

METHOD FOR PROTECTING SECRET KEY CRYPTOGRAPHIC SCHEMES

FIELD OF THE INVENTION

This invention relates to a method for protecting secret key cryptographic schemes and extends to a novel challenge-response authentication method for use in protecting devices used in secret key cryptographic schemes.

BACKGROUND TO THE INVENTION

A GSM telephone network requires the use of a challenge-response protocol to authenticate users on its network. When a SIM (subscriber identification module) card is issued to a subscriber it is programmed to contain a unique random number called a secret key. Each SIM card is also programmed with an International Mobile Subscriber Identity (IMSI). There is a unique IMSI for each and every mobile telephone on a GSM network worldwide. The issuer of the SIM, in most instances a network provider, is also supplied with the IMSI and the corresponding key.

When a network operator wishes to authenticate a SIM, it will send a challenge to the SIM based on the SIM's IMSI. Each network operator uses a standard algorithm for the challenge-response method and the efficacy of the system relies largely on the strength of the algorithm.

The network will, in most instances, have a database of suitable challenges and expected responses based on the SIM's IMSI. The network will thus select a suitable challenge and send it over the air to the SIM card. The SIM card will apply a cryptographic scheme, being a combination of cryptographic algorithm and secret key, to the challenge and produce a response. The SIM's computed response is then sent over the air to the network operator that issued the challenge. If the response agrees with the response expected by the network operator, the SIM has been authenticated.

The algorithm used in such a system may be, and frequently is, public knowledge and thus it is obviously of critical importance that the secret key for a particular subscriber remains secret. It should be as difficult as possible to deduce the key even when a large number of challenges and corresponding responses may be examined.

In particular, issuing challenges that are related in some way should not produce predictable responses, with a comparatively high probability. If one applies the same algorithm to two different challenges and the same response is generated to both (termed a collision) or if one can predict the outcome to a challenge that has been varied slightly on a previous challenge, then the algorithm is said to be cryptographically weak. In other words, an algorithm that (for most secret keys) produces responses that with comparatively high probability are related to changes in the challenge is not cryptographically safe.

Thus, with a weak algorithm, a series of similar challenges may produce like or predictable responses from which it is possible to work backwards, using the known algorithm, to deduce the secret key of an encoding device such as a SIM card. As an example, the COMP128-1 algorithm was shown to produce the same responses with high probability when the challenge was varied in respect of certain of the byte pairs in the challenge. It was possible to produce a collision with two different challenges and to work backwards to deduce a corresponding byte pair of the secret key. By repeating this process, it was found that all eight of the byte pairs in the COMP128-1 secret key eventually gave like answers to similar challenges. It was therefore possible to deduce the entire secret key.

Once the secret key is known, the SIM card can be cloned and fraudulent telephone charges can be billed to the user of the original SIM card. Since COMP128-1 is a widely fielded authentication scheme in GSM networks, some network operators are becoming worried about the risk posed by GSM-cloning worldwide. To implement a new algorithm on a network would involve the re-programming of every SIM card on that network and would therefore be a very expensive and inconvenient operation. To phase a new algorithm in over time would involve running two separate algorithms simultaneously and would also be inconvenient and costly to network operators.

However, it has been found that certain secret key values may exist specific to a given algorithm, even when that algorithm is weak, which are far less likely to produce predictable responses or collisions when the challenges are varied in some predictable way. To deduce the value of these secret keys is thus more difficult than for a randomly selected secret key value.

For the purposes of this specification a 'strong key byte pair' shall mean a secret key value which makes up a secret that, when subjected to related challenges, is less likely to produce related responses than for a secret key made up from randomly selected secret key values.

Also, a "BGW-style challenge" is a challenge as described in the Briceno, Goldberg and Wagner report.

25 OBJECT OF THE INVENTION

It is an object of the invention to provide a method of protecting a secret key in a cryptographic system that, at least partially, solves some of the abovementioned problems. It is also an object of the invention to provide a challenge response authentication method that, at least partially, solves some of the abovementioned problems.

30

SUMMARY OF THE INVENTION

In accordance with a first aspect of the present invention, there is provided a method for protecting a secret key cryptographic scheme including the steps of:

generating a set of strong key byte pairs for a given algorithm;
 selecting from the set a predetermined number of strong key byte pairs to at least partly form a secret key of predefined length;
 programming an encoding device with the secret key.

A further feature of example embodiments of the invention may provide for an algorithm to select the strong key byte pairs that comprise the secret key.

Another feature may provide for the secret key to be programmed into a SIM card operable on a GSM network.

Still further features may provide for the cryptographic scheme to be a GSM authentication scheme operating with the COMP128-1 algorithm and for the strong key byte pairs to be such that a collision is not produced at round 2 of the COMP128-1 algorithm application when a BGW-style challenge is used on the algorithm.

Still further features may provide for the secret key (expressed in hexadecimal) to be formed using any one or more of the strong key byte pairs below:

```

000B 003F 005B 006D 0119 01A8 01F8 0293 031E 035A 036B 03BA
03CF 03FC 0452 04CA 0532 05A9 05E0 063B 0657 085C 089F 09CE
0A88 0AA6 0B00 0B7F 0BD2 0C42 0CE8 0D18 0D9D 0E14 0EA4 0EA9
0ED9 0F4A 0F4D 0F6F 0FA5 0FD0 0FE6 1011 1056 10AD 10CF 1110
116B 11C4 11DA 11DB 1228 123D 12BA 12CB 12E8 140E 14BF 1588
1596 15D6 15E0 1638 1643 1728 173A 180D 1871 18C3 1901 192F
1935 1965 1975 1978 19CD 1A5C 1ABB 1B20 1BA4 1BB4 1BC0 1C68
1CD7 1D37 1D5F 1D87 1E03 1E1E 1E20 1F44 1F54 1FCA 201B 201E
2057 2069 2079 207B 2137 21C8 2268 22DC 23B5 23CF 2432 2581
25A5 2685 2691 273E 276E 2777 2793 2812 2817 2859 28AC 2A61
2C39 2CD2 2CD7 2D6D 2E7B 2E93 2EE1 2F19 3074 3088 30BA 30F8
31BB 31D4 3205 3224 32E4 3334 3374 3433 34FA 3519 354E 3650
3668 36AE 371D 3721 3751 378C 379E 3816 38F9 392C 3977 39D9
39FA 3A17 3A80 3ABE 3B06 3BE4 3BE7 3BEB 3C78 3CD0 3CD3 3D12
3D9D 3DF6 3E27 3E5C 3E5D 3F00 3FC9 3FCB 406D 40EA 414E 4184
41A3 41A5 420C 425F 42BA 42DF 4316 43E9 441F 4489 44FE 45D1
4651 46A0 48D9 494A 49A7 49AB 49B1 49CB 49F9 4A0F 4A49 4A6F

