

**ENCRYPTION/DECRYPTION METHOD AND ENCRYPTION/DECRYPTION
APPARATUS**

ABSTRACT

In a scrambler used in the transmission side, a decryptor for generating a work key from a data key and system keys uses the same decryption algorithm as that used in a decryptor for encryption in the OFB mode. Under this condition, in a descrambler used in the receiving side, a decryptor for generating a work key from a data key and system keys can use the same decryption algorithm as that used in a decryptor for encryption in the OFB mode. In addition, another decryptor can use the same decryption algorithm. Therefore, one decryptor can serve as these three decryptors. The scale of the descrambler configuration can be reduced.

Figure 1