Pontifícia Universidade Católica do Rio Grande do Sul
Teste e Confiabilidade de Sistemas
Professor Dr. Rafael Garibotti

Nome: Leonardo Pahim e Rafaella Doki
Turma: 590
Data de Entrega: 21/06/2020

CRYPT

1. Introdução

A proposta para este trabalho é a implementação de casos de testes para um algoritmo de criptografia, com uma entrada de 128 bits implementado a partir de 3 algoritmos(XTEA, AES e Blowfish).
Cabeçalho: void crypt (uint32_t* key, uint32_t* input, uint8_t type, uint8_t enc_dec, uint32_t* output).

key: Ponteiro para a chave criptográfica que pode ter 128-bits, 192-bits ou 256-bits;

Input: Mensagem a ser criptografada e que tem 128-bits, ponteiro;

Type: Indica qual versão do algoritmo é utilizado:

0 = XTEA;
1 = AES-128;
2 = AES-192;
3 = AES-256;
4 = BLOWFISH-128;
5 = BLOWFISH-192;
6 = BLOWFISH-256;

end_dec: Indica codificação ou decodificação:

0 = codificação (encoder)
1 = decodificação (decoder)

Output: Mensagem cifrada de 128-bits, e também é um ponteiro

Segue abaixo os links para código fonte no GIT e o teste no Travis:

- https://github.com/LeonardoPahim/Testes_TravisCI_TF
- https://www.travis-ci.com/github/LeonardoPahim/Testes_TravisCI_TF

2. Desenvolvimento

2.1. Casos de Teste

SUMÁRIO	
CONSTANTE	VALOR
input[4]	{0xA5A5A5A5L, 0x01234567L, 0xFEDCBA98L, 0x5A5A5A5AL}
key_4[4]	{0xDEADBEEFL, 0x01234567L, 0x89ABCDEFL, 0xDEADBEEFL}
key_6[6]	{0x3F72A512L, 0x2C937A9FL, 0xDEADBEEFL, 0xA5218F39EL, 0x3B4C26A6L, 0x01234567L, 0xA2376CFBL, 0xA25C3D7A0L}
key_8[8]	{0x3F72A512L, 0x2C937A9FL, 0xDEADBEEFL, 0xA5218F39EL, 0x3B4C26A6L, 0x01234567L, 0xA2376CFBL, 0xA25C3D7A0L}
XTEA_encoded[4]	{0x089975E9L, 0x2555F334L, 0xCE76E4F2L, 0x4D932AB3L}
AES_128_encoded[4]	{0x237549D4L, 0xCDCEA7BEL, 0x0FE7D162L, 0xCC9161D3L}
AES_192_encoded[4]	{0x5C69F75CL, 0x7BD3C3EBL, 0xAAD816BEL, 0xB05A9785L}
AES_256_encoded[4]	{0x2E3D06DDL, 0x333C7DC3L, 0x8FE99503L, 0x00EACE54L}
BLOWFISH_128_encoded[4]	{0x24B9C5E1L, 0xB06FBF71L, 0x5527E5FAL, 0x3502EE1AL}
BLOWFISH_192_encoded[4]	{0x57A73CF1L, 0xE9F5774EL, 0x9F46D5CFL, 0x8CF3A0C0L}
BLOWFISH_256_encoded[4]	{0x4D0B2FD6L, 0x9C5BEB43L, 0xD5857AB7L, 0x4882A23BL}
fail_message	"This test was meant to fail"

