Criptanaliza Criptosistemului $S(26)$

Să presupunem că plaintextul este un text peste alfabetul $\{A, B, \ldots, Z\}$ (de exemplu, un text în limba engleză în care, am păstrat literele mari, am convertit literele mici în litere mari şi am eliminat toate celelalte simboluri (cifrele, spaţiile, virgulele, punctele etc.)) şi că vom folosi, de exemplu, cheia π specificată în tabelul următor:

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N

Criptotextul va fi obţinut înlocuind peste tot în plaintext 'A' cu 'O', 'B' cu 'P', ..., 'Y' cu 'M' şi 'Z' cu 'N'.

Pentru partea de criptanaliză, esenţial este să remarcăm că substituţiile (fiind funcţii bijective) păstrează particularităţile textului iniţial.

De exemplu, analizând criptotextul interceptat, vom găsi că cel mai frecvent simbol în criptotext este 'S' cu $12,5\%$ şi vom trage concluzia că acesta corespunde celei mai frecvente litere din plaintext. Deşi noi nu cunoaştem plaintextul (tocmai de acest text suntem interesaţi...), ştim că acesta este un text în limba engleză. Conform statisticilor, în textele în limba engleză, litera 'E' este cea mai frecventă ($12,702\%$). Astfel, este clar că $\pi(\mathrm{E}) = \mathrm{S}$ (adică 'E'-urile din plaintext au fost înlocuite peste tot cu litera 'S').

Raţionamentul de mai sus poate fi continuat - dacă cel mai frecvent simbol în criptotext exceptând 'S' este 'H', cu $9,1\%$, putem trage concluzia că $\pi(\mathrm{T}) = \mathrm{H}$, deoarece litera 'T' este a doua literă (fiind devansată numai de litera 'E') ca frecvenţă în textele în limba engleză (cu $9,056\%$).

Marea problemă este că, în textele în limba engleză, există litere foarte apropiate ca frecvenţă, cum ar fi 'C' şi 'U' ($2,782\%$, respectiv, $2,758\%$) sau chiar 'R' şi 'H' ($5,987\%$, respectiv, $6,094\%$). În aceste cazuri, deciziile luate numai pe baza analizei frecvenţei literelor simple pot fi greşite.

Se pot folosi statisticile existente pentru digrame (grupe de câte două litere) sau trigrame (grupe de câte trei litere). De exemplu, să presupunem că cea mai frecventă trigramă în criptotext este 'H**V**S'. În textele în limba engleză, cea mai frecventă trigramă este 'T**H**E' - astfel, rezultă că $\pi(\mathrm{H}) = \mathrm{V}$. Mergând mai departe, putem determina $\pi(\mathrm{O})$ în următorul mod - în limba engleză, cele mai frecvente digrame care conţin 'T' pe prima poziţie sunt 'TH' şi 'T**O**' (în această ordine). Căutând în criptotext cele mai frecvente digrame care conţin 'H' pe prima poziţie (am determinat deja că $\pi(\mathrm{T}) = \mathrm{H}$) vom găsi 'HV' şi 'H**C**' - rezultă că $\pi(\mathrm{O}) = \mathrm{C}$.

Se pot găsi astfel de reguli pentru a determina, pas cu pas, toate componentele cheii.