بسمه تعالی

تاریخ: ۰۱/۰۹/۱۲ **تمرین سری دوم**

دانشکده مهندسی برق و کامپیوتر **مبانی امنیت**

جواب تمرینات را تا ۰۱/۰۹/۳۰ در سامانه LMS آپلود کنید.

تنها یک فایل پیوست به شکل $\text{hw2} + \text{name} + \text{ID}$ ضمیمه شود. تمرینات را خودتان حل کنید و در صورت تشابه دو تکلیف به یکدیگر به هیچکدام نمره‌ای تعلق نخواهد گرفت.

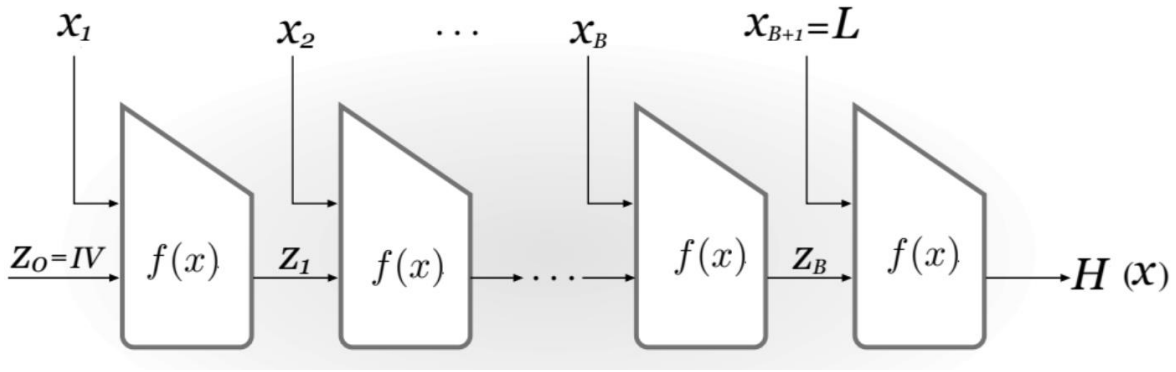
۱- تابع چکیده‌ساز H را در نظر بگیرید که طول خروجی آن ۱۱ بیت است. فرض کنید که

$$H(secret) = 01011000101$$

باشد. هدف این است که با انتخاب پیام‌های تصادفی و محاسبه چکیده آنها به پیامی برسیم که مقدار چکیده آن برابر $H(\text{secret})$ باشد. به چه تعداد باید تلاش کنیم که به احتمال ۵۰ درصد یک برخورد ایجاد شود.

۲- اگر تابع چکیده‌ساز H برخوردتاب باشد، آیا لزوما تابع $H(H(x))$ نیز برخوردتاب است.

۳- در ساختار مرکل دامگارد زیر فرض کنید که بلوک آخر یعنی طول پیام حذف شود آیا می‌توان برای تابع چکیده‌ساز متناظر یک برخورد پیدا کرد.



۴- به طور مختصر حمله Length extension attack را به توابع چکیده‌ساز توضیح دهید.

۵- برای m هایی که $gcd(m,n) \neq 1$ است، نشان دهید که رابطه رمز گشایی RSA درست است.

۶- رمزگذاری RSA با پدینگ OAEP را بررسی و اینکد و دیکد مربوط به پدینگ را بنویسید.