

Trabajo Práctico 1:

Conjunto de instrucciones MIPS

Jimenez, Ruben, *Padrón Nro. 92.402*
rbnm.jimenez@gmail.com

Reyero, Felix, *Padrón Nro. 92.979*
felixcarp@gmail.com

Suárez, Emiliano, *Padrón Nro. 78.372*
emilianosuarez@gmail.com

Primera Entrega: 30/04/2015

1er. Cuatrimestre de 2015

66.20 Organización de Computadoras – Práctica Jueves
Facultad de Ingeniería, Universidad de Buenos Aires

Resumen

Se implementó una versión simplificada del programa **sha1** de UNIX.
Para nuestra implementación.

1. Introducción

Este Trabajo Práctico pretende familiarizarse con la programación en assembly y el concepto de ABI.

Para ello, implementaremos el algoritmo **sha1** de UNIX en código *Assembly*, mientras que la interpretación de argumentos del programa y la lectura de archivos será realizada en lenguaje *C*.

Además, se utilizará *GXemul* para simular una máquina *MIPS* corriendo una versión reciente del sistema operativo *NetBSD*.

El programa implementado, muestra por *stdout* un checksum generado a partir del contenido de los archivos pasados por parámetro. En caso de no especificarse algún archivo, se mostrarán un checksum a partir de lo ingresado por *stdin*.

2. Implementación

2.1. Arquitectura

En una primera versión se trabajó con una función *sha* íntegramente desarrollada en *Assembly*, con un stack mas grande. Pero tuvimos problemas con el *malloc* al intentar reservar memoria para los bloques a procesar por el algoritmo. Como una alternativa, probamos utilizar la función *malloc* de *C* desde *Assembly*, realizando *syscall* e incluso, utilizando la versión en *Assembly* de *mymalloc.S* que se encuentra en el grupo.

Con ninguna de estas opciones lograr que la función *sha* funcionara correctamente, por lo que decidimos modularizarla de la siguiente manera.

main.c

Cuerpo principal del programa, donde se realiza la lectura de los parámetros de los archivos.

Cada uno de estos archivos, es guardado en memoria dinámica con un tamaño máximo de 1000 bytes (utilizando *malloc*). En caso que el tamaño del archivo supere dicho tamaño, se reasigna memoria dinámica mediante la utilización de *realloc*, para disponer un bloque de memoria donde quepa el archivo (bloque de igual tamaño al tamaño del archivo).

relleno.S

Donde se encuentra la implementación en *Assembly* de la función *calcularRelleno*.

Dicha función cuenta con un stack donde se almacena la longitud original así como la longitudRelleno que es la longitud que incluye el relleno para poder determinar la cantidad de bloques finales a procesar.

También se almacena en el stack la variable *cantBloques* que determina la cantidad de bloques a procesar.

La dificultad de este método fue la de tratar longitudes que ocupan 64 bits, para ello se tuvo que manejar dos registros uno que tenga los 32 bits mas significativos y otro para los 32 restantes, usando el carry que produce la suma de la parte menos significativa para actualizar la parte mas significativa de la longitud final.

trozo.S

Donde se encuentra la implementación en *Assembly* de la función *cargarTrozos*.

Dicha función, además de los registros obligatorios, contiene en su stack dos “saved registers” *s0* y *s1* que almacenan los punteros hacia los vectores “trozos” y “bloques” y los registros para almacenar las variables “*i*” y “*mask*”. En el cuerpo de la función se hace uso de los 8 registros temporales para distintas asignaciones necesarias.

Luego de guardar los parámetros con los que viene la función, inicializar “*i*” y cargar la “*mask*” a un temporal, genera las 16 primeras palabras del vector de 80, trayendo byte a byte desde “bloques” y generando con operaciones lógicas (and, or) y movimientos (*sll*) el word final que se guarda en “trozos”.

Luego desde la posicion 16 hasta la 80 con operaciones lógicas y rotaciones (xor y rol) se genera el resto del contenido del vector operando con los 16 words anteriores.

algoritmo.S

Donde se encuentra la implementación en *Assembly* de la función *algoritmoSha1*.

Dicha función, además de los registros obligatorios, contiene en su stack seis “saved registers” s2..s7 que almacenan los punteros hacia los valores de “a,b,c,d,e,f” y los registros para almacenar las variables “i”, “k” y “temp”. En el cuerpo de la función se hace uso de los 8 registros temporales para distintas asignaciones necesarias.

