به نام خداوند بخشنده مهربان

نویسنده و سازنده : سید علیرضا فاضلی آبلویی

الگوریتم رمزنگاری pkGet :

امروزه در این دنیای پر از هرج و مرج و سرقت اطلاعات ما نیاز به رمزنگاری داده های خود داریم . با پیشرفت انسان الگوریتم و روش های رمزنگاری متفاوتی به دنیا آمده است.

الگوریتم pkGet یکی از آن الگوریتم های رمزنگاری متن هستش . ما در مواقع مختلف نیاز داریم که داده متنی خود را رمزنگاری کنیم. الگوریتم pkGet میتوانید گزینه خوبی باشد که ساخته سید علیرضا فاضلی آبلویی است.

ریشه نام pkGet :

حرف p به معنای password و حرف k به معنای key و GET به معنای (دریافت کن) هستش.
در ادامه درباره ی تمام اینها صحبت خواهم کرد.

نحوه کار الگوریتم :

در این الگوریتم از دو الگوریتم معروف رمزنگاری یعنی الگوریتم مستوی و الگوریتم ویژنر استفاده شده است. اما نحوه کار این دو الگوریتم در درون برنامه ایی که ما ساختیم فرق میکند.

- ## مراحل رمزنگاری :

- **رمز مستوی** از دستهٔ رمزنگاری جانشینی می‌باشد. در این روش هر حرف به عدد متناظر با آن تصویر شده، سپس با استفاده از یک تابع ساده ریاضی رمز می‌شود و در نهایت عدد بدست آمده دوباره به حروف تبدیل می‌شود. به عبارت دیگر در این روش هر

حرف به حرف دیگری متناظر شده و سپس در رمزگشایی نیز حرف متناظر شده به حرف اول تبدیل می‌شود. در رمزنگاری نیازمند این است که روش مشخصی وجود داشته باشد که مشخص کند کدام حرف به کدام حرف متناظر می‌شود. برای مثال، در این روش که از ضعیفترین روش‌های رمزنگاری جانشینی می‌باشد هر حرف به وسیله تابع ((ax + b) mod 26) اندازه مقدار تغییر می‌باشد.
پس ما برای جانشینی رمز نیاز به دو کلید اصلی a و b داریم.
برنامه و الگوریتمی که ما ساختیم موقع ساخت رمز اول شروع به ساخت دو کلید A , B میکند و از این کلید ها برای ساخت مرحله اول رمز ما استفاده میکند و ما خروجی متن رمز شده را دریافت میکنیم.

- **سایفر ویژنر** روشی برای رمزنگاری یک متن الفبایی با استفاده از روش سزار بر مبنای حروف یک کلمهٔ کلید می‌باشد. در واقع شکل دیگری از روش رمزنگاری جانشینی است.

در رمزنگاری هر حرف از الفبایی به اندازهٔ عدد مشخصی شیفت پیدا می‌کند. به عنوان مثال، در رمزنگاری Caesar شیفت به اندازهٔ ۳ واحد به این صورت است که، A می‌شود D , B می‌شود E , Y می‌شود B و غیره. رمزگذاری Vigenère دارای چندین رمز Caesar به همراه مقادیر متفاوتی برای شیفت دادن، است. (different shift values)

برای رمزگذاری، می‌توان از جدول حروف استفاده کرد که به آن یک tabula recta، مربع Vigenère یا جدول Vigenère گفته می‌شود. این حروف الفبا ۲۶ بار در ردیف‌های مختلف نوشته شده‌است، هر الفبا در مقایسه با الفبای قبلی، شیفت چرخه ای به چپ دارد، متناسب با ۲۶ حالت رمزنگاری Caesar است. در نقاط مختلف فرایند رمزگذاری، از حرف الفبایی متفاوتی از یکی از ردیف‌ها استفاده می‌شود. الفبای مورد استفاده در هر نقطه به آن کلید (repeating keyword) بستگی دارد.

پس در اول ماجرا نیاز به پسورد داریم که خود کاربر پسورد را وارد میکند. و نسبت به آن پسورد ما رمزنگاری مربوطه را انجام میدهیم.

توضیح کلی و اصلی برنامه :

- رمزنگاری داد

ما از کاربر دو داده اصلی را دریافت میکنیم . 1- متنی که قراره رمزنگاری بشه 2- یک پسورد از طرف کاربر که فقط با این پسورد و کلید هایی که ما به کاربر میدیم قابل متن رمزنگاری شده ما قابل بازیابی هستش.

- وقتی متن را دریافت کردیم وارد الگوریتم مستوی میکنیم که توضیحش را اول کار داده ام و متن را با عدد های (کلید) های تصادفی که ساخته ایم رمزنگاری میکنیم به عنوان مثال ما متن hello را داده ایم و الگوریتم مستوی برای ما متن یا سایفر تکست xakkf را به عنوان مثال برای ما برمیگرداند.
- در الگوریتم ویژنر ما نیاز به یک پسورد و متن داریم . ما پسوردی را که از کاربر دریافت کرده ایم را و متن دریافتی از الگوریتم مستوی که به عنوان مثال xakkf بود را وارد الگوریتم وِیژنر میکنیم. حالا الگوریتم ویژنر نسبت به پسورد متن xakkf را تبدیل به متن رمز شده جدیدی میکنید به عنوان مثال : jasdu .
- حالا در انتهای کار ما برای کاربر یک لیستی از داده ها را میفرستیم . نکته : فقط با این داده هستن که کاربر میتواند به متن اصلی رمزنگاری شده دست یابد.

خروجی فرضی داده برنامه: : ciphertext : jasdu - password
mypassword - key a : 3 - key b : 5

- رمزگشایی متن رمز شده :

پس ما لیستی از داده ها را داریم

خروجی فرضی داده برنامه: : ciphertext : jasdu - password

mypassword - key a : 3 - key b : 5

برای رمزگشایی کافی است دو الگوریتم رمزگشایی مخصوص مستوی و ویژنر را داشته باشیم

باید به صورت معکوس رمزگشایی بکنیم.

اول از همه پسورد و متن رمز شده به عنوان مثال jasdu, mypassword را می دهیم که الگوریتم به ما متن رمزگشایی شده xakkf را میدهد.

ما متن را به الگوریتم مستوی میدهیم و لازم است دو کلید اصلی را که برنامه داده را به او بدهیم کلید اول و دوم.

بعد از آن متن رمزگشایی شده و به متن اصلی hello میرسیم.

نکته : اینها فقط توضیحات نحوه کارکرد الگوریتم و برنامه هستند و برنامه به صورت خیلی ساده ایی نوشته شده است و کار کردن با آن راحت است و بنده یک فایل آموزشی مربوطه با آن را قرار میدهم.