(12) PATENT ABRIDGMENT (11) Document No. AU-B-40524/89
(19) AUSTRALIAN PATENT OFFICE (10) Acceptance No. 607351

(54) Title
PUBLIC KEY DIVERSIFICATION METHOD

International Patent Classification(s)
(51)[5] **H04L 009/30**

(21) Application No. : **40524/89** (22) Application Date : **27.07.89**

(87) WIPO Number : **WO90/02456**

(30) Priority Data

(31) Number	(32) Date	(33) Country
8819767	19.08.88	GB UNITED KINGDOM
364949	12.06.89	US UNITED STATES OF AMERICA

(43) Publication Date : **23.03.90**

(44) Publication Date of Accepted Application : **28.02.91**

(71) Applicant(s)
NCR CORPORATION

(72) Inventor(s)
JEFFREY REGINALD AUSTIN

(74) Attorney or Agent
SHELSTON WATERS, 55 Clarence Street, SYDNEY NSW 2000

(57) Claim

1. A method of diversifying a key pair for use in public key cryptography by a requesting entity, including the step of generating at a parent entity, a public key N, e, where the modulus N is the product of first and second prime numbers P,Q and e is a corresponding public key integer value, characterized by the steps of: selecting third and fourth prime numbers R,S and transmitting to said requesting entity a first value N_{mi} and a second value $\varphi(N_{mi})$ where said first value $N_{mi} = N.R.S$ and where said second value $\varphi(N_{mi}) = \varphi(N).(R-1).(S-1)$, wherein the symbol φ represents Euler's totient function; selecting, at said requesting entity, fifth and sixth prime numbers T,U; and computing, at said requesting entity a third value N_m and a fourth value d_m, where $N_m = N_{mi}.T.U$, and where

$$d_m = \frac{1+K\varphi(N_m)}{e}$$

wherein

$$\varphi(N_m) = \varphi(N_{mi}).(T-1).(U-1)$$

and wherein K and d_m are integers, whereby d_m is adapted

.../2

to be used by said requesting entity as the secret key counterpart of the public key value e with respect to the modulus N_m.

OPI DATE 23/03/90 APPLN. ID 40524 / 89
AOJP DATE 26/04/90 PCT NUMBER PCT/US89/03253

PCT

INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(51) International Patent Classification 5 : H04L 9/30

A1

(11) International Publication Number: WO 90/02456

(43) International Publication Date: 8 March 1990 (08.03.90)

(21) International Application Number: PCT/US89/03253

(22) International Filing Date: 27 July 1989 (27.07.89)

(30) Priority data:

8819767.8	19 August 1988 (19.08.88)	GB
364,949	12 June 1989 (12.06.89)	US

(81) Designated States: AU, CH (European patent), DE (European patent), FR (European patent), GB (European patent), JP, NL (European patent).

Published
With international search report.

(71) Applicant: NCR CORPORATION [US/US]; World Headquarters, Dayton, OH 45479 (US).

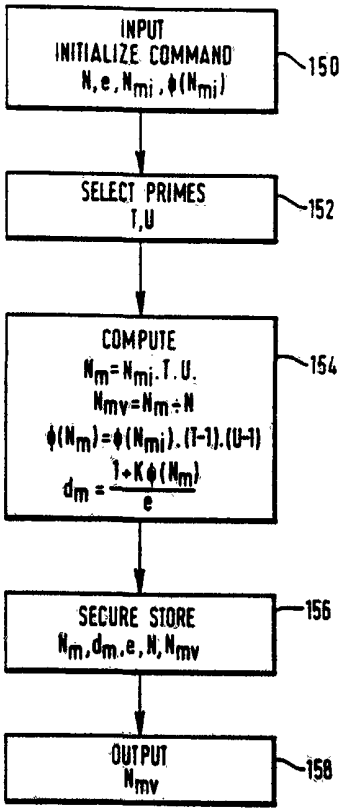
(72) Inventor: AUSTIN, Jeffrey, Reginald ; The White House, Tilford Road, Hindhead, Surrey GU26 6TD (GB).

(74) Agents: JEWETT, Stephen, F. et al.; Patent Division, NCR Corporation, World Headquarters, Dayton, OH 45479 (US).

(54) Title: PUBLIC KEY DIVERSIFICATION METHOD

(57) Abstract

A method is disclosed whereby individual members of a group of members or entities may be provided, under the control of a trusted member, referred to as the parent, with respective individual secret keys for use in public key cryptography, such that the matching public key can be readily derived, and group membership authenticated. The parent initially establishes a public key (e, N) where N = P.Q is the product of two primes. In response to a request from a group member, and the parent selects two further primes R, S and communicates two values dependent thereon to the requesting member, which selects two more primes T and U for use in conjunction with the received values to establish the member's secret key.