Luego de guardar los parámetros con los que viene la función e inicializar “i” , se generan 4 ramas distintas de condicionales con procesos distintos (dependiendo el valor de “i” en el for) donde a través de operaciones lógicas (and, not, xor, or) generan un valor que se almacena en “f” y se carga una constante “k” determinada para que luego se terminen de generar los valores que devuelve la función y se asignen a sus respectivas variables.

Las funciones *calcularRelleno*, *cargarTrozos* y *algoritmoSha1*, son llamadas desde la función *sha1* de *main.c*.

Los stacks de cada una de ellas que pueden observarse a continuación:

calcularRelleno	
Dir Mem	Valor
48	
44	ra
40	fp
36	gp
32	
28	longOrig
24	longOrig
20	longRelleno
16	longRelleno
12	a3
8	a2
4	a1
0	a0

cargarTrozos	
Dir Mem	Valor
36	
32	ra
28	fp
24	gp
20	mascara
16	i
12	a3
8	a2
4	a1
0	a0

algoritmoSha1	
Dir Mem	Valor
44	
40	ra
36	fp
32	gp
28	
24	temp
20	k
16	i
12	a3
8	a2
4	a1
0	a0

Registro	Valor
s0	bloques
s1	trozos
s2	a
s3	b
s4	c
s5	d
s6	e
s7	f

2.2. Diseño

Se desarrollo un programa que realiza la lectura a través del stdin o a través de archivos que se reciben por parámetro.

El comando acepta 2 parámetros para mostrar la Ayuda y la Versión del programa:

```
$ ./sha -h
$ ./sha --help
```

Para desplegar la ayuda del comando. Y los siguientes comandos para mostrar la versión:

```
$ ./sha -V
$ ./sha --version
```

Inicialmente el programa revisa la cadena de parametros ingresada y determina si el checksum debe generarse a partir de lo ingresado por *stdin* o a través del contenido del (o los) archivo(s).

Para esta última opción, se procesan los archivos de uno por vez, y para cada uno de ellos se genera el checksum a partir de sus datos.

Primero se obtiene el largo total del archivo, luego se llama a la función `calcularRelleno`, donde se obtiene una `longitudRelleno` que dividida por 8 determina la longitud del vector que se asigna en memoria dinámica para trabajar con el archivo completo.

Para completar el archivo, se llama a la función de C “asignarDatos” la cual se encarga de completar el vector anteriormente pedido con las características correspondientes que pide el preprocesamiento del algoritmo sha1 (a saber: el relleno consiste en un uno seguido de los ceros que sean necesarios, aunque el mensaje ya tenga la longitud deseada se debe efectuar el relleno, por lo que el número de bits de dicho relleno está en el rango de 1 a 512 bits, luego se le añade un bloque de 64 bits que represente la longitud del mensaje original antes de ser relleno).

Es decir, la totalidad del archivo mas el relleno que lo completa, queda alojado en memoria dinámica. A continuación se procede con la función `sha1`.

Una vez dentro de la función `sha1`, se llama a la función “calcularRelleno”, donde se obtiene una `longitudRelleno` que, dividida por 512, determina la cantidad de bloques finales a procesar. Se inicializan las variables y por una decisión de diseño se decidió trabajar con un vector de 80 palabras en memoria dinámica porque nos parecía que el stack quedaba muy engorroso para trabajarlo.

Por esta elección, tuvimos problemas con la asignación de memoria dinámica desde assembly por lo cual se dividió (como se menciona en este informe) en partes la función.

A continuación se procede a trabajar con el bloque de datos en un `while` donde primero se carga el vector de 80 en “cargarTrozos” y luego el algoritmo propiamente dicho en “algoritmosha1” para finalmente devolver el valor en 160 bits.

2.3. Compilación

Para compilar el programa se debe abrir una terminal en la carpeta donde están alojados los archivos fuentes (*src/*) y se ejecuta el siguiente comando:

```
../src$ gcc -g -O0 -Wall main.c algoritmo.S trozo.S relleno.S -o sha
```

Para generar el ejecutable *sha*.

3. Casos de Prueba

Algunos de los casos de pruebas realizados, pueden observarse a continuación:

```
root@:/home/gxemul/tprub/div# sha1 hola
SHA1 (hola) = ef443fee4da6bfb41651930de7ad99f29ed9f079
root@:/home/gxemul/tprub/div# ./sha hola
```

ef443fee4da6bfb41651930de7ad99f29ed9f079

```
root@:/home/gxemul/tprub/div# sha1 vacio
SHA1 (vacio) = da39a3ee5e6b4b0d3255bfef95601890afd80709
root@:/home/gxemul/tprub/div# ./sha vacio
da39a3ee5e6b4b0d3255bfef95601890afd80709
```

```
root@:/home/gxemul/tprub/div# sha1 prueba-dog
SHA1 (prueba-dog) = 2fd4e1c67a2d28fced849ee1bb76e7391b93eb12
root@:/home/gxemul/tprub/div# ./sha prueba-dog
2fd4e1c67a2d28fced849ee1bb76e7391b93eb12
```

```
root@:/home/gxemul/tprub/div# sha1 prueba-cog
SHA1 (prueba-cog) = de9f2c7fd25e1b3afad3e85a0bd17d9b100db4b3
root@:/home/gxemul/tprub/div# ./sha prueba-cog
de9f2c7fd25e1b3afad3e85a0bd17d9b100db4b3
```

