

ABSTRACT

To improve a communication system including two communication apparatuses in order to reduce a possibility of having communication thereof decrypted by a third party.

- 5 The communication system includes a first communication apparatus and a second communication apparatus, where one of the communication apparatuses encrypts transmission subject data to generate encrypted data and transmits it to the other communication apparatus which then decrypts received encrypted data. Before performing encryption, each of the communication apparatuses cuts the transmission subject data by a
- 10 predetermined number of bits to generate transmission subject cut data. In this case, each of the communication apparatuses varies the number of bits of the transmission subject cut data, and mixes dummy data of a size of which number of bits matches with the largest number of bits out of the numbers of bits of the transmission subject cut data into the transmission subject cut data other than that of the largest number of bits.