Description

TECHNICAL FIELD

The present invention relates to a communication system using text coded using cryptokeys, more particularly it relates to a cryptokey generation system which is able to maintain a high level of privacy and security, easy to operate, and enables common use by a plurality of entities, and to a communication system enabling communication by cryptotext using such common (shared) cryptokeys.

Diverse entities are covered by the present invention, such as human beings, apparatuses, machines, software, and the systems of which these form composite elements. Therefore, the cryptokey generation apparatus of the present invention generates cryptokeys able to be commonly used by these entities. Further, the communications system of the present invention may be applied to various forms of communication using the above-mentioned shared keys, for example, communication between a CPU chip and ROM chip, communications among IC cards, communications among IC cards, terminals, bank centers, and humans, communications among communication equipment of moving bodies, communications among personal radios, communications among telephones, communications among people, communications among host computers, terminals, and data bases, communications among computers in parallel computers, communications between CATV broadcasting stations and subscribers, satellite broadcasts, and other communications systems.

BACKGROUND ART

Various enciphering techniques have been proposed in the past with regard to data security, that is, maintenance of secrecy of data and establishment of privacy, authentication of entities, authentication of communication parties, and the like.

Enciphering techniques may be roughly classified into common key enciphering systems and public key systems (Imai et al, "Cryptography", Journal of the Television Society, Vol. 39, No. 12 (1985), pp. 1140 to 1147). In the common key enciphering system, a secret common key is determined in advance between the message sender and receiver, the sender transmits after enciphering plain text using the common key, and the receiver deciphers the same by the common key to return it to plain text. The public key system is generally known as the public key distribution system, the public key enciphering system, and the public key digital signature system. Details on these enciphering techniques are available in (1) A.G. Konheim, "Cryptography: A Primer", Wiley, New York, 1981, (2) C.H. Meyer et al, "Cryptograph", Wiley, New York, 1982, (3) D.E. Denning, "Cryptography and Data Security", Addison-Wesley, Reading, 1982, (4) D.W. Davies et al, "Security for Computer Networks", Wiley, Chichester, 1984, etc.

The afore-mentioned common key enciphering system is the most popular, but since the entities share the cryptokey with all envisioned communication parties by other enciphering means or physical means, when there are a large number of entities, problems arise in distribution of the key. That is, it is desirable to frequently change the common key, so tremendous problems arise when there are a large number of envisioned communication parties, making this unsuitable for cipher communications with large numbers of unspecified parties.

The afore-mentioned public key system is employed to solve the above-mentioned problem in key distribution. Explaining its gist, the entities prepare public data based on their own secret data and record the same in public files which freely allow reading, but are carefully controlled with regard to writing and erasure. At the time of transmission, they compute the cryptokey to be shared from their own secret data and the other party's public data. According to this system, in transmission, any entity can share the cryptokey by referring to the public files, making this suitable for application to cipher communications with large numbers of unspecified parties. Despite this advantage, a problem arises in that the system requires public files or a corresponding organization for management of public data. Further, considerable work is entailed when an entity referes to the public data of another party, and therefore the operability is poor.

The security achieved by cipher texts depends strongly on the factor that the entities party to the communications have the same cryptokey and entities other than those parties do not have the cryptokey, and thus a truly secure, efficient cryptokey sharing system is yet to be achieved.

DISCLOSURE OF THE INVENTION

The present invention has as its object the provision of a shared cyptokey generation system enabling an acquisition of a highly secret cipher text by a simple operation.

Further, the present invention has as its object the provision of a communication system enabling a transmission of cipher texts using a cryptokey generated by the above.

A common cryptokey generation system for generating a common cryptokey according to the invention to be used in securely communicating text from a first entity to a second entity, the first and second entities being remote from one another is characterised by and having respective unique first and second entity identifiers, the system comprising: a secret algorithm generation means for transforming the entity identifiers into a center algorithm, and for using the center algorithm to generate first and second secret algorithms, uniquely corresponding to the respective first and second entities; and first and second cryptokey generation means associated with the respective first and second entities and remote from each other for generating the common cryptokey, each of the first and second cryptokey generation means having storage means for storing the respective first and second algorithms and processing means operatively coupled to the storage means for processing the respective first and second secret algorithms in combination with the respective second and first entity identifiers to generate the common cryptokey.

According to a second aspect of the invention a common cryptokey generation system is provided for generating a common cryptokey to be used in securely communicating text from a transmitting entity to a plurality of receiving entities, each of the transmitting and receiving entities being remote from one another characterised by each entity having a unique entity identifier, the system comprising: a secret algorithim generation means for transforming the entity identifiers into a center algorithm, and for using the center algorithm to generate a plurality of entity algorithms, each of the entity algorithms uniquely corresponding to one of the entities: and a plurality of cryptokey generation means, each of the cryptokey generation means being uniquely associated with one of the transmitting and receiving entities and remote from others of the cryptokey generation means, for generating the common cryptokey, each of the cryptokey generation means having storage means for storing the corresponding entity algorithm and processing means operatively coupled to the storage means for processing the corresponding entity algorithm in combination with the entity identifiers of others of the entities to generate the common cryptokey.

A method for generating a common cryptokey to be used in securely communicating text from a first entity to at least one second entity, the first and second entities being remote from one anotheraccording to the invention is characterised by having respective unique first and second entity identifiers the method comprising: transforming the entity identifiers into a center algorithm, and using the center algorithm to generate first and second algorithms uniquely corresponding to the respective first and second entities; prestoring the first and second algorithms at the respective first and second entities; at the first entity, in response to an externally-applied command, processing the first algorithm in combination with the or each second entity identifier to generate the common cryptokey, enciphering the text using the common cryptokey, and transmitting a message including the enciphered text and the first and second entity identifiers to the or each second entity; and at the or each second entity, processing the second algorithm or algorithms in combination with the first entity identifier to generate the common cryptokey, and deciphering the enciphered text with the common cryptokey at the or each second entity.

In a first embodiment of the present invention, there is provided a shared cryptokey generation system provided with a secret algorithm generation apparatus, which, under requirements determined among a plurality of entities sharing a cryptokey, generates a center algorithm held secret by a center alone and applies identfiers, determined individually for each of the above mentioned plurality of entities, made public, and used semifixedly, to the above-mentioned center algorithm to produce secret algorithms distinct for each of the above-mentioned plurality of entities and a plurality of cryptokey generation means which have memories which store at least the above-mentioned secret algorithms and which are connected to the secret algorithm generation apparatus during the generation of secret algorithms in the above-mentioned secret algorithm generation apparatus, store the secret algorithms of the corresponding entities in the above-mentioned memory, and apply the identifiers of the party entities to receive or send cipher text to the said secret algorithms to thereby generate a common cryptokey.

Optimally, the above-mentioned secret algorithm generation apparatus can be provided with a plurality of first center algorithm generation apparatuses which operate mutually independently to respectively generate independent first center algorithms and an apparatus for combining the plurality of first center algorithms generated by the said first secret algorithm generation apparatuses and generating the distinct secret algorithm for each entity based on the combined center algorithm.

In a second embodiment of the present invention, there is provided a communication system using a share cryptokey which is provided with the above-mentioned secret algorithm generation apparatus, the above-mentioned plurality of cryptokey generation means, and at least one pair of sending and receiving entities connected via a transmission system, the sender entity cooperating with the above-mentioned cryptokey generation means and having a means for enciphering plain text using the common cryptokey

from said cryptokey generation means, the receiver entity cooperating with the above-mentioned cryptokey generation means and having a means for deciphering into plain text the cipher text sent via the above-mentioned transmission system from the above-mentioned sender entity based on the common cryptokey from said cryptokey generation means, and which transmits cipher text based on the above-mentioned common cryptokey.

BRIEF DESCRIPTION OF THE DRAWINGS

Figure 1 is a block diagram of a shared cryptokey generation system and a communication system using the shared cryptokey of a first embodiment of the present invention;

Fig. 2 is a view showing the generation of a center algorithm G in a secret algorithm generation apparatus 1 provided in the center of Fig. 1;

Fig. 3 shows the generation and distribution of secret algorithms for the entities using identifiers in the center of Fig. 1;

Fig. 5 is a view showing an example of the use of an IC card as the code generation means in Fig. 1 covering the entry of an entity A in the network, the issuance of an IC card for the entity A, and the computation of the cryptokey k for the entity A;

Fig. 6 and Fig. 7 are views showing one example of the generation of a center algorithm and a secret algorithm in the case of two entities;

Fig. 8 and Fig. 9 are views showing one example of the generation of a center algorithm and a secret algorithm in the case of three entities;

Fig. 10 is a general view showing another method for generation of the secret algorithm of the present invention for improving the security;

Fig. 11 is a block diagram of a shared cryptokey generation system and a communication system using the shared cryptokey of another embodiment of the present invention; and

Figs. 12(a) to (c) are general views of a conventional common key enciphering system, a conventional public key system, and a key predistribution system based on the present invention, respectively.

BEST MODE FOR CARRYING OUT THE INVENTION

Figure 1 illustrates a shared cryptokey generation system and a communication system using the synthesized shared cryptokey of a first embodiment of the present invention.

Figure 1 illustrates the case where there are two entities, A and B. Entity A and entity B are connected via a communication circuit 6, e.g., a public line. The sender entity, for example, entity A, is provided with a cipher text generation means 4 comprised of a means 41 for inputting the plain text to be transmitted, a means 42 for enciphering the plain text which is input based on a later-mentioned shared cryptokey k, and a means 43 for transmitting the cipher text. The receiver entity B is provided with a cipher text deciphering means 5 comprised of a means 51 for receiving the cipher text via the public line 6 and judging that it is communication text addressed to itself, a means 52 for deciphering the received cipher text to plain text using the shared key k, and a means 53 for outputting the deciphered plain text. The constructions of the cipher text generation means 4 and cipher text deciphering means 5 are known in the prior art. The enciphering means 42 and the deciphering means 52 may be realized by, for example, those disclosed in Fig. 8 of Japanese Examined Patent Publication (Kokoku) No. 59-45268 (claiming priority of February 24, 1975, based on U.S. Patent Application Serial No. 552684).

