Title: SYSTEM, TERMINAL, METHOD, AND SOFTWARE FOR COMMUNICATING MESSAGES

Abstract: A system for secure communication of a message from a first terminal to a second terminal being operated by a means of a communication network comprising an authenticating station for obtaining a random seed and a masked seed by applying a masking function to the seed by encrypting the message using the masked seed for transmitting the seed and the encrypted message to the authenticating station; the authenticating station comprising further means for obtaining a further random seed for receiving the seed and the encrypted message for recovering the further masked seed by applying the masking function to the seed by decrypting the encrypted message using the recovered masked seed and by applying a masking function to the further seed by encrypting the recovered message using the further masked seed for transmitting the further seed and the further encrypted message to the second terminal; the second terminal comprising receiving means for receiving the further seed and the further encrypted message for recovering the further masked seed by applying the masking function to the further seed by decrypting the further encrypted message using the recovered further masked seed.
Declaration under Rule 4.17:
— as to applicant’s entitlement to apply for and be granted a patent (Rule 4.17(ii))
— before the expiration of the time limit for amending the claims and to be republished in the event of receipt of amendments

Published:
— with international search report

For two-letter codes and other abbreviations, refer to the “Guidance Notes on Codes and Abbreviations” appearing at the beginning of each regular issue of the PCT Gazette.
System, terminal, method, and software for communicating messages

The invention relates to a system for secure communication of a message from a first terminal to a second terminal, the first terminal being operatively coupled to the second terminal by means of a communication network comprising an authenticating station.

The invention also relates to a first terminal, a second terminal, an authenticating station, a method and computer program products for use in such a system.

The problem of securely communicating a message between two parties is well known. It requires keeping the message secret while it is being communicated as well as authentication of the sending party and the receiving party. Secrecy and authentication may be provided to a certain extent by a telephony system. Someone answering a call as expected authenticates the other party.

In a mobile phone network, for example, in accordance with the GSM standard, ciphered telephone conversations are held between the mobile phone and the base station, as described in specification 3GPP TS 43.020 V5.0.0, section 4.3. This secures the telephone conversation against eavesdropping on the air interface only.

It is a drawback of this known system that it does not provide highly secure end-to-end communication between the first and the second terminal.

It is an object of the invention to provide a system of the type described in the opening paragraph, wherein the message may be securely communicated end-to-end, approaching the level of security of the subscription to the network.

The object is realized in the system comprising:

- the first terminal, comprising:
  - means for obtaining a random seed ($S_A$),
  - computing means for obtaining a masked seed ($M_A$) by applying a masking function ($F_A$) to the seed ($S_A$), and for obtaining an encrypted message ($K_A$) by encrypting the message ($M$) using the masked seed ($M_A$),
- transmitting means for transmitting the seed \( S_A \) and the encrypted message \( K_A \) to the authenticating station;
- the authenticating station, comprising:
- further means for obtaining a further random seed \( S_B \),
- receiving means for receiving the seed \( S_A \) and the encrypted message \( K_A \);
- further computing means for:
  a. recovering the masked seed \( M_A \) by applying the masking function \( F_A \) to the seed \( S_A \),
  b. recovering the message \( M \) by decrypting the encrypted message \( K_A \) using the recovered masked seed \( M_A \),
  c. obtaining a further masked seed \( M_B \) by applying a masking function \( F_B \) to the further seed \( S_B \), and
  d. obtaining a further encrypted message \( K_B \) by encrypting the recovered message \( M \) using the further masked seed \( M_B \),
- further transmitting means for transmitting the further seed \( S_B \) and the further encrypted message \( K_B \) to the second terminal;
- the second terminal, comprising:
- receiving means for receiving the further seed \( S_B \) and the further encrypted message \( K_B \);
- still further computing means for:
  a. recovering the further masked seed \( M_B \) by applying the masking function \( F_B \) to the further seed \( S_B \),
  - recovering the message \( M \) by decrypting the further encrypted message \( K_B \) using the recovered further masked seed \( M_B \).

The message may consist of or comprise a secret key for use in further secure communications between the terminals. The further secure communications may use the communication network, but may alternatively use another network, e.g. the Internet. The system may be used to bootstrap trusted secure communications between two subscribers without requiring a physical visit between them. An example of such usage is the secure establishment of a web community, where the message comprises a key for accessing the web community via the Internet, and the message is securely distributed to each member of the web community.

