**به نام خدا**

پروژه تسهیم راز درس رمزنگاری و امنیت

استاد درس: دکتر ملا

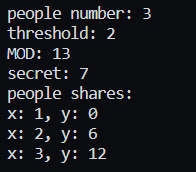
دانشجو: سیدعلی سادات خراسانی - 4003613036

**مراحل ورودی گرفتن و خروجی دادن پروژه**

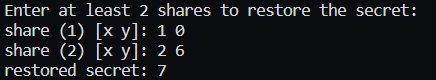
1. ابتدا باید اطلاعات اولیه را بعنوان ورودی بدهیم که شامل تعداد نفرات (n)، حداقل تعداد افراد برای رمزگشایی (t)، مود اعداد (MOD) و رازی که میخواهیم آنرا رمز کنیم (secret) است

نکته ای که وجود دارد این است که باید حتما مد (MOD) ما عددی اول باشد و همچنین مقدار t کمتر از مقدار n باشد تا پروژه کار کند در غیر اینصورت با خطا مواجه می‌شویم.

پس از ورود اطلاعات اولیه برنامه یکسری ضرایب رندوم را برای معادله ما میسازد و با استفاده از آن ضرایب (که secret بعنوان ضریب جمله 0 در نظر گرفته شده است) به تعداد افراد سهم های مختلف می سازد و سهم های ساخته شده برای کاربر نمایش داده می شوند.

****

1. حال باید برای رمزگشایی حداقل تعداد t سهم را کاربر وارد کند که بصورت x y وارد می شوند و سپس با استفاده از فرمول درون یابی لاگرانژ مقادیر محاسبه شده و راز بازیابی می‌شود

****