به نام هستی‌بخش

مبانی رمزنگاری

نیم‌سال دوم ۱۴۰۲-۱۴۰۳

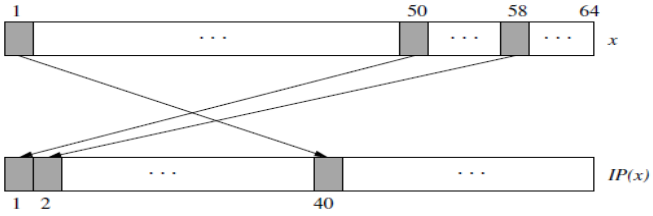
تمرین سری سوم

دانشکده‌ی مهندسی و علوم کامپیوتر

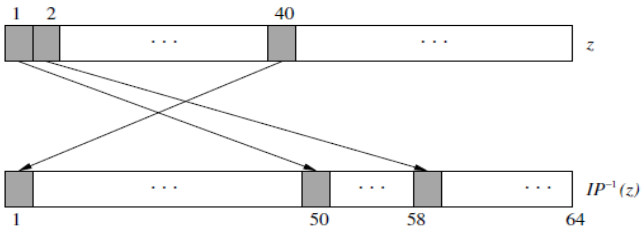
مدرس: دکتر سالاری فرد

۲۰ نمره این تمرین امتیازی است

۱. میدانیم در DES ابتدا متن اصلی وارد تابع IP شده و یک جایگشت روی آن اعمال میشود و در نهایت نیز IP^{-1} روی آن اعمال میشود. برای مثال IP زیر بیت ۵۸ ام را به اول میبرد و بیت اول را جای بیت ۴۰ ام قرار میدهد.



در IP^{-1} نیز بیت اول به خانه ۵۸ میرود و بیت ۴۰ به خانه ۱ برمیگردد.



حال امید برای الگوریتم رمزنگاری خود نیاز به یک تابع IP به همراه معکوس آن دارد و از شما میخواهد یک تابع IP به همراه معکوس آن برای او طراحی کنید و از صحت[۱] کار آن مطمئن شوید. تابع طراحی شده باید پراکندگی خوبی داشته باشد.(۱۰)

۲. 0x6A31E9FB را ورودی Expansion P-box در نظر گرفته و خروجی را مشخص کنید. (به همراه راه حل کامل) (۹)

۳. تنها جزء غیر خطی AES و DES کدام است و بدون این قسمت چه خطری این دو الگوریتم را تهدید میکند؟ (۱۰)

۴. محاسبات زیر را انجام دهید[۲]. (۴۲)

---

[۱] به ازای تمامی x ها، $IP(IP^{-1}(x))$ باید برابر با x باشد.

[۲] برای اطمینان حاصل کردن از درستی محاسبات خود در $GF(2)$ میتوانید از این برنامه استفاده کنید.

a) باقیمانده و خارج قسمت تقسیم زیر را مشخص کنید. (۱۴)

$$f = g.q + r \;/\; GF(5)$$
$$f = 4x^7 + 2x^4 + 3x^3 + x + 1$$
$$g = x^3 + 3x^2 + x$$

b) حاصل ضرب زیر را در $GF(2^8) = GF(2)[x]/(x^8 + x^4 + x^3 + x + 1)$ انجام دهید. (۱۳)

$$(x^5 + x^4 + x^3)(x^4 + x^2 + x)$$

c) معکوس 0xC2 را در $GF(2^8) = GF(2)[x]/(x^8 + x^4 + x^3 + x + 1)$ بدست آورید. (۱۵)

۵. خروجی forward S-box در AES را وقتی ورودی 0x51 است مشخص کنید. (به همراه راه حل کامل) (۱۲)

۶. درستی معکوس بودن عملیات های MixColumns و InverseMixColumns را با ورودی $0x0A050103$ نشان دهید. (۱۷)

۷. در دور دوم DES، زیر کلید و ورودی ها به صورت زیر هستند، L_2 و R_2 را محاسبه کنید. جداول لازم برای حل این سوال در صفحات ۶۰ تا ۶۷ کتاب مرجع آمده است. (۲۰ نمره امتیازی)

$$R_1 = 0x6A31E9FB$$
$$L_1 = 0x00000001$$
$$k_1 = 0xFFFFFFFF$$

- سوالات و ابهامات خود را ترجیحاً در گروه discussion مطرح کنید یا به @owmmid پیام دهید.
- در صورت مشاهده هرگونه تقلب نمره صفر برای تکلیف در نظر گرفته میشود.
- فرمت نامگذاری تکلیف به صورت زیر باشد:

CR-HW3_[STID]_[Name]

موفق باشید:)