INDEPENDENT EXTERNAL SECURITY MODULE FOR A DIGITALLY UPGRADEABLE TELEVISION SIGNAL DECODER

ABSTRACT OF THE DISCLOSURE

A decoder for descrambling encoded satellite transmissions comprises an internal security module and a replaceable security module. The program signal is scrambled with a key (704) and then the key itself is twice-encrypted (710,715) and multiplexed (732) with the scrambled program signal. The decoder (706) performs a first key decryption using the second secret serial number (SSN_2) stored within the decoder (712). The partially decrypted key is then further decrypted by the replaceable security module (714) using the first secret serial number (SSN_1) stored within the replaceable security module (717). The decoder then descrambles (708) the program using the twice-decrypted key. The replaceable security module (714) can be replaced, allowing the security system to be upgraded or changed following a system breach. Either security module may become the active security module to finally decrypt the seed, selectable by a signal transmitted from the encoder (721).

Also disclosed is a method for transmitting (1284) the encrypted keys and secret serial numbers to a plurality of broadcasters (1286) who may in turn multiplex this signal with their own program signals so that any given channel received by a subscriber (1289) contains the key and secret serial numbers. Additionally, the decoder (1306, 1390) may be upgradeable to accept both analog and digital video signals without significant redundant circuitry.

This Sheet Has Been Replaced

