Vigenere Cipher.

Suppose that our key is a sequence $(k_1, \ldots k_n, k_1, \ldots, k_n, \ldots)$ for some key length $n \in Z_+$. The keyspace K has cardinality m^n where m is the size of the alphabet, say $m = 27$. A cipher is then a function σ with the rule

$$\sigma_i(b_i) = (b_i + k_i) \mod m.$$

The likelihood function is the same as before, that is,

$$L(\sigma) = P(\sigma^{-1}(b_1)) \prod_{j=1}^{n-1} Q(\sigma^{-1}(b_{j+1}) \mid \sigma^{-1}(b_j)).$$

Our energy function is also the same as before, that is,

$$E = -\log P(\sigma^{-1}(b_1)) - \sum_{j=1}^{n-1} \log Q(\sigma^{-1}(b_{j+1}) \mid \sigma^{-1}(b_j)).$$

Suppose that the key length is known. If our current key is $(l1, \ldots, l_n, l_1, \ldots, l_n)$, then we may propose a new key by choosing an index $i \in \{1, \ldots n\}$ uniformly at random and then choosing a new letter l_i' uniformly at random.