1.2 Allgemeine Diskussion der Bitstrom-Verschlüsselung

Vorteile

- Der Verschlüsselungsalgorithmus und der Entschlüsselungsalgorithmus sind identisch, ...
- ... extrem einfach ...
- ... und sehr schnell – vorausgesetzt die Schlüsselfolge ist schon vorhanden. Für hohe Datenübertragungsraten kann man evtl. den Schlüsselbitstrom auf beiden Seiten vorherberechnen.
- Bei gut gewählter Schlüsselerzeugung ist sehr hohe Sicherheit möglich.

Nachteile

- Das Verfahren ist anfällig gegen Klartextraten; jedes erratene Klartextbit ergibt ein Schlüsselbit.
- Die Qualität der Schlüsselfolge ist sehr kritisch.
- Es gibt keine Diffusion – bei Blockchiffren war das ein sehr wichtiges Kriterium.
- Der Angreifer kann bei bekanntem Klartextstück das entsprechende Schlüsselstück ermitteln und dann den Klartext beliebig austauschen – z. B. „ich liebe dich“ durch „ich hasse dich“ ersetzen oder einen Geldbetrag von 1000 auf 9999 ändern.

Im Zusammenhang mit dem ersten Punkt hat der gewöhnliche Zeichensatz für Texte eine systematische Schwachstelle: Die Kleinbuchstaben `a..z` beginnen im 8-Bit-Code alle mit `011`, die Großbuchstaben `A..Z` alle mit `010`. Eine vermutete Folge von sechs Kleinbuchstaben enthüllt 6*3 = 18 Schlüsselbits.

[Das Auftreten vieler Nullen in den Leitbits der Bytes ist übrigens ein sehr wichtiges Erkennungsmerkmal für natürlichsprachigen Text in europäischen Sprachen.]

Kryptographische Sicherheit von Zufallsgeneratoren

Die entscheidende Frage an eine Pseudozufallsfolge bzw. an den sie erzeugenden Zufallsgenerator ist:

> Kann man aus einem bekannten (auch fragmentierten) Stück der Folge weitere Bits – vorwärts oder rückwärts – bestimmen?

Die Antwort für die „klassischen“, in statistischen Anwendungen und Simulationen verwendeten Zufallsgeneratoren wird JA sein. Wir werden aber auch Zufallsgeneratoren kennen lernen, die in diesem Sinne – vermutlich – kryptographisch sicher sind.