The center is provided, as a management organization, with an apparatus 1 for a generation of secret algorithms. This issues secret algorithms via means 2 and 3, which issue a shared cryptokey k for the entities A and B, respectively, through, e.g., IC cards. That is, the secret algorithm generation apparatus 1 receives as input the identifiers of entities A and B, for example, y_A and y_B , which encipher in a predetermined format their names or addresses, generates the center algorithm G as shown in Fig. 2, then holds the algorithm G secret and issues secret algorithms X_A and X_B. The identifiers y_A and y_B are, for example, input via ten-keys.

The secret algorithms X_A and X_B of the entities A and B are defined as follows using their own respective identifiers y_A and y_B:

$$X_A = G(y_A) \quad (1\text{-}1)$$

$$X_B = G(y_B) \quad (1\text{-}2)$$

The secret algorithm generation apparatus 1 has fitted to it cryptokey generation means 2 or 3 with built-in CPUs and memories able to perform reading/writing during the generation of the above-mentioned secret algorithms, e.g., IC cards. The secret algorithms are stored in the memories of the corresponding cryptokey generation means and issued from there. Figure 3 illustrates the state of issuance of secret algorithms X_A to X_D corresponding to the entities A to D. As is clear, for the entities C and D, the following secret algorithms X_C and X_D are issued using their respective own identifiers y_C and y_D:

$$X_C = G(y_C) \quad (1\text{-}3)$$

$$X_D = G(y_D) \quad (1\text{-}4)$$

Each entity, of course, stores its above secret algorithm secretly.

The algorithm in the present invention means a method of computation noted in a predetermined language. Computer programs in the common sense and data, logic circuits, graphs, tooling machines, Petri nets known as models of dynamic analysis of distribution systems, LSI patterns, etc. are all types of algorithms in the present invention.

The cryptokey generation means 2 and 3 in which the secret algorithms X_A and X_B issued as mentioned above are loaded are equipped at their respective corresponding own entities. When the entities A and B desire to share a cryptokey k, as shown in Fig. 1 and Fig. 4(a) and (b), the identifier of the other party to share the key, i.e., y_B for the entity A and y_A for the entity B, are input at the cryptokey generation means 2 and 3 equipped to the entities via the keyboards, etc. at the entities. The cryptokey generation means generate the shared cryptokey as follows by the built-in CPUs based on the secret algorithms stored in the memories and the input identifiers:

$$k = X_A(y_B) \quad (2\text{-}1)$$

$$k = X_B(y_A) \quad (2\text{-}2)$$

The cipher text generation means 4 and the cipher text deciphering means 5 use the shared cryptokey k for enciphering or deciphering.

The algorithms G, X_A , X_B , ... must be determined so as to enable computation of the same cryptokey k by the above procedure.

By the constitution mentioned above, the secret algorithms converted by the center algorithm known only to the center are distributed to the entities, thus maintaining secrecy. On the other hand, the entities are equipped with cryptokey generation means in which the secret algorithms are loaded, for example, IC cards, and need merely input the identifier of the other party, so the operation is extremely easy. In this case, the cryptokey k issued based on the identifier of the other party is used for enciphering and deciphering, so secrecy is improved.

Further, since there are several sets of identifiers and secret algorithms, for example, (y_A , X_A), (y_B , X_B), and (y_C , X_C), finding a secret algorithm for another identifier, for example, X_D for Y_D , requires a massive amount of computation and is practically unworkable, which is in general desirable. The condition means that the algorithm G of the center cannot in practice be computed from just (y_A , X_A), (y_B , X_B), (y_C , X_C), ...

As another embodiment of the present invention, if the above-mentioned secret algorithms are accommodated in a computer physically protected by one or a plurality of IC cards 2a, etc. as shown in Fig. 5, it is possible to construct a cryptokey sharing system having an even higher security.

In this case, the entities cannot take out their own secret algorithms. Even the action itself of several entities colluding and assembling their secret algorithms to derive the center algorithm G or an algorithm equivalent to G can be prevented. However, in the present invention, G is comprised so that security is maintained even if a plurality of secret algorithms are used, so even if the physical security of the IC cards, etc. is broken, the system as a whole is secure.

Further, the procedure for generating the shared cryptokeys may be performed internally in the IC cards, etc. in addition to being performed by simply inputting the identifiers, so the burden of work of the entities for sharing the cryptokeys is cut down tremendously.

In Fig. 5, an entity A applies to the center for entry into the network, an IC card 2a in which a secret algorithm is embedded is issued via a secret algorithm generation apparatus, the IC card 2a is provided to the entity A, then the identifier y_B of the entity B is input and a shared cryptokey k is generated. However, Fig. 5 shows the example of a secret algorithm embedded in a single IC card, but the secret algorithm can

be arbitrarily divided and separated in IC cards or magnetic cards, magnetic tape, bar codes, optical memories, IC memories, or floppy disks, and any other data storage medium and/or computer systems, IC cards, one-chip microcomputers, computing processors, and modems comprising the same, and any other apparatuses having computing abilities.

Next, an example will be shown of the method of preparation of the center algorithm G and secret algorithms.

First, consider the case of two entities A and B sharing a cryptokey.

Figure 6 shows the method of construction of the center algorithm G. For G, one first prepares the one-input one-output algorithms G_1 and G_2 and the two-input one-output algorithms H and ϕ. ϕ is made one which expresses a correspondence function.

One prepares the algorithms α_1 , α_2 , and β which handle the algorithms G_1 , G_2 , H, and ϕ, then synthesizes G_2 and H from α_1 to prepare the algorithm F_1 and synthesizes G_1 and H from α_2 to prepare the algorithm F_2.

Next, G_1 and G_2 are applied to the identifier y_A of the entity A, as a result of which Z_{A1} and Z_{A2} and the above-mentioned algorithms F_1 , F_2 , and ϕ are combined by the algorithm β, and the secret algorithm X_A of the entity A as shown in Fig. 7 is output.

The combination performed by the algorithms α_1 and α_2 in Fig. 6 is known as the algorithm combination method. F_1 and F_2 are expressed by the following equations as combination algorithms:

$$F_1 = H(\bullet, G_2(*)) \quad (3\text{-}1)$$

$$F_2 = H(G_1(\bullet), *) \quad (3\text{-}2)$$

However, the • and * each indicate identifiers (parameters). Here, the algorithms H, G_1 , and G_2 cannot in practice be derived from the combination algorithms F_1 and F_2 and it is difficult to learn the contents of F_1 and F_2. That is, it will be understood, this combination method produces obscure algorithms.

The fact that the secret algorithm X_A of the entity A of Fig. 7, comprised by the center algorithm G of Fig. 6, and the secret algorithm X_B of the entity B, comprised in the same way, function correctly can be confirmed as follows:

$$\begin{aligned} X_A(y_B) &= \phi(F_1(A_{A1}, y_B), F_2(y_B, Z_{A2})) \\ &= \phi(H(G_1(y_A), G_2(y_B)), \\ &\qquad H(G_1(y_B), G_2(y_A))) \\ &= \phi(H(G_1(y_B), G_2(y_A)), \\ &\qquad H(G_1(y_A), G_2(y_B))) \\ &= \phi(F_1(Z_{B1}, y_A), F_2(y_A, Z_{B2})) \\ &= X_B(y_A) \qquad \ldots (4) \end{aligned}$$

Other obscure algorithm combination methods are disclosed in (1) Matsumoto et al, "Asymmetric Cryptosystem Using Obscure Expressions of Enciphering Conversion", Papers of 1983 National Conference of Systems Division of Society of Electronic Communications, September 1983, No. S8-5, pp. 1-469 to 1-470 (in Japanese), (2) Matsumoto et al, "On Multivariate Polynomial Tuple Asymmetric Cryptosystems", February 7, 1986, 1986 Code and Data Security Symposium Materials E2, Code and Data Security Research Conference, Special Committee on Data Security of Society of Electronic Communications (in Japanese), (3) Matsumoto et al, "A Cryptographically Useful Theorum on the Connection Between Uni and Multivariate Polynomials", The Transaction of the IECE of Japan, Vol. E68, No. 3, pp. 139 to 146, March 1985, (4) Imai et al, "Algebraic Method for Constructing Asymmetric Cryptosystems", 3rd International Conference on Applied Algebra, Algebraic Algorithms and Symbolic Computation, Error Correcting Codes (July 15 to 19, 1985, Grenoble, France), Springer Verlag, etc. These may also be applied.

Next, a specific example of use of the center algorithm G and the matrix of secret algorithms X_A , X_B , etc. for the two entities A and B is shown.

The set comprised of all of the n rows and m column matrixes on the commutative ring R is expressed as $\mu_R(n, m)$. For R, use may be made, for example of the residue-class ring $Z_Q = \{0, 1, 2, \ldots q\text{-}1\}$, etc. using the non-negative integer q as the modulo.

First, G_1 , G_2 , and $H \in \mu_R$ (n, n) are selected and F_1 and F_2 $\in \mu_R$ of the combination algorithms

$$F_1 = HG_2^T \quad (5\text{-}1)$$

$$F_2 = G_1 H \quad (5\text{-}2)$$

are calculated. T in equation (5-1) shows a transposition.

