بسمه تعالی

مفاهیم پیشرفته معماری کامپیوتر	**تمرین ۱**	**نیمسال دوم ۹۶-۹۵**
دانشکده کامپیوتر	**تاریخ تحویل: شنبه ۹۵/۱۲/۲۱**	**مدرس: دکتر بیات سرمدی**

نکات

- تمرینات را سر موعد به استاد درس تحویل دهید.
- در صورت درج تمارین در بیشتر از یک صفحه، کلیه صفحات باید شامل نام، شماره دانشجویی و شماره تمرین بوده و با منگنه به هم وصل شده باشند.
- از قرار دادن تمارین در کاور خودداری فرمایید.
- سوالات در اولین کلاس تمرین بعد از موعد تحویل حل خواهند شد.
- اشکالات خود را در کلاس حل تمرین و یا از طریق ایمیل مطرح کنید.

mosanaei@ce.sharif.edu
salarifard@ce.sharif.edu

موفق باشید.

---

۱. جدول Zech را برای $F(x) = x^3 + x^2 + 1$ تشکیل دهید و با استفاده از آن عدد $x^{15} + x^8 + x^5 + x^3 + 1$ را از پایه چند جمله‌ای به پایه نرمال تبدیل کنید.

۲. فرض کنید یک عدد اول به صورت $P = 2^{192} - 2^{64} - 1$ داشته باشیم. در میدان $GF(P)$ پایه $\beta = 2^{32}$ را در نظر بگیرید. بنابراین عدد P را می‌توان در این پایه به صورت $P = \beta^6 - \beta^2 - 1$ نمایش داد. با توجه به مقدار P در این پایه معادلات زیر برقرار است:

$$\beta^6 - \beta^2 - 1 = 0 \implies \beta^6 \equiv (\beta^2 + 1) \bmod P \xrightarrow[\text{به طور مشابه}]{} \beta^7 \equiv (\beta^3 + \beta) \bmod P \dots$$

$$\beta^{11} \equiv (\beta^5 + \beta^3 + \beta) \bmod P$$

حال $d = (d_{11}, d_{10}, \dots, d_0)_\beta$ را در نظر بگیرید. واضح است که برای محاسبه $C = d \bmod P$، ارقام $d_5 - d_0$ از P کمتر بوده و نیاز به *reduction* ندارند. برای کاهش ارقام باقی مانده از الگوریتم زیر استفاده می‌شود. در این الگوریتم هر رقم توسط یک شش تایی مرتب به صورت زیر نمایش داده می‌شود.

$$d_7\beta^7 = d_7(\beta^3 + \beta) = (0, 0, d_7, 0, d_7, 0)_\beta$$

Algorithm 5: Integer modular reduction for $p = 2^{192} - 2^{64} - 1$

INPUT: Integer $d = (d_{11}, \dots, d_0)_{2^{32}} < (2^{192} - 2^{64} - 1)^2$.
OUTPUT: $c = d \bmod (2^{192} - 2^{64} - 1)$.

1. Define the 6-digit integers in the base $\beta = 2^{32}$:
   $e = (d_5, d_4, d_3, d_2, d_1, d_0)_\beta$, $f = (0, 0, d_7, d_6, d_7, d_6)_\beta$,
   $g = (d_9, d_8, d_9, d_8, 0, 0)_\beta$, $h = (d_{11}, d_{10}, d_{11}, d_{10}, d_{11}, d_{10})_\beta$.
2. $c = e + f + g + h \bmod (2^{192} - 2^{64} - 1)$
3. **return**(c)

بسمه تعالی

مفاهیم پیشرفته معماری کامپیوتر	**تمرین ۱**	**نیمسال دوم ۹۶-۹۵**
دانشکده کامپیوتر	**تاریخ تحویل: شنبه ۹۵/۱۲/۲۱**	**مدرس: دکتر بیات سرمدی**

این روش را برای $P = 2^{224} - 2^{96} + 1$ تعمیم دهید.

۳. میدان $GF(7)$ را در نظر بگیرید. حال مقدار اعداد $\frac{1}{2}$ و $\frac{1}{4}$ را در این میدان حساب کنید. آیا رابطه $\frac{1}{2} - \frac{1}{4} = \frac{1}{4}$ صادق است؟ (بله یا خیر) ثابت کنید. در صورت وجود یک عبارت دیگر به این فرم بیابید. (راهنمایی: می‌دانیم که $a.b \equiv 1 \, mod \, P$ یعنی $a = b^{-1}$).

۴. چند جمله‌ای مشخصه $F(x) = x^5 + x^3 + 1$ را روی میدان $GF(2^5)$ و پایه نرمال $\{0, x, x^2, x^4, x^8, x^{16}\}$ در نظر بگیرید. اگر $A = a_4x^{16} + a_3x^8 + a_2x^4 + a_1x^2 + a_0x$ و $B = b_4x^{16} + b_3x^8 + b_2x^4 + b_1x^2 + b_0x$ باشد، آنگاه حاصل $C = A.B \, mod \, F(x)$ و $D = A^2 \, mod \, F(x)$ را محاسبه کنید.

۵. یک ضرب کننده H2L LFSR-based طراحی کرده و پیچیدگی مساحت و زمان آن را محاسبه کنید.