# تکلیف دوم

مهدی حق‌وردی

۲۸ فروردین ۱۴۰۳

## ۱

**با توجه به سیستم رمزنگاری DES به سوالات زیر پاسخ دهید.**

آ) **تعداد کل عملیات‌های xor را بدست آورید.**

از آنجایی که DES یک ساختار فیستلی ۱۶ دوری است، در بیرون از تابع F، ۱۶ تا xor قرار دارد. و چون درون تابع F پس از عملیات extend یک بار با کلید xor انجام می‌گیرد پس اینجا هم ۱۶ تا عملیات xor داریم و در مجموع ۳۲ عملیات xor.

ب) **هدف از s-boxها را بنویسید.**

نوشتن رابطه‌ی جبری برای بیت‌های خروجی بر حسب بیت‌های ورودی و کلید **به دلیل وجود s-box** بسیار دشوار است.

ج) **پیچیدگی حمله‌ی جست‌وجوی جامع به این سیستم از چه مرتبه‌ای می‌باشد؟**

کلید DES، ۶۴ بیتی است که ۸ بیت آن بیت‌های parity هستند پس کلید مخفی آن تنها ۵۶ بیت طول دارد ← جستجوی کامل در DES از مرتبه‌ی $2^{56}$ است.

د) **دلیل استفاده از expansion s-box در DES Function چیست؟**

کلید ۵۶ بیتی DES توسط Key Scheduler به ۱۶ کلید ۴۸ بیتی تبدیل می‌شود و از آنجایی که طول بلاک DES ۶۴ بیت است و در ساختار فیستل تنها ۳۲ بیت آن به داخل تابع F می‌رود باید ۳۲ بیت ورودی را به ۴۸ بیت گسترش بدهیم تا بتوانیم آن را با کلید xor کنیم.

ه) **اگر خروجی سیستم رمزنگاری به یک سیستم رمزنگاری دیگر داده شود، چه تغییری در امنیت آن حاصل می‌شود؟ (double des) اگر این کار سه بار تکرار شود چطور؟ (triple des)**

- double des

در این حالت برای شکستن می‌توان از حمله‌ی تطابق در میانه استفاده کرد که مرتبه‌ی آن از $2^{112}$ به $2^{57}$ تقلیل می‌یابد.

- triple des

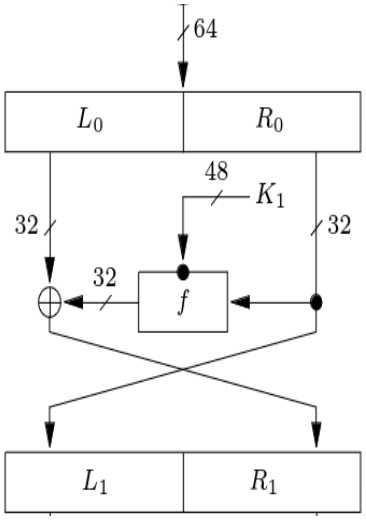
در این حالت هم (با استفاده از حمله‌ی تطابق در میانه) مرتبه بجای $2^{168}$ می‌شود: $2^{112}$ که البته در عمل قابل انجام نیست. در سال NIST ۲۰۱۷ منسوخ شدن 3DES را اعلام کرد.

و) ویژگی مکمل بودن این سیستم را ثابت کنید و توضیح دهید در آن صورت حمله به این سیستم از چه مرتبه‌ایست و چرا؟

خاصیت مکمل بودن DES:

$$\mathrm{DES_K(M)=C \Rightarrow DES_{\overline{K}}(\overline{M})=\overline{C}} \qquad (1)$$

(برای اثبات فقط یک دور را در نظر میگیریم) با توجه به ساختار فیستلی DES ورودی ابتدا به دو قسمت تقسیم میکند و سپس نیمه‌ی راست را (درون تابع F) با کلید xor می‌کند و سپس خروجی را با قسمت سمت چپ xor می‌کند.




که یعنی:

$$\begin{cases} P = L_0.R_0 \\ L_1 = R_0 \\ B = f(R_0 \oplus K_1) \\ R_1 = L_0 \oplus B \end{cases} \Rightarrow C = L_1.R_1 \qquad (۲)$$

حال اگر P و K را not کنیم:

$$\begin{cases} \overline{P} = \overline{L_0.R_0} \\ L_1 = \overline{R_0} \\ B = f(\overline{R_0} \oplus \overline{K_1}) \\ R_1 = \overline{L_0} \oplus B \end{cases} \Rightarrow \overline{C} = \overline{L_1.R_1} \qquad (۳)$$

پس در نتیجه:

$$E_k(P) = C \iff E_{\overline{k}}(\overline{P}) = \overline{C} \qquad (۴)$$

## ۲

**با استفاده از یک کلید رمز واحد، هر یک ازتبدیلات زیر را بر متن آشکار که تنها در بیت اول با هم تفاوت دارند، اعمال کنید. تعداد بیت‌های تغییر یافته پس از هرتبدیل را پیدا کنید. هرتبدیل را بطور مستقل اعمال کنید. در مورد اثر بهمنی پس از هرتبدیل بطور مستقل و سپس اثر بهمنی پس از اعمال یک راند توضیح دهید.**

آ) subBytes

ب) shiftRows

ج) mixColumns

د) addRoundKey

## ۳

**از بین مدهای عملیاتی ECB، CBC، OFB، CFB و CTR در کدام یک امکان افزایش سرعت در عمل رمزگذاری با استفاده از parallel processing یا پردازش موازی وجود دارد؟**