فاز سوم – رمزنگاری

رمزنگاری فرایندی به نسبت پیچیده تر از فاز های قبلیست که هدف کلی آن استفاده از الگوریتم های رمزنگاری پیچیده همانند AES و اعمال آن بصورت استراتژیک است به نحوی که هرگونه تعریف و استفاده از داده در چشم انسان نامفهوم جلوه کند و همچنین مقدار واقعی آن در حافظه موجود نباشد.

در این فاز تمرکز اصلی ما بر **رمزنگاری** در موارد initialize و assignment با استفاده از قانون گرامری literal و همچنین **رمزگشایی** این مقادیر رمزنگاری شده در موارد استفاده و با بهره وری از قانون گرامری primary است.

۱. رمزنگاری

در ابتدا لازم است این را بدانید که همواره ورودی الگوریتم های رمزنگاری یک استرینگ و خروجی آن نیز به همین صورت است، به همین دلیل ما از این قابلیت استفاده نموده و در خروجی مبهم ساز خود تمام تایپ های قابل قبول قانون variableDeclaratorID استفاده شده در فاز های قبل را به تایپ استرینگ تبدیل مینماییم تا هم لایه ی عمیقی از مبهم سازی را ایجاد کرده باشیم و همچنین بتوانیم با الگوریتم های رمزنگاری سینک شویم.

حال برای تحقق بخشیدن به یک رمزنگاری موثر لازم است انواع نیاز به رمزنگاری در مبهم سازی را بصورت کامل شناخت:

- رمزنگاری اولیه

ساده ترین نوع رمزنگاری در مبهم سازی است به این دلیل که کاملا رمزنگاری ای pre-compile بوده و مقادیر بصورت Literal و آماده توسط برنامه نویس تعبیه شده اند و نیاز به هیچگونه محاسبه قبل از رمزنگاری نیست.
برای این نوع رمزنگاری کلاس آماده ای به نام pyCipher در اختیارتان قرار می گیرد.

- رمزنگاری نهایی

در این رمزنگاری تمرکز ما بر assignment ها، معادله ها و به زبان ساده هرکجا که عبارات ترکیبی از "=" وجود داشته باشد است.
نکته ی مهم در این مرحله این است که مقداری که میخواهیم رمزنگاری کنیم هنوز محیا نیست و نیازمند انجام یکسری محاسبات هنگام اجرای کد است، به همین منظور نمیتوان پیش از کامپایل این رمزنگاری را انجام داد.

برای حل این مشکل کلاسی به زبان جاوا با نام jCipher در اختیارتان قرار میگیرد که توانایی رمزنگاری post-compile را داراست. (این کلاس توانایی های دیگری نیز دارد که در ادامه به آن اشاره میشود)

لازم به ذکر است که این دو نوع رمزنگاری باید بصورت ترتیبی و در دو پارس متفاوت صورت گیرند (رمزنگاری اولیه میتواند در پارس تغییر نام نیز انجام گردد)

۲. رمزگشایی

فرآیند رمزنگاری به طور اجتناب‌ناپذیری متغیرها و تخصیص‌ها را به شکلی تبدیل می‌کند که ممکن است آشفته و غیرقابل خواندن به نظر برسد. برای ایجاد تعادل بین امنیت و کارایی ما یک استراتژی رمزگشایی را پیاده‌سازی خواهیم کرد. این استراتژی تعیین می‌کند که در لحظات کلیدی، مانند assignment ها، statements ها و سایر عملیات‌های مرتبط، هر قطعه از داده‌های رمزنگاری شده، که ابتدا ممکن است غیرقابل خواندن به نظر برسد، رمزگشایی می‌شود. در اصل، این بدان معناست که هر زمان داده‌های رمزنگاری شده استفاده می‌شوند، آنها به طور بلادرنگ به شکل اصلی و معنادار خود از دیدگاه برنامه ما تبدیل می‌شوند. از آنجا که تایپ هر متغیر به استرینگ تغییر یافته است، نیاز است در مواقع استفاده از این متغیر ها،پس از رمزگشایی آنها را به تایپ اصلی خود پارس نماییم.

فرایند رمزگشایی نیز با توجه به این امر که همواره بصورت post-compile صورت میگیرد، با توابع کلاس jCipher صورت میگیرد.

توجه داشته باشید که در بعضی از موارد که پای مقادیر خام (literal) در میان است، ممکن است مجبور شویم که در همان جمله ابتدا آن را رمزنگاری و سپس رمزگشایی کنیم، زیر این مقادیر مثل متغیر ها ابتدا تعریف و سپس استفاده نمیشوند و به نوعی تعریف و کاربرد آن ها بصورت آنی در یک لحظه است به همین دلیل ابتدا آن ها را انکود و سپس دیکود میکنیم که در عین نامفهومی، کاربرد اصلی خود را از دست ندهند.

نحوه ی استفاده از کلاس های pyCipher و jCipher بصورت داکیومنت شده و همچنین در کلاس حل تمرین خدمتتان عرضه میگردد.

مثالی از خروجی فاز رمزنگاری

```
int a = 1;
int b = a * 2;
System.out.println(b * 3);
System.out.println("test");
```



```
String New_a = "3e";
String New_b = MyCipher.getInstance().encode(Integer.parseInt
    (MyCipher.getInstance().decode(New_a))*Integer.parseInt(MyCipher
    .getInstance().decode("c4"))
System.out.println(Integer.parseInt(MyCipher.getInstance().decode
    (New_b)) * Integer.parseInt(MyCipher.getInstance().decode("f2"
    )));
System.out.println(MyCipher.getInstance().decode("772db1e2"));
```

ارزیابی

فاز سوم پروژه

لطفا قبل از ارسال پروژه به نکات زیر توجه کنید:

۱. فایل ارسالی شما تنها یک فایل فشرده شده شامل کد و نتایج پروژه باشد. (.zip/.rar)

۲. نام فایل شما باید به صورت روبرو باشد:

YourFullName_YourStudentID

۳. توجه شود، ارائه به صورت مجازی برگزار خواهد شد، تمامی افراد گروه در روز ارائه باید حضور داشته باشند، در صورت عدم حضور هر یک از اعضا، نمره به آن شخص تعلق نخواهد گرفت.

🔔 مهلت ارسال در سامانه vc:

جمعه ــ ۱۵ تیر ــ ۱۴۰۳

موفق باشید 😊