```

```

4A80 4AB3 4AC5 4B4E 4B5B 4B93 4BC7 4CBA 4CCC 4D0F 4D4E 4D93
4DF4 4E35 4E41 4E4B 4E4D 4E76 4E7D 4E91 4EF6 5036 50C4 5137
5146 5204 5264 528E 53D7 541F 5489 548D 54E5 556B 55BE 5610
5665 56BA 56D8 5706 5720 5771 5889 58B7 5928 5983 5A03 5ACB
5AF1 5B00 5B4B 5BB7 5C08 5C1A 5C3E 5CA6 5CC8 5CCC 5CE1 5CE6
5D3E 5DC4 5E86 5EEC 5F1D 5F42 608E 60F9 612A 61DA 61F1 61F5
627D 6374 638A 63A0 63F0 6452 64A6 6519 6556 6676 6692 66D0
67A8 67E9 681C 6822 6836 68B4 6920 697B 6988 6A73 6A7C 6A8C
6AA7 6B03 6B11 6B55 6B6E 6BAD 6BE2 6C7B 6C84 6D00 6D2D 6D40
6DF9 6E27 6E6B 6E83 6EB1 6ED2 6F0F 6F4A 6FB0 6FCB 7070 7072
708C 70FC 7118 7157 7270 7291 729A 72AD 736A 73DE 73E0 7430
7433 7463 74B3 7519 764E 7666 7679 768F 7727 7739 7780 778A
77B5 77F5 7819 783C 78D8 7920 7976 7983 79A1 7A81 7B20 7B2E
7B69 7B6C 7B9D 7BCC 7BD2 7BF6 7C6A 7CF5 7CFD 7D4E 7D62 7D8D
7EF6 7EFE 7F0B 803A 804A 8077 80C6 8125 817A 8181 82A4 82B1
8359 836E 8379 8393 8441 846C 84DD 8526 85D4 865E 86A4 86AB
871D 878D 87BD 87F4 880A 8815 8830 8869 88D0 8944 8954 8958
899B 8A63 8A77 8AC1 8BA0 8EAF 8C37 8C6A 8C70 8D54 8D7D 8D87
8E52 8E60 8E97 8ED6 8EDE 8F76 90AF 90DD 9126 914E 9172 91F2
9266 929E 92B7 9302 9327 932E 934B 934D 9383 93DF 94AB 94D9
95B5 95F0 9615 96DE 96DF 978E 98A0 98DF 9A72 9B89 9BFF 9CF1
9D0D 9D3D 9D7B 9E37 9E92 9EBC 9F08 9FAC 9FBD 9FD4 9FEE 9FFC
A046 A063 A08B A098 A0B9 A0E7 A179 A1A6 A1E8 A2A2 A341 A3B1
A40E A41B A482 A486 A4C7 A4CE A4D2 A50F A525 A541 A5AB A5E9
A60A A65C A664 A6A1 A749 A76A A7E7 A801 A867 A905 A90E A9ED
AAEC AAF6 AB49 AB86 AB94 ABA5 ABFF AC28 AC9F ACB0 ACC7 AD10
AD6B AD72 AE36 AF8B AF90 B06F B0AC B149 B16E B182 B1A3 B1D1
B1E4 B1E8 B34A B374 B3E2 B41B B468 B4E0 B523 B577 B595 B5F5
B5F7 B6D3 B758 B75B B792 B7F0 B8E5 B8EC B9A0 BA03 BA12 BA30
BA42 BA4C BA56 BB1A BB31 BBEC BBF6 BC9E BCDE BCF3 BCFE BD87
BD9F BDCA BDD9 BE3A BE55 BED9 BF14 BFD4 C01B C0FC C18A C1EB
C318 C3F6 C411 C450 C45D C4D7 C54A C5C5 C680 C6D7 C74B C7A4
C7AC C7F1 C821 C85C C8CD C93F C9CA C9F5 CA04 CA1F CABD CAC9
CAE0 CB12 CB3F CB49 CB5A CB6F CC4C CC5C CC7B CCDE CD19 CDC8
CE09 CEA4 CEED CF03 CF10 CF23 D00F D03C D066 D088 D0D6 D145
D1B1 D1EA D20B D22C D26E D27B D2A4 D33C D3B6 D431 D485 D49F
D4BF D5E5 D615 D68E D6D0 D6E6 D71C D72C D753 D7C4 D7C6 D856
D878 D90E D939 D948 D994 D9BD D9BE DA11 DA61 DAF8 DB11 DC22
DD84 DD90 DE73 DE8E DE96 DEBC DECC DF42 DF93 DF96 DF98 E005
E015 E073 E0B4 E0CA E12E E15C E26B E2B3 E3F9 E432 E43B E4B1
E4E7 E554 E5B8 E5D5 E60F E65C E6D6 E73B E7A0 E7A7 E7E4 E80C
E812 E8A1 E8B1 E943 E967 E9A5 EA40 EAD1 EAFA EB3B EBC1 EC5E
ECAA ECB8 ECBB EDA9 EDCE EE9F EE5F F063 F095 F0B7 F15A F161
F19C F1C7 F291 F3BC F44D F487 F561 F577 F57C F5B5 F5C9 F5EE
F5FA F5FB F63D F64E F67B F67E F6AA F6BB F6C3 F7B5 F801 F830
F8DA F938 F949 F960 F96D F9E3 FA34 FA39 FAEA FAF5 FAFC FBF5
FC03 FC70 FC9F FCC0 FCFA FCFD FD7C FDFC FE44 FE7E FEBC FF9B
FFAB

```

Still further features may provide for the algorithm that forms the secret key for the COMP128-1 algorithm from the set of strong key byte pairs, expressed in pseudocode, to be:

// K_i is the key used in the COMP128-1 algorithm

```

Ki = new byte[16]
// Generate a pair of strong key bytes
for (j=0; j<8; j++)
{r = a random integer in the range 1 – 769
 k = the r-th value in the table of secret keys
 K[j] = the MSB of k
 K[j+8] = the LSB of k.}

```

Still further features may provide for the algorithm used to select the strong key byte pairs that comprise the secret key to be programmed into a SIM card operable in a GSM telephone network.

In accordance with a second aspect of the present invention, there is provided a challenge-response authentication method which includes applying an algorithm and a secret key comprising strong key byte pairs to a random challenge generated by a central network to produce a response at the central network and a response at the central network and a response on a given encoding device and comparing the responses to authenticate a user.

Further features of the method may provide for the challenge to be generated by a GSM network operator and for the responses to the challenge to be generated by the GSM network operator and on a SIM card operable on a GSM network.

A further feature of the method may provide for the challenge to be generated by a GSM network operator operating with the COMP-128-1 algorithm.

Further features of the method may provide for the secret key to be formed by the SIM card itself from a set of strong key byte pairs stored on the SIM card, and for the method to include the step of programming the SIM card with an algorithm used to form the secret key from the set of strong key byte pairs.

Still further features of the method may provide for the algorithm that forms the secret key for the COMP128-1 algorithm from the set of strong key byte pairs, expressed in pseudocode, to be:

```

// Ki is the key used in the COMP128-1 algorithm

```

```

Ki = new byte[16]
// Generate a pair of strong key bytes
for (j=0; j<8; j++)
{r = a random integer in the range 1 – 769
k = the r-th value in the table of secret keys
K[j] = the MSB of k
K[j+8] = the LSB of k.}

```

In accordance with a third aspect of the present invention, there is provided a SIM card operable on a GSM network programmed with a secret key.