Next, Z_{A1} , Z_{A2} , Z_{B1} , and $Z_{B2} \in \mu_R$ (l, n) are calculated as follows for y_A , $y_B \in \mu_R$ (l, n).

$$Z_{A1} = Y_A G_1 \quad (6\text{-}1)$$

$$Z_{A2} = y_A G_2 \quad (6\text{-}2)$$

$$Z_{B1} = Y_B G_1 \quad (6\text{-}3)$$

$$Z_{B2} = y_B G_2 \quad (6\text{-}4)$$

Therefore,

$$\begin{aligned} Z_{A1}F_1{y_B}^T &= (y_A G_1)(H{G_2}^T){y_B}^T \\ &= y_A(G_1 H)({G_2}^T{y_B}^T) \\ &= y_A(G_1 H)(y_B G_2)^T \\ &= y_A F_2 {Z_{B2}}^T \qquad \cdots (7) \end{aligned}$$

That is,

$$Z_{A1}F_1 y_B^T = y_A F_2 Z_{B2}^T \quad (8\text{-}1)$$

stands.

Similarly, the following equation stands:

$$Z_{B1}F_1 y_A^T = y_B F_2 Z_{A2}^T \quad (8\text{-}2)$$

Therefore, if the multiplication in the commutative ring R is expressed by *, the commutative of * and equations (8-1) and (8-2) give the following:

$$\begin{aligned} & (Z_{A1}F_1{y_B}^T) * (y_B F_2 {Z_{A2}}^T) \\ = \; & (y_B F_2 {Z_{B2}}^T) * (Z_{A1}F_1{y_B}^T) \\ = \; & (Z_{B1}F_1{y_A}^T) * (y_A F_2 {Z_{B2}}^T) \qquad \cdots (9) \end{aligned}$$

Here, if the algorithms G, X_A , and X_B are determined as follows:

$$G(y_A) = X_A \quad (10\text{-}1)$$

$$G(y_B) = X_B \quad (10\text{-}2)$$

$$X_A(y_B) = (Z_{A1}F_1 y_B^T) * (y_B F_2 Z_{A2}^T) \quad (11\text{-}1)$$

$$X_B(y_A) = (Z_{B1}F_1 y_A^T) * (y_A F_2 Z_{B2}^T) \quad (11\text{-}2)$$

then from equation (9),

$$X_A(y_B) = X_B(y_A) \quad (12)$$

stands.

Even in the case of three or more entities, it is possible to form the center algorithm G and the secret algorithms X_A, X_B, X_C, ... in the same way as with two entities. An example of this, i.e., the case of three entities, is shown in Fig. 8 and Fig. 9.

Finally, while slightly different from the above, a specific example constituted by the same way of thinking as the above is shown for the case of two entities.

The symmetric matrix $G \in \mu_R(n, n)$ is selected.

That is, $G = G^T$ is considered to stand.

The center algorithm G and the secret algorithms X_A and X_B are determined as:

$$G(y_A) = X_A \quad (13\text{-}1)$$

$$G(y_B) = X_B \quad (13\text{-}2)$$

$$X_A(y_B) = X_A(\phi(y_B))^T \quad (14\text{-}1)$$

$$X_B(y_A) = X_B(\phi(y_A))^T \quad (14\text{-}2)$$

However,

$$x_A = \phi(y_A)\, G \quad (15\text{-}1)$$

$$x_B = \phi(y_B)\, G \quad (15\text{-}2)$$

and ϕ is an algorithm which expresses the function from $\mu_R(l, n)$ to $\mu_R(l, n)$.

$\phi(y_A), \phi(y_B), \phi(y_C), \ldots$

is made linearly independent on the commutative ring R.

At this time,

$$\begin{aligned} & X_A(y_B) \\ &= x_A(\phi(y_B))^T \\ &= (\phi(y_A)\, G)(\phi(y_B))^T \\ &= (\phi(y_A)\, G\, (\phi(y_B))^T)^T \\ &= \phi(y_B)\, G^T (\phi(y_A))^T \\ &= (\phi(y_B)\, G)(\phi(y_A))^T \\ &= x_B(\phi(y_A))^T \\ &= X_B(y_A) \end{aligned} \quad \ldots (16)$$

That is,

$$X_A(y_B) = X_B(y_A) \quad (17)$$

stands. Therefore, the value of the above equation may be made the cryptokey k to be shared.

As mentioned in detail above, according to a first aspect of the present invention, a cryptokey common with another party which has never been met (never been communicated with) may be computed simply and securely by just inputting the identifier of the other party, thus enabling easy communications by cipher text among any parties.

The above explanation concerned a shared cryptokey generation apparatus and a communication system using a shared cryptokey known as the "key predistribution system (KPS)" invented by the present inventors.

Summarizing the above generation of the cryptokey by stages, the generation may be roughly classified into the following three stages (steps):

a. Step 1: Preparation of center algorithm
b. Step 2: Preparation and distribution of secret algorithms for use by entities
c. Step 3: Sharing of key by group of entities

Step 1 is an operation required for starting up a system or in renewal. Assume the center is a center p. This refers to the generation of a special algorithm, that is, a center algorithm G_P which just the center p holds secret. However, the agreement of all the entities or representatives of the entities is obtained regarding the method for generation of G_P.

Step 2 is an operation performed by the centers and entities when entities enters the network. Assume the entity is an entity i. The center p applies the center algorithm G_P to the identifiers yi of the entity distinct to the same, made public, and used semifixedly so as to prepare the secret algorithms $X_{pi} = G_P$ (yi) exclusive for the entity. The secret algorithms X_1i, X_2i, ..., X_si for the entity i are separately, or combined by a suitable method, distributed to the entity i, for example, by IC cards, etc. The entity i keeps secret the sets of secret algorithms received or the combinations of the same X_i.

Step 3 is an operation performed by the group sharing the cryptokey after the completion of steps 1 and 2. The entities belonging to the group input the identifiers of all the entities belonging to the group other than their own to their own secret algorithms and thereby share the same cryptokey k. For example, when the entity A and entity B wish to share the cryptokey k_{AB} , they respectively compute k_{AB} as follows:

$$k_{AB} = X_A^{(2)} (y_B) \quad (18\text{-}1)$$

$$k_{AB} = X_B^{(2)} (y_A) \quad (18\text{-}2)$$

Further, when entity A, entity B, and entity C wish to share a cryptokey k_{ABC} , they respectively compute k_{ABC} as follows:

$$k_{ABC} = X_A^{(3)} (y_B , y_C) \quad (19\text{-}1)$$

$$k_{ABC} = X_B^{(3)} (y_C , y_A) \quad (19\text{-}2)$$

$$k_{ABC} = X_C^{(3)} (y_A , y_B) \quad (19\text{-}3)$$

Here, $Xi^{(e)}$ indicates a secret algorithm of an entity i used when a group consisting of e number of entities shares a key.

Next, mention will be made of the general security of the KPS.

In the KPS, when distributing the secret algorithms, it is necessary to properly authenticate (identify) the entity to which the secret algorithm is to be transferred. Proper authentication of the entity (confirmation of the right person) is a main precondition of all the code means, however, so the problem of entity authentication is not unique to the KPS.

The key shared by a group under the KPS (master key) is distinct to each group and does not change insofar as the center algorithm is not renewed. Therefore, the KPS may be said to be a system for sharing a master key. Even when the master key is divulged outside the group, it is impossible to change to a new master key. Therefore, it is desirable to renew the center algorithm after a suitable period. However, if a group of two entities is sharing a key and use is made of a secret algorithm $Xi^{(3)}$ for sharing of a key for a group of three entities, by switching suitable random numbers, for example, pseudo random numbers and random numbers by the "linear congruence" method, etc., it is possible for the two entities to share a different key each time. For example, the entity A and entity B can share the common key k such as

$$k = X_A^{(3)} (y_B , r) \quad (20\text{-}1)$$

$$k = X_B^{(3)} (r, y_A) \quad (20\text{-}2)$$

using the random number r different from the identifiers of each entity.

Now then, in the KPS, data regarding the center algorithm is dispersed to the entities in the form of the secret algorithms Xi, so an individual entity or a number of cooperating entities can, by expending a suitable amount of computation, find the center algorithm or the secret algorithm X_t or a part thereof for an entity other than the cooperating entities.

By having the secret algorithms embedded in some sort of apparatus which is physically protected and has a computing ability, for example, an IC card having a built-in CPU and memory, and having the entities are able to execute the same without knowing their own secret algorithms, the center algorithm and the secret algorithms X_t of other entities or parts thereof will not be exposed. Therefore, in an environment where the physical security can be kept complete, any KPS is secure.

However, current IC cards and other forms of physical security cannot be said to be complete. In actuality, it is difficult to expect complete physical security, so measures such as making it necessary for a number of entities to collude (cooperate) to obtain sufficient data for determining the center algorithm or X_t or parts thereof or making it such that even when sufficient data is obtained, it would take a tremendous amount of computation to obtain the center algorithm or X_t or parts thereof will be demanded for a KPS. The former may be said to correspond to so-called unconditional security and the latter to so-called computational security.

Verification of unconditional security is in general not difficult, but verification of computational security cannot be easily performed at the present time without assumption of difficulties in resolving suitable problems such as with unique factorization in prime elements.

An explanation will now be given of the case of constructing an unconditionally secure KPS, in the sense of security so long as a certain number of entities do not collude, using the linear independence of vectors. In Fig. 10, first center algorithm generation apparatuses 1a to 1d in a plurality of mutually independent centers receive as input the identifier of entity A and generate first center algorithms $g_{p1}(x)$ to $g_{p4}(x)$ having a relationship of linear independence of vectors. Next, the apparatus 1e in the overall center combines the first center algorithms and generates the overall center algorithm $G_P(x)$. The secret algorithm X_A of the entity A is generated based on the center algorithm $G_P(x)$ in the apparatus 1e.

This system, of course, improves the security compared with the afore-mentioned embodiment using the secret algorithm, which was a case of one center. Below, a detailed explanation will be made of the means for expanding the KPS and improving the security based on linear algebra in the case of one center.