4. Conclusiones

El presente trabajo permitió la familiarización con las herramientas de compilación de código C y código assembly en un entorno que emula la arquitectura MIPS 32, asegurando la portabilidad del programa.

Además nos permitió conocer en detalle como se comporta el stack de una función en la programación en *Assembly*. Para esto último, fue de gran ayuda conocer previamente la implementación de las funciones en language C, para luego hacer la “traducción” a *Assembly* teniendo en cuenta la cantidad de argumentos, variables locales, tamaño de los datos, etc.

5. Apéndice

5.1. Código Fuente: main.c

```
1 #include <stdio.h>
2 #include <stdlib.h>
3 #include <string.h>
4
5 #define ERROR_OPEN_FILE 10
6 #define MAX_COUNT_FILES 50
7 #define HASH_LENGTH 20
8 #define MAX_FILE_SIZE 1000
9
10 void printHelp();
11 void printVersion();
12 void printError(char* msgError, int codeError);
13 char* setFileSize(FILE* fp, long long int *length);
14
15 int readFromStdInput(int argumentCount);
16
17 long long int calcularRelleno(long long int longitudOriginal);
18 void cargarTrozos(char *bloque, unsigned int *Trozos);
19 void algoritmoShal(unsigned int *Trozos, unsigned *a, unsigned *b,
20                  unsigned *c, unsigned *d, unsigned *e);
21
22 int shal(unsigned char *resultado, char *nombre_archivo, unsigned
23          long long longitudOriginal);
24 unsigned int leftrotate(unsigned int valor, int desplazamiento);
25 void asignarDatos(FILE* fp, unsigned char *bloques, long long int
26                  tamanioOriginal, long long int longitudRelleno);
27 void showChecksum(unsigned char *result);
28
29 int main(int argc, char* argv[]) {
30     int i = 0;
31     char* param;
32     char* files[MAX_COUNT_FILES];
33     unsigned char *result;
34     int fileCount = 0;
35     FILE* fp;
36     char *start;
37     long long int length;
38
39     if (readFromStdInput(argc)) {
40         int c;
41
42         fp = fopen("archivoAuxiliar.txt", "w+");
43         while ((c = fgetc(stdin)) != EOF) {
44             fputc(c, fp);
45         };
46
47         start = setFileSize(fp, &length);
48         long long int longitudRelleno = calcularRelleno(length);
49         char *bloques = malloc(longitudRelleno/8);
50         asignarDatos(fp, bloques, length, longitudRelleno); // se
51                     almacena el tamanioOriginal al final
52         shal(result, bloques, length);
53         showChecksum(result);
54
55         fclose(fp);
56         remove("archivoAuxiliar.txt");
57
58         return 0;
59     }
```

```

55 } else if (argc >= 2) { // Parse arguments
56     param = *(argv + 1);
57     if ((strcmp(param, "-h") == 0) || (strcmp(param, "--help"
58         == 0) ) {
59         printHelp();
60     }
61     else if ((strcmp(param, "-V") == 0) || (strcmp(param, "--
62         version") == 0)) {
63         printVersion();
64     }
65 }
66 // Search for files
67 for(i = 1; i < argc; i++) {
68     if (*argv[i] != '-') {
69         files[fileCount++] = argv[i];
70     }
71 }
72
73 // Process each file
74 for(i = 0; i < fileCount; i++) {
75     result = malloc(HASH_LENGTH);
76
77     if (NULL == (fp = fopen(files[i], "r"))) {
78         fprintf(stderr, "Files '%s' doesn't exist.", files[i]);
79         exit(ERROR_OPEN_FILE);
80     }
81
82     start = setFileSize(fp, &length);
83     long long int longitudRelleno = calcularRelleno(length);
84     char *bloques = malloc(longitudRelleno/8);
85
86     fp = fopen(files[i], "r");
87     asignarDatos(fp, bloques, length, longitudRelleno); // se
88         almacena el tamañoOriginal al final
89     sha1(result, bloques, length);
90     fclose(fp);
91 }
92 showChecksum(result);
93
94 return 0;
95 }
96
97 char* setFileSize(FILE* fp, long long int *length) {
98     int character;
99     char *start;
100     int n = 0;
101
102     fseek(fp, 0, SEEK_END);
103     *length = ftell(fp);
104
105     fseek(fp, 0, SEEK_SET);
106
107     start = malloc(MAX_FILE_SIZE);
108
109     if ((*length) > MAX_FILE_SIZE) {
110         start = realloc(start, (*length));
111     }
112
113     *length *= 8; // devuelve el tamaño en bits