In accordance with a fourth aspect of the present invention, there is provided a secret key comprising at least some strong key byte pairs. The secret (expressed in hexadecimal) may be formed using any one or more of the strong key byte pairs below:

```

000B 003F 005B 006D 0119 01A8 01F8 0293 031E 035A 036B 03BA
03CF 03FC 0452 04CA 0532 05A9 05E0 063B 0657 085C 089F 09CE
0A88 0AA6 0B00 0B7F 0BD2 0C42 0CE8 0D18 0D9D 0E14 0EA4 0EA9
0ED9 0F4A 0F4D 0F6F 0FA5 0FD0 0FE6 1011 1056 10AD 10CF 1110
116B 11C4 11DA 11DB 1228 123D 12BA 12CB 12E8 140E 14BF 1588
1596 15D6 15E0 1638 1643 1728 173A 180D 1871 18C3 1901 192F
1935 1965 1975 1978 19CD 1A5C 1ABB 1B20 1BA4 1BB4 1BC0 1C68
1CD7 1D37 1D5F 1D87 1E03 1E1E 1E20 1F44 1F54 1FCA 201B 201E
2057 2069 2079 207B 2137 21C8 2268 22DC 23B5 23CF 2432 2581
25A5 2685 2691 273E 276E 2777 2793 2812 2817 2859 28AC 2A61
2C39 2CD2 2CD7 2D6D 2E7B 2E93 2EE1 2F19 3074 3088 30BA 30F8
31BB 31D4 3205 3224 32E4 3334 3374 3433 34FA 3519 354E 3650
3668 36AE 371D 3721 3751 378C 379E 3816 38F9 392C 3977 39D9
39FA 3A17 3A80 3ABE 3B06 3BE4 3BE7 3BEB 3C78 3CD0 3CD3 3D12
3D9D 3DF6 3E27 3E5C 3E5D 3F00 3FC9 3FCB 406D 40EA 414E 4184
41A3 41A5 420C 425F 42BA 42DF 4316 43E9 441F 4489 44FE 45D1
4651 46A0 48D9 494A 49A7 49AB 49B1 49CB 49F9 4A0F 4A49 4A6F
4A80 4AB3 4AC5 4B4E 4B5B 4B93 4BC7 4CBA 4CCC 4D0F 4D4E 4D93
4DF4 4E35 4E41 4E4B 4E4D 4E76 4E7D 4E91 4EF6 5036 50C4 5137
5146 5204 5264 528E 53D7 541F 5489 548D 54E5 556B 55BE 5610
5665 56BA 56D8 5706 5720 5771 5889 58B7 5928 5983 5A03 5ACB
5AF1 5B00 5B4B 5BB7 5C08 5C1A 5C3E 5CA6 5CC8 5CCC 5CE1 5CE6
5D3E 5DC4 5E86 5EEC 5F1D 5F42 608E 60F9 612A 61DA 61F1 61F5
627D 6374 638A 63A0 63F0 6452 64A6 6519 6556 6676 6692 66D0
67A8 67E9 681C 6822 6836 68B4 6920 697B 6988 6A73 6A7C 6A8C
6AA7 6B03 6B11 6B55 6B6E 6BAD 6BE2 6C7B 6C84 6D00 6D2D 6D40
6DF9 6E27 6E6B 6E83 6EB1 6ED2 6F0F 6F4A 6FB0 6FCB 7070 7072
708C 70FC 7118 7157 7270 7291 729A 72AD 736A 73DE 73E0 7430
7433 7463 74B3 7519 764E 7666 7679 768F 7727 7739 7780 778A
77B5 77F5 7819 783C 78D8 7920 7976 7983 79A1 7A81 7B20 7B2E
7B69 7B6C 7B9D 7BCC 7BD2 7BF6 7C6A 7CF5 7CFD 7D4E 7D62 7D8D
7EF6 7EFE 7F0B 803A 804A 8077 80C6 8125 817A 8181 82A4 82B1

```

```

8359 836E 8379 8393 8441 846C 84DD 8526 85D4 865E 86A4 86AB
871D 878D 87BD 87F4 880A 8815 8830 8869 88D0 8944 8954 8958
899B 8A63 8A77 8AC1 8BA0 8BAF 8C37 8C6A 8C70 8D54 8D7D 8D87
8E52 8E60 8E97 8ED6 8EDE 8F76 90AF 90DD 9126 914E 9172 91F2
9266 929E 92B7 9302 9327 932E 934B 934D 9383 93DF 94AB 94D9
95B5 95F0 9615 96DE 96DF 978E 98A0 98DF 9A72 9B89 9BFF 9CF1
9D0D 9D3D 9D7B 9E37 9E92 9EBC 9F08 9FAC 9FBD 9FD4 9FEE 9FFC
A046 A063 A08B A098 A0B9 A0E7 A179 A1A6 A1E8 A2A2 A341 A3B1
A40E A41B A482 A486 A4C7 A4CE A4D2 A50F A525 A541 A5AB A5E9
A60A A65C A664 A6A1 A749 A76A A7E7 A801 A867 A905 A90E A9ED
AAEC AAF6 AB49 AB86 AB94 ABA5 ABFF AC28 AC9F ACB0 ACC7 AD10
AD6B AD72 AE36 AF8B AF90 B06F B0AC B149 B16E B182 B1A3 B1D1
B1E4 B1E8 B34A B374 B3E2 B41B B468 B4E0 B523 B577 B595 B5F5
B5F7 B6D3 B758 B75B B792 B7F0 B8E5 B8EC B9A0 BA03 BA12 BA30
BA42 BA4C BA56 BB1A BB31 BBEC BBF6 BC9E BCDE BCF3 BCFE BD87
BD9F BDCA BDD9 BE3A BE55 BED9 BF14 BFD4 C01B C0FC C18A C1EB
C318 C3F6 C411 C450 C45D C4D7 C54A C5C5 C680 C6D7 C74B C7A4
C7AC C7F1 C821 C85C C8CD C93F C9CA C9F5 CA04 CA1F CABD CAC9
CAE0 CB12 CB3F CB49 CB5A CB6F CC4C CC5C CC7B CCDE CD19 CDC8
CE09 CEA4 CEED CF03 CF10 CF23 D00F D03C D066 D088 D0D6 D145
D1B1 D1EA D20B D22C D26E D27B D2A4 D33C D3B6 D431 D485 D49F
D4BF D5E5 D615 D68E D6D0 D6E6 D71C D72C D753 D7C4 D7C6 D856
D878 D90E D939 D948 D994 D9BD D9BE DA11 DA61 DAF8 DB11 DC22
DD84 DD90 DE73 DE8E DE96 DEBC DECC DF42 DF93 DF96 DF98 E005
E015 E073 E0B4 E0CA E12E E15C E26B E2B3 E3F9 E432 E43B E4B1
E4E7 E554 E5B8 E5D5 E60F E65C E6D6 E73B E7A0 E7A7 E7E4 E80C
E812 E8A1 E8B1 E943 E967 E9A5 EA40 EAD1 EAF4 EB3B EBC1 EC5E
ECAA ECB8 ECBB EDA9 EDCE EE9F EE9F F063 F095 F0B7 F15A F161
F19C F1C7 F291 F3BC F44D F487 F561 F577 F57C F5B5 F5C9 F5EE
F5FA F5FB F63D F64E F67B F67E F6AA F6BB F6C3 F7B5 F801 F830
F8DA F938 F949 F960 F96D F9E3 FA34 FA39 FAEA FAF5 FAFC FBF5
FC03 FC70 FC9F FCC0 FCFA FCFD FD7C FDFC FE44 FE7E FEBC FF9B
FFAB

```

In accordance with a fifth aspect of the present invention, there is provided an algorithm, expressed in pseudocode, to form a secret key for a cryptographic scheme using the COMP128-1 algorithm from a set of strong key byte pairs to be:

// K_i is the key used in the COMP128-1 algorithm

$K_i = \text{new byte}[16]$

// Generate a pair of strong key bytes

for ($j=0$; $j<8$; $j++$)

{ $r = \text{a random integer in the range } 1 - 769$

$k = \text{the } r\text{-th value in the table of secret keys}$

$K_i[j] = \text{the MSB of } k$

$K_i[j+8] = \text{the LSB of } k.$ }

In accordance with a sixth aspect of the present invention, there is provided a GSM network using a challenge-response authentication method which includes applying an algorithm and a secret key comprising at least some strong key byte pairs to a random challenge generated by a central network to produce a response at the central network and a response on a given encoding device and comparing the responses to authenticate a user.

DETAILED DESCRIPTION OF THE INVENTION

An embodiment of the invention is described by way of example only and should not be construed as limiting the scope of the invention in any way.

One of the most widely used algorithms for mobile telephone networks is called the COMP128-1 algorithm. The algorithm uses a 16 byte secret key, which means the probability of determining the whole key by chance is 1 in 2^{128} . This is called the key space. Such a vast key space effectively nullifies the possibility of revealing a secret key in a SIM card based on pure chance.

