تکلیف سری دوم

مهیار عنصری ۹۶۳۲۰۹۳

سوال اول:

بخش اول:

چون عمل رمزنگاری و رمزگشایی باید یکسان باشد و در رمزگشایی از کلیدها به ترتیب معکوس استفاده می‌کنیم داریم:

ترتیب رمزنگاری: $K_1 \to K_2 \to K_3 \to \dots \to K_{16}$

در رمزگشایی: $K_{16} \to K_{15} \to K_{14} \to \dots \to K_1$

پس باید کلیدهای (K_1 و K_{16}) و (K_2 و K_{15}) و ... برابر باشند ←

$$\boxed{K_i = K_{17-i}}$$

بخش دوم:

باید تمام بیت‌های C_0 و D_0 یکسان باشند تا اثر شیفت بیت از بین برود.

① $C_0: \overbrace{0\dots0}^{8\text{ بار}}$ و $D_0: \overbrace{0\dots0}^{8\text{ بار}}$ ② $C_0: \overbrace{0\dots0}^{8\text{ بار}}$ و $D_0: \overbrace{F\dots F}^{8\text{ بار}}$

③ $C_0: \underbrace{F\dots F}_{8\text{ بار}}$ و $D_0: \underbrace{0\dots0}_{8\text{ بار}}$ ④ $C_0: \underbrace{F\dots F}_{8\text{ بار}}$ و $D_0: \underbrace{F\dots F}_{8\text{ بار}}$

$\boxed{\text{پس ۴ حالت داریم.}}$

بخش سوم:

طول کلید ← 2^{56} ← کل فضای حالت

کلیدهای ضعیف ← ۴

$$\Longrightarrow \text{Probability} = \frac{4}{2^{56}} = \frac{1}{2^{54}}$$

بخش چهارم:

با استفاده از weak-Key ها عمل diffusion به خوبی انجام نمی‌شود و تطابق به کمک تکرار کار را کمتر افزایش می‌یابد. اگر شاخص IC را برای کلیدهای ضعیف و قوی اندازه‌گیری کنیم مشاهده می‌کنیم در متن‌های کوچک فاصله کلید ضعیف و قوی بیشتر از این فاصله در متن‌های بزرگ است پس از کلیدهای ضعیف در متن‌های کوتاه نباید استفاده کنیم.

بخش پنجم:

هرکدام از C_0 و D_0 باید با تناوب ۲ تکرار شوند:

پس ۶ حالت داریم ← $\binom{4}{2} = 6$ ← انتخاب ۲ تا از این مجموعه ← $\{11\dots1111 \text{ و } 1010\dots1010 \text{ و } 10\dots1010 \text{ و } 00\dots00\}$

بخش ششم:

از ۱۶ دور موجود الگوریتم DES، بسته به اینکه دور زوج یا فرد است یکی از کلیدها انتخاب می‌شود ← هرکدام ۸ دفعه

بخش هفتم:

$P(\text{کلید ضعیف}) = \frac{1}{2^{54}}$ $P(\text{کلید ضعیف احتمالی}) = \frac{48}{2^{56}}$

$P(\text{کلید نیمه‌ضعیف}) = \frac{12}{2^{56}}$

$$\to P = \frac{4+12+48}{2^{56}} = \frac{2^6}{2^{56}} = \frac{1}{2^{50}}$$

Scanned by CamScanner

سوال دوم

بخش اول:

S-box ها غیرخطی هستند و درحقیقت تنها عنصر غیرخطی این الگوریتم هستند و باعث ایجاد Confusion می‌گردند و چون غیرخطی هستند به کمک روش‌های خطی قابل شکستن نیستند.

بخش دوم:

$x_1 = 101010 \rightarrow S_i(x_1) = 0110$

$x_2 = 010101 \rightarrow S_i(x_2) = 1100$

$x_1 \oplus x_2 = 111111$, $S_i(x_1) \oplus S(x_2) = 1010$

$S_i(x_1 \oplus x_2) = 1101 \neq S_i(x_1) \oplus S_i(x_2) = 1010 \Longrightarrow$ بخاطر غیرخطی بودن S-box ها

بخش سوم:

ورودی = 100011

ستون = 001 = 1

سطر = 11 = 3

$\rightarrow S_i(100011) = 12$

سوال سوم

بخش اول:

ورودی: 000 .... 1000 ... 000

بیت ۵۷ ام

ورودی $\rightarrow$ [Initial Permutation] $\rightarrow$ 000... | 000... 000 (L | R) $\xrightarrow{R}$ [expansion] $\rightarrow$ 0100...1 $\rightarrow$ ⊕ $\rightarrow$ 0100... 001

بیت ۳۲ ام

K = 00...00 (۴۸ بیت)

بیت دوم

بیت ۴۸ ام

S_1 و S_8 تغییر می‌کنند $\rightarrow \begin{cases} S_1 = 010000 \\ S_8 = 000001 \end{cases}$ و $S_2 = S_3 = S_4 = S_5 = S_6 = S_7 = 000000$

بخش دوم:

برطبق جدول ص ۶۲ کتاب:

$S_1: 010000 \rightarrow 0011$ $S_2: 000000 \rightarrow 1111$ $S_3: 000000 \rightarrow 1010$ $S_4: 000000 \rightarrow 0111$

$S_5: 000000 \rightarrow 0010$ $S_6: 000000 \rightarrow 1100$ $S_7: 000000 \rightarrow 0100$ $S_8: 000000 \rightarrow 0001$

بعد از Permutation داریم:

1101 0000 0101 1000 0101 1011 1001 1110

بخش سوم:

با توجه به جدول های S-box برای دو ورودی که تنها در یک بیت تفاوت داشته باشند خروجی S-box ها حداقل در ۲ بیت باهم متفاوت هستند.