Número do Teste	NOME DO TESTE	CASOS DE TESTE
1	<XTEA_test_encoding>	[{input},{XTEA_encoded}]
2	<XTEA_test_decoding>	[{XTEA_encoded},{input}]
3	<AES_128_test_encoding>	[{input},{AES_128_encoded}]
4	<AES_128_test_decoding>	[{AES_128_encoded},{input}]
5	<AES_192_test_encoding>	[{input},{AES_192_encoded}]
6	<AES_192_test_decoding>	[{AES_192_encoded},{input}]
7	<AES_256_test_encoding>	[{input},{AES_256_encoded}]
8	<AES_256_test_decoding>	[{AES_256_encoded},{input}]
9	<BLOWFISH_128_test_encoding>	[{input},{BLOWFISH_128_encoded}]
10	<BLOWFISH_128_test_decoding>	[{BLOWFISH_128_encoded},{input}]
11	<BLOWFISH_192_test_encoding>	[{input},{BLOWFISH_192_encoded}]
12	<BLOWFISH_192_test_decoding>	[{BLOWFISH_192_encoded},{input}]
13	<BLOWFISH_256_test_encoding>	[{input},{BLOWFISH_256_encoded}]
14	<BLOWFISH_256_test_decoding>	[{BLOWFISH_256_encoded},{input}]
15	<AES_128_encoding_bad_input>	[{input},{AES_128_encoded}]
16	<BLOWFISH_128_encoding_bad_input>	[{input},{BLOWFISH_128_encoded}]
17	<AES_256_encoding_bad_type>	[{input},{AES_256_encoded}]
18	<AES_192_encoding_bad_type>	[{input},{AES_192_encoded}]
19	<AES_192_encoding_bad_key>	[{input},{AES_192_encoded}]
20	<BLOWFISH_256_decoding_bad_key>	[{input},{input}]
21	<XTEA_encoding_empty_key>	[{input},{input}]
22	<XTEA_decoding_empty_input>	[{input},{input}]
23	<AES_192_bad_enc_dec>	[{input},{AES_192_encoded}]
23	<BLOWFISH_128_bad_enc_dec>	[{input},{input}]

2.2. Casos de Teste das Classes de Valor Limite

CASOS DE TESTES DA CLASSE DE VALOR LIMITE	
VARIÁVEL DE ENTRADA	**SAÍDA**
KEY	
(key_6, local_input, 6, 1, output)	ERRO: key deveria ser de 256 e não de 192
(key_8, local_input, 5, 1, output)	ERRO: key deveria ser de 192 e não de 256
(key_8, local_input, 4, 1, output)	ERRO: key deveria ser de 128 e não de 256
INPUT	
(key_6, input3, 5, 1, output)	ERRO: input deveria ser de 128 e não de 64
TYPE	
(key_8, local_input, 2, 1, output)	ERRO: type 2 é AES-192 e não de 256 como esta na key
(key_6, local_input, 9, 1, output)	ERRO: type 9 não está declarado
ENC_DEC	
(key_4, local_input, 6, 3, output)	ERRO: enc_dec 3 não está declarado
OUTPUT	
(key_6, input_local, 5, 1, output3)	ERRO: output deveria ser de 128 e não de 64

2.3. Classes de Equivalência

CLASSES DE EQUIVALÊNCIA		
VARIÁVEL DE ENTRADA	**CLASSES DE EQUIVAÊNCIA VÁLIDAS**	**CLASSES DE EQUIVALÊNCIA INVÁLIDAS**
key	Ponteiro para chave criptográfica que pode ter 128-bits, 192-bits, 256-bits	key diferente de 128 bits
		key diferente de 192 bits
		key diferente de 256 bits
input	Ponteiro de 128-bits	Input diferente de 128 bits
type	Indica a versão do algoritmo que é utilizado, 0 = XTEA; 1 = AES-128; 2 = AES-192; 3 = AES-256; 4 = BLOWFISH-128; 5 = BLOWFISH-192; e 6 = BLOWFISH-256	Type tem que ser menor do que 0
		Type tem que ser maior do que 6
enc_dec	Indica codificação ou decodificação, onde 0 = decodificação e 1 = codificação	enc_dec diferente de 0
		enc_dec diferente de 1
output	Ponteiro de 128-bits	output diferente de 128 bits

