### **Hash functions**

**Submission deadline: 2023-04-09 23:59:59** 16655.332 sec

Evaluation: 5.0000

**Max. assessment:** 5.0000 (Without bonus points)

**Submissions:** 21 / 20 Free retries + 10 Penalized retries (-10 % penalty each retry)

**Advices:** 2 / 2 Advices for free + 2 Advices with a penalty (-10 % penalty each advice)

Your task is to implement a function (or set of functions, not the whole program) that finds **any** message whose hash (**SHA-512**) starts from the left on a sequence of zero bits.

The bit order is big-endian: Byte 0 from MSB to LSB, Byte 1 from MSB to LSB, ..., last byte from MSB to LSB.

For example, byte 0010 0111 (0x27) starts with a sequence of two zero bits.

The function is requested in two variants:

- basic solution (function findHash). Implementation of this function is mandatory.
- An enhanced solution (function findHashEx). Implementing this function is not compulsory, but the task will fail to compile without the supplied "dummy" implementation. Implement the function if you decide to pursue the bonus.

The parameters of the functions you implement are:

int findHash (int bits, char \*\* message, char \*\* hash)

- bits the desired number of zero bits in the message hash.
- message output parameter. This parameter contains the data for which the corresponding hash was found. The result is stored as your dynamically allocated hexadecimal C string (terminated by \0).
- hash output parameter. This is the hash of the message message from the previous parameter; again it is a dynamically allocated hexadecimal C string.
- The function's return value is 1 on success, 0 on failure or incorrect parameters. These are typically the required number of null bits, which makes no sense.

int findHashEx (int bits, char \*\* message, char \*\* hash, const char \* hashFunction)

- An extension to the findHash function. All parameters and return values remain the same as in the basic variant.
- hashFunction a new parameter that specifies which hash function should be used to find a sequence of null bits. The specified hash function name is compatible with the EVP\_get\_digestbyname function.

You don't have to worry about releasing dynamically allocated memory (message and hash, but only if the function succeeds). The test environment will ensure their correct release. However, all other memory work is up to you.

Submit a source file that contains the implementation of the requested findHash or findHashEx function. You can also add your other support functions that are called from findHash (or findHashEx) to the source file. The function will be called from the test environment, so strictly following the specified function interface is essential.

Use the code from the attached archive below as a basis for implementation. The sample contains a test function main; the values given are used in the basic test. Note that the header file insertion and the main function are wrapped in a conditional compilation block (#ifdef/#endif). Please leave the conditional translation blocks in the commit source file as well. Conditional translation will simplify your work. You can run and test the program when compiled on your machine. When compiling on Progtest, the main function and the header file insertion "disappear", i.e., it will not interfere with the header files and the main function of the test environment.

The sample also contains the checkHash function, which you will (quite probably) have to implement for your local testing. The function is wrapped in a conditional compilation block (=not tested). Still, it is helpful to implement it to verify the correctness of your solution.

### Notes:

- ATTENTION! A submitted assignment on Progtest does not guarantee a completed assignment! For more information, please get in touch with your tutor.
- You can use both C and C++ language resources in your implementation. From the STL library, only std::vector and std::string are available for this task.
- Do not add additional header files. The current list is more than sufficient. If you do decide to add other header files, inserting
  them will result in a compilation error.

Sample data:			Download
Submit:	Выберите файл	Файл не выбран	Submit



• Evaluator: computer

- · Program compiled
- Test 'Zakladni test podle ukazky': success
  - result: 100.00 %, required: 100.00 %
  - Total run time: 0.001 s (limit: 15.000 s)
  - Mandatory test success, evaluation: 100.00 %
- Test 'Test osetreni nespravnych vstupu': success
  - result: 100.00 %, required: 50.00 %
  - Total run time: 0.000 s (limit: 14.999 s)
  - Mandatory test success, evaluation: 100.00 %
- Test 'Test velkymi daty': success
  - result: 100.00 %, required: 50.00 %
  - Total run time: 2.379 s (limit: 14.999 s)
  - Mandatory test success, evaluation: 100.00 %
- Test 'Test nahodnymi daty + mem debugger': success
  - result: 100.00 %, required: 50.00 %
  - Total run time: 0.047 s (limit: 2.000 s)
  - Mandatory test success, evaluation: 100.00 %
- Test 'Bonus: Test osetreni nespravnych vstupu (vice hashovacich funkci)': success
  - result: 100.00 %, required: 100.00 %
  - Total run time: 0.001 s (limit: 1.000 s)
  - Optional test success, evaluation: 100.00 %
- Test 'Bonus: Test vice hashovacimi funkcemi': success
  - result: 100.00 %, required: 100.00 %
  - Total run time: 0.002 s (limit: 1.000 s)
  - Bonus test success, evaluation: 110.00 %
- Overall ratio: 110.00 % (= 1.00 \* 1.00 \* 1.00 \* 1.00 \* 1.00 \* 1.10)
- Total percent: 110.00 %
- Total points: 1.10 \* 5.00 = 5.50

