**Einleitung**

Wir reden Heute über das Thema PGP

Wir haben die Präsentation in folgende Bereiche geteilt:

Zuerst kommt ein kurzer Steckbrief

Dann reden wir darüber Wofür wir Sicherheit überhaupt brauchen

Nach dem erzählen wir euch etwas über die Geschichte und entstehung von PGP

* Eigenschaften
* OpenPGP

**Steckbrief**

**Wofür braucht man Sicherheit**

Vor der Erfindung von Computern musste die Regierung Briefe aufwendig mit Wasserdampf aufmachen. Mit dem häufigeren Nutzen von Online Nachrichten musste die Regierung einfach deine Nachrichten Abfangen.

Im Gegensatz zu dem Brief öffnen kann man Nachrichten in großen maße abfangen.

Man kann Heutzutage auch jedes Gesräch mithören und bei bestimmten Keywords schlägt dann ein Algorythmus Alarm, sodass diese Personen genauer unter die Lupe genommen werden.

Selbst der bravste Bürger will seine Geheimnisse keinem Fremden erzählen, deswegen braucehn wir Sicherheit und Datenschutz.

**Geschichte**

Viele begeisterte Freiwillige tippten dann den Code vom Buch ab und flugs stand der Code der Weltgemeinschaft in digitaler Form (PGPi) zur Kompilierung zur Verfügung. Denn die Regierung war nicht in der Lage den Export von Büchern zu verbieten.

PGP Verschlüsselung durfte damals nicht ohne Lizenz exportiert werden. Sie unterlag, wie der Waffenhandel, dem US-Exportgesetz

Das liegt daran das die eingesetzten, komplexen Verschlüsselungsalgorithmen nicht einmal durch den amerikanischen Geheimdienst geknackt werden konnten. Deswegen wollten sie den Export der PGP Verschlüsselung verhindern.

**Eigenschaften**

Dabei wird die eigentliche Nachricht auf die einfachere symmetrische Weise verschlüsselt, aber der verwendete Schlüssel erfährt die komplexere asymmetrische Verschlüsselung. Es wird bei diesem Verfahren also jedes Mal gemäß Zufallsprinzip ein neuer symmetrischer Schlüssel, der Session Key, erzeugt.

und dann an die Nachricht angehängt. Auf diese Weise kann die Nachricht völlig problemlos gleichzeitig für mehrere Empfänger verschlüsselt werden

Alle Nachrichten werden an einen bestimmten Empfänger mit seinem öffentlichen Schlüssel verschlüsselt werden, um schließlich nur mit dessen privatem Schlüssel wieder entschlüsselt werden zu können

**OpenPGP**

OpenPGP ist ein nicht proprietäres Protokoll

PGP und später OpenPGP sind zum Standard aller E-Mails Verschlüsselungen geworden