Figure 11 shows an example of application of a KPS illustrating schematically the constitution corresponding to Fig. 1. In the figure, the sending side entity A receives as input the identifier y_B of the other party and applies the secret algorithm X_A to generate the shared key k, then applies the same to the enciphering means 42a to generate a cipher text C from the message m. The combination means 44a combines the cipher text C, other party's identifier y_B , and its own identifier y_A and sends to the other party information comprised of the "addressee (y_B), sender (y_A), and cipher text (C)" via a transmission means (not shown) and a circuit (channel) 6. The receiving side entity B receives the transmitted data as input via a receiving means (not shown) and judges in the selection means 54a if the communication text is addressed to itself using its own identifier y_B. If the communication text is addressed to itself, it sends the other party's identifier y_A and cipher text C to a separation means 55a. The separation means 55a separates the other party's identifier y_A and cipher text C. The other party's identifier y_A is applied to an IC card or other cryptokey generation means 3a and the shared cryptokey k is generated via the secret algorithm X_B. The deciphering means 52a restores the message m from the transmitting side by applying the shared cryptokey k to the cipher text C.

In this way, by using the KPS, it is possible to simply realize mail communications such as in normal mail, i.e., one-directional cipher communications. Even when there are two or more addresses, it is possible to perform so-called "multiple address authentication" and mail communications.

Note that, of course, this may also be applied to dialog type communications such as with telephones.

A description will now be given on a KPS based on linear algebra. The case of one center has already been discussed in the embodiment related to Fig. 1 to Fig. 8.

The system defined below will be named the "linear scheme".

Assume g is a prime number power and m, s, and h are non-negative integers. When the vector Q is

$$Q = GF(q) \quad (21)$$

the vector space formed by all the m-th dimensional row vectors on Q is expressed by Q^m.

Assume the entity is entity i and the identifier yi thereof is the element of the set I. Assume that if i does not equal j, then yi does not equal yj.

Further, R_r is an algorithm which expresses the injection from I to Q^m (one to one mapping).

The center, e.g., the center p, where p = 1, 2, ... or s, selects independently from the other entities randomly and uniformly h number of m-th symmetric matrixes G_{p1} , G_{p2} , ... G_{ph} on Q and generates the center algorithm G_p. G_p is defined as an algorithm for generating the secret algorithm X_{pi} for each yi ∈ I

$$X_{pi}(\xi) = xpiR_r(\xi)^T \quad (22)$$

However, X_{pi} is an h x m matrix on Q defined by the following:

$$X_{pi} = \begin{bmatrix} R_r(yi)G_{p1} \\ R_r(yi)G_{p2} \\ \vdots \\ R_r(yi)G_{ph} \end{bmatrix} \quad \ldots (23)$$

T means transportation. ξ indicates a variable set for inputting an identifier yj of the other party.

The entity i acquires the algorithms X_{pi} from the centers and produces from there the secret algorithms Xi exclusive for the entity i in the following way:

$$Xi(\xi) = xiR_r(\xi)^T \quad (24)$$

$$Xi = \sum_{p=1}^{s} x\ pi \quad \ldots (25)$$

The center p must, it is important, transfer the algorithms X_{pi} only to the entity i.

Note that if IC cards, etc. are used, it is possible to automatically obtain the secret algorithms Xi. For example, the entity i first obtains the IC cards, initializes them so that anyone can write on them but only the entity i can read them, transfers them to the centers, and has the centers input the X_{pi} , with the sums taken successively in the IC cards. Finally, at the stage of preparation of Xi, the IC cards are returned to the entity i.

If any case, in the end, the entity i holds the secret algorithms Xi.

When the entity i and entity j desire to share a cryptokey, the entity i calculates xi(yj) as the key and the entity j Xj(yi). Xi(yj) and Xj(yi) are both h-th dimensional column vector: on Q. That the two match can be easily derived from the definitions of Xi and Xj.

The above explanation was of the case where a group is comprised of two entities, but in general in the case of a group comprised of a number of entities (e ≥ 2), the same system can be realized by use of multilinear mapping for the e number of entities instead of the afore-mentioned Gpi, i.e., the bilinear mapping.

Next, consider the security of the linear scheme. As attacks on the system, it is necessary to consider both attacks by the centers and attacks by the entities.

Complete breaking of the system would be equivalent to determining a matrix consisting of the matrixes G_1 , G_2 , ..., G_h comprising

$$Gj = \sum_{p=1}^{s} G_{pj} \ (j = 1, 2, \ldots, h) \quad \ldots (26)$$

the said matrix being:

$$G = [G_1 , G_2 \ldots G_h] \quad (27)$$

Therefore, so long as all the centers do not collude, i.e., even if several centers collude, the center algorithm G cannot be determined completely. Therefore, none of the cryptokeys of any group can be determined at all.

Further, so long as rank G number of entities do not collude, the center algorithm G cannot be completely determined at all. The probability is large of rank G being m or a value close to m.

However, it is true that even with collusion of a number of entities less than rank G, the larger the number of colluding entities, the more the amount of data on G, and therefore, the more the amount of data on the secret algorithms of the entities that can be obtained. Therefore, the following conclusion is obtained when considering to what degree colluding entities can determine the cryptokeys of the other entities.

Assume the set of all the entities entered in the system is E. At this time, to satisfy the condition that:

"Even if all the entities belonging to the partial set E_B of E collude, the cryptokey shared between any two entities belonging to E - E_B cannot be determined at all,"

it is necessary and sufficient that

"the vector $R_r(yi)$ for each $i \in E - E_B$ be linearly independent from the set of the vectors $\{R(yi)|j \in E_B\}$."

Therefore, it is possible to talk about this shifting the problem of security of collusion of the entities to the problem of linear independence in

$$U = \{R_r(yi)|i \in E\}$$

In particular, a close connection arises with the "theory of linear coding".

In actuality, if the linear code of n code length and m number of inspection symbols, which makes the matrix able to horizonally arrange the transposed vectors of all the vectors belonging to the set U of the vectors the parity inspection matrix, is made C, then "the existence of a coding word of Hamming weight w at C" and "the existence of a case where keys between other entities can be determined by collusion of (w-l) entities" are equivalent.

In particular, that "the minimum Hamming weight of C minimum distance be b+2 or more" is a sufficient condition for "any key among entities not being able to be determined at all by collusion of any b entities".

Therefore, the algorithm R_r may be selected based on an algebraic/algebraic and geometric code theory. In this case, if yi is considered a suitable vector, $R_r(yi)$ becomes one which arranges a monomial for the component yi. Therefore, the algorithm X becomes a tuple. As the corresponding linear code, an (e) - GRM coding, BCH coding, RS coding, Goppa coding, etc. are used (Koh et al, "Coding Theory", Corona Co., 1975 (in Japanese)). However, evaluation of R_r (computation) cannot be performed efficiently when m is large.

However, translating the theorum of Gilbert-Varsharmov in the coding theory into the KPS language, the following is obtained:

When the prime number power q and the non-negative integers m and b are given,

$$\frac{M}{n} \leq \phi\left(\frac{b}{n}\right) \quad (28)$$

however, there is a linear scheme which satisfies

$$\phi(X) = X\log_q(q-l) - x\log_q X - (l-x)\log_q(l-x) \quad (29)$$

and has b number or more allowable colluding entities, a storage capacity of the secret algorithms of $hm\log_{2q}$ (bit), and a total number of entities n. Here, h is any positive integer.

Further, it may be derived from the results of the coding theory that the majority of linear schemes have parameters satisfying equation (28).

Therefore, the algorithm for generating a reproducible affine random number series at a high speed may be selected as R_r.

In this regard, there is a difference from the usual method of use of linear coding. In usual applications, due to the need to realize a deciphering algorithm with good efficiency, use is made of codes using some sort of structure, but in the linear scheme for the KPS, there is no need at all to consider the efficiency of the algorithm corresponding to the deciphering, so use may be made of random codes.

The results of the above study on the security of the linear scheme are summarized in Table 1.

Table 1

Attack method	Target of attack	
	Complete breaking of system	Obtaining keys of other group
1. Collusion of several centers	Impossible so long as all centers do not collude.	
2. Collusion of several entities	Possible if rank G number of more of entities collude. Impossible if less than rank G number of entities collude. rank G m.	Possible if b + l number or more entities collude. Impossible if b number or less entities collude. b is determined by linear independence of set U.
3. Collusion of several centers and several entities	Possible if all centers collude. Same as 2. when there are some centers not colluding.	

Next, evaluation will be made of the various storage capacities and computation amounts for the linear scheme.

The centers store the algorithm R_r and h number of symmetric matrixes G_{p1} , G_{p2} , ... G_{ph}. When entities enter, they calculate $R_r(yi)$ and further multiply R(yi) with G_{p1} , G_{p2} , ... G_{ph} to find Xpi, so the storage capacities and computation amounts shown in Table 2 are required. Table 2 shows the complexity of the linear scheme by the storage capacity and the computation amount.

Table 2

Item	Storage capacity (bit)	Computation amount
Centers	[Storage capacity of R_r] + $\frac{1}{2}hm(m+1)\log_2 q$	[Computation amount of evaluation of R_r] + Q computations $O(hm^2)$ times
Entities	[Storage capacity of R_r] + $hm\log_2 q$	[Computation amount of evaluation of R_r] + Q computations $O(hm)$ times
Cryptokeys obtained	$h\log_2 q$	

Further, the entities store the algorithm R_r and the matrix xi. When sharing keys, they calculates $R_r(yi)$ and multiply $R_r(yj)^T$ to find the cryptokeys, so the storage capacities and computation amounts shown in Table 2 are required.

Note that when m and b are given, n, defined by the Gilbert-Varsharmov bound, can approximate

$$n = m2^{m/b}$$

when b/n is small.

Examples of the values when q = 2 and h = 64 are shown in Table 3.