```

```

114
115     while ((character = fgetc(fp)) != EOF) {
116         start[n++] = (char)character;
117     }
118     start[n] = '\0';
119
120     return start;
121 }
122
123 void printHelp()
124 {
125     fprintf(stdout, "$ tp1 -h\n");
126     fprintf(stdout, "Usage:\n");
127     fprintf(stdout, "    tp1 -h\n");
128     fprintf(stdout, "    tp1 -V\n");
129     fprintf(stdout, "    tp1 [file ...]\n");
130     fprintf(stdout, "Options:\n");
131     fprintf(stdout, "    -V, --version    Print version and quit.\n");
132     ;
133     fprintf(stdout, "    -h, --help      Print this information and
134         quit.\n\n");
135     fprintf(stdout, "Examples:\n");
136     fprintf(stdout, "    tp1 foo\n");
137     fprintf(stdout, "    echo \"hello\" | tp1\n");
138 }
139
140 int sha1(unsigned char *resultado, char *bloques, unsigned long
141 long longitudOriginal)
142 {
143     long long int longitudRelleno = calcularRelleno(
144         longitudOriginal);
145     //preprocesamiento
146     long long int cantBloques = longitudRelleno/512; //longArchivo/
147         tamaño bloque    bloque = 512bits
148
149     ////procesar el bloque en 4 rondas de 20 pasos cada ronda
150     //la memoria temporal cuenta con 5 registros ABCDE
151     unsigned A=0x67452301;
152     unsigned B=0xEFCDAB89;
153     unsigned C=0x98BADCFE;
154     unsigned D=0x10325476;
155     unsigned E=0xC3D2E1F0;
156
157     //unsigned int trozos[80]; //big endian
158     unsigned int trozos[80]; // = malloc(80*sizeof(int));
159
160     // int indice = 0;
161     int i;
162     unsigned a = 0;
163     unsigned b = 0;
164     unsigned c = 0;
165     unsigned d = 0;
166     unsigned e = 0;
167
168     while(cantBloques--)
169     {
170         cargarTrozos(bloques, trozos);
171
172         a = A;
173         b = B;
174         c = C;
175         d = D;

```

```

171         e = E;
172
173         algoritmoSha1(trozos,&a,&b,&c,&d,&e);
174
175         A += a;
176         B += b;
177         C += c;
178         D += d;
179         E += e;
180
181     }
182
183     // hh = (h0 leftshift 128) or (h1 leftshift 96) or (h2
184         leftshift 64) or (h3 leftshift 32) or h4
185     for(i = 0;i<4;i++)
186     {
187         resultado[i] = (A>>(24-8*i));
188         resultado[i+4] = (B>>(24-8*i));
189         resultado[i+8] = (C>>(24-8*i));
190         resultado[i+12] = (D>>(24-8*i));
191         resultado[i+16] = (E>>(24-8*i));
192     }
193     return 0;
194 }
195
196 //un bloque tiene 64 bytes
197 void asignarDatos(FILE *fp, unsigned char *bloques,long long int
198     tamanioOriginal, long long int longitudRelleno)
199 {
200     // FILE *fp = fopen(file,"r");
201
202     char caracter;
203     int indice =0;
204     int i =0;
205     int cantBitsRelleno = 0;
206     char relleno = 0x80; //minimo relleno
207     char rellenoCero = 0x00;
208     unsigned mascara = 0x00000000000000FF;
209
210     while( (caracter =getc(fp)) != EOF)
211     {
212         *(bloques+indice) = caracter;
213         indice++;
214     }
215
216     cantBitsRelleno = (longitudRelleno - tamanioOriginal);
217     cantBitsRelleno = cantBitsRelleno - 64 - 8; //restamos 64 bits
218         de tamanio y los 8 bits basicos de relleno;
219     *(bloques+indice) = relleno;
220     indice++;
221
222     for(i = 0;i<(cantBitsRelleno/8);i++)
223     {
224         *(bloques+indice) = rellenoCero;
225         indice++;
226     }
227
228     for(i = 0;i<8;i++)
229     {
230         *(bloques+indice) = (tamanioOriginal>>(56-8*i)) & mascara;

