162162

30 JAN 2003

CRYPTOGRAPHIC COMMUNICATION PROCESS AND APPARATUS

Abstract of the Disclosure

A communication system, which includes an origination space, a communications channel, and a destination space associated with the origination space via the communications channel. The origination space includes an encryption engine for generating an output symbol O_t based on an input symbol I_t and means for receiving an encrypt key, an encrypt text/key relation, and the input symbol. The destination space includes a decryption engine for generating a decrypted symbol I'_t based on the output symbol received from the origination space via the communications channel and means for receiving a decrypt key and a decrypt text/key relation. The encrypt text/key relation controls the encryption engine such that $O_t = \alpha_N(t) + \pi_N[\alpha_{N-1}(t) + \pi_{N-1}[\alpha_{N-2}(t) + \ldots + \pi_2[\alpha_1(t) + \pi_1[I_t + \alpha_0(t)]] \ldots]]$, mod W, where α_N, $\alpha_{N-1}, \ldots, \alpha_1, \alpha_0$ are N+1 additive transformations defined by the encrypt key, where $\pi_N, \pi_{N-1}, \ldots, \pi_2, \pi_0$ are N permutations defined by the encrypt key, and where W represents the number of possibilities for each permutation defined by the encrypt key. The decrypt text/key relation controls the decryption engine such that $I'_t = \pi_1^{-1}[\pi_2^{-1}[\pi_3^{-1} \ldots [\pi_{N-1}^{-1}[\pi_N^{-1}[O_t - \alpha'_N(t)] - \alpha'_{N-1}(t)] - \ldots - \alpha'_3(t)] - \alpha'_2(t)] - \alpha'_1(t)] - \alpha'_0(t)$, mod W, where π_i^{-1} is defined by the decrypt key as the inverse of the permutation π_i, where $\alpha'_N, \alpha'_{N-1}, \ldots, \alpha'_1, \alpha'_0$ are N+1 additive transformations defined by the decrypt key, and where W represents the number of possibilities for each inverse permutation defined by the decrypt key.

G00002