

Pretty Good Privacy

Table of contents

1 Einführung.....	2
2 Mein öffentlicher Schlüssel.....	2

1. Einführung

[PGP](http://de.wikipedia.org/wiki/PGP) (<http://de.wikipedia.org/wiki/PGP>) ist ein asymmetrische Verschlüsselungsverfahren, d.h. es gibt zwei verschiedene Schlüssel, einen privaten und einen öffentlichen Schlüssel. [PGP](http://de.wikipedia.org/wiki/PGP) (<http://de.wikipedia.org/wiki/PGP>) wird hauptsächlich für die Verschlüsselung von Nachrichten, also E-Mails benutzt. Die PGP-Verschlüsselung gilt als ausreichend sicher, d.h. der [NSA](http://de.wikipedia.org/wiki/NSA) (<http://de.wikipedia.org/wiki/NSA>) oder andere Geheimdienste müssen etliche Stunden [Supercomputer](http://de.wikipedia.org/wiki/Supercomputer) (<http://de.wikipedia.org/wiki/Supercomputer>) rechnen lassen, um die Nachricht zu entschlüsseln.

2. Mein öffentlicher Schlüssel

Wenn Du mir eine geheime Nachricht schicken willst musst Du die Nachricht mit meinem öffentlichen Schlüssel verschlüsseln. Dann kann nur ich die Nachricht entschlüsseln. Zusätzlich kannst Du die Nachricht noch mit deinem privaten Schlüssel verschlüsseln, damit ist zusätzlich gesichert, dass die Nachricht wirklich von Dir kommt.

[PGP-Key](http://stuff.fts-online.de/FrankSommer.asc) (<http://stuff.fts-online.de/FrankSommer.asc>)