Kryptografie und -analyse, Zusammenfassung Vorlesung 3

Henry Haustein

Wie funktionieren Transpositionen, MM-Substitutionen und PM-Substitutionen?

Transposition = Vertauschen der Zeichen des Klartextes
MM-Substitutionen (monoalphabetisch, monographisch): ein Buchstabe des Klartextes wird mit einem Buchstaben ersetzt. Die Buchstaben zu denen ersetzt wird kommen aus einem Alphabet ⇒ eineindeutige Zuordnung PM-Substitutionen (polyalphabetisch, monographisch): wie MM-Substitutionen, nur dass die Buchstaben zu denen ersetzt wird, aus mehreren Alphabeten kommen ⇒ eindeutige Zuordnung

Was sind Ansätze zur Analyse dieser Verfahren?

Da die statistischen Eigenschaften der Klartexte erhalten bleiben (zumindest bei MM-Substitutionen und Transpositionen), versucht man über diese, wieder an die Klartexte heranzukommen.

Wie wird bei der Analyse von PM-Substitutionen, in denen der Schlüssel periodisch wiederholt wird, vorgegangen?

Zuerst muss die Schlüssellänge bestimmt werden, z.B. mit dem Kasiski-Test oder Friedman-Test. Danach kann man den Schlüsseltext in Blöcke unterteilen, die mit dem selben Schlüssel verschlüsselt worden sind. Innerhalb dieser Blöcke findet nur eine MM-Substitution statt, diese kann man knacken.

Wie werden statistische Charakteristika von Klartexten in natürlichen Sprachen durch die Verschlüsselung mit klassischen Verfahren beeinflusst?

Die Häufigkeiten der Buchstaben, Digramme und Trigramme bleiben erhalten bei MM-Substitutionen.