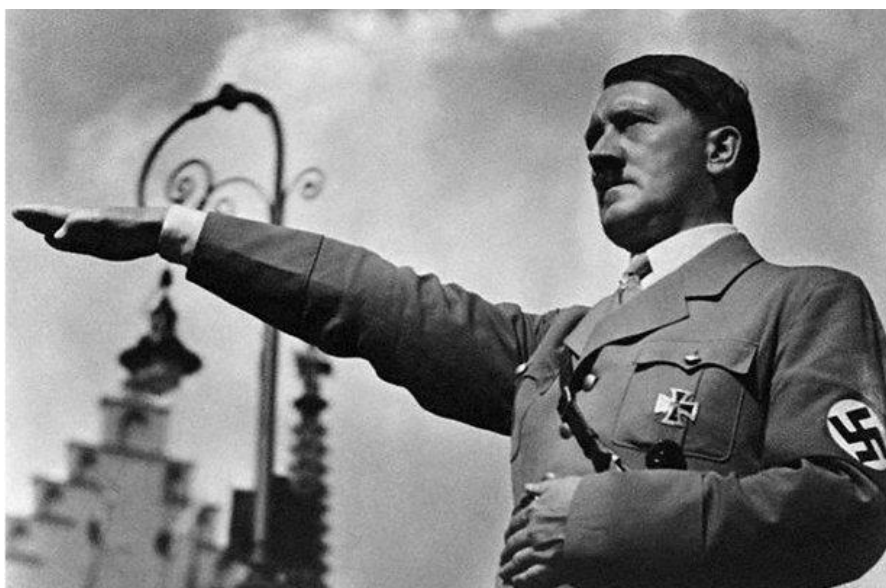
اهداف پروژه :

- کار با ساختمان داده مپ

در این پروژه قرار است با استفاده از ساختمان داده مپ یک ماشین انیگما را شبیه سازی کنید.

## جنگ جهانی 2.1

شما در زمان جنگ جهانی دوم هستید و می‌خواهید با روش‌های مختلف، از حرکات بعدی متحدین خبردار شده و جلوی برد آنها را در این جنگ بگیرید. اما با دیدن نمونه‌ای از پیام رد و بدل شده بین آلمانی‌ها فهمیدید که آنها پیام‌های خود را رمزگذاری (Encipher) کرده‌اند. پس از مدتی جاسوس‌های شما اطلاع داده‌اند که آلمانی از دستگاهی به اسم انیگما (Enigma) برای رمزگذاری کردن پیام‌های خود استفاده می‌کنند. شما با آلن تورینگ و گروهی از نخبه‌ها جمع شده‌اید و قرار است که انیگما را بشکنید (Decipher) و حرکات بعدی آلمانی‌ها را خنثی کنید.



خیلیا با دیدن قیافه دستگاه، انصراف دادند و کنار کشیدند حتی آلن تورینگ! شما قرار است به تنهایی در این پروژه، کدی بنویسید که کد رمزگذاری شده آلمانی‌ها را گرفته و پیام اصلی آنرا چاپ کند!

ساز و کار + قطعات انیگما

کیبورد

ورودی دستگاه است که با فشردن کلید مربوط به هر حرف، آن حرف وارد فاز کدگذاری می‌شود.

## پلاگ برد

در جلوی دستگاه حروف A-Z قرار گرفته اند و با 8 سیم دو به دو به هم وصل می شوند و عملکرد آن به این صورت است که اگر حرف F به X وصل شده باشد اگر پس از پردازش ها، خروجی F بود، چراغ X روشن می شود و اگر ورودی X بود به F تبدیل شده و وارد روتور ثابت می شود.

## روتور ثابت

3 روتور متحرک که در قسمت بعدی قرار است توضیح داده شوند، نسبت به این روتور ثابت می چرخند.