However, in a report released by Briceno, Goldberg and Wagner (the 'BGW report'), it was shown that with physical access to a SIM card using the COMP128-1 algorithm, an off-the shelf smart card reader and a computer, the secret key in that SIM card could be deduced using approximately 150 000 challenges. This took approximately 8 hours working with a system that produces 6,25 challenges per second.

The SIM and in particular the secret key on that SIM and the known algorithm were subjected to a number of specially selected challenges to which they produced a response in each instance.

Due to weaknesses in the algorithm it was found that by varying certain pairs of bytes in a series of challenges, and only those bytes, the responses were found to be the same with comparatively high probability. Using the like responses and the known challenges it was possible to work backwards, using the known algorithm, to deduce which bytes in the secret key would give like responses.

Each such collision revealed two bytes of the sixteen-byte key and with sufficient challenges it was found possible to reveal all sixteen bytes of the key. With the secret key revealed, a new SIM with the same secret key can be programmed and used. The charges for that new SIM will be billed to the account of the user of the original SIM. This is termed SIM-cloning or GSM-cloning.

The COMP128-1 algorithm has 40 rounds of application. It has been found that a collision after round 40 is more than likely a result of a collision that occurred at round 2 in the algorithm when a pair of challenges of the form identified in the BGW report are used and which has been carried through the remaining rounds of application. Round 2 collisions are far more likely to occur than those in the subsequent rounds and, as such, the byte pairs are easier to reveal at this round than in subsequent rounds. To put this difference in perspective, one needs to issue approximately 23000 challenges to have a reasonable chance of witnessing a round 2 collision whereas approximately 260000 challenges are required to witness a round 3 collision with the same probability as for the round 2 collision. This simplifies the deduction of the secret key from the results of the application of the challenge to the algorithm and secret key.

There are 65536 possible values for a pair of key bytes. Each and every pair of key bytes was tested and it was found, surprisingly, that certain pairs of key bytes do not produce collisions at round 2 of the COMP128-1 algorithm for challenges of the form used in the BGW report. In other words these byte pairs were strong key byte pairs for the purposes of a round 2 collision of the COMP128-1 algorithm.

This characteristic means that these numbers will not produce like responses at round 2 of the algorithm to a slightly varied challenge and effectively offer no clues as to the value of a particular key-byte in the secret key when producing that response. Seven hundred and sixty nine pairs of key bytes were found not to produce a collision at round 2 of the COMP128-1 algorithm. As was explained earlier most of the weak keys in the COMP128-1 algorithm were weak because of their susceptibility to a collision at round 2 of the algorithm, and thus these keys are significantly stronger and more difficult to reveal than keys which do produce such a collision. The strong key bytes for the COMP128-1 algorithm, which in this case are in the form of strong key byte pairs (expressed in hexadecimal), were found to be the following:

```

000B 003F 005B 006D 0119 01A8 01F8 0293 031E 035A 036B 03BA
03CF 03FC 0452 04CA 0532 05A9 05E0 063B 0657 085C 089F 09CE
0A88 0AA6 0B00 0B7F 0BD2 0C42 0CE8 0D18 0D9D 0E14 0EA4 0EA9
0ED9 0F4A 0F4D 0F6F 0FA5 0FD0 0FE6 1011 1056 10AD 10CF 1110
116B 11C4 11DA 11DB 1228 123D 12BA 12CB 12E8 140E 14BF 1588
1596 15D6 15E0 1638 1643 1728 173A 180D 1871 18C3 1901 192F
1935 1965 1975 1978 19CD 1A5C 1ABB 1B20 1BA4 1BB4 1BC0 1C68
1CD7 1D37 1D5F 1D87 1E03 1E1E 1E20 1F44 1F54 1FCA 201B 201E
2057 2069 2079 207B 2137 21C8 2268 22DC 23B5 23CF 2432 2581
25A5 2685 2691 273E 276E 2777 2793 2812 2817 2859 28AC 2A61
2C39 2CD2 2CD7 2D6D 2E7B 2E93 2EE1 2F19 3074 3088 30BA 30F8
31BB 31D4 3205 3224 32E4 3334 3374 3433 34FA 3519 354E 3650
3668 36AE 371D 3721 3751 378C 379E 3816 38F9 392C 3977 39D9
39FA 3A17 3A80 3ABE 3B06 3BE4 3BE7 3BEB 3C78 3CD0 3CD3 3D12
3D9D 3DF6 3E27 3E5C 3E5D 3F00 3FC9 3FCB 406D 40EA 414E 4184
41A3 41A5 420C 425F 42BA 42DF 4316 43E9 441F 4489 44FE 45D1
4651 46A0 48D9 494A 49A7 49AB 49B1 49CB 49F9 4A0F 4A49 4A6F
4A80 4AB3 4AC5 4B4E 4B5B 4B93 4BC7 4CBA 4CCC 4D0F 4D4E 4D93
4DF4 4E35 4E41 4E4B 4E4D 4E76 4E7D 4E91 4EF6 5036 50C4 5137
5146 5204 5264 528E 53D7 541F 5489 548D 54E5 556B 55BE 5610
5665 56BA 56D8 5706 5720 5771 5889 58B7 5928 5983 5A03 5ACB
5AF1 5B00 5B4B 5BB7 5C08 5C1A 5C3E 5CA6 5CC8 5CCC 5CE1 5CE6
5D3E 5DC4 5E86 5EEC 5F1D 5F42 608E 60F9 612A 61DA 61F1 61F5
627D 6374 638A 63A0 63F0 6452 64A6 6519 6556 6676 6692 66D0
67A8 67E9 681C 6822 6836 68B4 6920 697B 6988 6A73 6A7C 6A8C
6AA7 6B03 6B11 6B55 6B6E 6BAD 6BE2 6C7B 6C84 6D00 6D2D 6D40
6DF9 6E27 6E6B 6E83 6EB1 6ED2 6F0F 6F4A 6FB0 6FCB 7070 7072
708C 70FC 7118 7157 7270 7291 729A 72AD 736A 73DE 73E0 7430
7433 7463 74B3 7519 764E 7666 7679 768F 7727 7739 7780 778A
77B5 77F5 7819 783C 78D8 7920 7976 7983 79A1 7A81 7B20 7B2E
7B69 7B6C 7B9D 7BCC 7BD2 7BF6 7C6A 7CF5 7CFD 7D4E 7D62 7D8D
7EF6 7EFE 7F0B 803A 804A 8077 80C6 8125 817A 8181 82A4 82B1
8359 836E 8379 8393 8441 846C 84DD 8526 85D4 865E 86A4 86AB
871D 878D 87BD 87F4 880A 8815 8830 8869 88D0 8944 8954 8958
899B 8A63 8A77 8AC1 8BA0 8BAF 8C37 8C6A 8C70 8D54 8D7D 8D87
8E52 8E60 8E97 8ED6 8EDE 8F76 90AF 90DD 9126 914E 9172 91F2
9266 929E 92B7 9302 9327 932E 934B 934D 9383 93DF 94AB 94D9
95B5 95F0 9615 96DE 96DF 978E 98A0 98DF 9A72 9B89 9BFF 9CF1
9D0D 9D3D 9D7B 9E37 9E92 9EBC 9F08 9FAC 9FBD 9FD4 9FEE 9FFC
A046 A063 A08B A098 A0B9 A0E7 A179 A1A6 A1E8 A2A2 A341 A3B1
A40E A41B A482 A486 A4C7 A4CE A4D2 A50F A525 A541 A5AB A5E9
A60A A65C A664 A6A1 A749 A76A A7E7 A801 A867 A905 A90E A9ED
AAEC AAF6 AB49 AB86 AB94 ABA5 ABFF AC28 AC9F ACB0 ACC7 AD10
AD6B AD72 AE36 AF8B AF90 B06F B0AC B149 B16E B182 B1A3 B1D1
B1E4 B1E8 B34A B374 B3E2 B41B B468 B4E0 B523 B577 B595 B5F5
B5F7 B6D3 B758 B75B B792 B7F0 B8E5 B8EC B9A0 BA03 BA12 BA30
BA42 BA4C BA56 BB1A BB31 BBEC BBF6 BC9E BCDE BCF3 BCFE BD87
BD9F BDCA BDD9 BE3A BE55 BED9 BF14 BFD4 C01B C0FC C18A C1EB
C318 C3F6 C411 C450 C45D C4D7 C54A C5C5 C680 C6D7 C74B C7A4
C7AC C7F1 C821 C85C C8CD C93F C9CA C9F5 CA04 CA1F CABD CAC9
CAE0 CB12 CB3F CB49 CB5A CB6F CC4C CC5C CC7B CCDE CD19 CDC8
CE09 CEA4 CEED CF03 CF10 CF23 D00F D03C D066 D088 D0D6 D145
D1B1 D1EA D20B D22C D26E D27B D2A4 D33C D3B6 D431 D485 D49F
D4BF D5E5 D615 D68E D6D0 D6E6 D71C D72C D753 D7C4 D7C6 D856
D878 D90E D939 D948 D994 D9BD D9BE DA11 DA61 DAF8 DB11 DC22
DD84 DD90 DE73 DE8E DE96 DEBC DECC DF42 DF93 DF96 DF98 E005