			Total	Average	Maximum	Function name
SW metrics:		Functions:	7			
	SW metrics:	Lines of code:	72	10.29 ± 14.03	39	findHashEx
		Cyclomatic complexity:	33 4	.71 ± 6.09	17	findHashEx

21	2023-04-09 15:39:08	Download
Submission status:	Evaluated	
Evaluation:	4.5000	

## · Evaluator: computer

- Program compiled
- Test 'Basic test with example input data': success
  - result: 100.00 %, required: 100.00 %
  - Total run time: 0.001 s (limit: 15.000 s)
  - Mandatory test success, evaluation: 100.00 %
- Test 'Invalid input test': success
  - result: 100.00 %, required: 50.00 %
  - Total run time: 0.000 s (limit: 14.999 s)
  - Mandatory test success, evaluation: 100.00 %
- Test 'Big input test': success
  - result: 100.00 %, required: 50.00 %
  - Total run time: 2.493 s (limit: 14.999 s)
  - Mandatory test success, evaluation: 100.00 %
- Test 'Random test + mem debugger': success
  - result: 100.00 %, required: 50.00 %
  - Total run time: 0.024 s (limit: 2.000 s)
  - Mandatory test success, evaluation: 100.00 %
- Test 'Bonus: Invalid input test (more hash functions)': success
  - result: 100.00 %, required: 100.00 %
  - Total run time: 0.000 s (limit: 1.000 s)
  - Optional test success, evaluation: 100.00 %
- Test 'Bonus: More hash function test': failed
  - result: 28.57 %, required: 100.00 %
  - Total run time: 0.002 s (limit: 1.000 s)
  - Bonus test failed, evaluation: No bonus awarded
  - Failed (invalid output) [Unlock advice (55 B)]
  - Failed (invalid output) [Unlock advice (55 B)]
    Failed (invalid output) [Unlock advice (55 B)]

  - Failed (invalid output) [Unlock advice (55 B)]
  - Failed (invalid output) [Unlock advice (61 B)]
  - Failed (invalid output) [Unlock advice (58 B)] Failed (invalid output) [Unlock advice (61 B)]
  - Failed (invalid output) [Unlock advice (61 B)] Overall ratio: 100.00 % (= 1.00 \* 1.00 \* 1.00 \* 1.00 \* 1.00)

Advices used: 2

Penalty due to advices: None (2 <= 2 limit)</li>

Retries penalty: 10.00 % (= (21 - 20) \* 10 %)

Total percent: 90.00 % (= 1.00 \* 0.90)

Total points: 0.90 \* 5.00 = 4.50

Total Average Maximum Function name

Functions: 6 -- -- -- SW metrics:

Lines of code: **117 19.50**  $\pm$  **11.81 35** findHashEx

Cyclomatic complexity: 28  $4.67 \pm 2.36$  7 findHashEx

20 2023-04-09 15:37:30 Download

Submission status: Evaluated Evaluation: 0.0000

### • Evaluator: computer

Program compiled

• Test 'Basic test with example input data': success

• result: 100.00 %, required: 100.00 %

■ Total run time: 0.001 s (limit: 15.000 s)

■ Mandatory test success, evaluation: 100.00 %

• Test 'Invalid input test': success

result: 100.00 %, required: 50.00 %

■ Total run time: 0.000 s (limit: 14.999 s)

Mandatory test success, evaluation: 100.00 %

• Test 'Big input test': Abnormal program termination (Time limit exceeded)