## روتور متحرک

انیگما از 3 تا روتور متحرک تشکیل شده است که روی هر کدام حاوی حروف A-Z هستند که یک مدار الکتریکی متغیر تشکیل می دهند. عملکرد آنها مانند عقربه های ساعت است، به طوریکه روتور شماره 1 با یک دور کامل چرخیدن، روتور بعدی را یکی می چرخاند و یک حرف جلو می رود و روتور سوم هم با یک دور چرخیدن روتور دوم یکی حرکت می کند. وقتی که حرفی وارد روتور اول می شود، به حرف متناسب با آن در طرف دیگر روتور اول تبدیل می شود (C به W). سپس وارد روتور بعدی شده و در روتور دوم نیز به یک حرفی مپ شده (W به Q) و وارد روتور سوم شده و به حرفی دیگر مپ شده (Q به K) و سپس K وارد رفلکتور می شود.

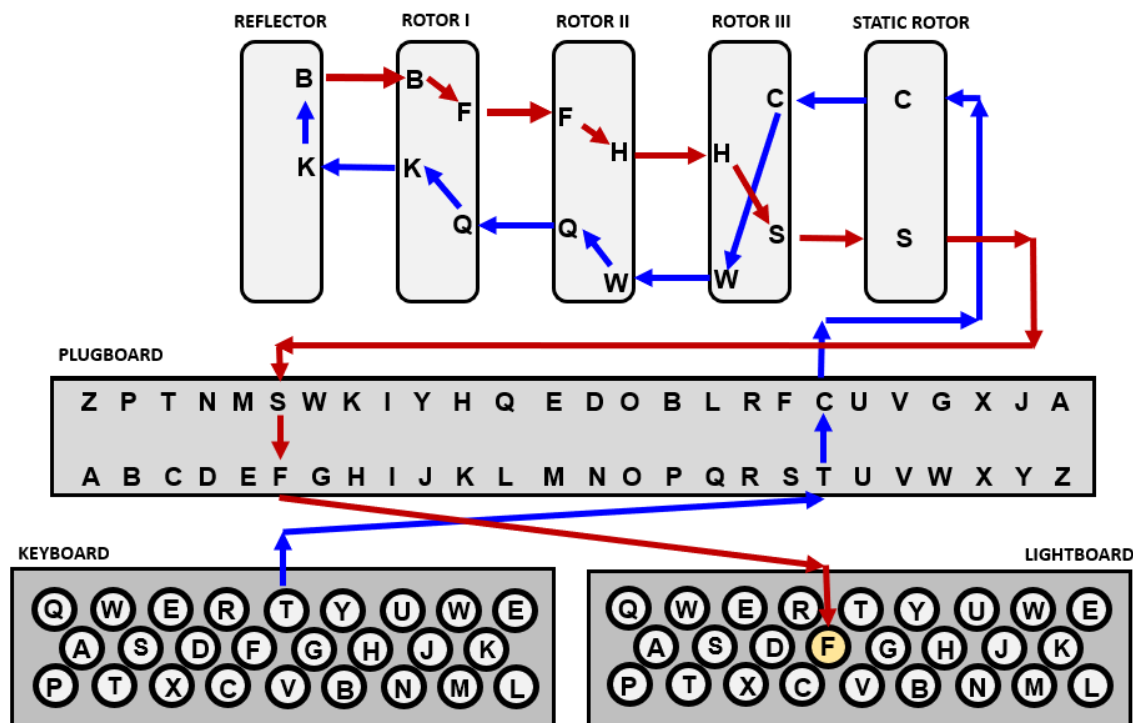
روتورها چند نوع هستند که نوع آنها و نحوه مپ کردن آن در هر نوع روتور مشخص است.

## رفلکتور

حرف موزدنظر پس از عبور حرف از روتورها، به رفلکتور می رسد. در این مرحله حرف ورودی به این قطعه، به یک حرف دیگر مپ شده و همان راه طی شده را باز می گردد ( روتور متحرک ← روتور ثابت ← پلاگ برد ). نحوه مپ شدن هم به این صورت است: A به Z، B به Y، C به X و ...