```

E015 E073 E0B4 E0CA E12E E15C E26B E2B3 E3F9 E432 E43B E4B1
 E4E7 E554 E5B8 E5D5 E60F E65C E6D6 E73B E7A0 E7A7 E7E4 E80C
 E812 E8A1 E8B1 E943 E967 E9A5 EA40 EAD1 EAF8 EB3B EBC1 EC5E
 ECAA ECB8 ECBB EDA9 EDCE EE9F EEF5 F063 F095 F0B7 F15A F161
 F19C F1C7 F291 F3BC F44D F487 F561 F577 F57C F5B5 F5C9 F5EE
 F5FA F5FB F63D F64E F67B F67E F6AA F6BB F6C3 F7B5 F801 F830
 F8DA F938 F949 F960 F96D F9E3 FA34 FA39 FAEA FAF5 FAFC FBF5
 FC03 FC70 FC9F FCC0 FCFA FCFD FD7C FDFC FE44 FE7E FEBC FF9B
 FFAB

If the secret key for a SIM card in a system using the COMP128-1 algorithm is generated using only strong key byte pairs, it has been found that the possibility of deducing the secret key by selectively varying the challenge and analysing the results was significantly reduced.

It will be appreciated by those skilled in the art that if one reduces the number of variables with which one can make up the secret key (that is instead of 65536 keys to choose from you now only have 769) then the key space is significantly reduced. In this instance the key space is reduced by a factor of $2^{51.3}$. Previously, the key space for the COMP128-1 algorithm was 2^{128} . Now that key space is 769^8 or $2^{76.7}$. However, even with this reduction in key space, the key space of $2^{76.7}$ is still large enough to prevent decryption of a secret key by pure brute force attack.

It will be appreciated that a number of variations can be made to the above embodiment without departing from the scope of the invention. Any algorithm which is susceptible to collisions, not only the COMP128-1 algorithm and not only in a GSM environment, being used in a cryptographic scheme would benefit from the application of the invention. Similarly, any encoding device may be used instead of a SIM card and the network operator can be replaced by a suitable central network capable of communicating with a particular encoding device on a public communication system. Furthermore, the collision can occur at any round of application of a given algorithm and thus the strong key byte pairs may be determined on the basis that they are not susceptible to collisions in that particular round of the attack.

CLAIMS

1. A method for protecting a secret key cryptographic scheme including the steps of generating a set of strong key byte pairs for a given algorithm, selecting from the set a predetermined number of strong key byte pairs to at least partly form a secret key of predetermined length, and programming an encoding device with the secret key.
2. A method as claimed in claim 1 in which an algorithm selects the strong key byte pairs that comprise the secret key.
3. A method as claimed in claim 1 or 2 in which the secret key is programmed into a SIM card operable on a GSM network.
4. A method as claimed in any one of claims 1 to 3 in which the cryptographic scheme is a GSM authentication scheme operating with the COMP128-1 algorithm and the strong key byte pairs are such that a collision is not produced at round 2 of the COMP128-1 algorithm application when a BGW-style challenge is used on the algorithm.
5. A method as claimed in any one of claims 1 to 4 in which the secret key (expressed in hexadecimal) is formed using any one or more of the strong key byte pairs below:

```

000B 003F 005B 006D 0119 01A8 01F8 0293 031E 035A 036B 03BA
03CF 03FC 0452 04CA 0532 05A9 05E0 063B 0657 085C 089F 09CE
0A88 0AA6 0B00 0B7F 0BD2 0C42 0CE8 0D18 0D9D 0E14 0EA4 0EA9
0ED9 0F4A 0F4D 0F6F 0FA5 0FDD 0FE6 1011 1056 10AD 10CF 1110
116B 11C4 11DA 11DB 1228 123D 12BA 12CB 12E8 140E 14BF 1588
1596 15D6 15E0 1638 1643 1728 173A 180D 1871 18C3 1901 192F
1935 1965 1975 1978 19CD 1A5C 1ABB 1B20 1BA4 1BB4 1BC0 1C68
1CD7 1D37 1D5F 1D87 1E03 1E1E 1E20 1F44 1F54 1FCA 201B 201E
2057 2069 2079 207B 2137 21C8 2268 22DC 23B5 23CF 2432 2581
25A5 2685 2691 273E 276E 2777 2793 2812 2817 2859 28AC 2A61
2C39 2CD2 2CD7 2D6D 2E7B 2E93 2EE1 2F19 3074 3088 30BA 30F8
31BB 31D4 3205 3224 32E4 3334 3374 3433 34FA 3519 354E 3650
3668 36AE 371D 3721 3751 378C 379E 3816 38F9 392C 3977 39D9
39FA 3A17 3A80 3ABE 3B06 3BE4 3BE7 3BEB 3C78 3CD0 3CD3 3D12
3D9D 3DF6 3E27 3E5C 3E5D 3F00 3FC9 3FCB 406D 40EA 414E 4184
41A3 41A5 420C 425F 42BA 42DF 4316 43E9 441F 4489 44FE 45D1
4651 46A0 48D9 494A 49A7 49AB 49B1 49CB 49F9 4A0F 4A49 4A6F
4A80 4AB3 4AC5 4B4E 4B5B 4B93 4BC7 4CBA 4CCC 4D0F 4D4E 4D93

