



ساختمان های داده

دکتر سید ابوالقاسم میرروشندل

طراح : پویا ریوندی

پروژه ی سوم

داستان پروژه:

آلن کوچک تصمیم دارد موضوعی را با دوستش در میان بگذارد اما شهادت گفتن آن را ندارد پس ابتدا تصمیم می گیرد تا نامه ای برای او بنویسد. پس نوشتن چند خط، متوجه می شود که اگر نامه به دست شخص دیگری برسد اتفاقات بدی در انتظار او هستند پس دست به کار می شود تا نامه را به صورت رمزی بنویسد. آلن بسیار باهوش است و همینطور می داند که دوست او نیز مانند خودش است پس تصمیم می گیرد برای زبان رمزی اش از صف اولویت (Priority queue) استفاده کند.

هدف پروژه:

هدف از این پروژه، استفاده از ساختمان داده Heap یا Priority queue برای پیاده سازی متود رمز نگاری و رمز گشایی یک متن می باشد.

مقدمه:

روش های فراوانی برای رمزنگاری وجود دارند که از مهمترین آنها می توان به روش تعویض حروف (Letter substitution) اشاره کرد.

ساده ترین شکل این روش اختصاص حروف مختلف به یکدیگر می باشد برای متوجه شدن بهتر مثال زیر آمده است که در آن مثلا حرف Z به حرف H اختصاص داده شده است:

Hello → Zujjq

پس به راحتی می توان متوجه شد که کلید این رمز، جایگشتی از حروف الفبای انگلیسی است. همانطور که احتمالا حدس می زنید، رمز جابجایی حروف ساده به راحتی با دنبال کردن الگو ها قابل رمزگشایی است.

به این معنی که می توان کلید آن را به راحتی و البته با داشتن متن کافی به دست آورد. (رمزگشایی)

رمزنگاری:

زبان رمزی آلن، ورژنی متفاوت از روش جابجایی حروف است با این تفاوت که هر حرف از ابتدا به حرف دیگری اختصاص داده نمی شود بلکه ریشه صف اولیت تعیین می کند که به جای حرف بعدی چه حرفی قرار گیرد، به این صورت که در ابتدا به هر حرف یک عدد از ۱ تا ۲۶ اختصاص داده می شود و حروف به ترتیب خاصی به یک صف اولویت اضافه می شوند.

این ترتیب خاص به همراه اعداد اختصاص یافته به حروف، کلید رمز آلن هستند.

رمزنگاری به این صورت انجام می شود که برای پیدا کردن جایگزین هر حرف، به تعداد عدد اختصاص یافته به آن، عمل حذف ریشه از heap را انجام می دهیم و حروف حذف شده را وارد یک صف می کنیم و حرف آخری که حذف می شود، جایگزین حرف اصلی خواهد بود. و این کار را آنقدر انجام می دهیم تا تعداد عناصر heap از شماره عدد بعدی کمتر شود. سپس حروف داخل صف را به ترتیب دوباره به heap اضافه می کنیم و ادامه می دهیم تا تمام متن کد شود.

توجه کنید که شماره ی حرفی که انتخاب شده باید با حرفی که کد شده جابجا شود.

رمزگشایی با کلید:

ابتدا با کلید، صف اولویت را تشکیل می دهیم. سپس جمله کد شده را به ترتیب حروف می خوانیم. برای مثال حرف ز را می بینیم. حال آنقدر ریشه heap را حذف میکنیم تا به حرف ز برسیم. در نهایت تعداد حذف ها را می شماریم و متوجه می شویم که حرف ز جایگزین چه حرفی بوده است. به جابجایی شماره ی حروف توجه کنید.

فرمت ورودی و خروجی:

ورودی بخش اول پروژه هر رشته شامل حروف کوچک انگلیسی می باشد که در خروجی باید معادل کد شده آن به صورت بالا دیده شود.

ورودی بخش دوم پروژه ترتیبی از ۲۶ حروف الفبای انگلیسی به همراه اعداد اختصاص یافته به هرکدام به عنوان کلید رمز و همینطور متن رمز می باشد که در خروجی باید متن اصلی دیده شود.

جزئیات پیاده سازی:

حتماً باید ساختمان داده های مورد استفاده در برنامه را خودتان پیاده سازی کنید و تنها استفاده از آرایه بلامانع است.

نکات تکمیلی:

- پیاده سازی تنها رمزنگاری یا تنها رمزگشایی درصد **بسیار کمی** از نمره پروژه را به همراه خواهد داشت.
- پیاده سازی به صورت تک نفره است و هیچ محدودیتی برای زبان برنامه نویسی وجود ندارد.
- همه ی ساختمان داده های مورد نیاز، باید با توجه به تعریف پروژه پیاده سازی شوند. استفاده از ساختمان داده های آماده مجاز نیست.
- بحث و بررسی میان دانشجویان آزاد است اما هر دانشجو موظف است پروژه را به تنهایی انجام دهد و در هنگام تحویل حضوری، به تمام جزئیات کد کاملاً مسلط باشد. با موارد تقلب و کپی کردن، طبق تشخیص دوستان حل تمرین، برخورد جدی خواهد شد.
- توجه کنید که کدهای شما باید خوانا و دارای کامنت گذاری مناسب باشد.
- در کلاس کوئرای **Data Structures 971** با رمز **guilan96** ثبت نام کرده، نام و شماره ی دانشجویی خود را به درستی وارد کنید. عواقب بی دقتی در این مورد، به عهده ی دانشجو است.
- برای پرسش و پاسخ درباره ی پروژه، فقط از سامانه ی کوئرای درس مربوطه، اقدام کنید.
- پوشه ی مربوط به کد پروژه را (در صورت نیاز همراه با فایل pdf شرح انجام پروژه، نحوه ی اجرای برنامه، گزارش مربوط به تحلیل ساختمان داده ها و محاسبات انجام شده) در قالب یک فایل zip و در بخش مربوطه بارگذاری کنید. عواقب بی دقتی در این مورد، به عهده ی دانشجو است.
- زمان بندی و چگونگی تحویل حضوری پروژه، متعاقباً اعلام خواهد شد.