```

```

230         indice++;
231     }
232 }
233 }
234
235 //devuelve el tamaño en bits
236 long long int calcularTamañoArchivo(char* nombreFile)
237 {
238     long long int tamaño =0;
239     FILE *fp = fopen(nombreFile, "r");
240     fseek(fp,0,SEEK_END);
241     tamaño = ftell(fp)*8;
242     return tamaño;
243 }
244
245
246 unsigned int leftrotate(unsigned int valor, int desplazamiento)
247 {
248     desplazamiento %=32;
249     unsigned retorno;
250     retorno = (valor << desplazamiento) | (valor >> (32 -
        desplazamiento));
251     return retorno;
252 }
253
254 void printVersion()
255 {
256     fprintf(stdout, "Copyright (c) 2015\n");
257     fprintf(stdout, "Conjunto de instrucciones MIPS. v1.0.0\n\n");
258 }
259
260 void printError(char* msgError, int codeError)
261 {
262     fprintf(stderr, "%s\n", msgError);
263     exit(codeError);
264 }
265
266 void showChecksum(unsigned char *result) {
267     int i;
268     for(i = 0; i < 20; i++) {
269         unsigned char aux = result[i];
270         aux<<=4;
271         aux>>=4;
272         printf("%x", (result[i]>>4));
273         printf("%x", aux);
274     }
275     printf("\n");
276 }
277
278 int readFromStdInput(int argumentCount) {
279     return (int)(argumentCount < 2);
280 }

```

../src/main.c

5.2. Código Fuente: relleno.S

```

1
2 #include <mips/regdef.h>
3
4     .text

```

```

5  .align 2
6
7  .globl calcularRelleno
8  .ent  calcularRelleno
9
10 calcularRelleno:
11  .frame $fp, 48, ra
12  .set noreorder
13  .cload t9
14  .set reorder
15  subu sp, sp, 48
16  .cprestore 0
17
18
19  sw ra, 44(sp)
20  sw $fp, 40(sp)
21  sw gp, 36(sp)
22  move $fp, sp
23
24  sw a0, 48($fp)
25  sw a1, 52($fp)
26  #sw a2, 56($fp)
27  #sw a3, 60($fp)
28
29  #obtencion del tamaño del relleno
30
31  #-----operaciones en 64 bits
32
33  li t0, 0
34  li t1, 0      #el tamaño debe venir en bits
35  move t0, a0   #t1|t0 = longArchivoRelleno
36  move t1, a1
37  li t4, 512
38
39  bucle_relleno:
40  remu t2, t0, t4  #calculo el valor de la longitud en modulo 512 (
41  resto)
42  beqz t2, fin_bucle_relleno #no es necesario considerar la parte
43  mas significativa
44  #suma de los 64 bits
45  addiu t2, t0, 8  #agrego 1 byte
46  sltu t3, t2, t0  #(t3 =1) de carry si el resultado es mas chico
47  que el sumando
48  move t0, t2      #volvamos el valor a t0
49  beqz t3, bucle_relleno
50  addiu t1, t1, 1   #sumamos 1 al la parte mas significativa
51  b bucle_relleno  #solucionar la suma en 64 bits
52
53  fin_bucle_relleno:
54  slti t2, t0, 65  #si t0<65 entonces t2 =1 y agregamos 512 bits
55  beqz t2, obtener_bloque
56  addiu t2, t0, 512 #agrega un bloque de 512 extra
57  sltu t3, t2, t0
58  move t0, t2
59  beqz t3, obtener_bloque #si no hay acarreo no sumar al mas
60  significativo
61  addiu t1, t1, 1   #t1|t0 = longArchivoRelleno
62
63  obtener_bloque:
64  sw t0, 16($fp)   #guardo la longitud relleno en 64 bits en el
65  stack

```

```

61 sw t1,20($fp)
62 sw a0,24($fp) #guardo la longitud original en 64 bits en el
   stack
63 sw a1,28($fp)
64
65 move v0,t0
66 move v1,t1
67
68 lw $fp, 40(sp)
69 lw ra, 44(sp)
70 lw gp, 36(sp)
71 addu sp, sp, 48
72
73 # Retorno.
74 #
75 j ra
76 .end calcularRelleno