3. Execuções

3.1. Execução do Valgrind com Memcheck

```
valgrind --leak-check=full --show-leak-kinds=all ./cov
==5342== Memcheck, a memory error detector
==5342== Copyright (C) 2002-2017, and GNU GPL'd, by Julian Seward et al.
==5342== Using Valgrind-3.13.0 and LibVEX; rerun with -h for copyright info
==5342== Command: ./cov
==5342==
test/CryptTest.c:74:XTEA_test_encoding:PASS
test/CryptTest.c:82:XTEA_test_decoding:PASS
test/CryptTest.c:89:AES_128_test_encoding:PASS
test/CryptTest.c:95:AES_128_test_decoding:PASS
test/CryptTest.c:104:AES_192_test_encoding:PASS
test/CryptTest.c:110:AES_192_test_decoding:PASS
test/CryptTest.c:119:AES_256_test_encoding:PASS
test/CryptTest.c:125:AES_256_test_decoding:PASS
test/CryptTest.c:134:BLOWFISH_128_test_encoding:PASS
test/CryptTest.c:140:BLOWFISH_128_test_decoding:PASS
test/CryptTest.c:149:BLOWFISH_192_test_encoding:PASS
test/CryptTest.c:155:BLOWFISH_192_test_decoding:PASS
test/CryptTest.c:164:BLOWFISH_256_test_encoding:PASS
test/CryptTest.c:170:BLOWFISH_256_test_decoding:PASS
test/CryptTest.c:266:BLOWFISH_128_encoding_bad_input:FAIL: Element 2 Expected 0x5527E5FA Was 0x742A21AE. This test was meant to fail
test/CryptTest.c:274:AES_256_encoding_bad_type:FAIL: Element 0 Expected 0x2E3D06DD Was 0xDE9AF90B. This test was meant to fail
test/CryptTest.c:291:AES_192_encoding_bad_key:FAIL: Element 0 Expected 0x5C69F75C Was 0x83B4A0AF. This test was meant to fail
test/CryptTest.c:299:BLOWFISH_256_decoding_bad_key:FAIL: Element 0 Expected 0xA5A5A5A5 Was 0x00F88848. This test was meant to fail
test/CryptTest.c:308:XTEA_encoding_empty_key:FAIL: Element 0 Expected 0xA5A5A5A5 Was 0x936DD794. This test was meant to fail
test/CryptTest.c:315:XTEA_decoding_empty_input:FAIL: Element 0 Expected 0xA5A5A5A5 Was 0xB6BA2612. This test was meant to fail
test/CryptTest.c:325:XTEA_decoding_bad_input:FAIL: Element 0 Expected 0xA5A5A5A5 Was 0xAB3225FD. This test was meant to fail
test/CryptTest.c:333:AES_192_bad_enc_dec:FAIL: Element 0 Expected 0x5C69F75C Was 0x7E73782C. This test was meant to fail
test/CryptTest.c:344:BLOWFISH_128_bad_enc_dec:FAIL: Element 0 Expected 0xA5A5A5A5 Was 0x607C9296. This test was meant to fail
==5342==
==5342== HEAP SUMMARY:
==5342==     in use at exit: 0 bytes in 0 blocks
==5342==   total heap usage: 42 allocs, 42 frees, 5,642 bytes allocated
==5342==
==5342== All heap blocks were freed -- no leaks are possible
==5342==
==5342== For counts of detected and suppressed errors, rerun with: -v
==5342== ERROR SUMMARY: 0 errors from 0 contexts (suppressed: 0 from 0)
```

3.2. Execução do Valgrind com Cachegrind

```
==5452==
==5452== I   refs:      12,884,590
==5452== I1  misses:         1,727
==5452== LLi misses:         1,674
==5452== I1  miss rate:       0.01%
==5452== LLi miss rate:       0.01%
==5452==
==5452== D   refs:       8,742,622  (6,231,081 rd   + 2,511,541 wr)
==5452== D1  misses:         5,152  (    3,998 rd   +     1,154 wr)
==5452== LLd misses:         3,543  (    2,591 rd   +       952 wr)
==5452== D1  miss rate:        0.1% (      0.1%     +       0.0%  )
==5452== LLd miss rate:        0.0% (      0.0%     +       0.0%  )
==5452==
==5452== LL refs:            6,879  (    5,725 rd   +     1,154 wr)
==5452== LL misses:          5,217  (    4,265 rd   +       952 wr)
==5452== LL miss rate:         0.0% (      0.0%     +       0.0%  )
```