```

```

4DF4 4E35 4E41 4E4B 4E4D 4E76 4E7D 4E91 4EF6 5036 50C4 5137
5146 5204 5264 528E 53D7 541F 5489 548D 54E5 556B 55BE 5610
5665 56BA 56D8 5706 5720 5771 5889 58B7 5928 5983 5A03 5ACB
5AF1 5B00 5B4B 5BB7 5C08 5C1A 5C3E 5CA6 5CC8 5CCC 5CE1 5CE6
5D3E 5DC4 5E86 5EEC 5F1D 5F42 608E 60F9 612A 61DA 61F1 61F5
627D 6374 638A 63A0 63F0 6452 64A6 6519 6556 6676 6692 66D0
67A8 67E9 681C 6822 6836 68B4 6920 697B 6988 6A73 6A7C 6A8C
6AA7 6B03 6B11 6B55 6B6E 6BAD 6BE2 6C7B 6C84 6D00 6D2D 6D40
6DF9 6E27 6E6B 6E83 6EB1 6ED2 6F0F 6F4A 6FB0 6FCB 7070 7072
708C 70FC 7118 7157 7270 7291 729A 72AD 736A 73DE 73E0 7430
7433 7463 74B3 7519 764E 7666 7679 768F 7727 7739 7780 778A
77B5 77F5 7819 783C 78D8 7920 7976 7983 79A1 7A81 7B20 7B2E
7B69 7B6C 7B9D 7BCC 7BD2 7BF6 7C6A 7CF5 7CFD 7D4E 7D62 7D8D
7EF6 7EFE 7F0B 803A 804A 8077 80C6 8125 817A 8181 82A4 82B1
8359 836E 8379 8393 8441 846C 84DD 8526 85D4 865E 86A4 86AB
871D 878D 87BD 87F4 880A 8815 8830 8869 88D0 8944 8954 8958
899B 8A63 8A77 8AC1 8BA0 8BAF 8C37 8C6A 8C70 8D54 8D7D 8D87
8E52 8E60 8E97 8ED6 8EDE 8F76 90AF 90DD 9126 914E 9172 91F2
9266 929E 92B7 9302 9327 932E 934B 934D 9383 93DF 94AB 94D9
95B5 95F0 9615 96DE 96DF 978E 98A0 98DF 9A72 9B89 9BFF 9CF1
9D0D 9D3D 9D7B 9E37 9E92 9EBC 9F08 9FAC 9FBD 9FD4 9FEE 9FFC
A046 A063 A08B A098 A0B9 A0E7 A179 A1A6 A1E8 A2A2 A341 A3B1
A40E A41B A482 A486 A4C7 A4CE A4D2 A50F A525 A541 A5AB A5E9
A60A A65C A664 A6A1 A749 A76A A7E7 A801 A867 A905 A90E A9ED
AAEC AAF6 AB49 AB86 AB94 ABA5 ABFF AC28 AC9F ACB0 ACC7 AD10
AD6B AD72 AE36 AF8B AF90 B06F B0AC B149 B16E B182 B1A3 B1D1
B1E4 B1E8 B34A B374 B3E2 B41B B468 B4E0 B523 B577 B595 B5F5
B5F7 B6D3 B758 B75B B792 B7F0 B8E5 B8EC B9A0 BA03 BA12 BA30
BA42 BA4C BA56 BB1A BB31 BBEC BBF6 BC9E BCDE BCF3 BCFE BD87
BD9F BDCA BDD9 BE3A BE55 BED9 BF14 BFD4 C01B C0FC C18A C1EB
C318 C3F6 C411 C450 C45D C4D7 C54A C5C5 C680 C6D7 C74B C7A4
C7AC C7F1 C821 C85C C8CD C93F C9CA C9F5 CA04 CA1F CABD CAC9
CAE0 CB12 CB3F CB49 CB5A CB6F CC4C CC5C CC7B CCDE CD19 CDC8
CE09 CEA4 CEED CF03 CF10 CF23 D00F D03C D066 D088 D0D6 D145
D1B1 D1EA D20B D22C D26E D27B D2A4 D33C D3B6 D431 D485 D49F
D4BF D5E5 D615 D68E D6D0 D6E6 D71C D72C D753 D7C4 D7C6 D856
D878 D90E D939 D948 D994 D9BD D9BE DA11 DA61 DAF8 DB11 DC22
DD84 DD90 DE73 DE8E DE96 DEBC DECC DF42 DF93 DF96 DF98 E005
E015 E073 E0B4 E0CA E12E E15C E26B E2B3 E3F9 E432 E43B E4B1
E4E7 E554 E5B8 E5D5 E60F E65C E6D6 E73B E7A0 E7A7 E7E4 E80C
E812 E8A1 E8B1 E943 E967 E9A5 EA40 EAD1 EAFA EB3B EBC1 EC5E
ECAA ECB8 ECBB EDA9 EDCE EE9F EE5F F063 F095 F0B7 F15A F161
F19C F1C7 F291 F3BC F44D F487 F561 F577 F57C F5B5 F5C9 F5EE
F5FA F5FB F63D F64E F67B F67E F6AA F6BB F6C3 F7B5 F801 F830
F8DA F938 F949 F960 F96D F9E3 FA34 FA39 FAEA FAF5 FAFC FBF5
FC03 FC70 FC9F FCC0 FCFA FCFD FD7C FDFC FE44 FE7E FEBC FF9B
FFAB

```

6. A method as claimed in any one of the preceding claims in which the algorithm that forms the secret key for the COMP128-1 algorithm from the set of strong key byte pairs, expressed in pseudocode, is:

// K_i is the key used in the COMP128-1 algorithm

$K_i = \text{new byte}[16]$

```
// Generate a pair of strong key bytes
for (j=0; j<8; j++)
{r = a random integer in the range 1 – 769
k = the r-th value in the table of secret keys
Kj[j] = the MSB of k
Kj[j+8] = the LSB of k.}
```

7. A method as claimed in any of claims 1 to 6 in which the algorithm used to select the strong key byte pairs that comprise the secret key is programmed into a SIM card operable in a GSM telephone network.
8. A challenge-response authentication method which includes applying an algorithm and a secret key comprising strong key byte pairs to a random challenge generated by a central network to produce a response at the central network and a response on a given encoding device, and comparing the responses to authenticate a user.
9. A method as claimed in claim 8 in which the challenge is generated by a GSM network operator, and the responses to the challenge are generated by the GSM network operator and on a SIM card operable on a GSM network.
10. A method as claimed in claim 9 in which the challenge is generated by a GSM network operator operating with the COMP-128-1 algorithm.
11. A method as claimed in any one of claims 8 to 10 in which the secret key is formed by the SIM card itself from a set of strong key byte pairs stored on the SIM card, and the SIM card is programmed with an algorithm used to form the secret key from the set of strong key byte pairs.
12. A method as claimed in claim 11 in which the algorithm that forms the secret key for the COMP128-1 algorithm from the set of strong key byte pairs, expressed in pseudocode, is:

```
// Ki is the key used in the COMP128-1 algorithm
Ki = new byte[16]
```

```
// Generate a pair of strong key bytes
for (j=0; j<8; j++)
  {r = a random integer in the range 1 – 769
  k = the r-th value in the table of secret keys
  Kj[j] = the MSB of k
  Kj[j+8] = the LSB of k.}
```

