به نام هستی‌بخش

مبانی رمزنگاری

نیم‌سال اول ۱۴۰۲-۱۴۰۳

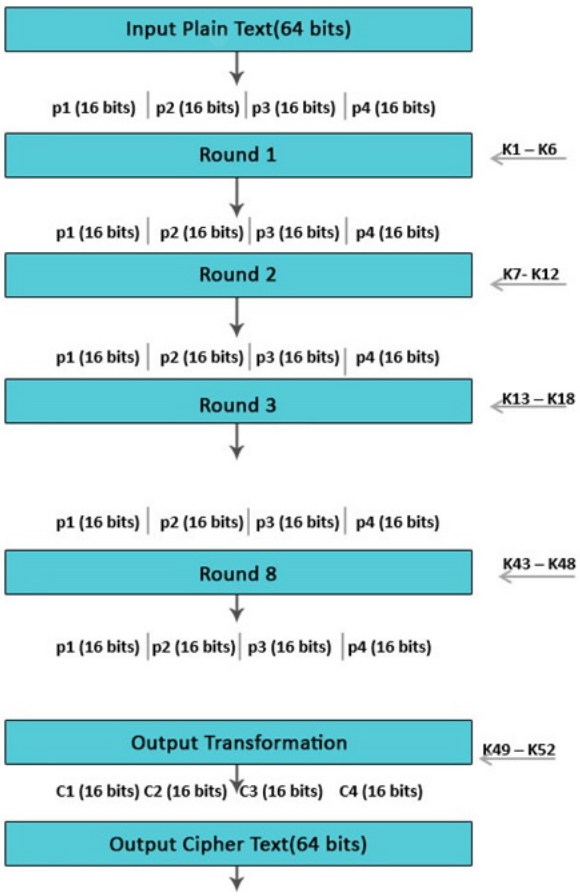
پروژه اول

دانشکده‌ی مهندسی و علوم کامپیوتر

مدرس: دکتر راضیه سالاری فرد

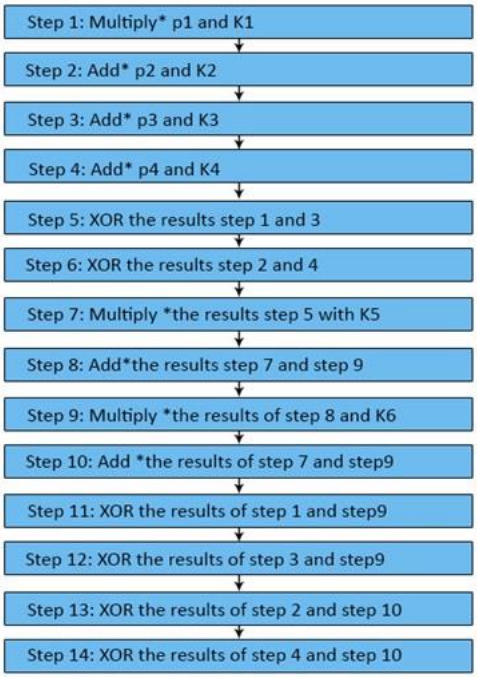
این پروژه شامل ۳ بخش است که با تکمیل سه بخش به صورت کامل، نمره این پروژه کامل خواهد شد.

۱. الگوریتم رمزنگاری بلوکی طراحی شده است که به عنوان ورودی ۶۴ بیت متن ساده(plaintext) و کلید ۱۲۸ بیت دریافت کرده و ۶۴ بیت متن رمزی‌شده(ciphertext) را به عنوان خروجی تولید می‌کند. ساختار کلی آن به شکل زیر است:



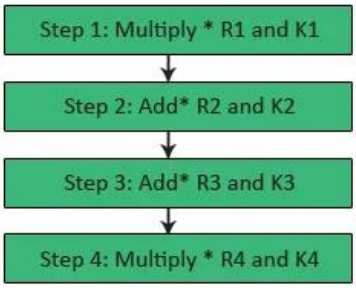
همانطور که در شکل مشخص است، این الگوریتم دارای ۸ دور(round) اصلی و یک دور پایانی است و در هر دور ۶۴ بیت ورودی خود را به صورت ۴ تا داده ۱۶ بیتی دریافت و هر دور نیز ۶ زیرکلید ۱۶ بیتی

استفاده می‌شود. دور آخر این الگوریتم(output transformation) نیز ۴ تا داده ۱۶ بیتی دریافت و از ۴ زیرکلید ۱۶ بیتی استفاده می‌شود و در نهایت متن رمز را می‌سازد. ساختار هر دور شامل مراحل زیر است:



توجه: Step11,step12,step13,step14 به ترتیب p1,p2,p3,p4 دور بعد هستند.

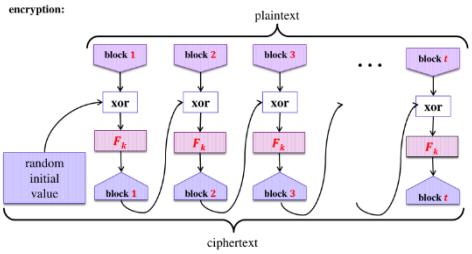
ساختار دور آخر به شکل زیر است:



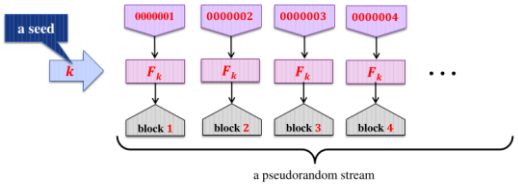
سه عملیات اصلی این الگوریتم XOR و 2^{16} addition modulo و $2^{16} + 1$ multiplication modulo است. از شما خواسته شده است که بخش رمزگذاری(encryption) آن را با زبان‌های سطح بالا پیاده‌سازی کنید.

۲. در این بخش برای افزایش امنیت الگوریتم آن را با مد CBC و مد counter پیاده‌سازی کنید.

Cipher-Block Chaining (CBC)



Counter mode (CTR)



توجه: سعی کنید که الگوریتم بخش اول را به صورت ماژولار پیاده‌سازی کنید که راحت بتوانید از آن در مدهای CBC و Counter استفاده کنید.

توجه: زبان‌های مجاز برای پیاده‌سازی این پروژه، زبان‌های جاوا، پایتون و جاوااسکریپت است.

موفق باشید