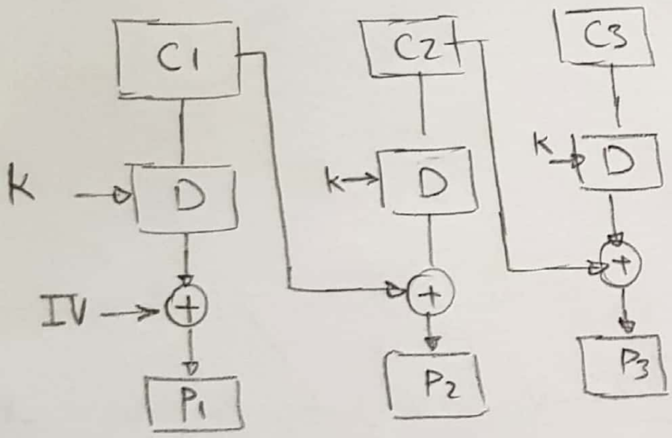
تمرین سری پنجم — باسمه تعالی — مبانی رمزنگاری و امنیت شبکه

پوریا دادخواه _ ۹۴۱۰۴۴۸۵ — دکتر میرحسینی

۱_ در رمزگشایی CBC برای بدست آوردن هر قالب P_i به C_i و C_{i-1} نیاز داریم. [به جز در مرحله اول که از IV استفاده شده] هم‌چنین این قالب‌ها به صورت موازی بدست می‌آیند.



الف) از آن جا که C_1 و C_2 خطا دارند، این خطا علاوه بر قالب P_1 و P_2، P_3 را نیز تخریب می‌کند. => ۳ قالب تخریبی هستند.

DES-blocks => 192_bit حداکثر خطا

ب) در این حالت جای C_1، C_2 عوض شده پس با توجه به شکل P_1، P_2، P_3 اشتباه خواهد شد.

=> 192-bit خطا

۲_ الف) این بخش مربوط به تأثیر کلید در سیستم رمزنگاری است و معادل آن در بلوک "Add Round key" در AES وجود دارد.

ب) "Mix Column"؛ زیرا در این مرحله بایت‌های مختلف روی همدیگر اثر می‌گذارند.

ب) "SubByte" ؛ زیرا این مرحله، عملیات غیرخطی را وارد AES می‌کند.

ت) "ShiftRow" ؛ زیرا این بایت‌ها خاصیت برقرار می‌کند.

ث) خیر معادل در AES ندارد؛ زیرا در واقع AES هیچ مرحله‌ای نیز ندارد زیرا:
MixColumn بایت می‌شود هر بایتی در ستون با هر بایت دیگر در ستون جایگزین شود پس نیاز به Swap کردن
سطر نیست، Shift بایت‌ها از یک ستون به ستون دیگر می‌برد بنابراین نیازی به Swap کردن
ستون‌ها نیست.

۳- در الگوریتم تولید زیرکلید از 64 بیت اولیه، 8 بیت دور ریخته می‌شود و پس بیت‌های باقی‌مانده به دو بخش
28 بیتی تقسیم می‌شوند. در هر مرحله شیفت دایروی داده می‌شود و به دور بعدی منتقل می‌شود.

ب) اگر بیت‌های کلید اولیه‌ای باشند که شیفت دایروی دو بخش 28 بیتی را تغییر ندهد (یعنی هر بخش، ۰ یا 28 بیت 1 داشته باشد) همه زیرکلیدها یکسان خواهند بود و در نتیجه DES با کلید داده‌شده خاصیت Involution خواهد بود

$K_R, K_L = [11\cdots1]_{28} : [00\cdots0]_{28}$

$K_1 = [11\cdots11]_{56}$ $\quad K_3 = [\underbrace{00\cdots0}_{28}\ \underbrace{11\cdots11}_{28}]$

$K_2 = [\underbrace{11\cdots1}_{28}\ \underbrace{00\cdots0}_{28}]$ $\quad K_4 = [00\cdots0]_{56}$

ب) تعداد شیفت برای تولید کلید در هر دور طبق این روال است

دور	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
تعداد شیفت	1	1	2	2	2	2	2	2	1	2	2	2	2	2	2

حال برای اینکه برای دو کلید k, k' داشته باشیم $DES_k^{-1} = DES_{k'}$ باید k, k' داشته باشیم:

