



Whitenoise Laboratories (Canada) Inc.

Contact: Andre Brisson

Email: abrisson@wnlabs.com

April 15, 2008

Vancouver, British Columbia, Canada

RSA Factoring Challenges Broken - NO WINNER for the \$100,000 Whitenoise Security Challenge

For years and years and years and years the pre-eminent security company RSA has been running [contests and challenges to factor RSA public encryption keys](#). Each RSA challenge key has been broken. The largest RSA key factored to date is 194 digits long or 663 bits in strength and required only five months to break.

The new RSA position is that [they do not believe in running contests any more](#) because “the industry has a considerably more advanced understanding of the cryptanalytic strength...” This is an interesting position after running contests for decades to validate their security. Perhaps this change in position is because the advancements in hardware, processing and factoring to break these keys has outstripped the strength of the keys. Pandemic global digital theft raises serious concerns about the current state of digital security.

Even RSA founder “[Adi Shamir pointed out in a message posted on the internet in November, that safety hangs by a fragile thread. All it would take is one particular advance in mathematics, or one tiny error in a computer chip, and the entire edifice of Internet commerce \(including online banking\) would come crashing down.](#)” **Keith Devlin, National Post**

Published: Tuesday, February 12, 2008

Whitenoise is a broadly [patented](#), new generation, symmetric key technology. In contrast to RSA public keys, the weakest Whitenoise key used in commercial products is [240,000 bits that generates random key streams greater than 10⁶⁰ bytes long](#). See slide 12.

The [\\$100,000 Whitenoise Security Challenge](#) took a page from our forebear RSA’s lead.

The contest and prize money were meant to challenge the bona fides of the security industry, security companies and cryptanalysts. It was also to validate that [Whitenoise cannot be broken](#).

In October 2007 Whitenoise issued the following challenge very publicly: [“the global community including any governments, security companies, universities, enterprises, security groups, black hat groups, hackers and consumers are challenged to compromise Whitenoise security.”](#)

Andre Brisson

Whitenoise Laboratories (Canada) Inc.

Business Development

Phone: 604-724-5094 Fax: 604-873-2467 1

Email: abrisson@wnlabs.com



Cryptography icons, cryptanalysts, leaders from the defense industry, academics and government officials were notified and publicly challenged. This challenge was further publicized broadly on the Internet and on security products sold through Office Depot.

[Whitenoise is not susceptible to factoring and brute force attacks](#) because of its architecture. As such the nature of the Whitenoise challenge is different than factoring RSA keys.

The [contest file](#) was a video encrypted with a very small portion of the Whitenoise [contest key](#). This key segment did not repeat and the key is significantly longer than the encrypted movie. In addition, Whitenoise tested completely [random](#) against the NIST test suite.

One million bytes of contest key stream were provided to all the institutions to provide them enough material to attempt to recreate the Whitenoise contest key and thereby decrypt the Whitenoise contest file and collect the \$100,000.

There was no winner of the \$100,000 Whitenoise Security Challenge. There were no submissions to collect this reward over the six month contest period despite the many registered institutions and contestants. Many thanks to [SCA Promotions](#) for sponsoring the contest.

Whitenoise Laboratories (Canada) Inc. is a Vancouver security company. Whitenoise sits on the [Advisory Committee](#) of the British Columbia Institute of Technology CST programs.