

## Tarea 1

### Programación en Ensamblador con ARM

Fecha de asignación: 26 de febrero, 2020  
Grupos: 1 persona

Fecha de entrega: 08 de marzo, 2020  
Profesor: Luis Chavarría Zamora

Para los siguientes ejercicios de programación, desarrolle la solución al problema planteado de manera clara y correcta. Debe incluir en cada caso un diagrama de flujo y el código en lenguaje ensamblador ARM (ARMv4) que soluciona cada problema, con los comentarios significativos del caso, de forma que quede en claro la solución del mismo:

1. Un programa generador de números pseudoaleatorios mediante un *linear feedback shift register* (LFSR) de tipo Fibonacci, usando como semilla la tercera letra de su apellido en minúscula, por ejemplo: Chavarría,  $a \rightarrow 61$ , debe generar 20 números aleatorios desde la posición 0x500. El polinomio de realimentación es:  $x^8 + x^6 + x^5 + x^4 + 1$ .

Suponga que hay una interfaz que proviene de una PC, a través de una interfaz serie/paralela. El algoritmo debería hacer una petición de envío de términos hacia la PC, a través de la interfaz, escribiendo un valor de 0xF0, en la dirección de memoria 0x600. Una vez enviada la petición, debería esperar por el comando de respuesta (valor de 0xFF), en la dirección de memoria 0x604. Cuando se reciba este comando, se debería comenzar el cálculo si el número es primo y escribir el resultado desde la posición 0x700 (1 si es primo, 0 si no es primo). Se debe analizar cada número, no se permite escribir cada número primo en una lista a mano (es decir que los números primos los escriba el programador).

2. Algoritmo para encriptar y desencriptar contraseñas:

- a) Un programa que, a partir de una cadena de caracteres escrito en la posición de memoria 0x500, encripte el nombre: **Claude Shannon** según el siguiente procedimiento (5 puntos):
  - 1) Suma 23d al caracter y da un resultado.
  - 2) Realiza operación xor entre el resultado del punto anterior y el valor consecutivo en un generador LFSR de tipo Fibonacci.
  - 3) Reemplaza el caracter original con el resultado de los pasos anteriores, el largo de la frase encriptada será guardado en 0x620.
- b) Un programa que, según el procedimiento anterior, desencripte una contraseña encriptada, de forma que se obtenga la contraseña original.

Como consideraciones generales se tienen:

- 1) La cadena tiene una longitud N. Dicha longitud se encuentra almacenada en la dirección de memoria 0x620.

- 2) Debe realizar el proceso inverso mostrado en el punto (a).
- 3) El inicio de la cadena de caracteres descriptada debe ser escrito en la dirección 0x700.

El trabajo debe seguir los siguientes lineamientos:

- Debe usar la herramienta [VisUAL](#). No se aceptarán trabajos en otras herramientas.
- Se debe enviar el \*.S correctamente documentado internamente.
- Como cualquier documento técnico, la ortografía y el formato deben ser impecables.
- La entrega se debe realizar por medio del TEC-Digital en la pestaña de evaluación, no más tarde de la fecha de entrega a las 11:59 pm. No se aceptarán trabajos después de esta hora y fecha.
- Los documentos serán sometidos a control de plagios para eliminar cualquier intento de plagio con trabajos anteriores similares o copias textuales.