Table 3

m	hm	hm^2	b	$n = b \cdot 2^{m/b}$	hn
2^7	2^{13}	2^{20}	2	2^{65}	2^{71}
			2^2	2^{34}	2^{40}
			2^3	2^{19}	2^{25}
2^{10}	2^{16}	2^{26}	2^4	2^{68}	2^{74}
			2^5	2^{37}	2^{43}
			2^6	2^{22}	2^{28}
2^{13}	2^{19}	2^{32}	2^7	2^{71}	2^{77}
			2^8	2^{40}	2^{46}
			2^9	2^{25}	2^{31}
2^{16}	2^{22}	2^{38}	2^{10}	2^{74}	2^{80}
			2^{11}	2^{43}	2^{49}
			2^{12}	2^{28}	2^{34}

From Table 3, it will be seen that when, for example, $m = 2^{13}$ and $b = 2^8$, with a linear scheme where the centers store about 4 Gbits and the entities store about 512 Kbits, breaking the system as a whole would require collusion of all of the centers or collusion of about 8192 or more entities. Since it is impossible to determine the key among two entities even with the collusion of up to 256 other entities, 64 bits of keys can be shared among any two entities among the up to about 2^{40} (= 10^{12}) entities. As opposed to this, when the primitive system is taken of sharing in advance a key with all entities, the entities must store about 64 Tbits (1[Tbit] = 1024 [Gbit]).

To study the features of the KPS based on the present invention, let us compare other conventional systems.

In the past, for cipher communications, use has been made of the common key enciphering system shown in Fig. 12(a) and the public key systems shown in Fig. 12(b). Figure 12(b) shows, from left to right, the public key distribution system, public key enciphering system, and public key signature system.

On the other hand, the KPS based on the present invention may be schematized as shown in Fig. 12-(c).

Table 4 shows the results of a comparison of the above systems. In Table 4, systems I a and b correspond to (a) and (b) in Fig. 12a, systems II a, b, and c correspond to (a), (b), and (c) in Fig. 12(b), and system III shows the KPS of the present invention of Fig. 12(c). For the evaluation, the complexity of the entities is shown. For the storage capacity, there is the amount of communications upon entry into the system: communications amount (1), the amount of communications for preparation of cipher communications: communications amount (2), and the amount of computations for the preparation of cipher communications. Further, for the evaluation of the center side, the necessity of the center (yes, no), center load, "big brother" nature of the center (BB), and difficulty of mail communications are given.

From Table 4, it will be understood that the KPS of the present invention is superior overall to other conventional systems with regard to cipher communications among large numbers of unspecified entities.

Table 4

System		Complexity				Center			Mail communiccations
		Storage capacity amount	Communications amount (1)	Communications amount (2)	Computation am't	Present	Load	BB	
I	a	Large 0(n)	Large 0(n) with σ & α	None	None	No	-	-	Possible
	b	Small 0(l)	Small 0(l) with σ & α	Small 0(l) with σ & α	None	Yes	Large	Large	Difficult
II	a	Large 0(n)	Large 0(n) with α	None	None/ small	No	-	-	Possible
	b	Small 0(l)	Small 0(l) with α	Small 0(l) with α	None/ small	Yes	Large	Med.	Difficult
	c	Small 0(l)	Small 0(l) with α	Small 0(l) with α	None/ small	Yes	Small	Med.	Difficult
III		Medium 0(m)	Media 0(S) + with σ & α	None	Small	Yes	Small	Yes + +	Possible

(Note)
n: Total number of entities of network
S: Number of centers
m: Security parameters
σ: Secrecy required
α: Authenticity required

+: Reducible to 0(l)
+ +: Sufficiently small by increasing S

Above, a detailed explanation was made of the linear scheme for KPS.

There may be other methods for realization of KPS besides the linear scheme. For example, it is conceivable to construct the center algorithm as an obscure algorithm by the algorithm generation method. For details on the obscure algorithm generation method, see the afore-mentioned references.

EXPLANATION OF REFERENCE SYMBOLS

1	Secret algorithm generation apparatus
2, 3	Cryptokey generation means
4	Cipher generation means
5	Cipher text deciphering means.
6	Circuit
41	Input means
42	Enciphering means
43	Transmission means
44a	Combination means
51	Receiving means
52	Deciphering means
53	Output means
54a	Selection means
55a	Separation means

Claims

1. A common cryptokey generation system for generating a common cryptokey to be used in securely communicating text from a first entity (A) to a second entity (B), the first and second entities being remote from one another characterised by and having respective unique first and second entity identifiers (Y_A, Y_B), the system comprising: a secret algorithm generation means (1) for transforming the entity identifiers into a center algorithm (G), and for using the center algorithm to generate first and second secret algorithms (X_A, X_B) uniquely corresponding to the respective first and second entities; and first and second cryptokey generation means (2,3) associated with the respective first and second entities and remote from each other for generating the common cryptokey (K), each of the first and second cryptokey generation means having storage means for storing the respective first and second algorithms and processing means operatively coupled to the storage means for processing the respective first and second secret algorithms in combination with the respective second and first entity identifiers to generate the common cryptokey (K).

2. A common cryptokey generation system according to claim 1, wherein said secret algorithm generation apparatus is provided with a plurality of first center algorithm generation apparatuses (1a to 1d) which operate mutually independently to respectively generate independent first center algorithms (gp1(x)-,gp2(x),...) and an apparatus (1e) for combining the plurality of first center algorithms generated by the said first secret algorithm generation apparatuses and generating the distinct secret algorithm for each entity based on the combined center algorithm.

3. A common cryptokey generation system according to claim 2, wherein said first center algorithms (G) are generated by the algorithm combination method.

4. A common cryptokey generation system according to claim 2 or 3, wherein said first center algorithms (G) are generated maintaining the linear independence of vectors.

5. A common cyptokey generation system according to claim 1, wherein said center algorithm (G) is generated by the algorithm combination method.

6. A common cryptokey generation system according to claim 1, wherein the cryptokey generation means (2,3) are respectively provided with means for storing the secret algorithms, protecting them physically, and having computating capacities for cryptokey generation.

* C L M S *

Above, a detailed explanation was made of the linear scheme for KPS.

There may be other methods for realization of KPS besides the linear scheme. For example, it is conceivable to construct the center algorithm as an obscure algorithm by the algorithm generation method. For details on the obscure algorithm generation method, see the afore-mentioned references.

EXPLANATION OF REFERENCE SYMBOLS

1	Secret algorithm generation apparatus
2, 3	Cryptokey generation means
4	Cipher generation means
5	Cipher text deciphering means
6	Circuit
41	Input means
42	Enciphering means
43	Transmission means
44a	Combination means
51	Receiving means
52	Deciphering means
53	Output means
54a	Selection means
55a	Separation means

Claims

1. A common cryptokey generation system for generating a common cryptokey to be used in securely communicating text from a first entity (A) to a second entity (B), the first and second entities being remote from one another characterised by and having respective unique first and second entity identifiers (Y_A, Y_B), the system comprising: a secret algorithm generation means (1) for transforming the entity identifiers into a center algorithm (G), and for using the center algorithm to generate first and second secret algorithms (X_A, X_B) uniquely corresponding to the respective first and second entities; and first and second cryptokey generation means (2,3) associated with the respective first and second entities and remote from each other for generating the common cryptokey (K), each of the first and second cryptokey generation means having storage means for storing the respective first and second algorithms and processing means operatively coupled to the storage means for processing the respective first and second secret algorithms in combination with the respective second and first entity identifiers to generate the common cryptokey (K).

2. A common cryptokey generation system according to claim 1, wherein said secret algorithm generation apparatus is provided with a plurality of first center algorithm generation apparatuses (1a to 1d) which operate mutually independently to respectively generate independent first center algorithms (gp1(x)-,gp2(x),...) and an apparatus (1e) for combining the plurality of first center algorithms generated by the said first secret algorithm generation apparatuses and generating the distinct secret algorithm for each entity based on the combined center algorithm.

3. A common cryptokey generation system according to claim 2, wherein said first center algorithms (G) are generated by the algorithm combination method.

4. A common cryptokey generation system according to claim 2 or 3, wherein said first center algorithms (G) are generated maintaining the linear independence of vectors.

5. A common cyptokey generation system according to claim 1, wherein said center algorithm (G) is generated by the algorithm combination method.

6. A common cryptokey generation system according to claim 1, wherein the cryptokey generation means (2,3) are respectively provided with means for storing the secret algorithms, protecting them physically, and having computating capacities for cryptokey generation.

7. A common cryptokey generation system according to any one of claims 1 to 6, wherein the cryptokey generation means are semiconductor integrated circuit cards (2a) having memories and computing devices.

8. A common cryptokey generation system for generating a common cryptokey to be used in securely communicating text from a transmitting entity (A) to a plurality of receiving entities (B...), each of the transmitting and receiving entities being remote from one another characterised by each entity having a unique entity identifier (Y_A, Y_B,...), the system comprising: a secret algorithim generation means (1) for transforming the entity identifiers into a center algorithm (G), and for using the center algorithm to generate a plurality of entity algorithms, each of the entity algorithms (X_A,X_B...) uniquely corresponding to one of the entities: and a plurality of cryptokey generation means (2,3...), each of the cryptokey generation means being uniquely associated with one of the transmitting and receiving entities and remote from others of the cryptokey generation means, for generating the common cryptokey, each of the cryptokey generation means having storage means for storing the corresponding entity algorithm and processing means operatively coupled to the storage means for processing the corresponding entity algorithm in combination with the entity identifiers of others of the entities to generate the common cryptokey (K).

9. A common cryptokey generation system using a share cryptokey according to claim 8, said sender entity being adapted to send, in addition to said cipher text, the receiver identifier and its own identifier and said receiver entities being adapted to extract said receiver identifier from the received data and confirm that the data is addressed to it, and further adapted to extract the sender identifier and apply it to said cryptokey generation means so as to generate a common cryptokey.

