What Exactly Are the NSA's 'Groundbreaking Cryptanalytic Capabilities'?

The latest Snowden document is the US intelligence "black budget." There's a lot of information in the few pages the *Washington Post* decided to publish, including an introduction by Director of National Intelligence James Clapper. In it, he drops a tantalizing hint: "Also, we are investing in groundbreaking cryptanalytic capabilities to defeat adversarial cryptography and exploit internet traffic."

Honestly, I'm skeptical. Whatever the NSA has up its top-secret sleeves, the mathematics of cryptography will still be the most secure part of any encryption system. I worry a lot more about poorly designed cryptographic products, software bugs, bad passwords, companies that collaborate with the NSA to leak all or part of the keys, and insecure computers and networks.

Those are where the real vulnerabilities are, and where the NSA spends the bulk of its efforts.

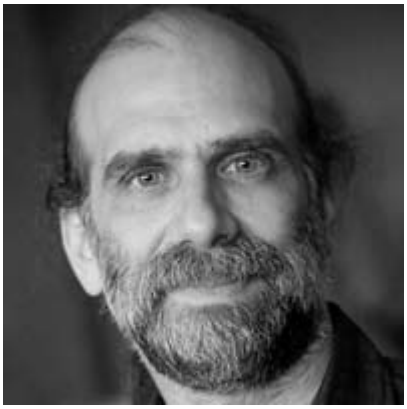
This isn't the first time we've heard this rumor. In a WIRED article last year, longtime NSA-watcher James Bamford wrote:

According to another top official also involved with the program, the NSA made an enormous breakthrough several years ago in its ability to cryptanalyze, or break, unfathomably complex encryption systems employed by not only governments around the world but also many average computer users in the US.

We have no further information from Clapper, Snowden, or this other source of Bamford's. But we can speculate.

Perhaps the NSA has some new mathematics that breaks one or more of the popular encryption algorithms: AES, Twofish, Serpent, triple-DES, Serpent. It wouldn't be the first time this happened. Back in the 1970s, the NSA knew of a cryptanalytic technique called "differential cryptanalysis" that was unknown in the academic world. That technique broke a variety of other academic and commercial algorithms that we all thought secure. We learned better in the early 1990s, and now design algorithms to be resistant to that technique.

It's very probable that the NSA has newer techniques that remain undiscovered in academia. Even so, such techniques are unlikely to result in a practical attack that can break actual encrypted plaintext.



Bruce Schneier

Bruce Schneier is a security technologist and author. His latestbook is *Liars and Outliers: Enabling the Trust Society Needs to Survive.*

READ MORE

The naive way to break an encryption algorithm is to brute-force the key. The complexity of that attack is 2^n, where *n* is the key length. All cryptanalytic attacks can be viewed as shortcuts to that method. And since the efficacy of a brute-force attack is a direct function of key length, these attacks effectively shorten the key. So if, for example, the best attack against DES has a complexity of 2^{39}, that effectively shortens DES's 56-bit key by 17 bits. That's a really good attack, by the way.

Right now the upper practical limit on brute force is somewhere under 80 bits. However, using that as a guide gives us some indication as to how good an attack has to be to break any of the modern algorithms. These days, encryption algorithms have, at a minimum, 128-bit keys.

That means any NSA cryptoanalytic breakthrough has to reduce the effective key length by at least 48 bits in order to be practical.

Whatever the NSA has up its top-secret sleeves, the mathematics of cryptography will still be the most secure part of any encryption system.

There's more, though. That DES attack requires an impractical 70 terabytes of known plaintext encrypted with the key we're trying to break. Other mathematical attacks require similar amounts of data. In order to be effective in decrypting actual operational traffic, the NSA needs an attack that can be executed with the known plaintext in a common MS-Word header: much, much less.

So while the NSA certainly has symmetric cryptanalysis capabilities that we in the academic world do not, converting that into practical attacks on the sorts of data it is likely to encounter seems so impossible as to be fanciful.

More likely is that the NSA has some mathematical breakthrough that affects one or more public-key algorithms. There are a lot of mathematical tricks involved in public-key cryptanalysis, and absolutely no theory that provides any limits on how powerful those tricks can be.

Breakthroughs in factoring have occurred regularly over the past several decades, allowing us to break ever-larger public keys. Much of the public-key cryptography we use today involves elliptic curves, something that is even more ripe for mathematical breakthroughs. It is not unreasonable to assume that the NSA has some techniques in this area that we in the academic world do not. Certainly the fact that the NSA is pushing elliptic-curve cryptography is some indication that it can break them more easily.

If we think that's the case, the fix is easy: increase the key lengths.

The NSA can make use of everything discovered and openly published by the academic world, as well as everything discovered by it in secret.

Assuming the hypothetical NSA breakthroughs don't totally break public-cryptography — and that's a very reasonable assumption— it's pretty easy to stay a few steps ahead of the NSA by using ever-longer keys. We're already trying to phase out 1024-bit RSA keys in favor of 2048-bit keys. Perhaps we need to jump even further ahead and consider 3072-bit keys. And maybe we should be even more paranoid about elliptic curves and use key lengths above 500 bits.

One last blue-sky possibility: a quantum computer. Quantum computers are still toys in the academic world, but have the theoretical ability to quickly break common public-key algorithms — regardless of key length — and to effectively halve the key length of any symmetric algorithm.

I think it extraordinarily unlikely that the NSA has built a quantum computer capable of performing the magnitude of calculation necessary to do this, but it's possible. The defense is easy, if annoying: stick with symmetric cryptography based on shared secrets, and use 256-bit keys.

There's a saying inside the NSA: "Cryptanalysis always gets better. It never gets worse." It's naive to assume that, in 2013, we have discovered all the mathematical breakthroughs in cryptography that can ever be discovered. There's a lot more out there, and there will be for centuries.

And the NSA is in a privileged position: It can make use of everything discovered and openly published by the academic world, as well as everything discovered by it in secret.

The NSA has a lot of people thinking about this problem full-time. According to the black budget summary, 35,000 people and $11 billion annually are part of the Department of Defense-wide Consolidated Cryptologic Program. Of that, 4 percent — or $440 million — goes to “Research and Technology.”

That’s an enormous amount of money; probably more than everyone else on the planet spends on cryptography research put together. I’m sure that leads to a lot of interesting — and occasionally groundbreaking — cryptanalytic research results, maybe some of it even practical.

Still, I trust the mathematics.

By Bruce Schneier 09 Apr 2013

Whatever the NSA has up its sleeves, it has a lot of people thinking about this problem full-time. ***Photo: Wikimedia Commons***