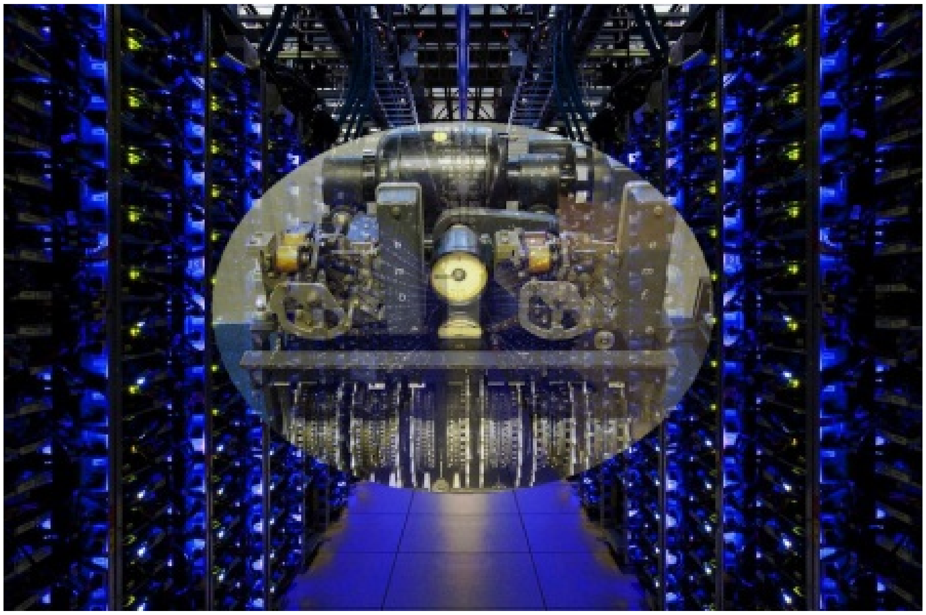
Dual Layer Encryption: A Proposal for Sidestepping Potential Backdoors

www.thelastbastille.com/2016/05/22/dual-layer-encryption-proposal-sidestepping-potential-backdoors/

*"How can we know whether someone has deliberately planted their own security hole in PGP? What if **the government** (pick any government) induced the PGP Corporation to insert a 'backdoor' that allows the police, FBI, KGB-reincarnated, et cetera to decrypt our messages and files with ease? The source code for various PGP versions is public. Expert computer programmers – definitely **not** employed by the PGP Corporation – can pounce on each new version and study the code carefully…[n]ot once has an alarm been raised that a deliberate weakness was inserted into PGP…[a]s a software test engineer, I must admit that code examination has its limits."*

– *David Ross*



Phil Zimmermann, the creator of Pretty Good Privacy, has repeatedly denied that his creation has any backdoors. Despite being investigated for three years by U.S. Customs for alleged export control violations, which he was cleared of, Zimmermann's PGP is feared by certain Americans to be compromised in some way, whether it be technologically by the NSA or by Zimmermann simply handing over such a backdoor to the federal government. Last time I checked, in *this* country there is such a thing as the presumption of innocence before being *proven* guilty, not the other way around; folks who care about strong cryptography ought to give Zimmermann the benefit of the doubt by taking him at his word.

As an advocate for PGP, I have encouraged people to learn about the history of PGP as well as how to configure it with their email clients. Most grumbling I've come across while assisting others set up PGP over the years usually stems from individuals who are reluctant to use email clients at all, because they enjoy the convenience that comes from using webmail they access via their chosen Internet browser. If they could, they'd prefer to spend Federal Reserve Notes on smartphone apps rather than spend 15 – 20 minutes downloading and using free and open-source software.

Yet, what if, on the off chance, the NSA inevitably will install their own backdoor, if they haven't already, given their cryptanalytic capabilities? Should that be the case, what then? One solution, I think, to that concern is what could be called dual encryption.