```

../src/relleno.S

5.3. Código Fuente: trozo.S

```

1 #
2 #s0 puntero a bloques
3 #s1 puntero a trozos
4 #
5
6
7 #include <mips/regdef.h>
8
9 .text
10 .align 2
11
12 .globl cargarTrozos
13 .ent cargarTrozos
14
15 cargarTrozos:
16 .frame $fp, 48, ra
17 .set noreorder
18 .cpload t9
19 .set reorder
20 subu sp, sp, 40
21 .cprestore 0
22
23 sw gp,24(sp)
24 sw $fp,28(sp)
25 sw ra,32(sp)
26 move $fp, sp
27
28 #guardo los parametros con que vine #void cargarTrozos(char *
   bloques,int *indice,unsigned int *trozos)
29
30 sw a0, 40($fp) #ptero a bloques
31 sw a1, 44($fp) # ptero a trozos
32 sw a2, 48($fp) # nada
33 sw a3, 52($fp) # nada
34
35 #cargo los parametros
36 move s0,a0
37 move s1,a1
38

```

```

39 sw zero,16($fp)    # i=0
40 li t0,255          # mascara 0x000000ff
41 sw t0,20($fp)      #mascara en 28
42
43 FOR16PRIMEROS:
44 #traigo los datos
45 lw t0,16($fp)      #t0 cargo i
46 lw t5,20($fp)      #t5 = mascara
47
48 #comienzo
49
50 lbu t6,0(s0)        #t6 cargo el byte al que apunta (t4 = bloques +
                    # indice), lo carga de 0 a 7
51 and t6,t6,t5        #t6 con el and de la mascara, queda 00 00 00
                    ALGO
52 sll t6,t6,8         #lo muevo 8 lugares, quedaria 00 00 ALGO 00
53
54 addiu s0,s0,1        #(*(bloques+indice+1)
55 lbu t7,0(s0)        #t7 cargo el byte al que apunta (t4 = bloques +
                    # indice + 1), lo carga de 0 a 7
56 and t7,t7,t5        #t7 con el and de la mascara, queda 00 00 00
                    ALGO
57 or t6,t6,t7         #suma logica de t6 y t7, quedaria 00 00 ALGO ALGO
58 sll t6,t6,8         #muevo quedaria 00 ALGO ALGO 00
59
60 addiu s0,s0,1        #(*(bloques+indice+2) (ya habia sumado 1
                    # antes)
61 lbu t7,0(s0)        #t7 cargo el byte al que apunta (t4 = bloques +
                    # indice + 2), lo carga de 0 a 7
62 and t7,t7,t5        #t7 con el and de la mascara, queda 00 00 00
                    ALGO
63 or t6,t6,t7         #suma logica de t6 y t7, quedaria 00 ALGO ALGO
                    ALGO
64 sll t6,t6,8         #muevo quedaria ALGO ALGO ALGO 00
65
66 addiu s0,s0,1        #(*(bloques+indice+3) (ya habia sumado 1
                    # antes)
67 lbu t7,0(s0)        #t6 cargo el byte al que apunta (t4 = bloques +
                    # indice + 3), lo carga de 0 a 7
68 and t7,t7,t5        #t6 con el and de la mascara, queda 00 00 00
                    ALGO
69 or t6,t6,t7         #suma logica de t6 y t7, quedaria ALGO ALGO ALGO
                    ALGO
70
71 #GUARDO
72 sw t6, 0(s1)        #guardo t6 en (t2 = trozos + i*4)
73
74 #AUMENTO VARIABLES
75
76
77 addiu t0,t0,1        #i = i + 1
78 sw t0,16($fp)      #guardo
79
80 addiu s1,s1,4        # avanzo a la sig palabra
81 addiu s0,s0,1        # avanzo al sig byte
82
83 addiu t7,t0,-16
84 beqz t7,FOR16TO80
85
86 b FOR16PRIMEROS
87
88

