Damit Geheimes geheim bleibt ...

Das einzig sichere System ...

Bereits mit dem Auftreten der Schriftsprache ergab sich die Notwendigkeit für die Anwender (Fürsten , Pharaonen und Kirchenfürsten) beim Transport ihrer Nachrichten , die Kenntnisnahme der Nachricht durch Unberechtigte (Boten , Räuber) auszuschließen.

Seit dieser Zeit wird mehr oder weniger wirkungsvoll c h i f f r i e r t .

Nur *Chiffrierung* macht aus dem Inhalt (Klartext) der Nachricht ein für den Unberechtigten scheinbar regelloses Kauderwelsch , den Geheimtext .

Dieses Kauderwelsch , das der unberechtigte Dritte nun Lesen darf , ohne daß sich ihm der Inhalt erschließt , kann nun per Bote , als Drahttelegramm oder Funkspruch / Telefonat übertragen werden . Jeder Unberechtigte kann sich nun in Besitz der chiffrierten Nachricht bringen , ohne daß er zum klartextlichen Inhalt der Nachricht vordringen kann .

Die eben abgefangene (chiffrierte) Nachricht ist aber für den Unberechtigten nun wertlos geworden, weil er keinen Zugang zum Inhalt hat.

Beginnt nun der unberechtigte Angreifer mit mathematischen Methoden zum Klartext der abgefangenen Nachricht vordringen zu wollen, dann ist die für die Ermittlung des Klartextes benötigte Zeit , die Zeit , in der die Nachricht sicher ist , abhängig von folgenden Eigenschaften :

- **von der Vielzahl der Deutungsmöglichkeiten des Geheimtextes,**
- **von der Vielzahl der Möglichkeiten einer Schlüsseleinstellung ,**
- **von der Regellosigkeit / der Zufälligkeit des Schlüssels.**

Ein eindrucksvolles Beispiel :
Ein Chiffriersystem hat eine Möglichkeit der Einstellung eines 10- stelligen dekadischen Schlüssels . Von dem 10- stelligen Schlüssel wissen nur Sie und Ihr Gesprächspartner. Der Unberechtigte Dritte mit einem Computer , der 1.000 Schlüsseleinstellungen pro Sekunde durchspielen kann, benötigt im Durchschnitt über 0,5 Jahre, um zum Klartext Ihrer Verbindung zu gelangen. Bei einem 12-stelligen Schlüssel benötigt dieser Computer schon über 30 Jahre.
Die heutigen praktischen nationalen Verhältnisse und technischen Möglichkeiten gehen aber davon aus , daß der sogenannte 64-bit Standard-Schlüssel mit einem Schlüsselraum von 10^{19} Möglichkeiten und auf diese Entschlüsselungsaufgabe konzentrierte Rechnerleistung sicher allen Angriffsversuchen ca. 10 Tagen widersteht (sogenannte taktische Sicherheit).

Die führenden Mathematiker der ganzen Welt waren und sind sich darin einig : Jeder vom Menschen konstruierte oder programmierte (Pseudo-) Zufalls-generator ist unsicher. *Absolute Sicherheit* in Cryptosystemen geben nur durch echte Zufallsgeneratoren generierte Folgen.

Die führenden Mathematiker der ganzen Welt waren und sind sich auch darin einig : nur Derjenige , der Kenntnis des Schlüssels besitzt, kann auch in Echtzeit den Klartext / Inhalt bestimmen.

Grundsätze der Sicherheit von Nachrichten

0. **Unverschlüsselte (offene) Verbindungen können von jedermann und jederzeit entlang der Leitung vom Sender bis zum Empfänger abgehört werden.**

1. **Höchste Sicherheit einer Verbindung ist dann gegeben, wenn es sich um eine durchgängige verschlüsselte Verbindung vom Teilnehmer A (Sender) zum Teilnehmer B (Empfänger)handelt (Ende zu Ende Chiffrierung)**

2. **Höchste Sicherheit einer Verbindung ist dann gegeben, wenn nur die Teilnehmer A und B Kenntnis des Schlüssels besitzen.**

3. **Höchste Sicherheit einer Verbindung ist dann gegeben, wenn die Schlüssel von einem echten Zufallsgenerator erzeugt werden und nur jeweils einmal für Teilnehmer A und B erzeugt werden.**

4. **Höchste Sicherheit einer Verbindung ist dann gegeben, wenn die Schlüssel nach bestimmter , nur den Teilnehmern A und B bekannten , regelloser Ordnung verändert werden (Schlüsselwechsel) .**

5. **Höchste Sicherheit einer Verbindung ist dann gegeben , wenn der sogenannte Schlüsselraum des benutzten Verfahrens (Länge des Schlüssels) möglichst groß ist.**

6. **Höchste Sicherheit einer Verbindung ist dann gegeben , wenn nach der Benutzung der Chiffrierverbindung der benutzte Schlüssel im Gerät nicht rekonstruierbar ist .**

7. **Sogenannter Komfort *(automat. Schlüssel*einstellung, - wechsel , Laut-sprechen ...) wirkt sich immer gravierend negativ auf die Sicherheit der Verbindung aus.**

Das INS bietet einfach bedienbare Ende – zu Ende Chiffriergeräte mit hoher , höchster und garantierter Sicherheit