به نام هستی‌بخش

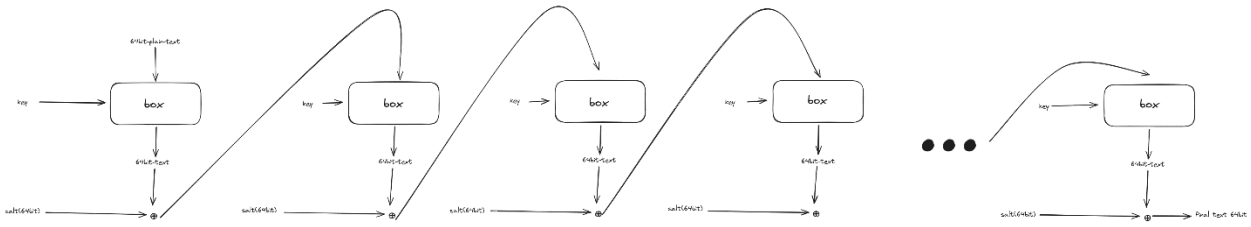
مبانی رمزنگاری

پروژه دوم

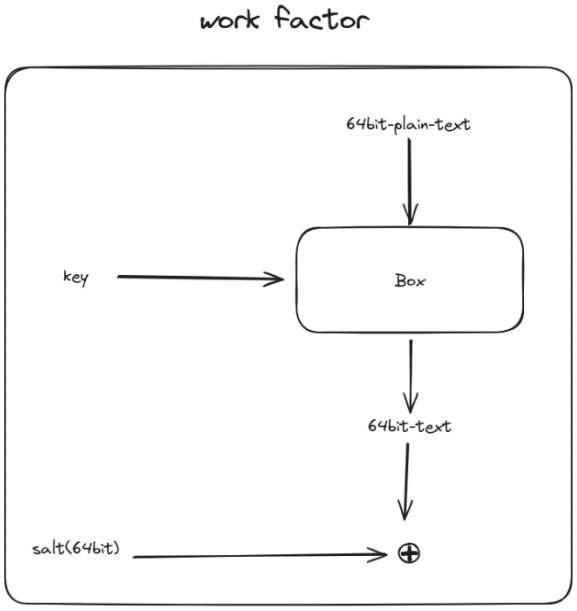
مدرس: دکتر راضیه سالاری فرد

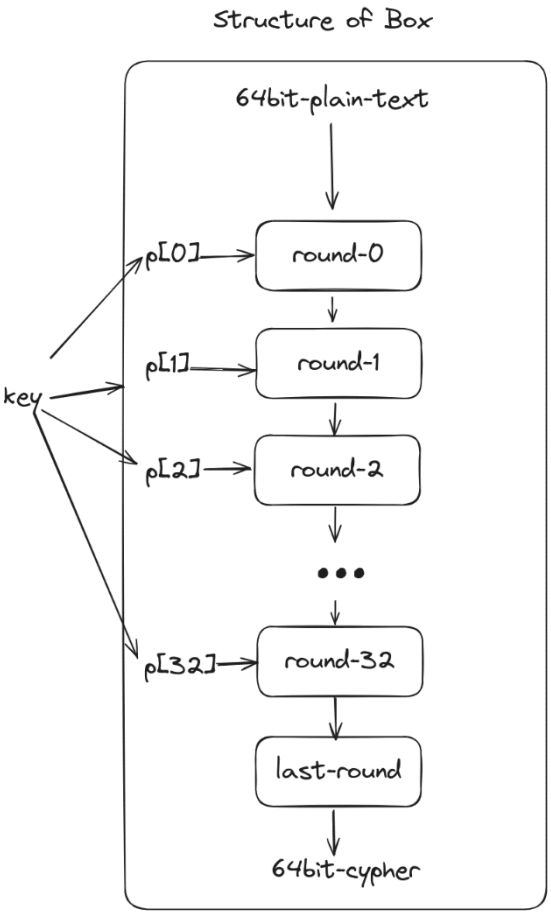
دانشکده‌ی مهندسی و علوم کامپیوتر

۱-الگوریتمی برای پیاده سازی تابع چکیده ساز طراحی شده است که به عنوان ورودی ۶۴ بیت متن ساده(plaintext) و ۳۲ تا زیرکلید ۳۲ بیتی و ۶۴ بیت salt و عدد صحیح عامل کار(work factor) دریافت می‌کند و ۶۴ بیت متن رمزی شده(cyphertext) را به عنوان خروجی تولید می‌کند. ساختار کلی آن به شکل زیر است:



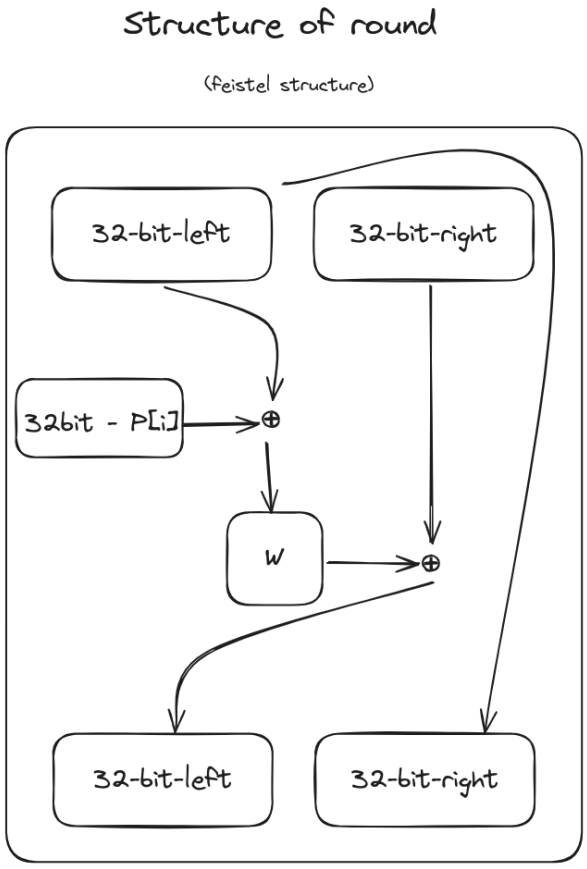
همانطور که در شکل مشخص است، ۶۴ بیت ورودی به همراه کلید به box وارد می‌شود و ۶۴ بیت خروجی با مقدار salt عملیات xor انجام می‌شود و به عنوان ورودی به دور بعد پاس داده می‌شود و این ساختار به تعداد دو به توان عامل کار(work factor) تکرار می‌شود و در نهایت متن رمزشده تولید می‌شود.



