

Only Denial Encryption is Durably Secure

Encryption without Deniability Is Temporary Security At Best

Nothing is more private than your conversations with yourself. To put order in our own thoughts we tend to write them down, read them back, re-think, etc. Alas, the most thoughtful people among us, are reluctant to use this simple private exercise because in the United States everything is 'discoverable'. Once you put something in writing, any court in the land can grab it, expose it, and use it against you. No restrictions. Private diaries have embarrassed, shamed, and convicted many a victims whose only crime was to express a momentary thought, a politically incorrect sentiment, or a curious impulse that surged from the trash bin of their subconscious. And the chilling impact of this reality denies millions of law abiding Americans the simple pleasure to converse with themselves with impunity.

Encryption, which is the technology of making your writings readable only to those who have a "reading key" is only useful if you can deny that key from the people you don't want reading your stuff. If you are a whistleblower, sending incriminating messages to, say, an investigative journalist, you are about to be confronted by your employer with a simple ultimatum: if you don't release your encryption key, you will be released from your job. Court issued discovery orders routinely mandate encryption users to reveal their reading key, thereby neutralizing the question of how strong is that particular encryption.

Regular encryption by its very nature is a trap more than it is a sanctuary. When you send off an encrypted message you surrender its contents without any ability to backtrack or deny. It's like sending off your treasures in a locked box. Your treasures are in the hands of whoever holds this box. It may take him some time to break the lock, but you cannot prevent him from breaking it, nor can you yank your treasures out of his hands. All main stream encryption schemes are breakable, and their security hinges on the expected time it would take to break the lock. It's only a question of time. And if an employer, or judge can force you to hand over the key, the box will be opened forthwith, and your message therein will be fully exposed, denying you any option to say: this is not what the message means.

Everything you send off on the wire, or on wireless, any message that passes through a public channel, is likely scooped by various governments, and non government organizations, and it become a ticking bomb, counting down to full exposure of your private matters.

It's a feat of promotion, and advertising that this killer-fact has been clouded and obscured by the purveyors and vendors of encryption products and protocols. What is even more stunning is the fact that as early as 1917 an American by the name of Gilbert Vernam has secured a patent that resolves this modern encryption flaw. The Vernam cipher is fully deniable. That means that if your employer demands that you provide the key to your encrypted message, you can comply and give him an innocuous key that points to a harmless message that you supposedly sent -- not the real message that you sent over to that investigating journalist. And what's more, nobody can prove that you are misleading. Deniability is the ability to credibly tie in your encrypted message with a harmless plain message, and thereby avoiding the exposure of the true message you sent out. Encryption without deniability is like leaving your family treasures in a marked locked box, left on the street -- hoping the thieves will tire from picking the lock.

The 1917 Vernam cipher is cumbersome, and inconvenient to use. It's successor the "Denial Cryptography" cipher (US Patent 6,823,068) is easy, and convenient.

Check us out: <http://youdeny.com>

An [AGS Encryptions Ltd.](#) product