3.3. Execução do Valgrind com Callgrind

```
==5542==
==5542== Events    : Ir
==5542== Collected : 12884587
==5542==
==5542== I   refs:      12,884,587
```

3.4. Execução do Valgrind com Massif

```
#Massif
valgrind --tool=massif ./cov -v
==5614== Massif, a heap profiler
==5614== Copyright (C) 2003-2017, and GNU GPL'd, by Nicholas Nethercote
==5614== Using Valgrind-3.13.0 and LibVEX; rerun with -h for copyright info
==5614== Command: ./cov -v
==5614==
test/CryptTest.c:74:XTEA_test_encoding:PASS
test/CryptTest.c:82:XTEA_test_decoding:PASS
test/CryptTest.c:89:AES_128_test_encoding:PASS
test/CryptTest.c:95:AES_128_test_decoding:PASS
test/CryptTest.c:104:AES_192_test_encoding:PASS
test/CryptTest.c:110:AES_192_test_decoding:PASS
test/CryptTest.c:119:AES_256_test_encoding:PASS
test/CryptTest.c:125:AES_256_test_decoding:PASS
test/CryptTest.c:134:BLOWFISH_128_test_encoding:PASS
test/CryptTest.c:140:BLOWFISH_128_test_decoding:PASS
test/CryptTest.c:149:BLOWFISH_192_test_encoding:PASS
test/CryptTest.c:155:BLOWFISH_192_test_decoding:PASS
test/CryptTest.c:164:BLOWFISH_256_test_encoding:PASS
test/CryptTest.c:170:BLOWFISH_256_test_decoding:PASS
test/CryptTest.c:266:BLOWFISH_128_encoding_bad_input:FAIL: Element 2 Expected 0x5527E5FA Was 0x742A21AE. This test was meant to fail
test/CryptTest.c:274:AES_256_encoding_bad_type:FAIL: Element 0 Expected 0x2E3D06DD Was 0xDE9AF90B. This test was meant to fail
test/CryptTest.c:291:AES_192_encoding_bad_key:FAIL: Element 0 Expected 0x5C69F75C Was 0x83B4A0AF. This test was meant to fail
test/CryptTest.c:299:BLOWFISH_256_decoding_bad_key:FAIL: Element 0 Expected 0xA5A5A5A5 Was 0x00F88848. This test was meant to fail
test/CryptTest.c:308:XTEA_encoding_empty_key:FAIL: Element 0 Expected 0xA5A5A5A5 Was 0x936DD794. This test was meant to fail
test/CryptTest.c:315:XTEA_decoding_empty_input:FAIL: Element 0 Expected 0xA5A5A5A5 Was 0xB6BA2612. This test was meant to fail
test/CryptTest.c:325:XTEA_decoding_bad_input:FAIL: Element 0 Expected 0xA5A5A5A5 Was 0xAB3225FD. This test was meant to fail
test/CryptTest.c:333:AES_192_bad_enc_dec:FAIL: Element 0 Expected 0x5C69F75C Was 0x7E73782C. This test was meant to fail
test/CryptTest.c:344:BLOWFISH_128_bad_enc_dec:FAIL: Element 0 Expected 0xA5A5A5A5 Was 0x607C9296. This test was meant to fail
==5614==
```