Cumulative test time exceeded, killed after:: 15.002 s (limit: 14.999 s)

Mandatory test failed, evaluation: 0.00 %

Overall ratio: 0.00 % (= 1.00 \* 1.00 \* 0.00)

Advices used: 2

Penalty due to advices: None (2 <= 2 limit)</li>

Total percent: 0.00 %

• Total points: 0.00 \* 5.00 = 0.00

Total Average Maximum Function name

Functions: 6 -- -- -- SW metrics:

Lines of code: 117 19.50  $\pm$  11.81 35 findHashEx

Cyclomatic complexity: **28 4.67**  $\pm$  **2.36 7** findHashEx

19	2023-04-09 15:22:29	Download
Submission status:	Evaluated	
Evaluation:	5.0000	

### • Evaluator: computer

- Program compiled
- Test 'Basic test with example input data': success
  - result: 100.00 %, required: 100.00 %
  - Total run time: 0.001 s (limit: 15.000 s)
  - Mandatory test success, evaluation: 100.00 %
- Test 'Invalid input test': success
  - result: 100.00 %, required: 50.00 %
  - Total run time: 0.000 s (limit: 14.999 s)
  - Mandatory test success, evaluation: 100.00 %
- Test 'Big input test': success
  - result: 100.00 %, required: 50.00 %
  - Total run time: 5.340 s (limit: 14.999 s)
  - Mandatory test success, evaluation: 100.00 %
- Test 'Random test + mem debugger': success
  - result: 100.00 %, required: 50.00 %
  - Total run time: 0.049 s (limit: 2.000 s)
  - Mandatory test success, evaluation: 100.00 %
- Test 'Bonus: Invalid input test (more hash functions)': success
  - result: 100.00 %, required: 100.00 %
  - Total run time: 0.000 s (limit: 1.000 s)
  - Optional test success, evaluation: 100.00 %
- Test 'Bonus: More hash function test': failed
  - result: 28.57 %, required: 100.00 %
  - Total run time: 0.002 s (limit: 1.000 s)
  - Bonus test failed, evaluation: No bonus awarded
     Failed (invalid output) [Unlock advice (55 B)]
  - Failed (invalid output) [Unlock advice (55 B)]
  - Failed (invalid output) [Unlock advice (55 B)]

Failed (invalid output) [Unlock advice (55 B)]

- Failed (invalid output) [Unlock advice (61 B)]
  Failed (invalid output) [Unlock advice (58 B)]
- Failed (invalid output) [Unlock advice (61 B)]
- Failed (invalid output) [Unlock advice (61 B)] Overall ratio: 100.00 % (= 1.00 \* 1.00 \* 1.00 \* 1.00 \* 1.00)
- Advices used: 2
- Penalty due to advices: None (2 <= 2 limit)
- Total percent: 100.00 % Total points: 1.00 \* 5.00 = 5.00

Total Average Maximum Function name

**Functions:** 6 SW metrics:

Lines of code:  $117 19.50 \pm 11.81$ 35 findHashEx Cyclomatic complexity: 28  $4.67 \pm 2.36$ 7 findHashEx

2023-04-06 18:50:17 18 **Download** 

**Submission status: Evaluated Evaluation:** 0.0000

## · Evaluator: computer

- Program compiled
- Test 'Basic test with example input data': success
  - result: 100.00 %, required: 100.00 %
  - Total run time: 0.001 s (limit: 15.000 s)
  - Mandatory test success, evaluation: 100.00 %
- Test 'Invalid input test': success
  - result: 100.00 %, required: 50.00 %
  - Total run time: 0.000 s (limit: 14.999 s)
  - Mandatory test success, evaluation: 100.00 %
- Test 'Big input test': Abnormal program termination (Time limit exceeded)
  - Cumulative test time exceeded, killed after:: 15.004 s (limit: 14.999 s)
  - Mandatory test failed, evaluation: 0.00 %
- Overall ratio: 0.00 % (= 1.00 \* 1.00 \* 0.00)
- Advices used: 2
- Penalty due to advices: None (2 <= 2 limit)
- Total percent: 0.00 %
- Total points: 0.00 \* 5.00 = 0.00

