The WhibOx contest – edition 2

27 March 2019

www.cyber-crypt.com
CHES 2019 – CTF

• Goal: Design and break white-box implementation of AES-128
• Challenges as C code
• Start: 23.03.2019
• End: 21.08.2019

New in this edition:
• Bonus points for inversion of ciphertexts
• Efficiency of implementation is rewarded
Dashboard

15 Users!

2 Challenges!

1 / 1 Unbroken! / Uninverted!

2 / 0 Breaks! / Inversion!

Challenges

Challenges Ranking by Strawberry Scores

<table>
<thead>
<tr>
<th>Rank</th>
<th>id</th>
<th>Name</th>
<th>Peak</th>
<th>User</th>
<th>Status</th>
<th>Compiler</th>
<th>Performance</th>
<th>Publication Date</th>
<th>First Break / Inversion</th>
<th>Current</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>3</td>
<td>hopeful_liskov</td>
<td>11.98</td>
<td>Mugiwa</td>
<td>Standing</td>
<td>GCC</td>
<td>1.66</td>
<td>2019-03-23 15:34 UTC</td>
<td>-</td>
<td>11.98</td>
</tr>
<tr>
<td>2</td>
<td>14</td>
<td>goofy_archimedes</td>
<td>0.54</td>
<td>Yuri</td>
<td>Broken!</td>
<td>GCC</td>
<td>18.69</td>
<td>2019-03-25 21:33 UTC</td>
<td>2019-03-26 01:38 UTC</td>
<td>0.00</td>
</tr>
</tbody>
</table>
WhibOx – Edition 2

www.cyber-crypt.com/whibox-contest/