Scanned by CamScanner

سوال سوم

بخش چهارم:

باید خروجی را هنگامی که Plain text کاملاً صفر می‌باشد را حساب کنیم.

$L_0 = R_0 = 0 \Longrightarrow S_1 = S_2 = \dots = S_8 = 0$

برای خروجی S_1 تا S_8 داریم:

$S_1 = 1110$ $S_2 = 1111$ $S_3 = 1010$ $S_4 = 0111$

$S_5 = 0010$ $S_6 = 1100$ $S_7 = 0100$ $S_8 = 1101$

که بعد از Permutation خواهیم داشت:

1101 1000 1101 1000 1101 1011 1011 1100

اگر با جواب بخش دوم مقایسه کنیم شاهد تغییر در ثابت هستیم.

Scanned by CamScanner

سوال پنجم :

به طور کلی $2^4=16$ چند جمله ای متمایز از درجه ۴ وجود دارند که اگر ضرایب آن ها را به صورت برداری نمایش بدهیم داریم :

$$\underset{x^4}{\underline{(1,0,0,0,0)}}\ ,\ \underset{x^4+1}{\underline{(1,0,0,0,1)}}\ ,\ \underset{x^4+x}{\underline{(0,1,0,1,0)}}\ ,\ \dots\ ,\ \underset{x^4+x^3+x^2+x+1}{\underline{(1,1,1,1,1)}}$$

حال از بین این ۱۶ چندجمله ای ، آن هایی قابل کاهش هستند که ضریب جمله x^0 صفر باشد مثل :

$x^4+x^2+x = x(x^3+x+1) \longrightarrow$ در همه آن ها می توانیم از x فاکتور بگیریم

پس ۸ جمله فوق که ضریب x^0 برابر صفر است قابل کاهش هستند

$x^4+1 \longrightarrow (x+1)^4$

$x^4+x+1 \longrightarrow$ irreducible

$x^4+x^2+1 \longrightarrow (x^2+x+1)^2$

$x^4+x^3+1 \longrightarrow$ irreducible

$x^4+x^3+x+1 \longrightarrow (x+1)^2(x^2+x+1)$

$x^4+x^3+x^2+1 \longrightarrow (x+1)(x^3+x+1)$

$x^4+x^2+x+1 \longrightarrow (x+1)(x^3+x^2+1)$

$x^4+x^3+x^2+x+1 \longrightarrow$ irreducible

Scanned by CamScanner

سوال ششم

$\times$	0 000	1 001	x 010	$x+1$ 011	x^2 100	x^2+1 101	x^2+x 110	x^2+x+1 111
0 000	0	0	0	0	0	0	0	0
1 001	0	1	x	$x+1$	x^2	x^2+1	x^2+x	x^2+x+1
x 010	0	x	x^2	x^2+x	$x+1$	1	x^2+x+1	x^2+1
$x+1$ 011	0	$x+1$	x^2+x	x^2+1	x^2+x+1	x^2	1	x
x^2 100	0	x^2	$x+1$	x^2+x+1	x^2+x	x	x^2+1	1
x^2+1 101	0	x^2+1	1	x^2	x	x^2+x+1	$x+1$	x^2+x
x^2+x 110	0	x^2+x	x^2+x+1	1	x^2+1	$x+1$	x	x^2
x^2+x+1 111	0	x^2+x+1	x^2+1	x	1	x^2+x	x^2	$x+1$

$GF(2^3)$ دارای ۸ حالت برای ضرایب است (در رزم برداری) ← $\underset{0}{(0,0,0,0,0)}$ و $\underset{1}{(0,0,0,0,1)}$ و ... و $\underset{x^2+x+1}{(1,1,1,1)}$

بعضی اوقات در ضرب در اینجا ممکن است که درجه بالاتری به دست بیاید که آنگاه باید باقیمانده آن را به $P(x)$ حساب کنیم.
و هرجا در ضرب x^3 یا x^4 تولید شود به جای آن باقیمانده آن را می گذاریم و در نهایت اعداد متناظر چندجمله‌ای ها را به صورت بیت به بیت XOR می کنیم. در ادامه بعضی از محاسبات جدول به صورت نمونه آورده شده است:

$P(x) = x^3 + x + 1$

← به جای x^4 ، x^2+x می گذاریم

$\rightarrow x^3 \equiv x+1 \mod P(x)$ و هرکجا x^3 دیدیم به جای آن $x+1$ می گذاریم ← $x^4 = x^2 \cdot x^2 = x \cdot x^3 \equiv x \cdot (x+1) \equiv x^2+x \mod P(x)$

$x \cdot x^2 = x^3 \equiv x+1$

$x \cdot (x^2+1) = x^3 + x \equiv 1 \mod P(x)$

$x \cdot (x^2+x) = x^3 + x^2 \equiv x^2+x+1 \mod P(x)$

$x \cdot (x^2+x+1) = x^3 + x^2 + x \equiv x^2+1 \mod P(x)$

$(x+1) \cdot (x+1) = x^2+1$

$(x+1) \cdot x^2 = x^3 + x^2 \equiv x^2+x+1 \mod P(x)$

$(x+1) \cdot (x^2+1) = x^3 + x^2 + x + 1 \equiv x^2 \mod P(x)$

$(x+1) \cdot (x^2+x) = x^3 + x^2 + x^2 + 1 \equiv 2x^2 + 2x + 1 \equiv 1 \mod P(x)$

$(x+1) \cdot (x^2+x+1) = x^3 + 2x^2 + 2x + 1 \equiv x^3 + 1 \equiv x \mod P(x)$

Scanned by CamScanner