Theoretical reflections on the encoding of information with the program "Super Double Crypt"

Since centuries important information should be protected against foreign inspection. Already Herodot described in one of his scripts that the art of secret codes saved Greece from the invasion of the Persian king Xerxes.

In the modern times the good encryption of messages becomes more and more vital for companies and governments due to the electronic exchange of information. The main reason is that on the one side all information streams are very open to interested parties and on the other side powerful decryption tools in form of high speed computers are available nearly for anybody.

Looking at the data streams it is well known that all satellite based connections are under permanent inspection of the NSA of the USA. The same applies to the flow of e-mails which mainly is directed via American nodes. Open messages are inspected on the base of key words. This method allows the screening of huge information masses and the filtering out of interesting contents.

Having in mind, that the NSA has employed the biggest number of mathematicians of any other institution in the world and has installed the biggest computing power worldwide in form of various super computers, it is obvious for which purpose such an effort is maintained: the decryption of all collected information.

All existing encrypting methods have in common, that a data stream is encoded byte for byte with a more or less complex algorithm to achieve a secured file. The difference of the method is just the algorithm, but the one to one orientation from the open character to the encrypted one remains always the same. Here it can be assumed that the NSA is in possession of all existing algorithms.

Knowing also that a 56 bit key (7 bytes) was accepted by the NSA for the civil use, it must be realized that the existing computing power was able to decode an encrypted message with a known algorithm in a reasonable time.

The new invented encrypting method stops with the one to one conversion. By mixing up the encoded information with a white noise in various levels of the bit-structure, a further security is introduced. Besides the encrypting algorithm now also the position of the relevant character becomes part of the encoding philosophy. Even if the algorithm would be known, the position of the decoded byte remains a secret which only can be lifted by the knowledge of the correct key word. Furthermore there are two levels of encoding. In the first step, the information is condensed and encoded with the special packing software (like zip) and thereafter the real encoding is done as describe before, therefore "super **double** crypt" ! Out of this reason the encrypted message can even be shorter than the original, despite the fact, that about 50% white noise was sprinkled in.

In this respect all information encrypted with the Super Double Crypt cannot be decoded without the knowledge of the right key word!

But in case that the NSA comes also in possession of the new software, delivered by spies, the way of decoding a message can be found out by "try and error". Here three security measures can prevent an unwanted decryption of a secured message with a **short** key word:

1. Increase of the code word length to at least 10 characters or optimal 12 characters of 102 possible of a normal keyboard (decryption time for NSA 30 Mio. years for 12 characters).
2. Individualizing the software by changing the encryption method, because Super Double Crypt allows various ways of introducing white noise into the levels of the data stream.

The easiest way is the combination of 1. and 2. which gives a security far beyond any necessity.

With a key word length of **10** characters and the existence of an **utopistic** quantum computer - with a theoretical conversion time of 1ns (10^{-9} seconds) it would need about **3,865 years (three thousand eight hundred sixty five!)** to decode a message.

Because the software is based on just **one** key, there doesn't exist a super key which enables third parties to look into the encrypted information.

But any encryption software can contain a "Trojan Horse", even Super Double Crypt, if the programmer would be malicious.

That could be done as follows: One of the first characters of the noise header – which are always different – could point to the simple changed code word (for example a rotating shift right by one bit). Here the programmer could find the code word and would start a rotating shift left by one bit and could read out the code word. That can be prevented by the following procedure:

The source code of the program must be available. The inventor of the method must show the various steps of the conversion. Than it is proven that the code word never is incorporated into the codified data stream. Hereafter the same message is encrypted with the existing software in Visual Basic and will be compared with the encoded message of the root program. If no Trojan Horse is build in, both encoded message have to have the same length, the encoded characters have be on the same positions with the same code word and they must be decrypted reciprocal with the root - and the VB software.

With those measures – long key words and testing the software for Trojan Horses – any user of Super Double Crypt can be sure that no unauthorized person in the world is able to read the secured message now and in the future.

The inventor and programmer of Super Double Crypt, Prof. Dr. G.K. Brueck states here that the software contains no second key and no Trojan Horse and is generating encrypted files which are secured against any attack form any side, if the code word is at least of the length of 10 characters and contains besides characters also signs and symbols.

gkb, 8.8.2013