



The necessary add-on device for any critical communication channel using DES, AES, or any certified and widely used ciphersystem.

The law of unintended consequences strikes again: The Federal Government and the published cryptographic community have undertaken the extra effort to test and then certify a handful of ciphersystems so that cryptography users would not end up using an easy-to-crack ciphersystem. Thoroughly testing a cipher is a tedious and a prolonged effort, and so very few algorithms get certified, and everyone ends up using the very same ones. (“Certified” does not mean “unbreakable” it means: “Nobody bragged about breaking it, although many tried”). This state of affairs creates a very tempting target for the best and brightest cryptanalysts in the world -- some of them are our mortal enemies, most of them work in the secrecy of their national cyberwar institutions. Cracking a certified cipher which is used everywhere on the Internet, and in the air, means reading virtually all our civil secrets, gaining a quiet, deeply concealed yet powerful competitive edge during peace time, and claiming unprecedented data-intrusion capabilities when hostilities break out. In the asymmetric war that we find ourselves in, breaking our certified ciphers is the proverbial equivalent to finding the "Lost Ark". And what's more: the only way for the code breakers to exploit their feat is by keeping their breakthrough top-secret, pooh-poohing even the suspicion that it happened.

Has it? Our guess is as good as yours. Is California due for 'the Big One'? Even if it is, there is not much we can do about it. But we can easily respond to the threat of a mathematical compromise of DES, or AES.

SECond-SECurity™ responds to this threat by installing an *in-series* ciphersystem that is far from the headlines, is scarcely used (and hence was not massively cryptanalyzed). It is intractable and lightning fast (**Daniel™**). In its base mode it derives its key from the key used for the mainstay ciphersystem, and it operates without any measurable deterioration of performance. For all practical purposes your channel will look the same, and operate the same. Once **Daniel™** is installed it requires no more attention, no maintenance (unless you wish to refresh it), and no administrative burden. Yet, by double encrypting your data with **Daniel™** you are fully protected against the risk of a stealth violation of your integrity. With **SEC-SEC™** you are no longer vulnerable to a deeply concealed compromise of the certified cipher you are using.

Contact: Dr. Gideon Samid, Gideon@agsencryptions.com