encrypted data by re-encrypting the ciphertext received from the first user device without decryption by the re-encryption key in the storage means; and

a means (43) that transmits the obtained re-encrypted data to the second user device, wherein

the re-encryption key is generated based on a first private key corresponding to the public key for encryption, public information for generating a re-encryption key corresponding to the second private key, and a first random number generated by the re-encryption key generator.

~~20. The re-encryption device according to claim 19, wherein~~

~~the re-encryption key is generated independently of the ciphertext data before re-encryption.~~

20~~21~~. A program executed by a processor of a re-encryption key generator (30) that generates a re-encryption key to obtain re-encrypted data that can be decrypted by a second private key of a second user device after ciphertext data obtained by encrypting plaintext data by a public key for encryption of a first user device is re-encrypted without decryption and stored in a non-transitory computer-readable storage medium (M3), the program comprising:

a first program code causing the processor to perform processing to write a first private key corresponding to the public key for encryption into a first storage means (31) of the re-encryption key generator;

a second program code causing the processor to perform the processing to write public information for generating a re-encryption key corresponding to the second private key into a second storage means (32) of the re-encryption key generator;

a third program code causing the processor to perform processing (36) to generate a first random number; and

a fourth program code causing the processor to perform processing (34) to generate the re-encryption key based on the first private key, the public information for generating a re-encryption key, and the first random number.

~~22. The program according to claim 21, wherein the processor is caused to perform the processing to generate the re-encryption key independently of the ciphertext data before re-encryption.~~

21~~23~~. A program executed by a processor of a re-encryption device (40) capable of communicating with a re-encryption key generator (30) that generates a re-encryption key to obtain re-encrypted data that can be decrypted by a second private key of a second user device after ciphertext data obtained by encrypting plaintext data by a public key for encryption of a first user device is re-encrypted without decryption and stored in a non-transitory computer-readable storage medium, the program comprising:

a first program code causing the processor to perform processing to write the re-encryption key received from the re-encryption key generator into a storage means (41) of the re-encryption device;

a second program code causing the processor to perform processing (44) to obtain the re-encrypted data by re-encrypting the ciphertext data received from the first user device by the re-encryption key in the storage means without decryption; and

a third program code causing the processor to perform processing (43) to transmit the obtained re-encrypted data to the second user device, wherein

the re-encryption key is generated based on a first private key corresponding to the public key for encryption, public information for generating a second re-encryption key corresponding to the second private key, and a first random number generated by the re-encryption key generator.

2224. A program executed by a processor of an encryption device (20) capable of communicating with a re-encryption device (40) that uses a re-encryption key to obtain re-encrypted data that can be decrypted by a second private key of a second user device after ciphertext data obtained by encrypting plaintext data by a public key for encryption of a first user device is re-encrypted without decryption and stored in a non-transitory computer-readable storage medium (M2), the program comprising:

a first program code causing the processor to perform processing (22) to write the public key for encryption into a storage means (21) of the encryption device;

a second program code causing the processor to perform processing (24) to obtain the ciphertext data by encrypting the plaintext data using the public key for encryption in the storage means; and

a third program code causing the processor to perform processing (22) to transmit the obtained ciphertext data to the re-encryption device, wherein

the re-encryption key is generated based on a first private key corresponding to the public key for encryption, public information for generating a re-encryption key corresponding to the second private key, and a first random number generated by a re-encryption key generator that generates the re-encryption key.

2325. A program executed by a processor of a decryption device (50) that decrypts re-encrypted data obtained from the re-encryption device after obtaining the

re-encrypted data that can be decrypted by a second private key of a second user device after ciphertext data obtained by encrypting plaintext data by a public key for encryption of a first user device is re-encrypted by a re-encryption device (40) based on a re-encryption key without decryption and stored in a non-transitory computer-readable storage medium (M5), the program comprising:

a first program code causing the processor to perform processing (53) to write the second private key into a storage means (51) of the decryption device; and

a second program code causing the processor to perform processing (54) to obtain the plaintext data by decrypting the re-encrypted data based on the second private key in the storage means after receiving the re-encrypted data from the re-encryption device, wherein

the re-encryption key is generated based on a first private key corresponding to the public key for encryption, public information for generating a re-encryption key corresponding to the second private key, and a first random number generated by a re-encryption key generator that generates the re-encryption key.

~~26. The program according to any one of claims 23 to 25, wherein~~

~~the re-encryption key is generated independently of the ciphertext data before re-encryption.~~