



NEWS RELEASE

CertainKey Inc.

Suite 4560 CTTC
1125 Colonel By Dr.
Ottawa ON
K1S 5B6
www.certainkey.com
(613) 263-2983
Editorial Contact: Jean-Luc Cooke

June 15, 2004

FOR IMMEDIATE RELEASE

Obsolete and Popular Banking Algorithm Gains New Foe

Ottawa – CertainKey Inc., as a supporter and implementer of strong encryption, is proud to announce that it will award \$10,000 to the first person or group to find a collision* in MD5, a 128-bit message digest (security algorithm) used by companies such as Bank of America, Citibank, Fleet Bank, eTrade.com USA, and eBay.com.

According to cryptography industry experts, the algorithm became obsolete in 1998, yet remains in use and leaves secure systems vulnerable to attack. With this award, CertainKey hopes to accelerate the adoption of more cryptographically secure algorithms to replace MD5 in all industry applications that relate to cryptography, and encourage public awareness of data security in general.

“Anyone with one hundred thousand dollars and a strong knowledge in the area could break the system at will. That so many people are using it could be dangerous; it reflects the need for greater awareness in everyone,” comments Jean-Luc Cooke, President of the company.

While groups of cryptographers often offer cash prizes for proving vulnerabilities in apparently secure algorithms, they are not generally as popular as MD5, which is the most widely used cryptographic algorithm in software today. This cash prize differs from others offered by security firms in that the target algorithm is in current use – other contests attempt to prove ineffective the algorithms no company or organization use to protect their sensitive information.

Currently in the lead is www.md5crk.com, a group (also lead by Cooke) which has developed a distributed supercomputer that ranks among the 500 largest computers in the world, by some measures. Anticipating continued steady network growth in light of the new reward, the shared computing project should have a duplicate “snowflake” created within the next two years.

Please see attached sheet, or visit www.certainkey.com, for award rules and more information.

- 30 -

*Collision in a hash algorithm occurs when two distinct inputs produce the same output. A suitable metaphor for such a collision is two different weather systems producing two perfectly identical snowflakes.

Official Rules

Award

CertainKey will give one award of \$10,000 CAD in a lump sum to the individual or group that discovers the first collision in the MD5 hash algorithm as defined by RFC 1321.

Only one award will be given. CertainKey will verify the validity of all submitted claims and the award will be paid for the first verifiable collision.

A valid claim must include the following:

1. A description of the hardware and software used to find the collision.
2. The date, time and time zone of the discovery.
3. Provide a single point of contact, including an e-mail address, postal address and phone number where CertainKey can contact the claimant regarding the claim. In the case of a group effort, the group must designate an individual with whom CertainKey will correspond.

Further:

1. Full disclosure is required and as such CertainKey requires that rights be given to freely publish the methods, algorithms, source code and detailed descriptions of hardware without undue restrictions or cost. This disclosure is designed to further cryptographic knowledge, specifically in designing effective hash algorithms.
2. Claims including the above information must be made via e-mail to md5@certainkey.com with the following subject: MD5 collision claim white list
3. Efforts to discover a collision may not be carried out in a malicious manner. Any person or persons engaged in activities not in the scientific spirit of the competition will be disqualified and lose any claim to the award.

CertainKey reserves the right to make changes to these rules for clarification, to remove ambiguity and correct errors.