The system can be used for sharing a secret message between terminals subscribed on a single authenticating station, but alternatively, the system may also be used
between a first terminal subscribed to a first authenticating station, and a second terminal subscribed to a second authenticating station. This requires the additional step of securely forwarding the message from the first authenticating station to the second authenticating station. This has the advantage that the message may be exchanged securely between terminals that authenticate at respective authenticating stations, e.g. a first mobile phone subscribed to a first network operator and a second mobile phone subscribed to a second network operator. A further advantage is that the first or the second terminal or both the terminals may be roaming, i.e. away from their home network and served by a visiting network.

The security of the system has a basis in that only the first terminal and the authenticating station share the masking function $F_A$, and similarly, in that only the second terminal and the authenticating station share the masking function $F_B$.

Since each masking function is only shared between a terminal and the authenticating station, the user of the first terminal may be sure that only the authenticating station can generate the decryption key and recover the message. Similarly, the user of the second terminal may be sure that only the authenticating station can recover the message from the seed and generate the masked seed, ensuring that the message comes from a trusted source.

The components of the system, comprising the first and the second terminal and the authenticating station are each arranged to execute the intended actions in the order given, so as to collaborate for a secure communication of the message. A manual trigger by a user of the first terminal may initiate the actions from the first terminal, but also an automated trigger may do so, e.g. from a software application running on the first terminal.

The message may be in a digital or in an analog format. If the message is in an analog format, it may be converted into a digital format before the encryption. Alternatively, the encryption may be performed on the analog format of the message.

The transmitting may also comprise an identification of the second terminal, e.g. a medium access control (MAC) address, an Internet Protocol (IP) address, a Uniform Resource Identifier (URI) or Locator (URL), a Session Initiation Protocol (SIP) address, a subscriber identifier (IMSI), an equipment identifier (IMEI), or a telephone number as an E.164 address.

The transmitting may be performed with known signaling methods or channels, but it may also involve a method or channel dedicated to this purpose.
US patent 6373946B1 discloses a system for distributing enciphering key data in a satellite mobile telecommunication system. The enciphering key data is distributed from a remote node to both terminals, however, thus solving a problem other than that of securely communicating a message between the first and the second terminal.

In an embodiment, the system has the features of claim 2. This provides the advantage that the message may be distributed from the first terminal to both the second and the third terminal. It also saves execution time and power, because the authenticating station does not execute the first steps a second time. Furthermore, an overhead of the protocol between the first terminal and the authenticating station may be saved, because the transmitting may simply comprise a further identification of the third terminal.

Another advantage is the additional convenience for the user operating the first terminal, as lists of terminals may be addressed in one go.

This system may be used in particular for bootstrapping secure communications amongst a plurality of terminals. The system may be used for securely establishing one of the popular World Wide Web or Wireless Access Protocol communities on the Internet.

The system may be further expanded to include at least one further terminal, and as such is not limited to three terminals.

In another embodiment, the system has the features of claim 3. This further increases the ease of use for the end-users operating the terminals. Mobile phone networks are ubiquitous, such that the message may be exchanged with large numbers of terminals.

Since the masking function and the further masking function are respective authentication functions of the mobile phone network, this system fits in well with the typical mobile phone infrastructure, where a terminal gains access to the network after authentication with the authenticating station. This provides a strong authentication based on a secret key shared between a tamper-proof security module in the terminal and the authenticating station.

As the primitives of the system are already in place in a typical mobile phone network, the system is relatively easy to deploy, alleviating much of the burden of alternative systems.

Although the first terminal may consist of a mobile phone, the first terminal may also comprise further components like further coupled devices, e.g. a PDA or laptop computer.

It typically suffices that the transmitting means are part of a first mobile phone, and that the further receiving means are part of a second mobile phone.
The means for obtaining the random seed and the computing means may advantageously be implemented in a tamper-proof module, for example, a smartcard or a Subscriber Identity Module (SIM).

The first terminal dialing a particular telephone number dedicated for this purpose may trigger execution of the steps in the authenticating station. Alternatively, execution of the method may be triggered by wrapping the message and the address of the second terminal in a dedicated type of content for the ubiquitous Short Message Service (SMS) and sending the content to a particular dedicated destination address. Although messages may be communicated by means of SMS services, these services provide a lower level of security than the security level that may be achieved with a system according to the invention. This is especially the case if the computations are executed in the tamper-proof Secure Identification Module (SIM).

