f1f733n! @ 15 @ fIFTEEN

@The Security of PGP@

f1F733n @ iShroom @ phifTEEN

In this paper we will discuss the feasibility of breaking Pretty Good Privacy-encrypted plain texts.(I assume that the reader is not entirely new to cryptography.) PGP is composed of four different cryptographic modules: the Pseudo-Randon number generator, the MD5 One-Way Hash, the IDEA symetric block cipher, and the RSA Public-key Algorithm. We will focus on the encryption ones: the IDEA algorithm, and the RSA algorithm.

IDEA IDEA was finished in 1992 by foreign cryptographers. It works with data hunks 64 bits in size. There have been no breakthroughs in the cracking of IDEA so far. The only known way of breaking IDEA is by brute force, or trying all possible keys. It is believed to be one of the most secure secret-key algorithms around. The key size of idea is 128 bits. On average, you must search through half of the keys to find the right one. That is 127 bits or 170,141,183,460,469,231,731,687,303,715,884,105,728 keys on average that you must search before the correct one is found. If all the computers in the world were devoted to this (if pancakes were sentient=) it would take more than the estimated lifespan of the universe to crack one IDEA key. All this could change of course, with the advent of quantum computers, but we will leave that aside for now.

RSA RSA was developed by Rivest, Shamir, and Adleman in the year of 1997. It was the first public-key cryptography known an available to the public, (GCHQ had it before, but it was top secret) and it is the main component of PGP. Public-key cryptography is the only cryptography algorithm that you can freely distribute your key in and not compromise your security. They say that the security of RSA depends on the difficulty of factoring very large prime numbers. So in this case, brute force would be the factorization of primes. Actually, this has never been proven, so there may be a way to get the secret key other than brute-force. To public knowledge today, however, there is no other way to attack the algorithm than brute-force. With a large enough key-space, RSA today is probably safe. There are other papers which discuss key-size, so we will skip this for now. To give an example, though, a 1024 bit key would take an estimated 3 * 10 E 7 years on a 75mhz VAX. Thats 30,000,000 years for those of you who need it in base-10.

Conclusion

If even one of PGP’s cryptographic modules is compromised, than the whole system is compromised. however, all of the pieces have been exstensively tested and subjected to public scrutiny and found to be secure. PGP is safe for today’s standards if you have a big enough key size. I personally use a 4096-bit key, but that is just my paranoia. If you would like to learn more about PGP or anything related to encryption, I reccomend you pick up a copy of Bruce Schiener’s Applied Cryptography.