10. A common cryptokey generation system as claimed in any one of claims 1 to 5, the first entity (A) having an enciphering device (4) for enciphering the text according to the common cryptokey (K) and transmitting a message including the enciphered text and the first and second entity identifiers, and the second entity (B) having a deciphering device (5) for receiving and deciphering the message according to the common cryptokey, wherein the first cryptokey generation means (2) operatively coupled to the enciphering device for generating the common cryptokey in response to an externally-applied command, the first cryptokey generation means including the first storage means (2A) for storing the first entity algorithm and first processing means operatively coupled to the first storage means and to the enciphering device for processing the first entity algorithm in combination with the second entity identifier to generate the common cryptokey and for communicating the common cryptokey to the enciphering device; and second cryptokey generation means (3) operatively coupled to the deciphering device and remote from the first cryptokey generation means for generating the common cryptokey, the second cryptokey generation means including second storage means for storing the second entity algorithm and second processing means operatively coupled to the second storage means and to the deciphering device for processing the second entity algorithm in combination with the first entity identifier to generate the common cryptokey and for communicating the common cryptokey to the deciphering device.

11. A common cryptokey generation system as claimed in claim 8, the transmitting entity (A) having an enciphering device (42) for enciphering the text according to the common cryptokey (K) and transmitting a message including the enciphered text, the transmitting entity identifier (Y_A), and the entity identifiers (Y_B...) of the receiving entities, and the or each of the receiving entities (B...)having a deciphering device (62) for receiving and deciphering the message according to the common cryptokey, the center algorithm (G) being used to generate a first algorithm uniquely corresponding to the transmitting entity and one or more second algorithms each uniquely corresponding to the respective receiving entity or entities: transmitting entity cryptokey generation means operatively coupled to the enciphering device for generating the common cryptokey in response to an externally-applied command, the transmitting entity cryptokey generation means including first storage means (2A) for storing the first algorithm and first processing means operatively coupled to the first storage means and to the enciphering device for processing the first algorithm in combination with the entity identifiers of the receiving entities to generate the common cryptokey and for communicating the common cryptokey to the enciphering device; and a plurality of receiving entity cryptokey generation means, each of the receiving entity cryptokey generation means being associated with one of the receiving entities and being remote from others of the transmitting and receiving entity cryptokey generation means, for

generating the common cryptokey, each of the receiving entity cryptokey generation means having second storage means for storing one of the plurality of second algorithms uniquely corresponding to the respective receiving entity and second processing means operatively coupled to the second storage means and to the deciphering device for processing the one of the second algorithms in combination with the entity identifiers of the transmitting entity identifier and others of the receiving entities to generate the common cryptokey.

12. A method for generating a common cryptokey to be used in securely communicating text from a first entity (A) to at least one second entity (B), the first and second entities being remote from one another and characterised by having respective unique first and second entity identifiers (Y_A,Y_B...) the method comprising: transforming the entity identifiers into a center algorithm (G), and using the center algorithm to generate first and second algorithms ($G(Y_A)$,$G(Y_B)$ uniquely corresponding to the respective first and second entities; prestoring the first and second algorithms at the respective first and second entities; at the first entity, in response to an externally-applied command, processing the first algorithm in combination with the or each second entity identifier to generate the common cryptokey, enciphering the text using the common cryptokey, and transmitting a message including the enciphered text and the first and second entity identifiers to the or each second entity; and at the or each second entity, processing the second algorithm or algorithms in combination with the first entity identifier to generate the common cryptokey, and deciphering the enciphered text with the common cryptokey at the or each second entity.

13. A common cryptokey generation system according to claim 1, wherein the algorithm generation means include identifier transformation means for transforming each of the first and second entity identifiers to corresponding elements of a linear space.

14. A common cryptokey generation system according to claim 8, wherein the algorithm generation means include identifier transformation means for transforming each of the transmitting and receiving entity identifiers to corresponding elements of a linear space.

Patentansprüche

1. System zur Erzeugung eines gemeinsamen Geheimübertragungsschlüssels, der zum sicheren Übertragen von Text von einem ersten Wesen (A) zu einem zweiten Wesen (B) verwendet wird, wobei das erste und zweite Wesen voneinander entfernt sind, dadurch gekennzeichnet, daß es einen ersten und zweiten Identifikator (Y_A, Y_B) für das Wesen aufweist und daß das System die folgenden Bestandteile umfaßt: eine Geheimalgorithmuserzeugungseinrichtung (1) zur Umformung der Identifikatoren für die Wesen in einen zentralen Algorithmus (G) und zur Verwendung des zentralen Algorithmus zur Erzeugung eines ersten und zweiten Geheimalgorithmus (X_A, X_B), die dem jeweiligen ersten und zweiten Wesen entsprechen, und eine erste und zweite Geheimübetragungsschlüsselerzeugungseinrichtung (2, 3), die dem ersten und zweiten Wesen zugeordnet und voneinander entfernt angeordnet sind, um den gemeinsamen Geheimübertragungsschlüssel (K) zu erzeugen, wobei jede der ersten und zweiten Geheimübertragungsschlüsselerzeugungseinrichtungen Speichereinrichtungen zum Speichern des entsprechenden ersten und zweiten Algorithmus und Bearbeitungseinrichtungen aufweist, die mit den Speichereinrichtungen gekoppelt sind, um den entsprechenden ersten und zweiten Geheimalgorithmus in Kombination mit dem entsprechenden zweiten und ersten Identifikator für die Wesen zu bearbeiten und den gemeinsamen Geheimübertragungsschlüssel (K) zu erzeugen.

2. System zur Erzeugung eines gemeinsamen Geheimübertragungsschlüssels nach Anspruch 1, bei dem die Geheimalgorithmuserzeugungsvorrichtung mit einer Vielzahl der ersten Erzeugungsvorrichtungen (1a-1d) für den zentralen Algorithmus versehen ist, die voneinander unabhägig arbeiten, um in entsprechender Weise unabhängige erste zentrale Algorithmen (gp1(x), gp2(x),...) zu erzeugen, und mit einer Vorrichtung (1e) zum Kombinieren der Vielzahl der ersten zentralen Algorithmen, die von den ersten Geheimalgorithmuserzeugungsvorrichtungen erzeugt wurden, zum Erzeugen des getrennten Geheimalgorithmus für jedes Wesen auf der Basis des kombinierten zentralen Algorithmus.

3. System zur Erzeugung eines gemeinsamen Geheimübertragungsschlüssels nach Anspruch 2, bei dem die ersten zentralen Algorithmen (G) durch das Algorithmuskombinationsverfahren erzeugt werden.

* C L M S *

4. System zur Erzeugung eines gemeinsamen Geheimübertragungsschlüssels nach Anspruch 2 oder 3, bei dem die ersten zentralen Algorithmen (G) unter Aufrechterhaltung der linearen Unabhängigkeit von Vektoren erzeugt werden.

5. System zur Erzeugung eines gemeinsamen Geheimübertragungsschlüssels nach Anspruch 1, bei dem der zentrale Algorithmus (G) durch das Algorithmuskombinationsverfahren erzeugt wird.

6. System zur Erzeugung eines gemeinsamen Geheimübertragungsschlüssels nach Anspruch 1, bei dem die Geheimübertragungsschlüsselerzeugungseinrichtungen (2,3) jeweils mit Einrichtungen zum Speichern der Geheimalgorithmen versehen sind, um diese physikalisch zu schützen, wobei die Einrichtungen Rechenkapazitäten für die Geheimübertragungsschlüsselerzeugung besitzen.

7. System zur Erzeugung eines gemeinsamen Geheimübertragungsschlüssels nach einem der Ansprüche 1 bis 6, bei dem es sich bei den Geheimübertragungsschlüsselerzeugungseinrichtungen um Karten (2a) mit integrierten Halbleiterschaltungen handelt, die Speicher- und Rechenvorrichtungen aufweisen.

8. System zur Erzeugung eines gemeinsamen Geheimübertragungsschlüssels, der zum sicheren Übertragen von Text von einem Sendewesen (A) zu einer Vielzahl von Empfängerwesen (B ...) verwendet wird, wobei jedes der Sende- und Empfängerwesen voneinander entfernt sind, dadurch gekennzeichnet, daß jedes Wesen einen Identifikator (Y_A, Y_B, ...) für ein Wesen aufweist und das System die folgenden Bestandteile umfaßt: eine Geheimalgorithmuserzeugungseinrichtung (1) zum Umformen der Identifikatoren der Wesen in einen zentralen Algorithmus (B) zum Benutzen des zentralen Algorithmus zur Erzeugung einer Vielzahl von Wesenalgorithmen, wobei jeder der Wesenalgorithmen (X_A, X_B...) einem der Wesen entspricht, und eine Vielzahl von Geheimübertragungsschlüsselerzeugungseinrichtungen (2,3...), die jeweils einem der Sende- und Empfängerwesen zugeordnet und von anderen Geheimübertragungsschlüsselerzeugungseinrichtungen entfernt angeordnet ist, um den gemeinsamen Geheimübertragungsschlüssel zu erzeugen, und wobei jede der Geheimübertragungsschlüsselerzeugungseinrichtungen Speichereinrichtungen zum Speichern des entsprechenden Wesenalgorithmus und Bearbeitungseinrichtungen, die mit den Speichereinrichtungen gekoppelt sind, zum Bearbeiten des entsprechenden Wesenalgorithmus in Kombination mit den Wesenidentifikatoren von anderen Wesen aufweist, um den gemeinsamen Geheimübertragungsschlüssel (K) zu erzeugen.

