گزارش پروژه نهایی درس رمزنگاری

طرح تسهیم راز شمیر

تهیه‌کننده: عسل خائف

۴۰۰۳۶۲۳۰۱۴

استاد درس: دکتر حمید ملا

دستیار استاد: سرکار خانم سعیدی

توضیح کد (create_shares.py)

این کد برای ایجاد و توزیع سهم‌های یک راز با استفاده از الگوریتم Shamir's Secret Sharing طراحی شده است. در ادامه، بخش‌های مختلف کد و عملکرد آن‌ها توضیح داده شده است:

1. **تابع initialize_coefficients:**
   - **ورودی‌ها:**
     - secret: مقدار راز.
     - num_shares: تعداد سهم‌هایی که باید ایجاد شوند.
     - threshold: تعداد آستانه سهم‌هایی که برای بازسازی راز نیاز است.
     - mod: عدد پیمانه (باید بزرگتر از مقدار راز باشد).
   - **خروجی:** ضرایب چندجمله‌ای و مقدار راز.
   - **شرح:**
     - راز را به صورت پیمانه‌ای با عدد mod کاهش می‌دهد.
     - ضرایب چندجمله‌ای را به صورت تصادفی بین 1 و عدد mod انتخاب می‌کند.
   - **بازگشت:** ضرایب تولید شده و مقدار راز کاهش یافته.
2. **تابع create_shares:**
   - **ورودی‌ها:**
     - secret: مقدار راز.
     - num_shares: تعداد سهم‌هایی که باید ایجاد شوند.
     - threshold: تعداد آستانه سهم‌هایی که برای بازسازی راز نیاز است.
     - mod: عدد پیمانه (باید بزرگتر از مقدار راز باشد).
     - coefficients: لیستی از ضرایب چندجمله‌ای.
   - **خروجی:** لیستی از سهم‌ها.
   - **شرح:**
     - برای هر مقدار x از 1 تا num_shares، مقدار y با استفاده از چندجمله‌ای محاسبه می‌شود.
     - مقدار y به صورت پیمانه‌ای با عدد mod کاهش داده می‌شود.
   - **بازگشت:** لیستی از سهم‌ها.

3. **تابع display_polynomial:**
    - **ورودی‌ها:**
        - secret: مقدار راز.
        - coefficients: لیستی از ضرایب چندجمله‌ای.
    - **خروجی:** رشته‌ای که نمایانگر چندجمله‌ای است.
    - **شرح:**
        - چندجمله‌ای را با استفاده از مقدار راز و ضرایب به صورت یک رشته می‌سازد.
    - **بازگشت:** رشته‌ای که چندجمله‌ای را نمایش می‌دهد.
4. **تابع main:**
    - **ورودی‌های کاربر:**
        - از کاربر مقدار راز، تعداد سهم‌ها، تعداد آستانه و عدد پیمانه را می‌پرسد.
    - **شرح:**
        - ضرایب را با استفاده از تابع initialize_coefficients مقداردهی می‌کند.
        - چندجمله‌ای را با استفاده از تابع display_polynomial نمایش می‌دهد.
        - سهم‌ها را با استفاده از تابع create_shares ایجاد کرده و نمایش می‌دهد.

این کد با استفاده از چندجمله‌ای لاگرانژ سهم‌هایی را ایجاد می‌کند که می‌توان با داشتن تعداد کافی از آن‌ها راز اصلی را بازسازی کرد. ضرایب چندجمله‌ای به صورت تصادفی انتخاب می‌شوند و سهم‌ها بر اساس این چندجمله‌ای تولید می‌شوند.

توضیح کد (remake_secret.py)

1. **تابع lagrange_interpolate_at_zero:**
   - **ورودی‌ها:**
     - x_values: لیستی از مقادیر x سهم‌ها.
     - y_values: لیستی از مقادیر y سهم‌ها.
     - mod: عددی است که به عنوان پیمانه استفاده می‌شود.
   - **خروجی:** بازسازی رمز از طریق الگوریتم لاگرانژ.
   - **شرح:**
     - متغیر secret را با مقدار 0 شروع می‌کنیم.
     - برای هر مقدار y در y_values، یک چندجمله‌ای لاگرانژ محاسبه می‌شود.
     - برای هر چندجمله‌ای لاگرانژ، محاسبات معکوس ضربی انجام می‌شود.
     - مقادیر y در هر تکرار ضرب شده و به نتیجه نهایی افزوده می‌شود.
     - در نهایت، مقدار رمز بازسازی شده بازگشت داده می‌شود.
2. **تابع remake_secret:**
   - **ورودی‌ها:**
     - mod: عدد پیمانه.
     - shares: لیستی از سهم‌ها.
   - **خروجی:** رمز بازسازی شده.
   - **شرح:**
     - لیست مقادیر x و y را از لیست shares استخراج می‌کند.
     - تابع lagrange_interpolate_at_zero را فراخوانی کرده و مقدار بازسازی شده را بازگشت می‌دهد.
3. **تابع main:**
   - **ورودی‌های کاربر:**
     - از کاربر تعداد آستانه سهم‌های مورد نیاز برای بازسازی رمز و عدد مدول را می‌پرسد.
     - سپس سهم‌های مورد نیاز را از کاربر دریافت می‌کند.
   - **بازسازی و نمایش رمز:**
     - تابع remake_secret را فراخوانی می‌کند تا رمز را بازسازی کند.

- رمز بازسازی شده را نمایش می‌دهد.

نمونه‌های تست شده:

```
****Reconstruct the secret****
Enter the threshold number of shares needed to reconstruct the secret: 3
Enter the mod number used: 13
Enter the x value of the share: 1
Enter the y value of the share: 4
Enter the x value of the share: 2
Enter the y value of the share: 8
Enter the x value of the share: 3
Enter the y value of the share: 1

The reconstructed secret is: 2
```

```
****Create shares****
Enter the secret: 1000
Enter the number of shares to create: 10
Enter the threshold number of shares required to reconstruct the secret: 3
Enter a mod number (should be larger than the secret): 49

The polynomial used to generate shares is:
f(x) = 20 + 39x^1 + 10x^2

The generated shares are:
Share 1: 20
Share 2: 40
Share 3: 31
Share 4: 42
Share 5: 24
Share 6: 26
Share 7: 48
Share 8: 41
Share 9: 5
Share 10: 38
```