Both subscribers trust the network operator, which acts as a trusted third party. The message may consist of or comprise a public key for use in further secure communications between the terminals. In that case, the system ensures that the public key comes from an authenticated trusted terminal.

The system can be deployed with relatively little cost because only relatively minor changes to the existing mobile phone network are required. For the network operator, it has the advantage of allowing a new service offer to the end-users. Also, the service is relatively simple to deploy through the network.

The system may be combined in a relatively easy way with the billing functionality of the mobile phone network. Payments for using the system may be debited from an end-user account.

The system may also be adapted for use with a roaming terminal, where the system comprises a visitor location register for registering visiting subscribers. After communication between the authenticating station and the visitor location register, for example, carried by the mobile application part in a network with the signaling system number 7 set of standards, the visitor location register may act as a proxy for the authenticating station, having a replica of some data in the authenticating station.

In a particular embodiment of the system, the message may be an SMS message. This offers the advantage that part of the existing infrastructure may be used, e.g. an SMS message editor in the first terminal, an SMS message handling application like an inbox, outbox and menus for their control. It also offers the advantageous combination of a
relatively high security level, which approaches the security level of the subscription, with the convenience and popularity of SMS messaging.

In another embodiment, the system has the features of claim 4. A particularly popular type of mobile phone network is based on the GSM or UMTS standards. The A3 authentication function has proven to be secure and cost-effective in practice, while still leaving room for network operators to set parameters for specializing the authentication function for their network.

The above object and features of the system 100 of the present invention will be more apparent from the following description with reference to the drawings.

Fig. 1 is a block diagram of a system 100 according to the invention.

Fig. 2 shows an overview of a system 100 according to the invention.

Fig. 3 shows an overview of a system 100 with a third terminal according to the invention.

Fig. 4 is a block diagram of a system 100 with a third terminal according to the invention.

In the embodiment of Fig. 2, the system 100 comprises a first terminal 102, a second terminal 103 and a communication network 104 with an authenticating station 105. The first and the second terminal 102, 103 are adapted GSM or UMTS phones operatively coupled by means of a GSM communication network 104 which includes a home location register (HLR) 105. The system 100 is arranged for secure communication of a message M from the first terminal 102 to the second terminal 103.

The embodiment of Fig. 2 is shown in more detail in Fig. 1. The first terminal 102 has means 106 for obtaining a random seed $S_A$. The means 106 may be a random number generator and may be implemented in hardware, or partially or as a whole in software. One example is a linear congruential random number generator. The means 106 may also be used in creating the message M. This is particularly advantageous if the message M comprises a key for use with further communications between the terminals 102, 103, because such a key may be generated with the help of a random number generated by the means 106. This saves a random number generator.
The first terminal 102 has computing means 108 arranged to obtain a masked seed \( M_A \) by applying a masking function \( F_A \) to the seed \( S_A \). The computing means 108 may be or comprise a general-purpose processor as is commonly used in a computer like a desktop, a laptop, a handheld or a palmtop computer. The computing means 108 may also be or comprise a dedicated processor like an embedded processor in a GSM or UMTS phone, or a smartcard. The computing means 108 may partially or as a whole be tamper-proof, for example, like the ubiquitous Subscriber Identity Module (SIM) used in mobile phones, or a chipcard with an e-purse function. This has the advantage that it is relatively hard to tamper with the computing means 108 so as to manipulate its behavior or peek in its internals to recover e.g. the message \( M \) or the masking function \( M_A \), such that the effort to crack the computing means typically outweighs the gain in doing so.

The masking function \( M_A \) has the property that it masks the random seed \( S_A \) to which it is applied, such that it is relatively hard to recover the random seed \( S_A \) from the masked random seed \( M_A \).

Just like the further masking function \( F_B \), the masking function \( F_A \) may be respective authentication functions of the terminals 102, 103 of a mobile phone network 104. The masking function may be as simple as an exclusive one or with a serial number or a hardware key that differs between terminals.