Three or four years ago, Gary Hunt expressed to me that he had no faith in the Internet being a secure haven for private communications, as he had expressed in his article, *How Dangerous is Internet Communication to Patriots?*. He then told me that he had conceived the idea of dual encryption. His idea was to blend high-tech with low-tech cryptography into a very practical high security tool. He never wrote about dual encryption because he figured that his idea would spread organically from peer-to-peer.

What is dual encryption? Simply defined, it is a form of multiple encryption whereby one layer of encryption is digital whereas another layer uses a classical cipher. Digital encryption would be something like PGP for email, OTR for instant messaging, or ZRTP for VoIP calls. By contrast, classical cryptography entails the use of transposition ciphers, substitution ciphers, one-time pads, or other readily available ciphers.

The purpose of dual encryption is to frustrate cryptanalysts by tricking them into believing that even if they managed to crack the digital encryption being used, it becomes a moot point simply because what they perceive to be a cracked plaintext is in fact the ciphertext for the next layer. As such, until they crack that next layer, the "plaintext" they have cracked will just be unintelligible garbage.

So, what would dual encryption look like in practice? If an original message's plaintext was something like:

meet me at the docks seven pm on march twenty-third

Then the first encryption layer would be to utilize a classical cipher; for this hypothetical scenario, I'll use the easily crackable Caesar cipher, shifted five spaces where A = E, just for the sake of demonstrating proof-of-concept (not for real information security, of course). The ciphertext would appear as:

Qiix qi ex xli hsgow wizir tq sr qevgl xairxc xlnvh

Of course, this first layer must not be done on a computer with an Internet connection, for purposes of INFOSEC; instead, it ought to be done using graph paper.

Next, the second encryption layer would be to send that ciphertext through a digitally encrypted medium. For this scenario, PGP will the used (**note**: the following is *not* the actual encrypted message, but was copied from a webpage, and is shown here for visually conceptual purposes only!):

Now, the recipient of this dual encrypted email will need to decrypt both layers in order to read the original plaintext message about where and when the rendezvous is to occur.

First, the PGP encrypted email will need to be decrypted using public-key cryptography; once that's done, then the recipient will see the ciphertext for the second decryption layer. Upon using the Caeser cipher correctly, he'll then learn the details of the meet up. Obviously, if the sender's original plaintext message can be read by the recipient, then the dual-layer encryption method has been used successfully by both parties.

To simplify the two layers on both the sender's (encryption) and recipient's (decryption) ends, here is how they are equivalent:

- Encrypt layer one = decrypt layer two (classical)
- Encrypt layer two = decrypt layer one (digital)

Naturally, everything the recipient does is what the sender did, except in reverse order. It could be argued that dual encryption increases the possibility of a honestly innocent mistake being made during either encryption by the sender or decryption by the recipient, thereby making the communication impossible, yet that is the risk you incur should you choose to use this method. If anything, that would be a selling point for why practicing dual encryption ought to be done *before* it's actually needed.

Additionally, if the "paper-and-pencil" classical cipher you end up choosing to use requires a key, then that key should be relayed through a non-digital communications medium, whether it be something like a landline telephone or a dead drop. Not only that, but overly frequent practicing might give your adversaries (such as the feds) the means to crack your cipher of choice. Therefore, only practice enough in order to assure that your working knowledge of your chosen cipher is accurate and functioning properly; be sure to **burn** all graph paper once you have finished practicing.

Dual encryption is a proposed solution to the possibility of a secret backdoor to any sort of digital encryption protocol, whether presently or in the future. Cryptanalytic white hats, as well as members of the American Cryptogram Association, are encouraged to see if they can discover any single points of failure or any other weaknesses in this method, and either share them in the comments section below or send me an email [PGP public key]. Any further developed proof-of-concept that shows dual encryption's viability better than I have done here would be sincerely appreciated.

-----BEGIN PGP MESSAGE-----
Charset: utf-8
Version: GnuPG v1

[illegible]

-----END PGP MESSAGE-----

Click the image to see it clearly.