*162162*

01 JUL 2003

*G00002*

40

## ABSTRACT

A cryptographic device and method provide a repertoire of mappings and associated inverse mappings between plaintext and ciphertext vectors. The plaintext is partitioned block-by-block, the block size being user-selectable, such as N characters. Each mapping maps between a pair of N-dimensional plaintext and ciphertext vectors. The mapping or associated inverse mapping is implemented by a matrix with NxN matrix elements, where each element is allowed to take on a range of L values. By permuting the matrix elements within their range, the repertoire has a size ~ $L^{NxN}$. This size is immense even for moderate values of N and L. The users select one mapping or associated inverse mapping among the repertoire for respectively effecting the encryption or decryption. A secret key shared between the users includes information about the selected mapping or associated inverse mapping and may include values of N and L. To an outsider not privy to the secret key, the task of exhaustive research in the repertoire is computationally infeasible, especially if N and L are not known. In the preferred embodiment, a pseudo-random vector that varies block-by-block is added as another component to the ciphertext vector. A quick computational method is also described.

Figure 4.