

Microcrypt Pro® Information Security Site
Encryption issues with regards to security

September 2005

Information regarding FIKO SOFTWARE “Microcrypt Pro” Information Security Site

The **National Security Agency** (“NSA”) - Meade MD, USA - is the official communications security body of the USA government. It was given its charter by President Truman in the early 50's, and has continued research in cryptography till the present time. NSA is known to be the largest employer of mathematicians in the world, handling most of the fastest and most advanced computers available. Governments in general have always been prime employers of cryptanalysts and are always ahead of others.

We often hear about “secure” encryption, but in fact unless you use 2048-bit encryption nothing is “secure”, but the main thing is not to be secure or not, it's all about to Encrypt or not to Encrypt. Don't fool yourself by thinking that US government would allow any 128-bit+ algorithms released that they wouldn't be able to crack in a reasonable timeframe. There are several rumours out there saying that NSA is the home to super-crypto computers that can crack any encryption methods available. We're not sure whom to believe, but our guesses are that the US Government can crack much more than most of us think and there is no such thing as absolute safety concerning cryptography. One lucky guess and the code are broken, right?

Today, for RSA (which is a public key algorithm, 512 bits is considered a very weak key. 1024 bits is considered standard while, 2048 bits is recommended to be safe for a while at least. However, even if a person uses Microsoft's CryptoAPI who says that Microsoft didn't leave a backdoor open in those libraries for the NSA? So no matter what kind of encryption you use, the most important is that you do encrypt your valuable data in addition to other security measurements you take, all to protect your network, privacy and most of all your valuable data. Microcrypt Pro is here to help people, companies and organisations to at least encrypt their data in a secure way. It has a smooth user interface and easy to use. Our encryption is based on our own Microcrypt technology so as long as people out there don't know how it works, it's “safe”, and even if they did know, only a handful of people and computers would be able to “crack” the key and open your files. Look at Microsoft Word and Adobe Acrobat reader, they are both offering encryption but because it's embedded with their products also “password cracks” is available even as freeware over the Internet. That's how far encryption goes, nothing is in reality “safe”.

So why is Microcrypt good? First of all, if the structure or algorithm of encryption used is subject to open source like i.e. TwoFish, where the cipher text (“a message written in a secret code”) is reversible into pure text, there is not much help in encryption. However if the encryption algorithm offers at least a second round of encryption using a different algorithm, the cipher text would be scrambled even further which again would throw any agency or hacker into (hard) work because all they get in the first round of decryption is just data that is still scrambled.

So no doubt, Microcrypt Pro is here to stay and our Microcrypt Pro Enterprise Edition (“MCP.EE”) will be released by October/November 2005, also containing several other security measurements for password-, login-, image- and server protection – just to mention few...