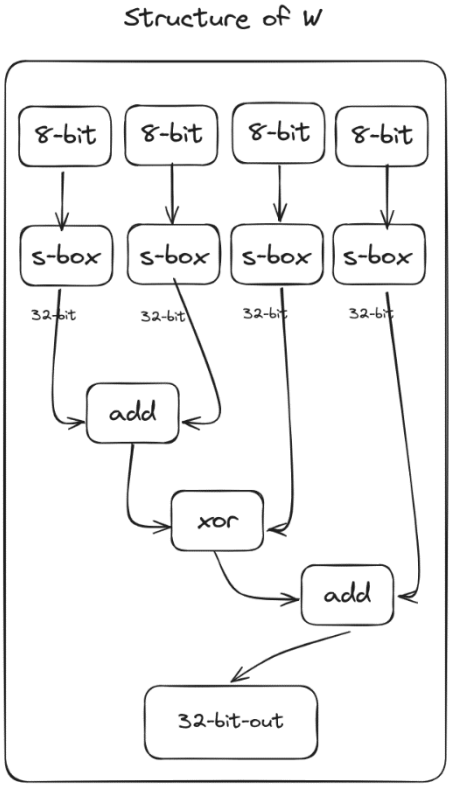


ساختار هر box به شکل رو به رو است که شامل ۳۲ دور است که برای هر دور از یک زیرکلید ۳۲ بیت استفاده می‌شود.(کلیدها در فایل keys.txt قرار دارد)

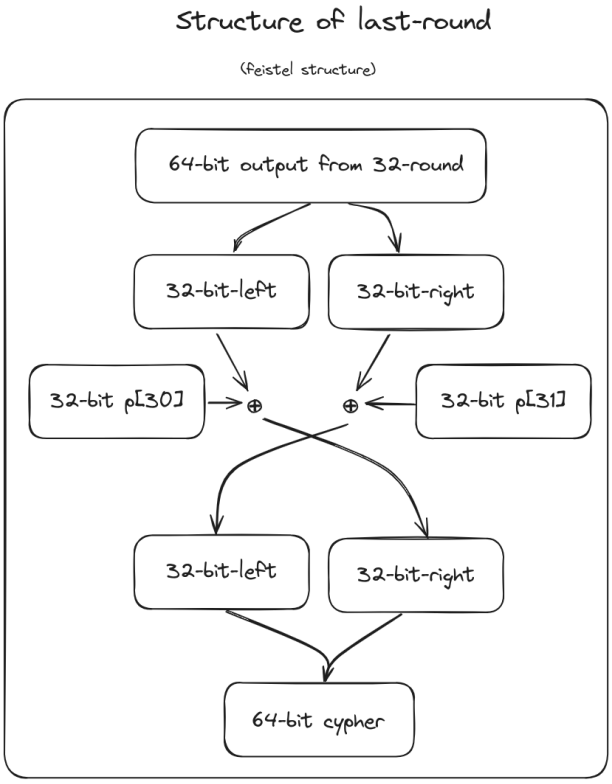
ساختار هر دور به شکل رو به رو است که شبیه به ساختار فیستل است. ۳۲ بیت چپ متن ساده به زیرکلید ۳۲ بیتی دور xor می‌شود و به تابع w پاس داده می‌شود، سپس نتیجه تابع w با ۳۲ بیت راست xor می‌شود و در ۳۲ بیت چپ دور بعد قرار می‌گیرد. ۳۲ بیت راست دور بعد نیز همان ۳۲ بیت چپ دور قبل است.(مطابق شکل)



ساختار تابع w به شکل رو به رو است که هر ۸ بیت به sbox پاس داده می‌شود و ۳۲ بیت خروجی تولید می‌شود که این خروجی‌ها مطابق شکل از عملیات‌های جمع ماژولار(جمع دو به توان ۳۲) و xor استفاده می‌کنند و در نهایت ۳۲ بیت خروجی تولید می‌شود.(sbox ها در فایل sbox.txt قرار دارد.)



ساختار دور اخر به شکل روبه رو است که مطابق شکل ۳۲ بیت چپ به ۳۲ بیت کلید ۱۶ ام xor می‌شود و در ۳۲ بیت راست قرار می‌گیرد و ۳۲ بیت راست با ۳۲ بیت کلید ۱۷ ام xor می‌شود و در ۳۲ بیت چپ قرار می‌گیرد و در نهایت ۶۴ بیت cypher تولید می‌شود.



توجه: زبان‌های مجاز برای پیاده سازی این پروژه، زبان‌های جاوا، پایتون و جاوا اسکریپت است.

موفق باشید