9. System zur Erzeugung eines gemeinsamen Geheimübertragungsschlüssels unter Verwendung eines gemeinsamen Geheimübertragungsschlüssels gemäß Anspruch 8, bei dem das Sendewesen zusätzlich zum Chiffretext den Empfängeridentifikator und seinen eigenen Identifikator senden kann und die Empfängerwesen den Empfängeridentifikator aus den empfangenen Daten extrahieren und bestätigen können, daß die Daten an diesen adressiert sind, sowie desweiteren den Senderidentifikator extrahieren und diesen den Geheimübertragungsschlüsselerzeugungseinrichtungen zuführen können, um einen gemeinsamen Geheimübertragungsschlüssel zu erzeugen.

10. System zur Erzeugung eines gemeinsamen Geheimübertragungsschlüssels nach einem der Ansprüche 1 bis 5, bei dem das erste Wesen (A) eine Chiffriervorrichtung (4) zum Chiffrieren des Textes gemäß dem gemeinsamen Geheimübertragungsschlüssel (K) und zum Übermitteln einer den chiffrierten Text und den ersten und zweiten Identifikator für die Wesen enthaltenden Botschaft aufweist und das zweite Wesen (B) eine Dechiffriervorrichtung (5) zum Empfangen und Dechiffrieren der Botschaft gemäß dem gemeinsamen Geheimübertragungsschlüssel besitzt, wobei die ersten Geheimübertragungsschlüsselerzeugungseinrichtungen (2) mit der Chiffriervorrichtung gekoppelt sind, um den gemeinsamen Geheimübertragungsschlüsselin Abhängigkeit von einem extern angelegten Befehl zu erzeugen, wobei die ersten Geheimübertragungsschlüsselerzeugungseinrichtungen die ersten Speichereinrichtungen (2A) zum Speichern des ersten Wesenalgorithmus und erste Bearbeitungseinrichtungen enthalten, die mit den ersten Speichereinrichtungen und der Chiffriervorrichtung gekoppelt sind, um den ersten Wesenalgorithmus in Kombination mit dem zweiten Wesenidentifikator zu bearbeiten und den gemeinsamen Geheimübertragungsschlüssel zu erzeugen und um den gemeinsamen Geheimübertragungsschlüssel mit der Chiffriervorrichtung in Verbindung zu bringen, und wobei zweite Geheimübertragungsschlüsselerzeugungseinrichtungen (3) mit der Dechiffriervorrichtung gekoppelt und entfernt von den ersten Geheimübertragungsschlüsselerzeugungseinrichtungen angeordnet sind, um den gemeinsamen Geheimübertragungsschlüssel zu erzeugen, wobei die zweiten Geheimübertragungsschlüsselerzeugungseinrichtungen zweite Speichereinrichtungen zum Speichern des zweiten Wesenalgorithmus und zweite

Bearbeitungseinrichtungen umfassen, die mit den zweiten Speichereinrichtungen und der Dechiffriervorrichtung gekoppelt sind, um den zweiten Wesenalgorithmus in Kombination mit dem ersten Wesenidentifikator zu bearbeiten und den gemeinsamen Geheimübertragungsschlüssel zu erzeugen und um den gemeinsamen Geheimübertragungsschlüssel mit der Dechiffriervorrichtung in Verbindung zu bringen.

11. System zur Erzeugung eines gemeinsamen Geheimübertragungsschlüssels nach Anspruch 8, bei dem das Sendewesen (A) eine Chiffriervorrichtung (42) zum Chiffrieren des Textes gemäß dem gemeinsamen Geheimübertragungsschlüssel(K) und zum Übertragen einer Botschaft, die den chiffrierten Text, den Sendewesenidentifikator (Y_A) und die Wesenidentifikatoren (Y_B...) der Empfangswesen enthält, aufweist und das oder jedes Empfangswesen (B...) eine Dechiffriervorrichtung (62) zum Empfangen und Dechiffrieren der Botschaft gemäß dem gemeinsamen Geheimübertragungsschlüssel besitzt, wobei der zentrale Algorithmus (G) benutzt wird, um einen ersten Algorithmus zu erzeugen, der dem Sendewesen entspricht, sowie einen oder mehrere zweite Algorithmen, die jeweils dem jeweiligen Wesen oder den Wesen entsprechenden, und wobei Sendewesen-Geheimübertragungsschlüsselerzeugungseinrichtungen mit der Chiffriervorrichtung gekoppelt sind, um den gemeinsamen Geheimübertragungsschlüsselin Abhängigkeit von einem extern angelegten Befehl zu erzeugen, wobei diese Sendewesen-Ge heimübertragungsschlüsselerzeugungseinrichtungen erste Speichereinrichtungen (2A) zum Speichern des ersten Algorithmus und erste Bearbeitungseinrichtungen, die mit den ersten Speichereinrichtungen und der Chiffriervorrichtung gekoppelt sind, zum Bearbeiten des ersten Algorithmus in Kombination mit den Wesenidentifikatoren der Empfangswesen aufweisen, um den gemeinsamen Geheimübertragungsschlüssel zu erzeugen und den gemeinsamen Geheimübertragungsschlüssel mit der Chiffriervorrichtung in Verbindung zu bringen, und wobei eine Vielzahl von Empfangswesengeheimübertragungsschlüsselerzeugungseinrichtungen vorgesehen ist, die jeweils einem der Empfangswesen zugeordnet von den anderen Sende- und Empfangswesengeheimübertragungsschlüsselerzeugungseinrichtungen entfernt sind, um den gemeinsamen Geheimübertragungsschlüssel zu erzeugen, wobei jede der Empfangswesen-Geheimübertragungsschlüsselerzeugungseinrichtungen zweite Speichereinrichtungen zum Speichern von einem aus der Vielzahl der zweiten Algorithmen, der dem jeweiligen Empfangswesen entspricht, und zweite Bearbeitungseinrichtungen aufweist, die mit den zweiten Speichereinrichtungen und der Dechiffriervorrichtung gekoppelt sind, um den einen der zweiten Algorithmen in Kombination mit den Wesenidentifikatoren des Empfangswesenidentifikators und anderen der Empfangswesen zu bearbeiten und den gemeinsamen Geheimübertragungsschlüssel zu erzeugen.

12. Verfahren zum Erzeugen eines gemeinsamen Geheimübertragungsschlüssels, der zum sicheren Übermitteln von Text von einem ersten Wesen (A) zu mindestens einem zweiten Wesen (B) verwendet wird, wobei das erste und zweite Wesen entfernt voneinander und dadurch gekennzeichnet sind, daß sie jeweils einen ersten und zweiten Wesenidentifikator (Y_A, Y_B....) besitzen, mit den folgenden Schritten: Umformen der Wesenidentifikatoren zu einem zentralen Algorithmus (G) und Verwenden des zentralen Algorithmus zur Erzeugung eines ersten und zweiten Algorithmus ($G(Y_A)$, $G(Y_B)$, die dem jeweiligen ersten Wesen entsprechen, Vorspeichern des ersten und zweiten Algorithmus am ersten und zweiten Wesen, Bearbeiten des ersten Algorithmus am ersten Wesen in Abhängigkeit von einem von außen angelegten Befehl in Kombination mit dem oder jedem zweiten Wesenidentifikator, um den gemeinsamen Geheimübertragungsschlüssel zu erzeugen, Chiffrieren des Textes unter Verwendung des gemeinsamen Geheimübertragungsschlüssels und Übermitteln einer Botschaft, die den chiffrierten Text und den ersten und zweiten Wesenidentifikator enthält, an das oder jedes erste oder zweite Wesen und Bearbeiten des zweiten Algorithmus oder der zweiten Algorithmen am zweiten Wesen oder an jedem zweiten Wesen in Kombination mit dem ersten Wesenidentifikator, um den gemeinsamen Geheimübertragungsschlüssel zu erzeugen, und Dechiffrieren des chiffrierten Textes mit dem gemeinsamen Geheimübertragungsschlüssel an dem oder an jedem zweiten Wesen.

13. System zur Erzeugung eines gemeinsamen Geheimübertragungsschlüssels nach Anspruch 1, bei dem die Algorithmuserzeugungseinrichtungen Identifikatorumformeinrichtungen zum Umformen des ersten und zweiten Wesenidentifikators zu entsprechenden Elementen eines linearen Raumes aufweisen.

14. System zur Erzeugung eines gemeinsamen Geheimübertragungsschlüssels nach Anspruch 8, bei dem die Algorithmuserzeugungseinrichtungen Identifikatorumformeinrichtungen zum Umformen eines jeden Sende- und Empfangswesenidentifikators in entsprechende Elemente eines linearen Raumes beinhalten.

* C L M S *

Revendications

1. Système de génération d'une clé cryptographique commune pour produire une clé cryptographique commune destinée à être utilisée pour communiquer, en toute sécurité, un texte d'une première entité (A) vers une seconde entité (B), ces première et seconde entités étant éloignées l'une de l'autre, caractérisé en ce qu'il comporte des identificateurs uniques (y_A,y_B) des première et seconde entités et en ce que le système comprend un moyen (1) de génération d'algorithmes secrets pour transformer les identificateurs des entités en un algorithme du centre (G) et pour utiliser l'algorithime du centre pour produire des premier et second algorithmes secrets (X_A,X_B) correspondant d'une manière unique aux première et seconde entités respectives, et des premiers et seconds moyens (2,3) de génération d'une clé cryptographique associés aux première et seconde entités respectives et éloignés les uns des autres, pour produire la clé cryptographique commune (k), chacun des premiers et seconds moyens de génération d'une clé cryptographique comportant des moyens de stockage pour emmagasiner les premier et second algorithmes secrets respectifs et des moyens de traitement couplés opérationnellement aux moyens de stockage pour traiter les premier et second algorithmes secrets respectifs en combinaison avec les identificateurs respectifs des seconde et première entités pour produire la clé cryptographique commune (k).

