Vigenere Cipher.

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

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

for $i = 1, \dots N$. The likelihood function is the same as before, that is,

$$L(\sigma) = P(\sigma_1^{-1}(b_1)) \prod_{j=1}^{n-1} Q(\sigma_{j+1}^{-1}(b_{j+1}) \mid \sigma_j^{-1}(b_j)).$$

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

$$E(\sigma) = -\log P(\sigma_1^{-1}(b_1)) - \sum_{j=1}^{n-1} \log Q(\sigma_{j+1}^{-1}(b_{j+1}) \mid \sigma_j^{-1}(b_j)).$$

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

Running Key Cipher.

Suppose that our key is a sequence $(k_1, \dots k_N)$ for some key length $N \in Z_+$, where N is the length of the text. The keyspace K has cardinality m^N where m is the size of the alphabet A, say $m = 27$. For a text of length N, a cipher is then the tuple (k, σ), where $\sigma : A^N \to A^N$ is a function with the rule

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

for $i = 1, \dots N$. But now suppose that the key is also of natural language. So our prior for the likelihood of a key $k \in K$ is

$$P(k) = P(k_1) \prod_{j=1}^{N-1} Q(k_{j+1} \mid k_j).$$

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

$$L(\sigma) = P(\sigma_1^{-1}(b_1)) \prod_{j=1}^{N-1} Q(\sigma_{j+1}^{-1}(b_{j+1}) \mid \sigma_j^{-1}(b_j)),$$

so our posterior is

$$P(k \mid b) = \frac{L(\sigma)P(k)}{P(b)} \propto L(\sigma)P(k).$$

Our energy function is the negative-logarithm of the posterior, that is,

$$E(k, \sigma) = -\log P(\sigma_1^{-1}(b_1)) - \sum_{j=1}^{N-1} \log Q(\sigma_{j+1}^{-1}(b_{j+1}) \mid \sigma_j^{-1}(b_j)) - \log(k_1) - \sum_{j=1}^{N-1} \log Q(k_{j+1} \mid k_j)$$

If our current key is $k = (k_1, \dots, k_N)$, then we may propose a new key by choosing an integer $m \in \{1, \dots, N\}$ at random and then choosing m distinct indices $i_1, \dots, i_m \in \{1, \dots, N\}$ uniformly at random. We then choose m new letters $k_{i_1}', \dots, k_{i_m}'$ uniformly at random. The new key is then $(k_1, \dots, k_{i_1}', \dots, k_{i_m}', \dots, k_N)$.