The respective authentication functions may be the A3 authentication functions of the first and the second terminal 102, 103 if the network 104 is a GSM mobile phone network. Alternatively, the A5, A8 or GEA3 functions may be used. In turn, each of these functions may rely on the KGCORE function. Advantages of these functions include that they allow keys with arbitrary but predetermined lengths. These functions are described, for example, in 3GPP TS 55.216 V6.2.0.

The computing means 108 are further arranged to obtain an encrypted message 109 by encrypting the message \( M \) using the masked seed \( M_A \) as a key for the encryption. The encryption may be based on secret key algorithms, for example, the DES or triple-DES algorithms, or on public key algorithms like ElGamal or Diffie-Helman cryptography.

The first terminal 102 has transmitting means 112 for transmitting the seed \( S_A \) and the encrypted message \( K_A \) to the authenticating station 105. The transmitting means 112 may be arranged to transmit through a medium that has a wire or is wireless, with e.g. an RF transmitter and an antenna in the latter case. The transmission may e.g. take place with an SMS or with an MMS. Conveying the encrypted message \( K_A \) to the authenticating station
105 may involve several links, for example, one wireless link to the base station of the GSM network, followed by wired links to the authenticating station.

The authenticating station 105 serves the purposes of authenticating the messages $K_A$ transmitted by the first terminal 102, re-encrypting the message, and forwarding the message to the destination terminal 103. The authenticating station 105 may be a HLR as is common in GSM networks, but it may also be a SIP server, or another server.

The authenticating station 105 has receiving means 115 for receiving the seed $S_A$ and the encrypted message $K_A$ from the first terminal, for example, a GSM receiver. The authenticating station 105 also has further computing means 116. The further computing means 116 may be e.g. a general-purpose or a dedicated processor. The authenticating station 105 also has a random number generator 113 for generating the further random seed $S_B$. The random number generator 113 may be implemented in the further computing means 116, for example, with a software routine implementing a linear congruential random number generator.

The authenticating station 105 is arranged to recover the further masked seed $M_A$ by applying the masking function $F_A$ to the seed $S_A$, recovering the message $M$ by decrypting the encrypted message $K_A$ using the recovered masked seed $M_A$, obtaining a further masked seed $M_B$ by applying a masking function $F_B$ to the further seed $S_B$, and obtaining a further encrypted message $K_B$ by encrypting the recovered message $M$ using the further masked seed $S_B$. These steps may be implemented largely in software routines executed by a processor comprised by the further computing means 116.

The authenticating station 105 has further transmitting means 120 for transmitting the further seed $S_B$ and the further encrypted message $K_B$ to the second terminal. Again, in a GSM network, this involves both wired and wireless links, from a HLR to a base station to the second terminal, which may be an adapted mobile phone.

The second terminal 103 has receiving means 121 and further computing means 122.

The receiving means 121 receive the further seed $S_B$ and the further encrypted message $K_B$, and the receiving means 121 may be part of e.g. an adapted GSM phone. The adaptation to the mobile phone may be limited to the software embedded or downloaded in the phone, with the advantage that the adaptations are relatively cheap. The further computing means 122 have the purposes of recovering the further masked seed $M_B$ by applying the masking function $F_B$ to the further seed $S_B$, and of recovering the message $M$ by decrypting the further encrypted message $K_B$ using the recovered further masked seed $M_B$. 
Subsequently, the recovered message $M$ may be stored, forwarded, presented or further processed.

In the embodiment of Fig. 3 and Fig. 4, the system has a third terminal 123. What has been stated about the second terminal 103 also holds for the third terminal 123. The third terminal 123 may well be identical to the second terminal 103. In this embodiment, the authenticating station 105 has still further means 124 for obtaining a still further random seed $S_C$, yet further computing means 126, and still further transmitting means 131 for transmitting the still further random seed $S_C$ and the still further encrypted message $K_C$ to the third terminal 123. The yet further computing means 126 are arranged to obtain a still further masked seed $M_C$ by applying a still further masking function $F_C$ to the still further random seed $S_C$, and obtaining a still further encrypted message $K_C$ by encrypting 130 the recovered message $M$ using the still further masked seed $M_C$. The third terminal 123 has still further receiving means 132 for receiving the still further random seed $S_C$ and the still further encrypted message $K_C$, yet still further computing means 133 for recovering the still further masked seed $M_C$ by applying the still further masking function $F_C$ to the still further random seed $S_C$, recovering the message $M$ by decrypting 134 the still further encrypted message $K_C$ using the still further masked seed $M_C$. Of course many more than two terminals may be part of the system. Moreover, many terminals may be addressed in one go when sending the message $M$ from the first terminal 102 to the authenticating station 105, such that the message $M$ is delivered to each addressed terminal.