2. Système de génération d'une clé cryptographique commune suivant la revendication 1 caractérisé en ce que l'appareil de génération des algorithmes secrets est pourvu d'une pluralité d'appareils (1a à 1d) de génération de premiers algorithmes du centre, qui fonctionnent indépendamment les uns des autres de manière à produire respectivement des premiers algorithmes du centre indépendants (gp1(x),gp2-(x),....) et un appareil (1e) pour combiner la pluralité de premiers algorithmes du centre produits par les appareils de génération des premiers algorithmes secrets et pour produire l'algorithme secret distinct pour chaque entité sur la base de l'algorithme du centre combiné.

3. Système de génération d'une clé cryptographique commune suivant la revendication 2 caractérisé en ce que les premiers algorithmes du centre (G) sont produits par la méthode de combinaison d'algorithmes.

4. Système de génération d'une clé cryptographique commune suivant l'une quelconque des revendications 2 ou 3 caractérisé en ce que les premiers algorithmes du centre (G) sont produits en maintenant l'indépendance linéaire de vecteurs.

5. Système de génération d'une clé cryptographique commune suivant la revendication 1 caractérisé en ce que l'algorithme du centre (G) est produit par la méthode de combinaison d'algorithmes.

6. Système de génération d'une clé cryptographique commune suivant la revendication 1 caractérisé en ce que les moyens (2,3) de génération de la clé cryptographique sont pourvus respectivement de moyens pour stocker les algorithmes secrets, pour les protéger physiquement et ayant des capacités de calcul pour la génération de la clé cryptographique.

7. Système de génération d'une clé cryptographique commune suivant l'une quelconque des revendications 1 à 6 caractérisé en ce que les moyens de génération de la clé cryptograpthique sont des cartes (2a) à circuit intégré semi-conducteur comportant des mémoires et des dispositifs de calcul.

8. Système de génération d'une clé cryptographique commune pour produire une clé cryptographique commune destinée à être utilisée lors de la communication, en toute sécurité, d'un texte à partir d'une entité émettrice (A) vers une pluralité d'entités réceptrices (B), chacune des entités émettrice et réceptrices étant éloignée des autres, caractérisé en ce que chaque entité a un identificateur d'identité unique (y_A,y_B) et le système comprend un moyen (1) de génération d'algorithmes secrets pour transformer les identificateurs des entités en un aligorithme du centre (G) et pour utiliser l'algorithme du centre (G) pour produire une pluralité d'algorithmes d'entité, chacun des algorithmes d'entité (X_A,X_B) correspondant d'une manière unique à l'une des entités, et une pluralité de moyens (2,3) de génération d'une clé cryptographique, chacun des moyens de génération d'une clé cryptographique étant associé d'une manière unique à l'une des entités émettrice et réceptrices et étant situé à distance des autres moyens de génération d'une clé cryptographique, afin de produire la clé cryptographique commune, chacun des moyens de génération d'une clé cryptographique comportant des moyens de stockage

* C L M S *

pour stocker l'algorithme d'entité correspondant et des moyens de traitement couplés opérationnellement aux moyens de stockage pour traiter l'algorithme d'entité correspondant en combinaison avec les identificateurs d'entité d'autres parmi les entités, afin de produire la clé cryptographique commune (k).

9. Système de génération d'une clé cryptographique commune utilisant une clé cryptographique partagée, suivant la revendication 8, caractérisé en ce que l'entité émettrice est adaptée de manière à émettre, en plus du texte chiffré, l'identificateur du récepteur et son propre identificateur et chacune des entités réceptrices est adaptée de manière à extraire l'identificateur de l'entité réceptrice à partir de la donnée roue et à confirmer que la donnée est adressée à elle, et elle est en outre adaptée de manière à extraire l'identificateur de l'entité émettrice et de l'appliquer aux moyens de génération d'une clé cryptographique de manière à produire une clé cryptographique commune.

10. Système de génération d'une clé cryptographique commune suivant l'une quelconque des revendications 1 à 5 caractérisé en ce que la première entité (A) comporte un dispositif de chiffrage (4) pour chiffrer le texte en accord avec la clé cryptographique commune (k) et elle émet un message comprenant le texte chiffré et les identificateurs des première et seconde entités, et la seconde entité (B) comprend un dispositif de déchiffrage (5) pour recevoir et déchiffrer le message en accord avec la clé cryptographique commune, les premiers moyens (2) de génération d'une clé cryptographique sont couplés opérationnellement au dispositif de chiffrage afin de produire la clé cryptographique commune en réponse à un ordre appliqué de l'extérieur, ces premiers moyens de génération d'une clé cryptographique comportant les premiers moyens de stockage (2A) pour stocker l'algorithme de la première entité et les premiers moyens de traitement couplés opérationnellement aux premiers moyens de stockage et au dispositif de chiffrage pour traiter l'algorithme de la première entité, en combinaison avec l'identificateur de la seconde entité, afin de produire la clé cryptographique commune, et pour communiquer la clé cryptographique commune au dispositif de chiffrage, et les seconds moyens (3) de génération d'une clé cryptographique sont couplés opérationnellement au dispositif de déchiffrage et ils sont situés à distance des premiers moyens de génération d'une clé cryptographique pour produire la clé cryptographique commune, les seconds moyens de génération d'une clé cryptographique comportant des seconds moyens de stockage pour stocker l'algorithme de la seconde entité et des seconds moyens de traitement couplés opérationnellement aux seconds moyens de stockage et au dispositif de déchiffrage pour traiter l'algorithme de la seconde entité en combinaison avec l'identificateur de la première entité, afin de produire la clé cryptographique commune et pour communiquer cette clé cryptographique commune au dispositif de déchiffrage.

11. Système de génération d'une clé cryptographique commune suivant la revendication 8 caractérisé en ce que l'entité émettrice (A) comporte un dispositif de chiffrage (42) pour chiffrer le texte en accord avec la clé cryptographique commune (k) et elle émet un message comportant le texte chiffré, l'identificateur (y_A) de l'entité émettrice et les identificateurs (y_B...) des entités réceptrices, l'entité réceptrice ou chacune des entités réceptrices (B...) comporte un dispositif de déchiffrage (62) pour recevoir et déchiffrer le message en accord avec la clé cryptographique commune, l'algorithme du centre (G) est utilisé pour produire un premier algorithme correspondant d'une manière unique à l'entité émettrice et un ou plusieurs seconds algorithmes correspondant chacun d'une manière unique à l'entité ou aux entités réceptrices respectives, des moyens de génération d'une clé cryptographique de l'entité émettrice sont couplés opérationnellement au dispositif de chiffrage afin de produire la clé cryptographique commune en réponse à un ordre appliqué de l'extérieur, les moyens de génération d'une clé cryptographique de l'entité émettrice comportent des premiers moyens de stockage (2A) pour stocker le premier algorithme et des premiers moyens de traitement couplés opérationnellement aux premiers moyens de stockage et au dispositif de chiffrage afin de traiter le premier algorithme en combinaison avec les identificateurs des entités réceptrices, afin de produire la clé cryptographique commune, et pour communiquer la clé cryptographique commune au dispositif de chiffrage, et il comporte une pluralité de moyens de génération d'une clé cryptographique des entités réceptrices, chacun des moyens de génération d'une clé cryptographique d'une entité réceptrice étant associé à l'une des entités réceptrices et étant situé à distance des autres moyens de génération d'une clé cryptographique de l'entité émettrice et des entités réceptrices, afin de produire la clé cryptographique commune, chacun des moyens de génération d'une clé cryptographique des entités réceptrice comporte des seconds moyens de stockage pour stocker l'un de plusieurs seconds algorithmes correspondant d'une manière unique à l'entité réceptrice respective, et des seconds moyens de traitement couplés opérationnellement aux seconds moyens de stockage et au dispositif de déchiffrage

* C L M S *

afin de traiter l'algorithme correspondant parmi les seconds algorithmes en combinaison avec les identificateurs de l'entité émettrice et ceux des entités réceptrices, afin de produire la clé cryptographique commune.

12. Procédé de génération d'une clé cryptographique commune destiné à être utilisé pour la communication, en toute sécurité, d'un texte à partir d'une première entité (A) vers au moins une seconde entité (B), les première et seconde entités étant éloignées l'une de l'autre et étant caractérisées par le fait qu'elles ont des identificateurs respectifs uniques des première et seconde identités (y_A,y_B), caractérisé en ce qu'il comprend les étapes consistant à transformer les identificateurs des entités en un algorithme du centre (G) et à utiliser cet algorithme du centre pour produire des premier et second algorithmes ($G(Y_A)$,$G(Y_B)$) correspondant respectivement, d'une manière unique, aux première et seconde entités, à préemmagasiner les premier et second algorithmes à l'endroit des première et seconde entités respectives, à traiter le premier algorithme, à l'endroit de la première entité, en réponse à un ordre appliqué de l'extérieur, en combinaison avec l'identificateur de la seconde entité ou chaque identificateur d'une seconde entité, afin de produire la clé cryptographique commune, à chiffrer le texte en utilisant la clé cryptographique commune et à émettre un message, comportant le texte chiffré et les identificateurs de la première et de la seconde entité, en direction de la seconde entité ou de chaque seconde entité, et à traiter le second algorithme ou les seconds algorithmes, à l'endroit de la seconde entité ou de chaque seconde entité, en combinaison avec l'identificateur de la première entité, afin de produire la clé cryptographique commune, et à déchiffrer le texte chiffré au moyen de la clé cryptographique commune, à l'endroit de la seconde entité ou de chaque seconde entité.

13. Système de génération d'une clé cryptographique commune suivant la revendication 1 caractérisé en ce que les moyens de génération de l'algorithme comportent un moyen de transformation d'identificateur afin de transformer chacun des identificateurs des première et seconde entités en des éléments correspondants d'un espace linéaire.

14. Système de génération d'une clé cryptographique commune suivant la revendication 8 caractérisé en ce que les moyens de génération de l'algorithme comportent un moyen de transformation d'identificateur afin de transformer chacun des identificateurs des entités émettrice et réceptrice en des éléments correspondants d'un espace linéaire.