1. (1.23 Stinson)

Suppose we are told that the plaintext

breathtaking

yields the ciphertext

UPOTENTOIFV

where the Hill Cipher is used (but m is not specified). Determine the encryption matrix.

2. (1.28 Stinson)

Decrypt the following ciphertext, obtained from the Autokey Cipher, by using exhaustive key search:

MALVVMAFBHBUQPTSOXALTGVWWRG

3. (1.20 Stinson)

Suppose we construct a key-stream in a synchronous cipher using the following method. Let $K \in \mathcal{K}$ be the key, let $\mathcal{L}$ be the keystream alphabet, and let $\sum$ be a finite set of states. First, an initial state $\sigma_0 \in \sum$ is determined from K by some method. For all $i \geq 1$, the state σ_i is computed from the previous state σ_{i-1} according to the following rule:

$\sigma_i = f(\sigma_{i-1}, K)$,

where $f: \sum \times \mathcal{K} \rightarrow \sum$. Also, for all $i \geq 1$, the key-stream element z_i is computed using the following rule:

$z_i = g(\sigma_i, K)$,

Where $g: \sum \times \mathcal{K} \rightarrow \mathcal{L}$. Prove that any keystream produced by this method has period at most $|\sum|$