Sicherheit

Wie funktioniert die 128 bit- Verschluesselung beim Internet Banking ?

Sicherheit im Internet wird **durch Verschlüsselung der übertragenen Daten** gewährleistet. Um die Daten zu verschlüsseln, werden Verschlüsselungsalgorithmen und verschiedene Verschlüsselungsverfahren (symmetrisch, asymmetrisch) benutzt.

Ein **Verschlüsselungsalgorithmus verwandelt** mit Hilfe eines besonderen Schlüssels einen **Klartext in einen unlesbaren chiffrierten Text** (Verschlüsselung), was auf gleiche Weise wieder rückgängig gemacht werden kann (Entschlüsselung).
Bei einem symmetrischen (oder konventionellen) Verschlüsselungsverfahren läßt sich im Gegensatz zu asymmetrischen Verfahren der zum Verschlüsseln benutzte Schlüssel aus demjenigen zum Entschlüsseln berechnen (und umgekehrt).

Asymmetrische (oder Public Key) Verschlüsselungsverfahren benutzen im Gegensatz zu symmetrischen Verfahren zwei verschiedene Schlüssel zum Ent- und Verschlüsseln, wobei sich der eine nicht aus dem anderen ermitteln läßt.

Die in den **Standardprodukten** verwendeten Verschlüsselungsalgorithmen, zum Beispiel RSA (asymmetrisches Verfahren) oder IDEA (symmetrisches Verfahren), sind als solche sicher.
Diese **Sicherheit** ist natürlich **nur bei entsprechender Schlüssellänge gegeben**, also vorzugsweise 1024 Bits oder mehr bei RSA und 128 Bits bei IDEA. Da Public-Key-Verfahren im Vergleich zu symmetrischen Algorithmen extrem langsam sind und unter bestimmten Umständen kann mit der sog. "Chosen-Plaintext-Attack", die ursprüngliche Nachricht ermittelt werden.

Um die Vorteile der Public-Key-Verfahren zu erhalten, und die höhere Geschwindigkeit der symmetrischen Algorithmen zu nutzen, **kombiniert man symmetrische und asymmetrische** Verfahren zu **hybriden Verschlüsselungsverfahren**.

Bei diesem Verfahren wird **für eine Nachricht ein zufälliger Schlüssel** (sogenannter **Session Key**) mit einem symmetrischen Verfahren erzeugt. Mit diesem Schlüssel wird anschließend die Nachricht verschlüsselt. Dieser Schlüssel wird dann mit einem Public-Key-Verfahren verschlüsselt und der verschlüsselten Nachricht angefügt. Dieses Verfahren wird zwischen Webbrowser und Webserver angewendet, wenn die Nachrichten mittels SSL verschlüsselt über HTTPS zu übertragen.

Die Schlüssellänge von SSL beträgt 128 Bit. **Eine mit dem SSL-Verfahren gesicherte Verbindung** wird im Programm Netscape Navigator/Communicator **durch ein geschlossenes Schloss** in der **linken unteren Ecke des Browserfensters angezeigt**.

Beim Microsoft Internet Explorer wird eine SSL-Verbindung auch durch ein geschlossenes Schloss am **unteren rechten Rand des Browserfensters**

angezeigt.

Eindeutige ID: #1327
Verfasser: Database3
Letzte Änderung: 2005-11-07 17:26