```



```

89 FOR16TO80:
90     #traigo los datos
91     lw  t0,16($fp)    #t0 cargo i
92
93     addiu s1,s1,-12    #t3 apunta a trozos(i - 3).. 3 lugares = 4
94                     bytesx3 = 12 bytes
95     lw  t4,0(s1)      #t4 traigo la palabra a la q apunta t3
96     addiu s1,s1,12
97
98     addiu s1,s1,-32    #t5 apunta a trozos(i - 8)
99     lw  t6,0(s1)      #t6 traigo la palabra a la que apunta t5
100    addiu s1,s1,32
101
102    xor   t4,t4,t6      #t4 = *(trozos + (i-3)) ^ *(trozos + (i-8))
103
104    addiu s1,s1,-56    #t5 apunta a trozos(i - 14)
105    lw  t6,0(s1)      #t6 traigo la palabra a la que apunta t5
106    addiu s1,s1,56
107
108    xor   t4,t4,t6      #t4 = *(trozos + (i-3)) ^ *(trozos + (i-8)) ^
109                     *(trozos + (i-14))
110
111    addiu s1,s1,-64    #t5 apunta a trozos(i - 16)
112    lw  t6,0(s1)      #t6 traigo la palabra a la que apunta t5
113    addiu s1,s1,64
114
115    xor   t4,t4,t6      #t4 = *(trozos + (i-3)) ^ *(trozos + (i-8)) ^
116                     *(trozos + (i-14)) ^ *(trozos + (i-16));
117
118    rol  t4,t4,1        #leftrotate 1 Åi?
119
120    sw  t4,0(s1)        #guardo t4 en t2 = trozos + i*4 es decir apunta a
121                     trozos[i]
122
123    addiu t0,t0,1        #i = i + 1
124    sw  t0,16($fp)      #guardo
125    addiu s1,s1,4        #t2 = avanza a la siguiente palabra
126
127    addiu t7,t0,-80
128    beqz t7,FinDelFor
129
130    b FOR16TO80
131
132 FinDelFor:
133
134     lw  $fp,28(sp)
135     lw  ra, 32(sp)
136     lw  gp, 24(sp)
137     addu sp, sp, 40
138
139     # Retorno.
140     #
141     j  ra
142     .end  cargarTrozos

```

../src/trozo.S

5.4. Código Fuente: algoritmo.S

1 #

```

2  #a0 puntero a trozos
3  #a1 a
4  #a2 b
5  #a3 c
6  #a4 d
7  #a5 e
8  #
9
10
11
12 #include <mips/regdef.h>
13
14 .text
15 .align 2
16
17 .globl algoritmoSha1
18 .ent algoritmoSha1
19
20 algoritmoSha1:
21 .frame $fp, 48, ra
22 .set noreorder
23 .cload t9
24 .set reorder
25 subu sp, sp, 48
26 .cprestore 0
27
28
29 sw gp,32(sp)
30 sw $fp,36(sp)
31 sw ra,40(sp)
32 move $fp, sp
33
34 sw a0, 48($fp) # trozos
35 sw a1, 52($fp) # a
36 sw a2, 56($fp) # b
37 sw a3, 60($fp) # c
38
39 la t0,4(a3) # dir
40 la t1,8(a3) # dir
41
42 sw t0, 64($fp) # d
43 sw t1, 68($fp) # e
44
45
46 #-----algoritmo-----
47
48 #
49 #s2 = a
50 #s3 = b
51 #s4 = c
52 #s5 = d
53 #s6 = e
54 #s7 = f (funcion)
55 #
56 #carga variables en s0..s7
57
58 move s1,a0
59 lw s2,0(a1)
60 lw s3,0(a2)
61 lw s4,0(a3)
62 lw s5,4(a3)
63 lw s6,8(a3)

```

```

64
65 #inicializar i de vuelta
66 sw zero,16($fp) # i = 0
67 lw t6,16($fp) # traigo i, t6 = i
68
69 PROCESO0A19:
70 lw t6,16($fp) # traigo i, t6 = i
71 move s7,zero
72
73 and s7,s3,s4 #en f(s7) <— (b & c)
74 not t0,s3 #t0 niego b
75 and t1,t0,s5 #en t1 <— ((~b) & d)
76 xor s7,s7,t1 #f(s7) <— (b & c) ^ ((~b) & d)
77
78 lw t2,ctek1 #carga en t2, k1
79 sw t2,20($fp) #es donde esta k en el stack
80
81
82 jal ASIGNACIONTEMPORAL
83
84
85 addiu t6,t6,1
86 sw t6,16($fp)
87
88 addiu t7,t6,-20
89 beqz t7,PROCESO20A39
90
91 b PROCESO0A19
92
93
94 PROCESO20A39:
95 lw t6,16($fp) # traigo i, t6 = i
96 move s7,zero
97
98 xor s7,s3,s4 #f <— b ^ c
99 xor s7,s7,s5 #f <— b ^ c ^ d
100
101 lw t0,ctek2 #carga en t0, k2
102 sw t0,20($fp) #es donde esta k en el stack
103
104
105 jal ASIGNACIONTEMPORAL
106
107
108 addiu t6,t6,1
109 sw t6,16($fp)
110
111 addiu t7,t6,-40
112 beqz t7,PROCESO40A59
113
114 b PROCESO20A39
115
116 PROCESO40A59:
117 lw t6,16($fp) # traigo i, t6 = i
118 move s7,zero
119
120 and s7,s3,s4 #en f(s7) <— (b & c)
121 and t0,s3,s5 #en t0 <— (b & d)
122
123 or s7,s7,t0 #f <— (b & c) | (b & d)
124
125 and t0,s4,s5 #en t0 <— (c & d)

