CHAINSAW : STOCHASTIC CIPHER

This symmetric, homophonic, and stochastic system requires a key vector k of K bits.

To encrypt a bit b, generate random vectors x of size K until $k \oplus x$ has a parity of b. Note that $k \oplus x$ is just the vector sum of k and x, with $1 + 1 = 0$. Since half of all vectors of K bits will work, this won't take long. Then x is the codeword for b, and k is replaced by $k \oplus x$. The process is repeated for each following plaintext bit.

In symbols, let $k_0 = k$, the system key. Let p_i be the ith bit of the plaintext vector. Let x_i be the randomly discovered codeword such $x_i \oplus k_i$ has a parity of p_i. Then $k_{i+1} = x_i \oplus k_i$, and x_i is appended to the ciphertext.

Decryption requires setting $k_0 = k$ and setting x_0 to the first K bits of the ciphertext. Then one calculates the parity of $k_0 \oplus x_0$ to recover p_0. Then $k_1 = k_0 \oplus x_0$ and x_2 is set equal to the next K bits of the ciphertext. This process is repeated until the ciphertext is consumed and all bits of the plaintext are recovered.