CLAIMS

1.- A method for generating at least one parameter, the said at least one parameter characterizing a cryptographic protocol, the method including at least the following steps of:

- selecting a text;

- initializing the value of a counter to an initial value;

- for each parameter, obtaining a value for the parameter, at least one value for the parameter being obtained by means of effectively implementing the following steps of:

  - computing an operation applied to the text and the value of the counter, so as to obtain a result,

  - applying a cryptographic hash function to the result so as to obtain a value for the parameter, the operation and the cryptographic hash function being specific to the said at least one parameter;

- testing the compliancy of each parameter value obtained with at least one criterion;

when at least one value does not comply with the said at least one criterion, incrementing the value of the counter by adding of an integer, and of iteration for iterating the steps of obtaining and testing; and

when each value is in compliance with the criterion, generating the parameters such that the value of each parameter is the value which complies with the said at least one criterion.

2.- The method according to claim 1, wherein the cryptographic protocol is selected from the group constituted of an elliptic curve, a curve belonging to a family of curves parameterized by at least one parameter and a key exchange protocol.

3.- the method for generating according to claim 1, wherein the parameters are the parameters of an elliptic curve, the parameters being a modulus (p), a first coefficient (d), and an order (q), wherein:

- a value for the modulus (p) is obtained by implementing a step of computing a first operation (O_1) applied to the text and the value of the counter, so as to obtain a first result (R1), and a step of applying a first cryptographic hash function (H1) to the first result (R1) so as to obtain the value for the modulus (p);

- a value for the first coefficient (d) is obtained by implementing a step of computing a second operation (O_2) applied to the text and the value of the counter, so as to obtain a second result (R2), and a step of applying a second cryptographic hash function (H2) to the second result (R2) so as to obtain the value for the first coefficient (d); and

- a value for the order (q) is obtained by implementing a step for determining based on the values of the modulus (p) and of the first coefficient (d),

each operation (O_1, O_2) preferably including a concatenation of the text.

4.- The method for generating according to claim 1, wherein the parameters are the parameters of an elliptic curve, the parameters being a modulus (p), a first coefficient (a), a second coefficient (b), and an order (q), in which:

- a value for the modulus (p) is obtained by implementing a step of computing a first operation (O_1) applied to the text and the value of the counter, so as to obtain a first result (R1), and a step of applying a first cryptographic hash function (H1) to the first result (R1) so as to obtain the value for the modulus (p);

- a value for the first coefficient (a) is obtained by implementing a step of computing a second operation (O_2) applied to the text and the value of the counter, so as to obtain a second result (R2), and a step of applying a second cryptographic hash function (H2) to the second result (R2) so as to obtain the value for the first coefficient (a);

- a value for the first coefficient (a) is obtained by effectively implementing a computation step of computing a third operation (O_3) applied to the text and the value of the counter, so as to obtain a third result (R3), and an application step of applying a third cryptographic hash function (H3) to the third result (R3) so as to obtain a value for the second coefficient (b); and

- a value for the order (q) is obtained by implementing a step for determining, based on the values of the modulus (p), of the first coefficient (a), and of the second coefficient (b),

each operation (O_1, O_2, O_3) preferably including a concatenation of the text.

5.- The method according to any one of claims 1 to 4, wherein the text satisfies at least one of the following properties:

- a first property according to which the text comprises of more than 16 characters;

- a second property according to which the text includes a date.

6.- The method according to any one of claims 1 to 5, wherein, in the step of testing of compliancy, a factoring of a first number into prime numbers is carried out in order to verify compliance with at least one criterion, the factory being carried out over the set of all prime factors that are lower than a threshold value, with the criterion being satisfied when the quotient obtained by dividing the first number by the product of the set of prime factors that are lower than the threshold value is prime.

7.- A method for transmitting an elliptic curve, the elliptic curve being characterized by the parameters generated by the method for generating according to claim 3 or 4, in which the transmission method includes only either the transmission of the value of the counter and the value of the order (q), or the transmission of the value of the counter and the value of the trace of the curve given by the difference between the modulus (p) and the order (q) to which is added the number 1.

8.- A method for encryption or decryption by using a cryptographic protocol, the cryptographic protocol being characterized by the parameters generated by the method for generating according to any one of claims 1 to 6.

9.- A readable information storage medium on which is stored a computer program comprising program instructions, the computer program being loadable onto a data processing unit and adapted to lead to the carrying out of a method according to any one of claims 1 to 8 when the computer program is carried out on the data processing unit.