

26 MAR 2002

- 23 -

ENCRYPTION APPARATUS, DECRYPTION APPARATUS, AND
AUTHENTICATION INFORMATION ASSIGNMENT APPARATUS, AND
ENCRYPTION METHOD, DECRYPTION METHOD, AND
AUTHENTICATION INFORMATION ASSIGNMENT METHOD

ABSTRACT OF THE DISCLOSURE

An encryption apparatus and an encryption method are provided which can prevent a cryptographic key or authentication
5 key from being broken. A voice stream is transmitted from a transmitting terminal to a receiving terminal. A bit stream of the voice stream includes speech bursts and speech pauses. Although the speech bursts are encrypted or provided with authentication information, the speech pauses are not encrypted
10 or provided with authentication information, and are transmitted without change. Thus carrying out the encryption or the assignment of the authentication information selectively in accordance with the type of the bit stream makes it possible to prevent the cryptographic key or authentication key from being
15 broken. Besides, it can reduce the processing amount of the encryption or authentication process, thereby being able to limit an increase in the information amount.

Figure 3

162162



G00002