

Das Public Key - Verfahren

Kommunikationspartner A hat 2 Schlüssel, Kommunikationspartner B hat 2 Schlüssel; diese werden mit einem Programm erzeugt.

Der erste Schlüssel ist der *geheime Schlüssel* (private key), der unter allen Umständen geheim gehalten werden muss. Die geheimen Schlüssel bezeichnen wir mit A-g und B-g. Der zweite Schlüssel ist der *öffentliche Schlüssel* (public key), der möglichst breit verteilt werden soll (mindestens A ↔ B). Wir bezeichnen die öffentlichen Schlüssel mit A-ö und B-ö.

Wichtig sind nun die folgenden Punkte:

- Aus dem öffentlichen Schlüssel ist der geheime Schlüssel nicht berechenbar.
- Was mit dem öffentlichen Schlüssel verschlüsselt wurde, ist nur mit dem dazugehörigen geheimen Schlüssel wieder zu entschlüsseln.
- Was mit dem geheimen Schlüssel verschlüsselt wurde, ist nur mit dem zugehörigen öffentlichen Schlüssel wieder zu entschlüsseln.

Damit können elektronische Dokumente verschlüsselt werden.

Verschlüsselung

Angenommen, A will B eine verschlüsselte E-Mail zukommen lassen. Dazu verschlüsselt A die E-Mail mit B-ö, dem öffentlichen Schlüssel von B. Die Nachricht ist nun nicht mehr im Klartext lesbar. Nur B kann diese Nachricht wieder entschlüsseln, da nur er im Besitz von B-g, dem geheimen Schlüssel, ist.