## لامپ برد

حرف تغییر یافته حین مراحل کد گذاری به برد لامپ برگشته و لامپ مربوط به حرف نهایی را روشن می کند.



The path taken by a letter through an Enigma machine as it is encrypted

یکی از جاسوس های تان به برنامه روزانه نحوه قرار گیری اولیه روتور و سیم ها دسترسی پیدا کرده و برای شما ارسال کرده است. شما با توجه به کد رمز گذاری شده و آن جدول زمانی، قرار است پیام اصلی را استخراج کنید! به لطف رفلکتور، اگر حالت اولیه این دستگاه را بدانیم هم میتوان Decipher کرد و Encipher صرفا کافی است کلید حرف مورد نظر خود را با همان ترکیب قبلی، فشار دهیم!

**دقت کنید برای قسمت روتور و پلاگ بورد و رفلکتور باید از ساختمان داده مپ استفاده کنید.**

در ورودی به شما یک عبارت رمز گذاری شده داده می شود و یک فایل زمان بندی برای ستاپ کردن انیگما در اختیار شما قرار می گیرد. ( این فایل شامل اطلاعاتی از قبیل نوع روتورهای مورد استفاده در این ماشین، و 8 عدد حروف دوتایی برای وصل کردن دو حرف پلاگ بورد به هم در تاریخ های مورد نظر)

دقت کنید به شما یک فایل شامل جدول زمان بندی ( تاریخ و اطلاعات لازم برای ستاپ کردن ماشین برای آن روز که شامل نوع روتور ها و جفت حرف های پلاگ برد می-باشد) داده می شود و باید انیگما را برای هر کدام از عبارات رمز گذاری شده، نسبت به تاریخی که دارند با استفاده از فایل زمان بندی تنظیم کرده و عبارت دیکد شده را در خروجی نمایش دهید.

HEIL HITLER!

برای مثال فرض کنید مولفه های انیگمای شما در تاریخ dd/mm/yyyy به صورت زیر باشد :

Plugboard: {AF, BM, GH, JC, XE, OP, NR, ZL}

رفلکتور : در بخش قبل توضیح داده شد

Rotor 3: {LUWJHIKDYCAXMNQBZTRFGESVPO}

Rotor 2: {QNGHSZAFEBJRLUCTXYIMPDWKOV}

Rotor 1: {CMFQSBHIOAKRTENZLDYWUGPJXV}

دقت کنید مانند شکل داده شده در قبل ورودی ابتدا وارد روتور ۳ و بعد از آن ۲ و ۱ می شود.

فرض کنید ورودی زیر به ماشین داده شود

Input: AB

خروجی ماشین به شکل زیر خواهد بود :

Output: G

روتور ۳ یکی میچرخد و به صورت زیر خواهد شد :

Rotor 3: {OLUWJHIKDYCAXMNQBZTRFGESVP}

و در نهایت خروجی به صورت زیر خواهد بود :

Output: GH

روتور ۳ یکی میچرخد و برای عملیات بعدی به صورت زیر خواهد شد :

Rotor 3: {POLUWJHIKDYCAXMNQBZTRFGESV}

## نکات تکمیلی :

- این پروژه بصورت تک نفری باید پیاده سازی شود.
- بستر پیاده سازی پروژه روی گیت هاب می باشد.
- سعی کنید هریک از بخش ها را در یک کامیت جداگانه انجام دهید.
- رعایت اصول کدنویسی تمیز بخش بسیار زیادی از نمره را به خود اختصاص می دهد و در صورتی که کد کاملاً به شکل غیر اصولی پیاده سازی شده باشد. تحویل گرفته نمی شود.
- استفاده از هر زبان، فریمورک و رابط های گرافیکی کاملاً آزاد است.
- به افرادی که از تکنولوژی های جدید استفاده کنند، توکن تمديد اضافه تر داده خواهد شد.