$k_1 = k'_{16}$, $k_2 = k'_{15}$, ... , $k_8 = k'_9$, ... , $k_{16} = k'_1$

این اتفاق زمانی رخ می‌دهد که بخش چپ k_L و راست k_R با دوره تناوب 2 تکرار شوند یعنی یکی از حالات زیر:

$k_L, k_R = \underbrace{11\cdots1}_{28}$ یا $\underbrace{00\cdots0}_{28}$ یا $\underbrace{1010\cdots10}_{28}$ یا $\underbrace{010101\cdots01}_{28}$

اگر حالت‌های ضعیف را کنار بگذاریم (یعنی هر دو بخش k_L, k_R فقط ۰ یا فقط 1 باشند)، 8 حالت باقی‌مانده نیمه‌ضعیف (Semi-key) خواهد بود.

۴_ کافی است ثابت کنیم:

$$a(x).b(x) \equiv 1 \mod (x^4+1)$$

$$a(x).b(x) = [(03)x^3+(01)x^2+(01)x+(02)].[(0B)x^3+(0D)x^2+(09)x+(0E)]$$

$$\overset{x^4+1}{\equiv} [(03).(0E)+(0B).(02)+(01).(09)+(01).(0D)]x^3$$

$$+[(01).(0E)+(01).(09)+(02).(0D)+(03).(0B)]x^2$$

$$+[(01).(0E)+(02).(09)+(03).(0D)+(01).(0B)]x$$

$$+[(02).(0E)+(03).(09)+(01).(0D)+(01).(0B)] =$$

$$0x^3+0x^2+0x+1 = 1$$ تنها LSB ضریب 1 برابر 1 هست و بقیه صفرند.

۵-

a)
$$\begin{bmatrix} 0f & 0b & 07 & 03 \\ 0e & 0a & 06 & 02 \\ 0d & 09 & 05 & 01 \\ 0c & 08 & 04 & 00 \end{bmatrix} \xrightarrow{XOR} b) \begin{bmatrix} 0d & 09 & 05 & 01 \\ 0c & 08 & 04 & 00 \\ 0f & 0b & 07 & 03 \\ 0e & 0a & 06 & 02 \end{bmatrix}$$

$$\xrightarrow{\text{Sub Bytes}} c) \begin{bmatrix} d7 & 01 & 6b & 7c \\ fe & 30 & f2 & 63 \\ 76 & 2b & c5 & 7b \\ ab & 67 & 6f & 77 \end{bmatrix} \Rightarrow d) \begin{bmatrix} d7 & 01 & 6b & 7c \\ 30 & f2 & 63 & fe \\ c5 & 7b & 76 & 2b \\ 77 & ab & 67 & 6f \end{bmatrix}$$

e)
$$\begin{bmatrix} 02 & 03 & 01 & 01 \\ 01 & 02 & 03 & 01 \\ 01 & 01 & 02 & 03 \\ 03 & 01 & 01 & 02 \end{bmatrix} \times \begin{bmatrix} d7 & 01 & 6b & 7c \\ 30 & f2 & 63 & fe \\ c5 & 7b & 76 & 2b \\ 77 & ab & 67 & 6f \end{bmatrix} = \begin{bmatrix} 57 & df & 62 & a5 \\ 94 & d8 & 50 & 89 \\ ef & e3 & 4d & 65 \\ 79 & c7 & 66 & 8f \end{bmatrix}$$

۶- این مسئله بنیادی برای این است که مطمئن شویم این ضرب که یک زمان ثابت می‌گیرند، مستقل از مقدار آرگیومنت (argument) ؟. راه آن هم می‌تواند این باشه که یک حلقه null (بدون انجام کار خاصی در آن حلقه) اضافه کنیم که این زمان را uniform تبدیل کنیم.

۷- الف) CBC one-loop امن تر است؛ تابع رمزنگاری یک حلقه کلی ماند حمله تفاضلی راست به سمت ساده تر شکل تر می کند.

ب) CBC three-loop سریع تر عمل می کند چون هر بلوک از سه loop ها شامل رمزنگاری یا رمزگشایی است. اما است که تصادفی دارد زیرا هر حلقه یک DES است و ست به حمله آسیب پذیر است.

۸- پس از رمزگشایی آخرین بایت متن آخر بیابد آن خواهد بود که چه تعداد از بیت ها باید به عنوان Padding از متن حذف شوند. در نتیجه ۲ حداقل یک بایت بیت ۲ عنوان Padding نیز خواهد بود.