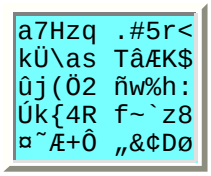
Kryptologie

Die polygraphische Substitution



Es werden jeweils *l*-Gramme von Buchstaben gemeinsam verschlüsselt.

Bigraphische Substitution

Buchstabenpaare (Bigramme) werden gemeinsam verschlüsselt. Die Chiffre wird am besten durch ein großes Quadrat (Seitenlänge $n = \#\Sigma$) beschrieben, das auch als Schlüssel dient.

Beispiel für das Standard-Alphabet:

	a	**b**	**c**	**d**	**...**
a	CA	FN	BL	...	...
b	SK	WM	...	...	...
c	HP	...	...	...	...
d	...	...	...	...	...
...	...	...	...	...	...

Das historisch älteste Beispiel stammt von Porta 1563. Seine Bigramm-Tafel hatte allerdings, dem Geschmack der Zeit folgend, als Geheimtextzeichen geheimnisvolle Symbole. Ein Bild ist hier zu sehen.

Eigenschaften

1. Der Schlüsselraum ist (maximal) die Menge aller Permutationen $\mathbf{S}(\Sigma^2)$, hat also $n^2!$ Elemente. Die effektive Schlüssellänge ist

$$d(F) \;=\; {}^2\log(n^2!) \approx n^2 \cdot {}^2\log(n^2) = 2\, n^2 \cdot {}^2\log(n).$$

Im Falle $n = 26$ ist das ungefähr 4500. Vollständige Schlüsselsuche ist außerhalb jeder denkbaren Rechenleistung.

2. Im Vergleich zur monalphabetischen (und monographischen) Substitution ist die Häufigkeitsverteilung der Einzelbuchstaben verschleiert. Eine statistische Analyse muss auf Bigramm-Häufigkeiten zurückgreifen und ist entsprechend schwieriger. Mustersuche und Suche nach wahrscheinlichen Wörtern sind allerdings vergleichsweise wenig erschwert; auch allgemeinere Angriffe mit bekanntem Klartext sind durchführbar.

3. Polygraphische Substitutionen (für *l*-Gramme) lassen sich auch als monoalphabetische Substitutionen deuten, nämlich über dem Alphabet $\Sigma^{\sim} = \Sigma^l$. Je größer *l* ist, desto mehr wird die Kryptoanalyse erschwert. Für die *allgemeine* polygraphische Substitution wächst der Aufwand zur

Beschreibung des Schlüssels allerdings wie n^l, also exponentiell in l; sie ist daher nur mit einem eingeschränkten Schlüsselraum realistisch verwendbar. Man braucht also eine Klasse von Substitutionen $\Sigma^l \to \Sigma^l$, die einfacher als durch die vollständie Wertetafel mit n^l Einträgen beschrieben werden.

Ein (bigraphisches) Beispiel dafür ist die PLAYFAIR-Chiffre.

4. Polygraphische Substitutionen sind die Vorläufer der modernen Block-Chiffren.

Autor: Klaus Pommerening, 3. November 1999; letzte Änderung: 11. Februar 2000.

E-Mail an Pommerening@imsd.uni-mainz.de.