The embodiments of the system 100 according to the invention as described above are each arranged to execute the method according to the invention.

Also, the above described embodiments of the first and the second terminal 102, 103, and of the authenticating station 105, may each have a processor programmed with a computer program product according to the invention, enabling each processor to execute its part of the method according to the invention.

It is noted that the above-mentioned embodiments illustrate rather than limit the invention, and that those skilled in the art will be able to design many alternative embodiments without departing from the scope of the appended claims. In the claims, any reference signs placed between parentheses shall not be construed as limiting the claim. Use of the verb "comprise" and its conjugations does not exclude the presence of elements or steps other than those stated in a claim. Use of the indefinite article "a" or "an" preceding an element does not exclude the presence of a plurality of such elements. The invention can be implemented by means of hardware comprising several distinct elements, and by means of a
suitably programmed computer. In a system or a device claim that enumerates several means, the same item of hardware may embody several of these means. The mere fact that certain measures are recited in mutually different dependent claims does not indicate that a combination of these measures cannot be used to advantage.

A ‘computer program’ is to be understood to mean any software product stored on a computer-readable medium, such as a floppy disk, downloadable via a network, such as the Internet, or marketable in any other manner.
<table>
<thead>
<tr>
<th>Fig.</th>
<th>Text 99</th>
<th>Abbr.</th>
</tr>
</thead>
<tbody>
<tr>
<td>100</td>
<td>system</td>
<td>S</td>
</tr>
<tr>
<td>M</td>
<td>message</td>
<td>M</td>
</tr>
<tr>
<td>102</td>
<td>first terminal</td>
<td>FT</td>
</tr>
<tr>
<td>103</td>
<td>second terminal</td>
<td>ST</td>
</tr>
<tr>
<td>104</td>
<td>communication network</td>
<td>CN</td>
</tr>
<tr>
<td>105</td>
<td>authenticating station</td>
<td>AS</td>
</tr>
<tr>
<td>106</td>
<td>means</td>
<td>M</td>
</tr>
<tr>
<td>Sa</td>
<td>random seed</td>
<td>RS</td>
</tr>
<tr>
<td>108</td>
<td>computing means</td>
<td>CM</td>
</tr>
<tr>
<td>109</td>
<td>encrypting</td>
<td></td>
</tr>
<tr>
<td>Ma</td>
<td>masked seed</td>
<td>MS</td>
</tr>
<tr>
<td>110</td>
<td>decrypting</td>
<td></td>
</tr>
<tr>
<td>Fa</td>
<td>masking function</td>
<td>MF</td>
</tr>
<tr>
<td>Ma</td>
<td>encrypted message</td>
<td>EM</td>
</tr>
<tr>
<td>112</td>
<td>transmitting means</td>
<td>TM</td>
</tr>
<tr>
<td>113</td>
<td>further means</td>
<td>FM</td>
</tr>
<tr>
<td>Sb</td>
<td>further random seed</td>
<td>FRS</td>
</tr>
<tr>
<td>115</td>
<td>receiving means</td>
<td>RM</td>
</tr>
<tr>
<td>116</td>
<td>further computing means</td>
<td>FCM</td>
</tr>
<tr>
<td>117</td>
<td>encrypting</td>
<td></td>
</tr>
<tr>
<td>Mb</td>
<td>further masked seed</td>
<td>FMS</td>
</tr>
<tr>
<td>118</td>
<td>decrypting</td>
<td></td>
</tr>
<tr>
<td>Fb</td>
<td>further masking function</td>
<td>MF</td>
</tr>
<tr>
<td>Kb</td>
<td>further encrypted message</td>
<td>FEM</td>
</tr>
<tr>
<td>120</td>
<td>further transmitting means</td>
<td>FTM</td>
</tr>
<tr>
<td>121</td>
<td>receiving means</td>
<td>RM</td>
</tr>
<tr>
<td>122</td>
<td>further computing means</td>
<td>SFCM</td>
</tr>
<tr>
<td>123</td>
<td>third terminal</td>
<td>TT</td>
</tr>
<tr>
<td>124</td>
<td>further means</td>
<td>SFM</td>
</tr>
<tr>
<td>125</td>
<td>further random seed</td>
<td>SFRS</td>
</tr>
<tr>
<td>126</td>
<td>further computing means</td>
<td>YFCM</td>
</tr>
<tr>
<td>127</td>
<td>3</td>
<td>further masked seed</td>
</tr>
<tr>
<td>128</td>
<td>3</td>
<td>further masking function</td>
</tr>
<tr>
<td>129</td>
<td>3</td>
<td>further encrypted message</td>
</tr>
<tr>
<td>130</td>
<td>3</td>
<td>encrypting</td>
</tr>
<tr>
<td>131</td>
<td>3</td>
<td>further transmitting means</td>
</tr>
<tr>
<td>132</td>
<td>3</td>
<td>further receiving means</td>
</tr>
<tr>
<td>133</td>
<td>3</td>
<td>further computing means</td>
</tr>
<tr>
<td>134</td>
<td>4</td>
<td>decrypting</td>
</tr>
</tbody>
</table>
CLAIMS:

