CLAIMS

1. An authentication-gaining apparatus comprising:

an acquiring unit that generates unique information;

an encrypting unit that encrypts the unique information using a cryptographic key, thereby generating encrypted information; and

a transmitting unit that repeatedly transmits an authentication request containing the encrypted information, to an authentication apparatus, during an authentication period,

wherein multiple authentication requests respectively containing encrypted information obtained by encrypting multiple pieces of unique information are transmitted during the authentication period.

2. The authentication-gaining apparatus according to claim 1, wherein the unique information contains any one of a random number value, a counter value, and time.

3. The authentication-gaining apparatus according to claim 1 or 2, wherein the cryptographic key is a key of common-key cryptography.

4. An authentication apparatus comprising:

a receiving unit that repeatedly receives an authentication request containing encrypted information obtained through encryption using a cryptographic key and transmitted from an authentication-gaining apparatus, during an authentication period;

a decrypting unit that decrypts the encrypted information, thereby acquiring decrypted information;

an authentication unit that judges whether or not the authentication-gaining apparatus is legitimate, using multiple authentication requests received during the authentication period and containing encrypted

information that has been decrypted; and

an output unit that outputs a judgment result by the authentication unit,

wherein the authentication-gaining apparatus that is legitimate transmits multiple authentication requests respectively containing encrypted information obtained by encrypting multiple pieces of unique information generated by the authentication-gaining apparatus, during the authentication period.

5. The authentication apparatus according to claim 4, wherein, if there are a predetermined number or more of duplicates in multiple pieces of decrypted information, the authentication unit judges that the authentication-gaining apparatus is not legitimate.

6. The authentication apparatus according to claim 4 or 5, wherein, if an authentication request is received more than a predetermined number of times during a predetermined period, the authentication unit judges that the authentication-gaining apparatus is not legitimate.

7. The authentication apparatus according to any one of claims 4 to 6, wherein, if authentication request receiving intervals in the authentication period include a receiving interval with a probability that is lower than a threshold, the authentication unit judges that the authentication-gaining apparatus is not legitimate.

8. The authentication apparatus according to any one of claims 4 to 7, wherein, if multiple pieces of decrypted information respectively acquired from the multiple authentication requests received during the authentication period do not match the unique information, the authentication unit judges that the authentication-gaining apparatus is not legitimate.

9. The authentication apparatus according to any one of claims 4 to 8, wherein the receiving unit intermittently receives an authentication request.

10. The authentication apparatus according to any one of claims 4 to 9, wherein the cryptographic key is a key of common-key cryptography.

11. An authentication request transmitting method comprising:

a step of generating unique information;

a step of encrypting the unique information using a cryptographic key, thereby generating encrypted information; and

a step of repeatedly transmitting an authentication request containing the encrypted information, to an authentication apparatus, during an authentication period,

wherein multiple authentication requests respectively containing encrypted information obtained by encrypting multiple pieces of unique information are transmitted during the authentication period.

12. An authentication method comprising:

a step of repeatedly receiving an authentication request containing encrypted information obtained through encryption using a cryptographic key and transmitted from an authentication-gaining apparatus, during an authentication period;

a step of decrypting the encrypted information, thereby acquiring decrypted information;

a step of judging whether or not the authentication-gaining apparatus is legitimate, using multiple authentication requests received during the authentication period and containing encrypted information that has been decrypted; and

a step of outputting a judgment result in the step of judging whether

or not the authentication-gaining apparatus is legitimate,

wherein the authentication-gaining apparatus that is legitimate transmits multiple authentication requests respectively containing encrypted information obtained by encrypting multiple pieces of unique information generated by the authentication-gaining apparatus, during the authentication period.

13. A program for causing a computer to execute:

a step of generating unique information;

a step of encrypting the unique information using a cryptographic key, thereby generating encrypted information; and

a step of repeatedly transmitting an authentication request containing the encrypted information, to an authentication apparatus, during an authentication period,

wherein multiple authentication requests respectively containing encrypted information obtained by encrypting multiple pieces of unique information are transmitted during the authentication period.

14. A program for causing a computer to execute:

a step of repeatedly receiving an authentication request containing encrypted information obtained through encryption using a cryptographic key and transmitted from an authentication-gaining apparatus, during an authentication period;

a step of decrypting the encrypted information, thereby acquiring decrypted information;

a step of judging whether or not the authentication-gaining apparatus is legitimate, using multiple authentication requests received during the authentication period and containing encrypted information that has been decrypted; and

a step of outputting a judgment result in the step of judging whether

or not the authentication-gaining apparatus is legitimate,

wherein the authentication-gaining apparatus that is legitimate transmits multiple authentication requests respectively containing encrypted information obtained by encrypting multiple pieces of unique information generated by the authentication-gaining apparatus, during the authentication period.