3.5. Execução do Valgrind com Helgrind

```
==5707== Helgrind, a thread error detector
==5707== Copyright (C) 2007-2017, and GNU GPL'd, by OpenWorks LLP et al.
==5707== Using Valgrind-3.13.0 and LibVEX; rerun with -h for copyright info
==5707== Command: ./cov -v
==5707==
test/CryptTest.c:74:XTEA_test_encoding:PASS
test/CryptTest.c:82:XTEA_test_decoding:PASS
test/CryptTest.c:89:AES_128_test_encoding:PASS
test/CryptTest.c:95:AES_128_test_decoding:PASS
test/CryptTest.c:104:AES_192_test_encoding:PASS
test/CryptTest.c:110:AES_192_test_decoding:PASS
test/CryptTest.c:119:AES_256_test_encoding:PASS
test/CryptTest.c:125:AES_256_test_decoding:PASS
test/CryptTest.c:134:BLOWFISH_128_test_encoding:PASS
test/CryptTest.c:140:BLOWFISH_128_test_decoding:PASS
test/CryptTest.c:149:BLOWFISH_192_test_encoding:PASS
test/CryptTest.c:155:BLOWFISH_192_test_decoding:PASS
test/CryptTest.c:164:BLOWFISH_256_test_encoding:PASS
test/CryptTest.c:170:BLOWFISH_256_test_decoding:PASS
test/CryptTest.c:266:BLOWFISH_128_encoding_bad_input:FAIL: Element 2 Expected 0x5527E5FA Was 0x742A21AE. This test was meant to fail
test/CryptTest.c:274:AES_256_encoding_bad_type:FAIL: Element 0 Expected 0x2E3D06DD Was 0xDE9AF90B. This test was meant to fail
test/CryptTest.c:291:AES_192_encoding_bad_key:FAIL: Element 0 Expected 0x5C69F75C Was 0x83B4A0AF. This test was meant to fail
test/CryptTest.c:299:BLOWFISH_256_decoding_bad_key:FAIL: Element 0 Expected 0xA5A5A5A5 Was 0x00F88848. This test was meant to fail
test/CryptTest.c:308:XTEA_encoding_empty_key:FAIL: Element 0 Expected 0xA5A5A5A5 Was 0x936DD794. This test was meant to fail
test/CryptTest.c:315:XTEA_decoding_empty_input:FAIL: Element 0 Expected 0xA5A5A5A5 Was 0xB6BA2612. This test was meant to fail
test/CryptTest.c:325:XTEA_decoding_bad_input:FAIL: Element 0 Expected 0xA5A5A5A5 Was 0xAB3225FD. This test was meant to fail
test/CryptTest.c:333:AES_192_bad_enc_dec:FAIL: Element 0 Expected 0x5C69F75C Was 0x7E73782C. This test was meant to fail
test/CryptTest.c:344:BLOWFISH_128_bad_enc_dec:FAIL: Element 0 Expected 0xA5A5A5A5 Was 0x607C9296. This test was meant to fail
==5707==
==5707== For counts of detected and suppressed errors, rerun with: -v
==5707== Use --history-level=approx or =none to gain increased speed, at
==5707== the cost of reduced accuracy of conflicting-access information
==5707== ERROR SUMMARY: 0 errors from 0 contexts (suppressed: 0 from 0)
```

3.6. Execução do cppcheck

```
cppcheck --enable=all --suppress=missingIncludeSystem src/blowfish.c src/crypt.c src/xtea.c src/aes.c
Checking src/aes.c ...
1/4 files checked 57% done
Checking src/blowfish.c ...
2/4 files checked 78% done
Checking src/crypt.c ...
3/4 files checked 86% done
Checking src/xtea.c ...
4/4 files checked 100% done
[src/crypt.c:16]: (style) The function 'crypt' is never used.
```

3.7. Execução do cov

Resultado do gcov (cobertura de código)

```
gcov -b crypt.c
File 'src/crypt.c'
Lines executed:90.00% of 10
Branches executed:100.00% of 8
Taken at least once:87.50% of 8
Calls executed:100.00% of 7
Creating 'crypt.c.gcov'

gcov -b blowfish.gcda
File 'src/blowfish.c'
Lines executed:100.00% of 80
Branches executed:100.00% of 20
Taken at least once:100.00% of 20
Calls executed:100.00% of 7
Creating 'blowfish.c.gcov'

gcov -b aes.gcda
File 'src/aes.c'
Lines executed:100.00% of 158
Branches executed:100.00% of 39
Taken at least once:100.00% of 39
Calls executed:100.00% of 59
Creating 'aes.c.gcov'

gcov -b xtea.gcda
File 'src/xtea.c'
Lines executed:100.00% of 31
Branches executed:100.00% of 8
Taken at least once:100.00% of 8
Calls executed:100.00% of 2
Creating 'xtea.c.gcov'
```