1. A system (100) for secure communication of a message (M) from a first terminal (102) to a second terminal (103), the first terminal (102) being operatively coupled to the second terminal (103) by means of a communication network (104) comprising an authenticating station (105), the system comprising:

- the first terminal (102), comprising:
  - means (106) for obtaining a random seed (S₁),
  - computing means (108) for obtaining a masked seed (M₁) by applying a masking function (F₁) to the seed (S₁), and for obtaining an encrypted message (K₁) by encrypting the message (M) using the masked seed (M₁),
  - transmitting means (112) for transmitting the seed (S₁) and the encrypted message (K₁) to the authenticating station;

- the authenticating station (105), comprising:
  - further means (113) for obtaining a further random seed (S₂),
  - receiving means (115) for receiving the seed (S₁) and the encrypted message (K₁);

- further computing means (116) for:
  a. recovering the masked seed (M₁) by applying the masking function (F₁) to the seed (S₁),
  b. recovering the message (M) by decrypting the encrypted message (K₁) using the recovered masked seed (M₁),
  c. obtaining a further masked seed (M₂) by applying a masking function (F₂) to the further seed (S₂), and
  d. obtaining a further encrypted message (K₂) by encrypting the recovered message (M) using the further masked seed (M₂),

- further transmitting means (120) for transmitting the further seed (S₂) and the further encrypted message (K₂) to the second terminal;

- the second terminal (103), comprising:
  - receiving means (121) for receiving the further seed (S₂) and the further encrypted message (K₂);
- still further computing means (122) for:
  a. recovering the further masked seed (M_B) by applying the masking function (F_B) to the further seed (S_B),
  b. recovering the message (M) by decrypting the further encrypted message (K_B) using the recovered further masked seed (M_B).

2. A system as claimed in claim 1, further comprising a third terminal (123), wherein
   - the authenticating station (105) further comprises:
     - still further means (124) for obtaining a further random seed (S_C),
     - yet further computing means (126) for:
       a. obtaining a still further masked seed (M_C) by applying a still further masking function (F_C) to the still further random seed (S_C), and
       b. obtaining a still further encrypted message (K_C) by encrypting (130) the recovered message (M) using the still further masked seed (M_C),
     - still further transmitting means (131) for transmitting the still further random seed (S_C) and the still further encrypted message (K_C) to the third terminal;
     - the third terminal (123) comprises:
       - still further receiving means (132) for receiving the still further random seed (S_C) and the still further encrypted message (K_C);
     - yet still further computing means (133) for:
       a. recovering the still further masked seed (M_C) by applying the still further masking function (F_C) to the still further random seed (S_C);
       b. recovering the message (M) by decrypting (134) the still further encrypted message (K_C) using the still further masked seed (M_C).

3. A system as claimed in claim 1, wherein the communication network (104) comprises a mobile phone network, and wherein the masking function (F_A) and the further masking function (F_B) are respective authentication functions of the mobile phone network.

