NEWS RELEASE

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

February 17, 2004 FOR IMMEDIATE RELEASE

Popular, Yet Obsolete, Banking Algorithm Broken

Ottawa – CertainKey Inc., as a supporter and implementer of strong encryption, announced June 15, 2004 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 at the time 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. CertainKey does own or sell any proprietary competing algorithm to MD5.

In August 2004 Xuejia Lai, Xaioyun Wang, and Hongbo Yu of the Dept. of Computer Science and Engineering at Shanghai Jiaotong University in Shanghai, China demonstrated a new technique to find collisions in several common security algorithms, most notably MD5. Their new technique found MD5 collisions in minutes on a standard computer where previously it would have taken many years. Today they published their findings to CertainKey, fulfilling the final requirement in claiming the prize.

"As a side-effect of these new findings, a malicious person can now more easily masquerade as a financial institution, or any other online site. This trickery, often carried out by spammers and referred to as "phishing", is unfortunately becoming far more common and is usually done for the purposes of harvesting usernames and passwords," comments Jean-Luc Cooke, President of CertainKey Inc.

While companies and individuals have offered cash prizes for proving vulnerabilities in apparently secure algorithms, those algorithms are generally not as popular as MD5. MD5 is the most widely used cryptographic algorithm in software today. By targeting a popular, widely used algorithm, the CertainKey cash prize differs from others offered in the past that targeted old and rarely used algorithms.

Please see attached sheet, or visit www.certainkey.com, for award details 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 individuals with two perfectly identical fingerprints.

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.

Contact for CertainKey:
Jean-Luc Cooke, CEO
Email: jlcooke@certainkey.com
Phone: 1-613-263-2983

Contact for Award Winners:
Professor Xiaoyun Wang
Email: xywang@sdu.edu.cn
Address:
Department of Computer Science and Engineering
Shanghai Jiaotong University
1954 Hua Shan Road
Shanghai 200030, P.R. China