Total Maximum Function name Average

**Functions:** 6 SW metrics:

Lines of code: 32 findHashEx 111  $18.50 \pm 10.56$ 

Cyclomatic complexity: 24  $4.00 \pm 2.00$ 7 main

17 2023-04-06 15:08:54 **Download** 

Submission status: **Evaluated Evaluation:** 0.0000

#### · Evaluator: computer

- Compile in 'pedantic' mode failed (10 % penalty). [Unlock advice (336 B)]
- Test 'Basic test with example input data': failed
  - result: 80.00 %, required: 100.00 %
  - Total run time: 0.001 s (limit: 15.000 s)
  - Mandatory test failed, evaluation: 0.00 %
  - Failed (invalid output) [Unlock advice (56 B)]
- Overall ratio: 0.00 %
- Advices used: 2
- Penalty due to advices: None (2 <= 2 limit)
- Total percent: 0.00 %
- Total points: 0.00 \* 5.00 = 0.00

Total Average Maximum Function name

**Functions:** 6 SW metrics:

Lines of code: 110  $18.33 \pm 10.39$ 32 findHashEx

Cyclomatic complexity: 24  $4.00 \pm 2.00$ 7 main

2023-04-05 17:33:33 16 Download

Submission status: **Evaluated**  Evaluation: 0.0000

### · Evaluator: computer

- Program compiled
- · Test 'Basic test with example input data': failed
  - result: 80.00 %, required: 100.00 %
    Total run time: 0.001 s (limit: 15.000 s)
    Mandatory test failed, evaluation: 0.00 %
  - Failed (invalid output) [Unlock advice (56 B)]
- o Overall ratio: 0.00 %
- Advices used: 2
- Penalty due to advices: None (2 <= 2 limit)
- Total percent: 0.00 %
- Total points: 0.00 \* 5.00 = 0.00

Total Average Maximum Function name

Functions: 6 -- -- -- SW metrics:

Lines of code: **117 19.50**  $\pm$  **9.98 32** findHashEx

Cyclomatic complexity: 28  $4.67 \pm 2.49$  9 main

 15
 2023-04-05 17:29:36
 Download

 Submission status:
 Evaluated

 Evaluation:
 0.0000

## • Evaluator: computer

- Program compiled
- o Test 'Basic test with example input data': failed
  - result: 80.00 %, required: 100.00 %
  - Total run time: 0.001 s (limit: 15.000 s)
  - Mandatory test failed, evaluation: 0.00 %
  - Failed (invalid output) [Unlock advice (56 B)]
- Overall ratio: 0.00 %
- Advices used: 2
- Penalty due to advices: None (2 <= 2 limit)</li>
- Total percent: 0.00 %
- Total points: 0.00 \* 5.00 = 0.00

Total Average Maximum Function name

Functions: 6 -- -- -- SW metrics:

Lines of code:  $117 19.50 \pm 9.98$  32 findHashEx

Cyclomatic complexity: **26 4.33**  $\pm$  **2.56 9** main

 14
 2023-04-05 16:59:04
 Download

 Submission status:
 Evaluated

 Evaluation:
 0.0000

#### · Evaluator: computer

- Program compiled
- Test 'Basic test with example input data': Abnormal program termination (Segmentation fault/Bus error/Memory limit exceeded/Stack limit exceeded)
  - Total run time: 0.010 s (limit: 15.000 s)
  - Mandatory test failed, evaluation: 0.00 %
- o Overall ratio: 0.00 %
- Advices used: 2
- Penalty due to advices: None (2 <= 2 limit)</li>
- Total percent: 0.00 %
- Total points: 0.00 \* 5.00 = 0.00

Total Average Maximum Function name

Functions: 6 -- -- -- SW metrics:

Lines of code: **113 18.83**  $\pm$  **9.99 32** findHashEx

Cyclomatic complexity: 24  $4.00 \pm 2.00$  7 main

13 2023-04-05 16:24:29 Download

Submission status: Evaluated

Evaluation: 0.0000

#### Evaluator: computer

· Program compiled

- Test 'Basic test with example input data': Abnormal program termination (Segmentation fault/Bus error/Memory limit exceeded/Stack limit exceeded)
  - Total run time: 0.012 s (limit: 15.000 s)
    Mandatory test failed, evaluation: 0.00 %
- Overall ratio: 0.00 %

