



INTELLIGENCE ARTICLES

Platinum Security Group Inc.
Crescent Building
850 N. Federal Highway
Stuart, FL
www.goargus.com

CHINESE CLAIM TO HAVE BROKEN U.S. CODE

Three Chinese cryptologists last month reported they had found a way to crack USG approved Secure Hash Algorithm-1, the Washington Times reported on 11 March.

The SHA-1 encryption is used widely within the USG, including DoD and the IC. It has been the Federal Information Processing Standard since 1994. SHA-1 is a security authentication device used to verify the integrity of digital media and ensure that data or messages, such as secure e-mail, are not changed during transmission.

Chinese researchers Xiaoyuan Wang, Yiqun Lisa Yin and Hongbo Yu reported in a paper dated 13 February that they had developed techniques effective for breaking SHA-1 without using time-consuming brute force attacks.

The National Institute of Standards and Technology said it could not confirm the Chinese code breaking but noted that the three researchers are reputable specialists with cryptographic expertise. NIST said the code breaking is of particular importance in digital signature applications, such as time-stamping, and notarization.

Due to advances in computing power, NIST said it plans to phase out SHA-1 in favor of the larger and stronger hash functions -- SHA-224, SHA-256, SHA-384 and SHA-512 -- by 2010.

Disclosure of the code breaking followed publication of a PRC defense white paper in December that identified the use of information technology as a central element of Chinese military doctrine. DoD officials say China believes its cyber-soldiers can successfully cripple the U.S. military by attacking key computer-run infrastructures and other information networks. (DKR)

###END###