```

```

126 or s7,s7,t0 #f <— (b & c) | (b & d) | (c & d)
127
128
129 lw t0,ctek3 #carga en t0, k3
130 sw t0,20($fp) #es donde esta k en el stack
131
132
133 jal ASIGNACIONTEMPORAL
134
135
136 addiu t6,t6,1
137 sw t6,16($fp)
138
139 addiu t7,t6,-60
140 beqz t7,PROCESO60A79
141
142 b PROCESO40A59
143
144 PROCESO60A79:
145 lw t6,16($fp) # traigo i, t6 = i
146 move s7,zero
147
148 xor s7,s3,s4 #f <— b ^ c
149 xor s7,s7,s5 #f <— b ^ c ^ d
150
151 lw t0,ctek4 #carga en t0, k4
152 sw t0,20($fp) #es donde esta k en el stack
153
154
155 jal ASIGNACIONTEMPORAL
156
157 addiu t6,t6,1
158 sw t6,16($fp)
159
160 addiu t7,t6,-80
161 beqz t7,return_algoritmo
162
163 b PROCESO60A79
164
165
166 ASIGNACIONTEMPORAL:
167
168 #ESTO FINALIZA EL FOR DE 80 CON EL ALGORITMO PER SE
169
170 rol t0,s2,5 #en t0 leftrotate a 5
171 addu t0,t0,s7 #t0 = t0 + f
172 addu t0,t0,s6 #t0 = t0 + f + e
173 lw t1,20($fp) #t1 cargo k
174 addu t0,t0,t1 #t0 = t0 + f + e + k
175
176 lw t1,16($fp) #t1 cargo i
177 sll t2,t1,2 #t2 = i*4
178 addu t3,s1,t2 #t3 = trozos + i*4 es decir apunta a trozos[i]
179 lw t4,0(t3) #t4 traigo la palabra a la q apunta t3
180
181 addu t0,t0,t4 #t0 = t0 + f + e + k + trozos[i]
182
183 sw t0,24($fp) #guardo t0 en temp (24($fp))
184 #sw s5,0(s6) #e = d;
185 move s6,s5
186 #sw s4,0(s5) #d = c;
187 move s5,s4

```

```

188     rol s4,s3,30      #c = leftrotate(b ,30);
189     #sw s2,0(s3)      #b = a;
190     move s3,s2
191     #sw t0,0(s2)      #a = temp;
192     move s2,t0
193
194     #AUMENTO I
195     #addiu t1,t1,1     #i = i + 1
196     #sw t1,16($fp)    #guardo
197
198     jalr ra
199
200 return_algoritmo:
201 #-----FIN algoritmo
202
203
204     lw a0, 48($fp)    # trozos
205     lw a1, 52($fp)    # a
206     lw a2, 56($fp)    # b
207     lw a3, 60($fp)    # c
208     lw t6, 64($fp)    # d
209     lw t7, 68($fp)    # e
210
211     sw s2,0(a1)
212     sw s3,0(a2)
213     sw s4,0(a3)
214     sw s5,0(t6)
215     sw s6,0(t7)
216
217
218     lw $fp,36(sp)
219     lw ra, 40(sp)
220     lw gp, 32(sp)
221     addu sp, sp, 48
222
223     # Retorno.
224     #
225     j ra
226     .end algoritmoSha1
227
228
229
230     .data # comienza zona de datos
231
232     cteA: .word 0x67452301
233     cteB: .word 0xEFCDAB89
234     cteC: .word 0x98BADCFE
235     cteD: .word 0x10325476
236     cteE: .word 0xC3D2E1F0
237     ctek1: .word 0x5A827999;
238     ctek2: .word 0x6ED9EBA1;
239     ctek3: .word 0x8F1BBCDC;
240     ctek4: .word 0xCA62C1D6;

```

../src/algoritmo.S

5.5. Bibliografía

Referencias

- [1] *US Secure Hash Algorithm 1 (SHA1)*
<http://tools.ietf.org/html/rfc3174>
- [2] *SHA1 Message Digest Algorithm Overview*
<http://www.herongyang.com/Cryptography/SHA1-Message-Digest-Algorithm-Overview.html>
- [3] *SHA 1*
<http://en.wikipedia.org/wiki/SHA-1>
- [4] *MIPS Assembly Language Guide*
http://www.cs.uni.edu/~fienup/cs041s08/lectures/lec20_MIPS.pdf
- [5] *MIPS Instruction Reference*
<http://www.mrc.uidaho.edu/mrc/people/jff/digital/MIPSir.html>