Universidad de Costa Rica
Facultad de Ingeniería
Escuela de Ingeniería Eléctrica
IE-0521 Estructuras de computadores II
I ciclo 2015

Tarea 3

Multiplicador en Verilog

Alejandro León Torres, B13645
Andrés Mora Zúñiga, B14463
Kenneth Vallecillo González, B16750
Grupo: 1

Profesor: Erick Carvajal Barboza

23 de agosto de 2015

Índice

Índice de figuras

Índice de tablas

1. Introducción

Implementación del AES en un FPGA http://www.dspace.espol.edu.ec/bitstream/123456789/24372/1/JorgeCeli_AES_NIOSII.pdf

Explicación de Criptografía simétrica, asimétrica e Híbrida. http://www.genbetadev.com/seguridad-info tipos-de-criptografia-simetrica-asimetrica-e-hibrida

Ejemplos de algoritmos de cifrado maso explicados. http://www.redeszone.net/2010/11/04/criptografia-algoritmos-de-cifrado-de-clave-simetrica/ http://www.uv.es/~sto/cursos/seguridad.java/html/sjava-12.html

Un buen sistema de cifrado pone toda la seguridad en la clave y ninguna en el algoritmo. En otras palabras, no debería ser de ninguna ayuda para un atacante conocer el algoritmo que se está usando. Sólo si el atacante obtuviera la clave, le serviría conocer el algoritmo.

2. Universidad Politécnica de Madrid

Los 2 grandes métodos de encriptación son las siguientes:

- Transposición: Las letras del texto en claro intercambian sus posiciones según cierto patrón, así en el texto cifrado aparecen las mismas letras pero con sus posiciones permutadas.
- Sustitución: Las letras del texto claro mantienen su posición pero son cambiadas por otro tipo sea otro abecedario, números u otros signos.

Criptoanálisis

3. Cifrado Simétrico

3.1. Cifrados de flujo

Cifran el mensaje con correspondencias bit a bit sobre el flujo (stream). Un ejemplo de cifrado de flujo es RC4.

3.2. Cifrados de Bloque

Cifran el mensaje dividiendo el flujo en bloques de k bits. Cada bloque se corresponde con otro diferente. Por ejemplo, un bloque con k=3 "010"se podría corresponder con "110". Algunos ejemplos de cifrado de bloque son los algoritmos AES o RC6.

4. Cifrado RC5

Se encuentra basado en una red Feistel.

4.1. Usos

- Procesamiento de Transacciones On Line (OLTP).
- Symbian.

- Protocolos de Seguridad de correo electrónico como PGP y S/MIME.
- RSA Data Security.

```
def imul(a,b) //   Recibe las palabras a y b.
producto = 0 //Inicializa el resultado.
for i in range(0,32,1): //Itera sobre los 32 bits de cada palabra.
if b & 0x1 == 1: // Y-logica de b con 1.
producto += a //Si el ultimo bit de b era un 1 sumo a.
a = a << 1 //Desplazo a hacia la izquierda.
b = b >> 1 //Desplazo b hacia la derecha.
return producto.
```

5. Links intro

http://www.seagate.com/staticfiles/SeagateCryptofaceoff.pdf https://hal.inria.fr/hal-00850899/document

6. Referencias

Referencias

[Hennessy, 2014] John L. Hennessy & David. A. Patterson.*Computer organization and design.* Morgan Kaufmann 5th ed.

[Harris, 2013] David Money Harris & Sarah L. Harris.*Digital Design and Computer Architecture.* Morgan Kaufmann 2nd ed.