Advices used: 2

Penalty due to advices: None (2 <= 2 limit)</li>

Total percent: 0.00 %

Total points: 0.00 \* 5.00 = 0.00

Total Average Maximum Function name

Functions: 6 -- -- -- SW metrics:

Lines of code: 113 18.83  $\pm$  9.99 32 findHashEx

Cyclomatic complexity: 24  $4.00 \pm 2.00$  7 main

12 2023-04-05 15:55:45 <u>Download</u>

Submission status:EvaluatedEvaluation:0.0000

#### · Evaluator: computer

Program compiled

- Test 'Basic test with example input data': Abnormal program termination (Segmentation fault/Bus error/Memory limit exceeded/Stack limit exceeded)
  - Total run time: 0.008 s (limit: 15.000 s)
    Mandatory test failed, evaluation: 0.00 %
- Overall ratio: 0.00 %
- Advices used: 2
- Penalty due to advices: None (2 <= 2 limit)</li>
- Total percent: 0.00 %
- Total points: 0.00 \* 5.00 = 0.00

Total Average Maximum Function name

Functions: 6 -- -- -- SW metrics:

Lines of code: **115 19.17**  $\pm$  **10.02 32** findHashEx

Cyclomatic complexity: 25  $4.17 \pm 2.48$  9 main

11 2023-04-05 15:47:03 Download

**Submission status:** Evaluated **Evaluation:** 0.0000

# • Evaluator: computer

- Program compiled
- Test 'Basic test with example input data': Abnormal program termination (Segmentation fault/Bus error/Memory limit exceeded/Stack limit exceeded)
  - Total run time: 0.010 s (limit: 15.000 s)
  - Mandatory test failed, evaluation: 0.00 %
- Overall ratio: 0.00 %
- Advices used: 2
- Penalty due to advices: None (2 <= 2 limit)</li>
- Total percent: 0.00 %
- Total points: 0.00 \* 5.00 = 0.00

Total Average Maximum Function name

Functions: 6 -- -- -- SW metrics:

Lines of code: **112 18.67**  $\pm$  **10.43 32** findHashEx

Cyclomatic complexity: 25  $4.17 \pm 2.48$  9 main

10 2023-04-05 15:45:45 <u>Download</u>

Submission status:EvaluatedEvaluation:0.0000

#### Evaluator: computer

- Compile in 'basic' mode failed. [Unlock advice (428 B)]
- Advices used: 2
- Penalty due to advices: None (2 <= 2 limit)
- Total percent: 0.00 %
- Total points: 0.00 \* 5.00 = 0.00

2023-04-03 13:19:01 **Download** 

Submission status: **Evaluated Evaluation:** 0.0000

### • Evaluator: computer

Program compiled

• Test 'Basic test with example input data': failed

• result: 80.00 %, required: 100.00 % Total run time: 0.001 s (limit: 15.000 s)

■ Mandatory test failed, evaluation: 0.00 %

Failed (invalid output) [Unlock advice (56 B)]

o Overall ratio: 0.00 %

Advices used: 2

Penalty due to advices: None (2 <= 2 limit)

Total percent: 0.00 %

Total points: 0.00 \* 5.00 = 0.00

Total Maximum Function name Average

**Functions:** 6 SW metrics:

Lines of code:  $119 19.83 \pm 10.49$ 32 findHashEx Cyclomatic complexity: 31  $5.17 \pm 3.58$ 11 checkHash t

R 2023-04-02 08:47:07 **Download** Submission status: **Evaluated** 0.0000 **Evaluation:** 

### · Evaluator: computer

Program compiled

Test 'Basic test with example input data': failed

result: 80.00 %, required: 100.00 %

■ Total run time: 0.001 s (limit: 15.000 s)

Mandatory test failed, evaluation: 0.00 %

Failed (invalid output) [Unlock advice (56 B)]

Overall ratio: 0.00 %

Advices used: 2

Penalty due to advices: None (2 <= 2 limit)

Total percent: 0.00 %

Total points: 0.00 \* 5.00 = 0.00

Total Average Maximum Function name

**Functions:** 6 SW metrics:

Lines of code: 141 23.50  $\pm$  7.34 32 findHashEx Cyclomatic complexity: 41  $6.83 \pm 3.58$ 11 checkHash