13. A secret key for a cryptographic scheme comprising at least some strong key byte pairs.
14. A secret key as claimed in claim 13 in which the secret key (expressed in hexadecimal) is formed using any one or more of the strong key byte pairs below:

```
000B 003F 005B 006D 0119 01A8 01F8 0293 031E 035A 036B 03BA
03CF 03FC 0452 04CA 0532 05A9 05E0 063B 0657 085C 089F 09CE
0A88 0AA6 0B00 0B7F 0BD2 0C42 0CE8 0D18 0D9D 0E14 0EA4 0EA9
0ED9 0F4A 0F4D 0F6F 0FA5 0FD0 0FE6 1011 1056 10AD 10CF 1110
116B 11C4 11DA 11DB 1228 123D 12BA 12CB 12E8 140E 14BF 1588
1596 15D6 15E0 1638 1643 1728 173A 180D 1871 18C3 1901 192F
1935 1965 1975 1978 19CD 1A5C 1ABB 1B20 1BA4 1BB4 1BC0 1C68
1CD7 1D37 1D5F 1D87 1E03 1E1E 1E20 1F44 1F54 1FCA 201B 201E
2057 2069 2079 207B 2137 21C8 2268 22DC 23B5 23CF 2432 2581
25A5 2685 2691 273E 276E 2777 2793 2812 2817 2859 28AC 2A61
2C39 2CD2 2CD7 2D6D 2E7B 2E93 2EE1 2F19 3074 3088 30BA 30F8
31BB 31D4 3205 3224 32E4 3334 3374 3433 34FA 3519 354E 3650
3668 36AE 371D 3721 3751 378C 379E 3816 38F9 392C 3977 39D9
39FA 3A17 3A80 3ABE 3B06 3BE4 3BE7 3BEB 3C78 3CD0 3CD3 3D12
3D9D 3DF6 3E27 3E5C 3E5D 3F00 3FC9 3FCB 406D 40EA 414E 4184
41A3 41A5 420C 425F 42BA 42DF 4316 43E9 441F 4489 44FE 45D1
4651 46A0 48D9 494A 49A7 49AB 49B1 49CB 49F9 4A0F 4A49 4A6F
4A80 4AB3 4AC5 4B4E 4B5B 4B93 4BC7 4CBA 4CCC 4D0F 4D4E 4D93
4DF4 4E35 4E41 4E4B 4E4D 4E76 4E7D 4E91 4EF6 5036 50C4 5137
5146 5204 5264 528E 53D7 541F 5489 548D 54E5 556B 55BE 5610
5665 56BA 56D8 5706 5720 5771 5889 58B7 5928 5983 5A03 5ACB
5AF1 5B00 5B4B 5BB7 5C08 5C1A 5C3E 5CA6 5CC8 5CCC 5CE1 5CE6
5D3E 5DC4 5E86 5EEC 5F1D 5F42 608E 60F9 612A 61DA 61F1 61F5
627D 6374 638A 63A0 63F0 6452 64A6 6519 6556 6676 6692 66D0
67A8 67E9 681C 6822 6836 68B4 6920 697B 6988 6A73 6A7C 6A8C
6AA7 6B03 6B11 6B55 6B6E 6BAD 6BE2 6C7B 6C84 6D00 6D2D 6D40
6DF9 6E27 6E6B 6E83 6EB1 6ED2 6F0F 6F4A 6FB0 6FCB 7070 7072
708C 70FC 7118 7157 7270 7291 729A 72AD 736A 73DE 73E0 7430
7433 7463 74B3 7519 764E 7666 7679 768F 7727 7739 7780 778A
77B5 77F5 7819 783C 78D8 7920 7976 7983 79A1 7A81 7B20 7B2E
7B69 7B6C 7B9D 7BCC 7BD2 7BF6 7C6A 7CF5 7CFD 7D4E 7D62 7D8D
7EF6 7EFE 7F0B 803A 804A 8077 80C6 8125 817A 8181 82A4 82B1
8359 836E 8379 8393 8441 846C 84DD 8526 85D4 865E 86A4 86AB
871D 878D 87BD 87F4 880A 8815 8830 8869 88D0 8944 8954 8958
```

```

899B 8A63 8A77 8AC1 8BA0 8BAF 8C37 8C6A 8C70 8D54 8D7D 8D87
8E52 8E60 8E97 8ED6 8EDE 8F76 90AF 90DD 9126 914E 9172 91F2
9266 929E 92B7 9302 9327 932E 934B 934D 9383 93DF 94AB 94D9
95B5 95F0 9615 96DE 96DF 978E 98A0 98DF 9A72 9B89 9BFF 9CF1
9D0D 9D3D 9D7B 9E37 9E92 9EBC 9F08 9FAC 9FBD 9FD4 9FEE 9FFC
A046 A063 A08B A098 A0B9 A0E7 A179 A1A6 A1E8 A2A2 A341 A3B1
A40E A41B A482 A486 A4C7 A4CE A4D2 A50F A525 A541 A5AB A5E9
A60A A65C A664 A6A1 A749 A76A A7E7 A801 A867 A905 A90E A9ED
AAEC AAF6 AB49 AB86 AB94 ABA5 ABFF AC28 AC9F ACB0 ACC7 AD10
AD6B AD72 AE36 AF8B AF90 B06F B0AC B149 B16E B182 B1A3 B1D1
B1E4 B1E8 B34A B374 B3E2 B41B B468 B4E0 B523 B577 B595 B5F5
B5F7 B6D3 B758 B75B B792 B7F0 B8E5 B8EC B9A0 BA03 BA12 BA30
BA42 BA4C BA56 BB1A BB31 BBEC BBF6 BC9E BCDE BCF3 BCFE BD87
BD9F BDCA BDD9 BE3A BE55 BED9 BF14 BFD4 C01B C0FC C18A C1EB
C318 C3F6 C411 C450 C45D C4D7 C54A C5C5 C680 C6D7 C74B C7A4
C7AC C7F1 C821 C85C C8CD C93F C9CA C9F5 CA04 CA1F CABD CAC9
CAE0 CB12 CB3F CB49 CB5A CB6F CC4C CC5C CC7B CCDE CD19 CDC8
CE09 CEA4 CEED CF03 CF10 CF23 D00F D03C D066 D088 D0D6 D145
D1B1 D1EA D20B D22C D26E D27B D2A4 D33C D3B6 D431 D485 D49F
D4BF D5E5 D615 D68E D6D0 D6E6 D71C D72C D753 D7C4 D7C6 D856
D878 D90E D939 D948 D994 D9BD D9BE DA11 DA61 DAF8 DB11 DC22
DD84 DD90 DE73 DE8E DE96 DEBC DECC DF42 DF93 DF96 DF98 E005
E015 E073 E0B4 E0CA E12E E15C E26B E2B3 E3F9 E432 E43B E4B1
E4E7 E554 E5B8 E5D5 E60F E65C E6D6 E73B E7A0 E7A7 E7E4 E80C
E812 E8A1 E8B1 E943 E967 E9A5 EA40 EAD1 EAF8 EB3B EBC1 EC5E
ECAA ECB8 ECBB EDA9 EDCE EE9F EEF5 F063 F095 F0B7 F15A F161
F19C F1C7 F291 F3BC F44D F487 F561 F577 F57C F5B5 F5C9 F5EE
F5FA F5FB F63D F64E F67B F67E F6AA F6BB F6C3 F7B5 F801 F830
F8DA F938 F949 F960 F96D F9E3 FA34 FA39 FAEA FAF5 FAFC FBF5
FC03 FC70 FC9F FCC0 FCFA FCFD FD7C FDFC FE44 FE7E FEBC FF9B
FFAB

```

15. A SIM card operable on a GSM network, the SIM card being programmed with a secret key as claimed in claim 13 or 14.
16. An algorithm, expressed in pseudocode, to form a secret key for a cryptographic scheme using the COMP128-1 algorithm from a set of strong key byte pairs comprising:

// K_i is the key used in the COMP128-1 algorithm

$K_i = \text{new byte}[16]$

// Generate a pair of strong key bytes

for ($j=0; j<8; j++$)