PUBLIC KEY DIVERSIFICATION METHOD

This invention relates to public key cryptography.

Public key cryptography is described, for example, in the article: Communications of the ACM, vol.21, No. 2, February 1978, pages 120 - 126, R.L. Rivest et al: "A Method for Obtaining Digital Signatures and Public-Key Cryptosystems". Briefly, in public key cryptography, a message is encrypted by representing it as a number M, raising M to a publicly specified power e, and then taking the remainder when the result is divided by a publicly specified product N, of two large secret prime numbers P and Q. Decryption is similar, except that a different, secret, power d is used, where

$$e.d = 1 \pmod{(P-1).(Q-1)}.$$

The security of such a system depends in part on the difficulty of factoring the publicly specified value N. A further feature of such a system is that messages can be "signed" using the secretly held decryption key d, and anyone can verify this signature using the publicly revealed encryption key e.

More particularly, if N is the product of two prime numbers P, Q, i.e., if

$$N = P.Q;$$

and if e is relatively prime to $\varphi(N)$, where

$$\varphi(N) = (P-1).(Q-1)$$

is Euler's totient function of N (the number of integers less than N which are relatively prime to N), then, in modulus N arithmetic, a value d can be determined (see for example, the aforementioned article by Rivest et al) which is the multiplicative inverse of e such that

$$e.d = 1 \pmod{\varphi(N)}.$$

The value d is commonly referred to as the secret key counterpart of the public key e.

Thus, if

$$X = Y^e \pmod N,$$

then

$$Y = X^d \pmod N$$

for all values of Y, $0 \leqslant Y < N$.

As mentioned above, this knowledge has been employed in the art of cryptography to design various ciphering systems where typically the integers e and N are disclosed to parties of the cryptographic sessions as a public ciphering key and the integer d is held by the party originating the keys as a secret key value.

Users of these techniques may therefore encipher data Y using the public key (e, N) in reasonable knowledge that only the holder of the secret key value d may decipher the data Y.

Similarly the holder of the secret key value d may encipher data X using (d, N) so that any party with knowledge of the public key values (e, N) may determine that only the holder of the secret key value d could have been the source of data X.

These procedures permit users of the technique to encipher sensitive data and also to digitally sign that data to authenticate its source.

The proof of the aforementioned relationships will now be established.

Given that

$$N = P.Q$$

and

$$e.d = 1 \bmod \varphi(N) \qquad (1)$$

where both P and Q are prime integers,

then

$$\varphi(N) = \varphi(P).\varphi(Q) = (P-1).(Q-1).$$

It will be shown that, if

$$X = Y^e \pmod N \qquad (2)$$

then

$$Y = X^d \pmod N. \qquad (3)$$

Note that if (3) is true, then from (2)

$$X = X^{e.d} \pmod N$$

From (1), $X^{e.d} = X^{1+K\varphi(N)} \pmod N$ where K is some integer.

Since P is prime, it is known (Fermat's "little" theorem) that

$$X^{P-1} = 1 \pmod P \text{ for all } X,\ 0 < X < P.$$

Therefore since P-1 divides $\varphi(N) = (P-1).(Q-1)$

$$X^{1+K\varphi(N)} = X \pmod P \text{ for all } X,\ 0 \leq X < P. \qquad (4)$$

Similarly, since Q is prime

$$X^{1+K\varphi(N)} = X \pmod Q \text{ for all } X,\ 0 \leq X < Q. \qquad (5)$$

Equations (4) and (5) imply that

$$X^{1+K\varphi(N)} = X \pmod{P.Q} \text{ for all } X,\ 0 \leq X < N,$$

i.e.

$$X = Y^e = X^{e.d} = X^{1+K\varphi(N)} = X \pmod N$$

Therefore, if

$$X = Y^e \pmod N$$

then

$$Y = X^d \pmod N$$

for all $Y,\ 0 \leq Y < N$

An object of the present invention is to provide a method by which a group consisting of a plurality of members or entities may provide any member of the group with a secret key for the purpose of deciphering data or digitally signing data, which secret key is known to that member only, but where the matching public key can be easily derived by any entity (whether or not a group member) and whereby it can be verified that the member using the secret key is a legitimate member of the group.