7 2023-04-02 08:46:02 **Download** Submission status: **Evaluated** 

#### · Evaluator: computer

**Evaluation:** 

Program compiled

Test 'Basic test with example input data': failed

result: 60.00 %, required: 100.00 %

Total run time: 0.001 s (limit: 15.000 s)

0.0000

Mandatory test failed, evaluation: 0.00 %

Failed (invalid output) [Unlock advice (56 B)]

Failed (invalid output) [Unlock advice (56 B)]

Overall ratio: 0.00 %

· Advices used: 2

Penalty due to advices: None (2 <= 2 limit)

Total percent: 0.00 %

Total points: 0.00 \* 5.00 = 0.00

Total Maximum Function name Average

**Functions:** 6 SW metrics:

Lines of code: 141 23.50  $\pm$  7.34 32 findHashEx

Cyclomatic complexity: 41  $6.83 \pm 3.58$ 11 checkHash 6 2023-04-02 08:45:14 **Download Submission status:** Evaluated **Evaluation:** 0.0000 • Evaluator: computer Program compiled • Test 'Basic test with example input data': failed result: 40.00 %, required: 100.00 % ■ Total run time: 0.001 s (limit: 15.000 s) ■ Mandatory test failed, evaluation: 0.00 % Failed (invalid output) [Unlock advice (56 B)] Failed (invalid output) [Unlock advice (56 B)] Failed (invalid output) [Unlock advice (56 B)] Overall ratio: 0.00 % Advices used: 2 Penalty due to advices: None (2 <= 2 limit) Total percent: 0.00 % Total points: 0.00 \* 5.00 = 0.00Total Maximum Function name Average **Functions:** -- --6 SW metrics: Lines of code:  $142\ 23.67 \pm 7.39$ 32 findHashEx Cyclomatic complexity: 42  $7.00 \pm 3.79$ 12 checkHash 2023-04-02 08:40:39 **Download Submission status:** Evaluated **Evaluation:** 0.0000 · Evaluator: computer Program compiled Test 'Basic test with example input data': failed • result: 60.00 %, required: 100.00 % ■ Total run time: 0.001 s (limit: 15.000 s) Mandatory test failed, evaluation: 0.00 % Failed (invalid output) [Unlock advice (56 B)] Failed (invalid output) [Unlock advice (56 B)] Overall ratio: 0.00 % Advices used: 2 Penalty due to advices: None (2 <= 2 limit) Total percent: 0.00 % Total points: 0.00 \* 5.00 = 0.00Total Maximum Function name Average **Functions:** 6 SW metrics: Lines of code: 32 findHashEx  $139 \ 23.17 \pm 7.31$ Cyclomatic complexity: 42  $7.00 \pm 3.79$ 12 checkHash 2023-04-02 08:32:40 **Download** Submission status: **Evaluated Evaluation:** 0.0000 · Evaluator: computer Program compiled • Test 'Basic test with example input data': failed result: 80.00 %, required: 100.00 % Total run time: 0.001 s (limit: 15.000 s) Mandatory test failed, evaluation: 0.00 % ☐ Failed (invalid output) o Overall ratio: 0.00 % Advices used: 1 Penalty due to advices: None (1 <= 2 limit) Total percent: 0.00 % Total points: 0.00 \* 5.00 = 0.00SW metrics: Total Average Maximum Function name **Functions:** 6 Lines of code: 141 23.50  $\pm$  7.34 32 findHashEx

Cyclomatic complexity:  $41 6.83 \pm 3.58$  11 checkHash

2	2023-04-02 08:30:15	Download
Submission status:	Evaluated	
Evaluation:	0.0000	
<ul> <li>Evaluator: compute</li> <li>Compile in</li> <li>Total percent: 0.00 %</li> <li>Total points: 0.00 * 5</li> </ul>	n 'basic' mode failed.	

1	2023-04-02 08:29:10	Download
Submission status:	Evaluated	
Evaluation:	0.0000	
<ul> <li>Evaluator: computer         <ul> <li>Compile in 'basic' mode failed. [Unlock advice (311 B)]</li> </ul> </li> <li>Total percent: 0.00 %</li> <li>Total points: 0.00 * 5.00 = 0.00</li> </ul>		