

CLAIMS

1. A method of securing a data item N; said data item in the form of a data item character string; for secure storage of a representation of the data item; the method comprising the steps of:
 - a. importing the character string comprising the data item into a first environment;
 - b. applying a first algorithm having at least a first data item argument to the data item character string thereby to form a first modified data item character string;
 - c. applying a second algorithm having at least a second data item argument to the first modified character string whereby the first modified data item character string is embedded in a second modified data item character string; said second modified data item character string in the form of a first data item prime number;
 - d. selecting a second data item prime number different from said first data item prime number;
 - e. defining at least the first data item prime number as a data item private key in respect of the data item; defining the product of the first data item prime number and the second data item prime number as a data item public key in respect of the data item;
 - f. deleting the data item character string from the first environment;
 - g. maintaining a data record associating the first data item prime number, the first algorithm and the second algorithm whereby the data item can be calculated by supply of arguments to the first algorithm and the second algorithm.
2. The method of claim 1 wherein an argument is the data item public key.
3. The method of claim 1 wherein an argument is the data item private key.
4. The method of claim 1 wherein an argument is the second

data item argument.

5. The method of claim 1 wherein an argument is the first data item argument.
6. The method of claim 4 wherein the second data item argument is the numerical value delta.
7. The method of claim 5 wherein the first data item argument is an ASCII look up table.
8. The method of any one of claims 1 to 7 wherein the first algorithm converts the character string into a numeric string.
9. The method of any one claims 1 to 8 wherein the second algorithm adds a numerical value delta to the first modified character string in order to form the second modified character string.
10. The method of any one claims 1 to 9 previous claim wherein in particular forms the algorithm is irreversible such that the data item character string 16 input into the first algorithm 17 cannot be obtained merely having possession of one or other of others of the arguments of the algorithm.
11. A distributed encryption system wherein data to be encrypted is:
 - a. placed on a primary server and then expanded and obfuscated to form an obfuscated string;
 - b. the obfuscated string is then encrypted using a symmetric encryption key to form an encrypted string;
 - c. a string of packing data is then progressively added to the encrypted string until resulting data string is computationally equivalent of the nearest prime number which is then defined as the initial prime number;
 - d. an additional prime number of similar length is generated and the initial prime number and the additional prime number are used to generate a public key using a predetermined public key algorithm.
12. The distributed encryption system of claim 11 wherein the initial prime number is deleted from memory and not stored.
13. The distributed encryption system of claim 11 or 12

wherein resultant components are then stored in disparate locations.

14. The distributed encryption system of claim 13 wherein the symmetric encryption key and the string of packing data are stored on a primary server; the public key is stored on a secondary server; and the additional prime number is stored on a tertiary server.
15. The distributed encryption system of any one of claims 11 to 14 wherein when the data is to be decrypted,
 - a. the public key and additional prime number are retrieved from their respective servers;
 - b. the public key is used in combination with the additional prime number are used to calculate the initial prime number using the predetermined public key algorithm;
 - c. the stored string of packing data is then subtracted from the resulting prime number and the resulting encrypted string is decrypted using the symmetric encryption key that was stored on the primary server and;
 - d. desired target data is de-obfuscated from the resulting expanded obfuscated data string using reverse of obfuscation rules used initially to originally obfuscated the data.
- ~~16. A data encryption system that encrypts a data string using an encryption key in order to produce an encrypted data string; the encrypted data string is then padded to expand it so as to produce the nearest prime number to the encrypted data string; and~~
~~wherein the system selects a second similar length prime number so as to create a private key pair; the product of the private key pair producing a public key.~~
- ~~17. The system of claim 16 wherein the public key and the second prime number of the private key pair are stored separately as well as the padding data and the encryption key initially used.~~
- ~~18. The system of claim 17 wherein the individual components would be stored in separate discreet locations.~~

- ~~19. The system of claim 17 or 18 wherein never would all of the components be stored in the same location.~~
- ~~20. The system of any one of claims 17 to 19 wherein the components must be stored in a minimum of two locations but the more different locations used the more secure the system would be.~~