Therefore, according to the present invention, there is provided a method of diversifying a key pair for use in public key cryptography by a requesting entity, including the step of generating at a parent entity, a public key N, e, where the modulus N is the product of first and second prime numbers P,Q and e is a corresponding public key integer value, characterized by the steps of: selecting third and fourth prime numbers R,S and transmitting to said requesting entity a first value N_{mi} and a second value $\varphi(N_{mi})$, where said first value N_{mi} = N.R.S and where said second value

$$\varphi(N_{mi}) = \varphi(N).(R-1).(S-1),$$

wherein the symbol φ represents Euler's totient function; selecting, at said requesting entity, fifth and sixth prime numbers T,U; and computing, at said requesting entity a third value N_m and a fourth value d_m, where

$$N_m = N_{mi}.T.U,$$

and where

$$d_m = (1+K\varphi(N_m))/e ,$$

wherein

$$\varphi(N_m) = \varphi(N_{mi}).(T-1).(U-1)$$

and wherein K and d_m are integers, whereby d_m is adapted to be used by said requesting entity as the secret key counterpart of the public key value e with respect to the modulus N_m.

In a particular application, the group of members or entities may be an international transaction card issuing association which has many members, for example of the order of thousands of members.

One embodiment of the invention will now be described by way of example, with reference to the accompanying drawings, in which:-

Fig. 1 is a block diagram of processing apparatus located at the group parent;

Fig. 2 is a flowchart illustrating a generation or set-up phase of operation of the parent processing apparatus;

Fig. 3 is a flowchart illustrating an operational phase of the parent processing apparatus in response to a member request;

Fig. 4 is a block diagram of processing apparatus located at a group member;

Fig. 5 is a flowchart illustrating a generation phase of operation for the member processing apparatus;

Fig. 6 is a flowchart illustrating an operational phase of the member processing apparatus; and

Fig. 7 is a flowchart illustrating an operational phase for an entity communicating with a group member.

As an aid to understanding the present invention, the mathematical principle underlying the invention will first be explained. Thus, the mathematical relationships established hereinabove for the case where

$$N = P.Q$$

is the product of two prime numbers are readily seen to be equally valid for the case where N is the product of more than two prime numbers, since for such a number N, all the integers, I which are factors of N satisfy

$$X^{I-1} = 1 \pmod{I}.$$

Thus, where, for example,

$$N = P.Q.R.S.T.U$$

is the product of six prime numbers,
then if

$$X = Y^{e} \pmod{N}$$

then

$$Y = X^{d} \pmod{N}$$

for all Y, $0 \leq Y < N$

provided that

$$e.d = 1 \pmod{\varphi(N)}$$

where

$$\varphi(N) = (P-1).(Q-1).(R-1).(S-1).(T-1).(U-1).$$

The preferred embodiment of the invention will now be described in relation to a group of members or entities of which one specified member is a trusted member herein referred to as the "parent". For such a group of members, three problems are addressed herein:-

1. Proof of group membership.
2. Protection of the individual member secret keys.
3. Easy derivation of the matching member public keys.

Referring now to Fig. 1, there is shown a block diagram of apparatus which is located at the parent. Such apparatus includes a security processor 10. The security processor 10 comprises a housing 12 which contains a microprocessor 14, a program PROM 16, a RAM (random access memory) working memory 18, a secure nonvolatile memory 20, a random number generator 22, tamper detection circuitry 24, and an input/output unit 26. The devices 14, 16, 18, 20, 22 and 26 are interconnected by an internal bus 28. The tamper detection circuity 24 is adapted to detect any unauthorized tampering with the housing 12, such as an attempt to penetrate the housing, and to provide a reset signal over a line 30 to reset the secure nonvolatile memory 20 in response to the detection of such tampering. An example of a suitable security processor is described in more detail in U.S. Patent No. 4,593,384.

The security processor 10 is connected over an external bus 32 to a plurality of peripheral devices, including a keyboard 34, which enables data to be manually entered, a display 36, a printer 38 which enables output data to be

printed and a communications interface 40 (such as a modem), which enables communication with remote devices to take place over a channel 42.

Refering now to Fig. 2, there is shown a flowchart for the security processor 10 located at the parent, during generation of a public key (e,N). In an initial input step, an initialize or set-up command is applied as shown at box 50, to condition the security processor 10 to perform the desired operation. Next, as shown at box 52, a routine provides for the selection of two large random prime numbers P and Q. Such routines are well-known. For instance, odd random numbers of the desired size can be generated by the random number generator 22 and tested for primality by probabilistic testing methods, as explained in the aforementioned article by Rivest et al.

Next, as shown at box 54, three values are derived, namely the value N, which is the product of P and Q; the value $\varphi(N)$ which is the product of P-1 and Q-1; and a value e which is relatively prime to $\varphi(N)$, that is to say, such that the greatest common divisor (gcd) of e and $\varphi(N)$ is 1. Preferably e is a prime number, for a reason which will be explained hereinafter. Then, as shown at box 56, the values N, $\varphi(N)$ and e are stored in the secure nonvolatile memory 20, Fig. 1. The values N and e are now available in response to a suitable request signal applied to the security processor 10, as indicated at output box 58.

