Practical demonstration of Bananb Target Collisions for Skein with NIST KAT files

Presented by
Danilo Gligoroski

Department of Telematics,
Faculty of Information Technology, Mathematics and Electrical Engineering
Norwegian University of Science and Technology - NTNU, NORWAY
Last year at CRYPTO 2010, Rump Session

Banana Attack

On Blue Midnight Wish by Gaëtan Leurent
Last year at CRYPTO 2010, Rump Session

Banana Attack
On Blue Midnight Wish by Gaëtan Leurent

This year on Rump Session

Bananb Attack
On Skein (and others)
Bananb Attack is a philosophical sibling to Banana Attack
Demonstration of Bananb Target Collisions for Skein with NIST KAT files

Message 1: ”Banana Attacks are crap”
Demonstration of Bananb Target Collisions for Skein with NIST KAT files

Message 1: "Banana Attacks are crap"

Message 2: "Banana Attacks are crap"
Demonstration of Bananb Target Collisions for Skein with NIST KAT files

Message 1: "h(s&@h3w%!Banana Attacks are crap"
Message 2: "h(s&@h3w%!Banana Attacks are craq"

Prepend a garbage
(computed by an undisclosed algorithm)
Demonstration of Bananb Target Collisions for Skein with NIST KAT files

Message 1: "h(s&@h3w%!Bananb Attacks are crap"
6828732640683377252142616E616E612041747461636B73206172652063726170
636B73206172652063726170

Message 2: "h(s&@h3w%!Bananb Attacks are craq"
6828732640683377252142616E616E612041747461636B73206172652063726171
636B73206172652063726171
Demonstration of Bananb Target Collisions for Skein with NIST KAT files

# ShortMsgKAT.txt
# Algorithm Name: Practical demonstration of Bananb Target Collisions for Skein with NIST KAT files
# Principal Submitter: Danilo Gligoroski for the Rump Session CRYPTO 2011

Len = 260
Msg = 6828732640683377252142616E616E612041747461636B73206172652063726170
MD = ??

Len = 260
Msg = 6828732640683377252142616E616E612041747461636B73206172652063726171
MD = ??

Produce a NIST KAT file
ShortMsgKAT.txt
**Demonstration of Bananb Target Collisions for Skein with NIST KAT files**

Compile and run genKAT256.exe provided in Skein submission package over ShortMsgKAT.txt and see the produced file ShortMsgKAT_256.txt
Demonstration of Bananb Target Collisions for Skein with NIST KAT files

# ShortMsgKAT_256.txt
# Algorithm Name: Practical demonstration of Bananb Target Collisions for Skein with NIST KAT files
# Principal Submitter: Danilo Gligoroski for the Rump Session CRYPTO 201

Len = 260
Msg = 6828732640683377252142616E616E612041747461636B73206172652063726170
MD = EBFEF527B76D55D886A5B91E64765274BFCAB9E78253F3411B4A0840CA5055D2

Len = 260
Msg = 6828732640683377252142616E616E612041747461636B73206172652063726170
MD = EBFEF527B76D55D886A5B91E64765274BFCAB9E78253F3411B4A0840CA5055D2
Why Skein, why not the other SHA-3 finalists?
Why Skein, why not the other SHA-3 finalists?

• Well, personally I could do BLAKE too, but I am not interested for the others

<table>
<thead>
<tr>
<th>64-bit mode, 512 bit hash</th>
<th>Speed cycles/byte</th>
</tr>
</thead>
<tbody>
<tr>
<td>skein512</td>
<td>7.83</td>
</tr>
<tr>
<td>blake512</td>
<td>7.94</td>
</tr>
<tr>
<td>sha512</td>
<td>11.67</td>
</tr>
<tr>
<td>keccakc512</td>
<td>12.84</td>
</tr>
<tr>
<td>jh512</td>
<td>13.70</td>
</tr>
<tr>
<td>groestl512</td>
<td>15.59</td>
</tr>
</tbody>
</table>
Thank you for your attention!