4. A system as claimed in claim 3, wherein the mobile phone network is a GSM network and wherein the respective authentication functions are the A3 authentication functions of the first (102) and the second terminal (103).
5. A first terminal (102) for use in a system according to claim 1.

6. An authenticating station (105) for use in a system according to claim 1.

7. A second terminal (103) for use in a system according to claim 1.

8. A method of securely communicating a message (M) from a first terminal (102) to a second terminal (103), the first and the second terminal being operatively coupled by means of a communication network (104) comprising an authenticating station (105), the method comprising the steps of:
   - the first terminal (102):
     - obtaining a masked seed (M₁) by applying a masking function (F₁) to a random seed (S₁);
     - obtaining an encrypted message (K₁) by encrypting the message (M) using the masked seed (M₁);
     - transmitting the random seed (S₁) and the encrypted message (K₁) to the authenticating station;
   - the authenticating station (105):
     - receiving the random seed (S₁) and the encrypted message (K₁);
     - recovering the masked seed (M₁) by applying the masking function (F₁) to the random seed (S₁);
     - recovering the message (M) by decrypting the encrypted message (K₁) using the masked seed (M₁);
     - obtaining a further masked seed (M₂) by applying a further masking function (F₂) to a further random seed (S₂);
     - obtaining a further encrypted message (K₂) by encrypting the message (M) using the further masked seed (M₂);
     - transmitting the further random seed (S₂) and the further encrypted message (K₂) to the second terminal;
   - the second terminal (103):
     - receiving the further random seed (S₂) and the further encrypted message (K₂);
     - recovering the further masked seed (M₂) by applying the further masking function (F₂) to the further random seed (S₂);
- recovering the message (M) by decrypting the further encrypted message (K_B) using the further masked seed (M_B).

9. A computer program product for execution on a processor of a first terminal (102), enabling the first terminal to execute its part of the method according to claim 1.

10. A computer program product for execution on a processor of an authenticating station (105), enabling the authenticating station to execute its part of the method according to claim 1.

11. A computer program product for execution on a processor of a second terminal (103), enabling the second terminal to execute its part of the method according to claim 1.
FIG. 1
FIG. 2

FIG. 3
INTERNATIONAL SEARCH REPORT

A. CLASSIFICATION OF SUBJECT MATTER
INV. H04L9/08

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
H04L

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the International search (names of data base and, where practical, search forms used)
EPO-Internal, WPI Data, INSPEC

C. DOCUMENTS CONSIDERED TO BE RELEVANT

<table>
<thead>
<tr>
<th>Category</th>
<th>Citation of document, with indication, where appropriate, of the relevant passages</th>
<th>Relevant to claim No.</th>
</tr>
</thead>
</table>

Further documents are listed in the continuation of Box C. See patent family annex.

* Special categories of cited documents:
  *A* document defining the general state of the art which is not considered to be of particular relevance
  *E* earlier document but published on or after the international filing date
  *L* document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another document or to give a special reason (as specified)
  *O* document referring to an oral disclosure, use, exhibition or other means
  *P* document published prior to the international filing date but later than the priority date claimed
  *T* later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
  *X* document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
  *Y* document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art
  *S* document member of the same patent family

Date of the actual completion of the International search 28 April 2006

Date of mailing of the International search report 18/05/2006

Name and mailing address of the ISA
European Patent Office, P.B. 5816 Patentlaan 2 NL – 2280 HV Rijswijk Tel: (+31-70) 340-2040, Tx: 31 651 epo nl, Fax: (+31-70) 340-5016

Authorized officer Apostolescu, R
<table>
<thead>
<tr>
<th>Category</th>
<th>Citation of document, with indication, where appropriate, of the relevant passages</th>
<th>Relevant to claim No.</th>
</tr>
</thead>
<tbody>
<tr>
<td>A</td>
<td>US 6 084 969 A (WRIGHT ET AL) 4 July 2000 (2000-07-04) column 6, line 36 - column 14, line 55</td>
<td>1-11</td>
</tr>
<tr>
<td>Patent document cited in search report</td>
<td>Publication date</td>
<td>Patent family member(s)</td>
</tr>
<tr>
<td>--------------------------------------</td>
<td>-----------------</td>
<td>-------------------------</td>
</tr>
<tr>
<td></td>
<td></td>
<td>WO 9934553 A1</td>
</tr>
</tbody>
</table>