

The RSA Security Breach:

Prepare for the possibility that the breach was a cover-up for the conclusive erosion of RSA intractability

Let AGS fit you with its universal Recovery Sticks!

On March 17, 2011 RSA warned its customers that its network had been breached and data had been stolen. Users of its SecurID authentication technology are 'at risk'.

The press release was expertly worded to de-sensationalize the story. "No big deal" just some unidentified data was compromised by some unknown hackers -- happens every day of the week. Consumers just have to be alert, that's all. In a world where 100 million Americans have been data-violated, this does not sound especially alarming.

Except that what was actually stolen is not clearly described, yet it appears as data that might help the thieves to fake the 40 millions RSA issued SecureID devices, guarding the privileged data of some 30,000 organizations. So from now on when we catch a hacker compromising a bank account, or a federal government secret by compromising an RSA secureID we will immediately point the fingers to the RSA data breach.

And that is what the people behind this breach may want you to think. To the experts who have been around the block once or twice, this smacks as the perfect cover for the most guarded secret in modern cryptography. So guarded that no one knows for sure, but the smart money is betting on the premise that China has developed an effective cryptanalysis of RSA, and probably of AES too. It's not a likely elegant math wizardry, it's probably a messy accelerated (Bayesian) brute-force, a hybrid of math insight, and fast computing -- a total capability to extract the RSA seed from a few output strings (that are in the open). It is this capability that the successful cryptanalysts so carefully guard. Because once it becomes known, (or strongly suspected) that the RSA intractability has eroded (we all know that it does erode, we just hope it does so slowly), then everyone will shift to ECC or other alternatives, and the hackers will have no advantage from their feat. In order to profit from their remarkable triumph to crack RSA, they need to keep everyone in the dark, and into believing that RSA is safe, and uncrackable.

There is no doubt that the intractability (security) of RSA and other short-key cipher systems is eroding daily. Also every day we grow more dependent on the same ciphers. We are headed towards a day of catastrophic proportions where a long serving cipher system, like RSA, will be clearly cracked and instantly unusable. When this day comes, cyberworld will be divided to those who have Recovery Sticks or their equivalent, and those who don't. Don't be penny wise and pound foolish -- inquire about AGS Recovery Sticks.

AGS Encryptions Ltd. is a noted cyber security firm, the providers of the only at-will intractability ciphersystem that can be used with variable security up to the mathematical unbreakability offered by One-Time-Pad (US Patent #6,823,068). AGS provides non-periodic pseudo-random bits, with any desired measured randomness, and is a security consultant to those who need to be guided by a carefully thought-out security strategy. We will tailor our Recovery Sticks to your needs.

We are confident that no other means in your cyber recovery arsenal is so effective, versatile, inexpensive, easy to use, a breeze to maintain, and the tool to be grateful for when your recovery is complete.

Let us give you an offer! Nancy@AGSEncryptions.com AGS Encryptions Ltd. Tel-Aviv, Israel * Washington DC, USA