{ r = a random integer in the range 1 – 769

k = the r -th value in the table of secret keys

$K_i[j]$ = the MSB of k

$K_i[j+8]$ = the LSB of k .}

17. A GSM network using a challenge-response authentication method which includes applying an algorithm and a secret key comprising at least some strong key byte pairs to a random challenge generated by a central network to produce a response at the central network and a response on a given encoding device and comparing the responses to authenticate a user.
18. A GSM network as claimed in claim 17 in which a GSM network operator operating with the COMP-128-1 algorithm operates the network.
19. A GSM network as claimed in claim 18 in which the secret key for the COMP128-1 algorithm is formed from a set of strong key byte pairs using an algorithm comprising:


```
// Ki is the key used in the COMP128-1 algorithm
Ki = new byte[16]
// Generate a pair of strong key bytes
for (j=0; j<8; j++)
{r = a random integer in the range 1 – 769
k = the r-th value in the table of secret keys
Ki[j] = the MSB of k
Ki[j+8] = the LSB of k.}
```
20. A GSM network as claimed in claim 19 in which the secret key (expressed in hexadecimal) is formed using any one or more of the strong key byte pairs below:

```
000B 003F 005B 006D 0119 01A8 01F8 0293 031E 035A 036B 03BA
03CF 03FC 0452 04CA 0532 05A9 05E0 063B 0657 085C 089F 09CE
0A88 0AA6 0B00 0B7F 0BD2 0C42 0CE8 0D18 0D9D 0E14 0EA4 0EA9
0ED9 0F4A 0F4D 0F6F 0FA5 0FD0 0FE6 1011 1056 10AD 10CF 1110
116B 11C4 11DA 11DB 1228 123D 12BA 12CB 12E8 140E 14BF 1588
1596 15D6 15E0 1638 1643 1728 173A 180D 1871 18C3 1901 192F
1935 1965 1975 1978 19CD 1A5C 1ABB 1B20 1BA4 1BB4 1BC0 1C68
1CD7 1D37 1D5F 1D87 1E03 1E1E 1E20 1F44 1F54 1FCA 201B 201E
2057 2069 2079 207B 2137 21C8 2268 22DC 23B5 23CF 2432 2581
25A5 2685 2691 273E 276E 2777 2793 2812 2817 2859 28AC 2A61
2C39 2CD2 2CD7 2D6D 2E7B 2E93 2EE1 2F19 3074 3088 30BA 30F8
31BB 31D4 3205 3224 32E4 3334 3374 3433 34FA 3519 354E 3650
3668 36AE 371D 3721 3751 378C 379E 3816 38F9 392C 3977 39D9
39FA 3A17 3A80 3ABE 3B06 3BE4 3BE7 3BEB 3C78 3CD0 3CD3 3D12
```

3D9D 3DF6 3E27 3E5C 3E5D 3F00 3FC9 3FCB 406D 40EA 414E 4184
41A3 41A5 420C 425F 42BA 42DF 4316 43E9 441F 4489 44FE 45D1
4651 46A0 48D9 494A 49A7 49AB 49B1 49CB 49F9 4A0F 4A49 4A6F
4A80 4AB3 4AC5 4B4E 4B5B 4B93 4BC7 4CBA 4CCC 4D0F 4D4E 4D93
4DF4 4E35 4E41 4E4B 4E4D 4E76 4E7D 4E91 4EF6 5036 50C4 5137
5146 5204 5264 528E 53D7 541F 5489 548D 54E5 556B 55BE 5610
5665 56BA 56D8 5706 5720 5771 5889 58B7 5928 5983 5A03 5ACB
5AF1 5B00 5B4B 5BB7 5C08 5C1A 5C3E 5CA6 5CC8 5CCC 5CE1 5CE6
5D3E 5DC4 5E86 5EEC 5F1D 5F42 608E 60F9 612A 61DA 61F1 61F5
627D 6374 638A 63A0 63F0 6452 64A6 6519 6556 6676 6692 66D0
67A8 67E9 681C 6822 6836 68B4 6920 697B 6988 6A73 6A7C 6A8C
6AA7 6B03 6B11 6B55 6B6E 6BAD 6BE2 6C7B 6C84 6D00 6D2D 6D40
6DF9 6E27 6E6B 6E83 6EB1 6ED2 6F0F 6F4A 6FB0 6FCB 7070 7072
708C 70FC 7118 7157 7270 7291 729A 72AD 736A 73DE 73E0 7430
7433 7463 74B3 7519 764E 7666 7679 768F 7727 7739 7780 778A
77B5 77F5 7819 783C 78D8 7920 7976 7983 79A1 7A81 7B20 7B2E
7B69 7B6C 7B9D 7BCC 7BD2 7BF6 7C6A 7CF5 7CFD 7D4E 7D62 7D8D
7EF6 7EFE 7F0B 803A 804A 8077 80C6 8125 817A 8181 82A4 82B1
8359 836E 8379 8393 8441 846C 84DD 8526 85D4 865E 86A4 86AB
871D 878D 87BD 87F4 880A 8815 8830 8869 88D0 8944 8954 8958
899B 8A63 8A77 8AC1 8BA0 8BAF 8C37 8C6A 8C70 8D54 8D7D 8D87
8E52 8E60 8E97 8ED6 8EDE 8F76 90AF 90DD 9126 914E 9172 91F2
9266 929E 92B7 9302 9327 932E 934B 934D 9383 93DF 94AB 94D9
95B5 95F0 9615 96DE 96DF 978E 98A0 98DF 9A72 9B89 9BFF 9CF1
9D0D 9D3D 9D7B 9E37 9E92 9EBC 9F08 9FAC 9FBD 9FD4 9FEE 9FFC
A046 A063 A08B A098 A0B9 A0E7 A179 A1A6 A1E8 A2A2 A341 A3B1
A40E A41B A482 A486 A4C7 A4CE A4D2 A50F A525 A541 A5AB A5E9
A60A A65C A664 A6A1 A749 A76A A7E7 A801 A867 A905 A90E A9ED
AAEC AAF6 AB49 AB86 AB94 ABA5 ABFF AC28 AC9F ACB0 ACC7 AD10
AD6B AD72 AE36 AF8B AF90 B06F B0AC B149 B16E B182 B1A3 B1D1
B1E4 B1E8 B34A B374 B3E2 B41B B468 B4E0 B523 B577 B595 B5F5
B5F7 B6D3 B758 B75B B792 B7F0 B8E5 B8EC B9A0 BA03 BA12 BA30
BA42 BA4C BA56 BB1A BB31 BBEC BBF6 BC9E BCDE BCF3 BCFE BD87
BD9F BDCA BDD9 BE3A BE55 BED9 BF14 BFD4 C01B C0FC C18A C1EB
C318 C3F6 C411 C450 C45D C4D7 C54A C5C5 C680 C6D7 C74B C7A4
C7AC C7F1 C821 C85C C8CD C93F C9CA C9F5 CA04 CA1F CABD CAC9
CAE0 CB12 CB3F CB49 CB5A CB6F CC4C CC5C CC7B CCDE CD19 CDC8
CE09 CEA4 CEED CF03 CF10 CF23 D00F D03C D066 D088 D0D6 D145
D1B1 D1EA D20B D22C D26E D27B D2A4 D33C D3B6 D431 D485 D49F
D4BF D5E5 D615 D68E D6D0 D6E6 D71C D72C D753 D7C4 D7C6 D856
D878 D90E D939 D948 D994 D9BD D9BE DA11 DA61 DAF8 DB11 DC22
DD84 DD90 DE73 DE8E DE96 DEBC DECC DF42 DF93 DF96 DF98 E005
E015 E073 E0B4 E0CA E12E E15C E26B E2B3 E3F9 E432 E43B E4B1
E4E7 E554 E5B8 E5D5 E60F E65C E6D6 E73B E7A0 E7A7 E7E4 E80C
E812 E8A1 E8B1 E943 E967 E9A5 EA40 EAD1 EAFA EB3B EBC1 EC5E
ECAA ECB8 ECBB EDA9 EDCE EE9F EEF5 F063 F095 F0B7 F15A F161
F19C F1C7 F291 F3BC F44D F487 F561 F577 F57C F5B5 F5C9 F5EE
F5FA F5FB F63D F64E F67B F67E F6AA F6BB F6C3 F7B5 F801 F830
F8DA F938 F949 F960 F96D F9E3 FA34 FA39 FAEA FAF5 FAFC FBF5
FC03 FC70 FC9F FCC0 FCFA FCFD FD7C FDFC FE44 FE7E FEBC FF9B
FFAB