Schutzziele der Informationssicherheit

Vertraulichkeit

Das offensichtlichste Ziel der Kryptographie ist **Vertraulichkeit**: Alice und Bob wollen über einen usiocheren Kanal miteinander kommunizieren, ohne dass ein Angreifer wie Eve die Inhalte ihrer Nachrichten lesen kann.

Dieses Ziel wird durch **Verschlüsselung** erreicht. Daten, die ohne besondere Entschlüsselungsmethoden gelesen werden können, werden *Klartext* genannt. Das Verfahren zum Chiffrieren von Klartext, so dass dessen Inhalt unerkannt bleibt, wird Verschlüsselung genannt.

Verschlüsseln von Klartext ergibt ein unleserliches Zeichengewirr, das dann Verschlüsselungstext oder *Chiffrat*, manchmal auch *Geheimtext* genannt wird. Mit der Verschlüsselung bleiben Informationen unbefugten Personen verborgen, selbst wenn ihnen die Daten im verschlüsselten Zustand vorliegen. Das Verfahren des Zurückführens von chiffriertem Text in den ursprünglichen Klartext wird als Entschlüsselung bezeichnet.

Integrität

Das zweite Schutzziel der IT-Sicherheit, das durch Kryptographie erreicht werden soll, ist es, die **Integrität** von Daten sicherzustellen. Dabei soll verhindert werden, dass Daten bei der Übermittlung zwischen Alice und Bob **verändert** werden können. Diese Daten können verschlüsselt sein, das ist jedoch nicht unbedingt notwendig. Es ist auch denkbar, dass Daten im Klartext übermittelt werden, aber dennoch sichergestellt werden soll, dass sie während es Kommunikationsvorgangs nicht verändert werden.

Authentizität

Ein weiteres wesentliches Schutzziel, das nicht sofort einsichtig ist, ist die Authentizität. Die Frage, die hier beantwortet werden soll ist, wie sichergestellt werden kann, dass Alice tatsächlich mit Bob kommuniziert und nicht beispielsweise von Beginn der Kommunikation an mit Eve.

Aufgaben

1. Übernimm das Schema oben auf dieser Seite in dein Heft und ergänze an passender Stelle die kryptologischen Fachbegriffe, die du bis jetzt gelernt hast.
2. Erläutere die drei Ziele der Kryptographie (**Vertraulichkeit, Authentizität, Integrität**).
3. Bewerte die beiden dir bisher bekannten kryptographischen Verfahren im Hinblick auf die drei Ziele.