Refering to Fig. 3, there is shown a flowchart for the security processor 10 located at the parent during an operational phase, in response to a request signal supplied from a group member. Thus, as shown at box 70, the security processor 10 receives as an input, a member request command together with a member identification, ID, identifying the group member supplying the request.

Then, as shown at box 72, a routine provides for the selection of two large prime numbers R and S, different from the primes P and Q. Next, as shown at box 74, a value N_{mi} is computed, which is the product of N, R and S:

$$N_{mi} = N.R.S,$$

and also the value $\varphi(N_{mi})$, where

$$\varphi(N_{mi}) = \varphi(N).(R-1).(S-1).$$

Next, as shown at box 76, the value of the member ID is stored in the secure memory 20, together with the values of $N_{mi}, \varphi(N_{mi})$. These stored values are now available for output from the security processor 10, as shown at box 78, and may be displayed, printed or supplied to a security processor 110, Fig. 4, located at the requesting member, which will now be described.

Refering to Fig. 4, there is shown a block diagram of apparatus which is located at each member of the group. The provided apparatus is similar to the apparatus located at the parent, and described hereinabove with reference to Fig. 1. Thus, the member apparatus includes a security processor 110, having a housing 112 which contains a microprocessor 114, a program PROM 116, a RAM working memory 118, a secure nonvolatile memory 120, a random number generator 122, tamper detection circuitry 124 and an input/output unit 126. An internal bus 128 interconnects the various devices as shown in Fig. 4. The tamper detection circuitry 124 can issue a reset signal over a line 130 in response to the detection of an attempt to penetrate the housing 112. Reference is again directed to U.S. Patent No. 4,593,384 for a more detailed description of a suitable security processor. The security processor 110 is connected over an external bus 132 to a keyboard 134, a display 136, a printer 138 and a communications interface 140, enabling communication with remote devices to take place over a channel 142.

Referring now to Fig. 5, there is shown a flowchart for the security processor 110 located at the group member, during a key generation phase for the group member. Initially, an initialize command is supplied to the processor 110, together with the values N,e, N_{mi} and $\varphi(N_{mi})$, which may be derived from a cipher generated by the security processor 10 at the parent and transmitted over the channels 42 and 142 to the security processor 110. Next, as shown at box 152, a routine is effected to select two large prime numbers T and U. It should be understood that all the prime numbers P, Q, R, S, T, U should be different. The parent selects P, Q, R and S and can ensure their difference. However, the member does not know these values and could accidentally select T or U equal to P, Q, R or S. For large primes this probability is remote. However, for smaller primes the probability may be of concern. This probability may be avoided by the parent supplying to the security processor 110 a magnitude boundary for T, U values.

For example, if

$$P, Q, R, S > 2^{150}$$

then

$$T, U < 2^{150}$$

It should further be understood that, in order not to restrict the choice of primes at the member, the value of e initially selected by the parent should be a prime number, thereby ensuring the relative primality of e with respect to any $\varphi(N_m)$ value.

Next, as shown at box 154, four values are computed. Firstly, a value N_m, which is the product of N_{mi}, T and U:

$$N_m = N_{mi}\ T.U.$$

Secondly, by dividing N_m by N, a value N_{mv} is computed:

$$N_{mv} = \frac{N_m}{N}$$

The value N_{mv} will be referred to herein as the "member

variant". Thirdly, the value $\varphi(N_m)$ is computed as the product of $\varphi(N_{mi})$, T-1 and U-1:

$$\varphi(N_m) = \varphi(N_{mi}).(T-1).(U-1).$$

Finally, an integer d_m is computed from the formula

$$d_m = \frac{1+K\varphi(N_m)}{e},$$

In this formula, K is an integer value desirably selected such that d_m which is the member's secret key, is the smallest integer computable from the formula. It is pointed out that steps 152 and 154, carried out at the member processor 110 have the effect of preventing the parent from determining the member's $\varphi(N_m)$, and hence the member's secret key, since the parent would need to factor $T.U = N_m/N_{mi}$ in order to obtain T-1 and U-1, and such factorization is infeasible with T and U being suitably large prime numbers. Similarly the member, knowing N, N_{mi} and $\varphi(N_{mi})$ cannot feasibly determine the parent $\varphi(N)$ and thus P, Q, since this requires the factorization of $R.S = N_{mi}/N$. Thus, it will be appreciated that the value $\varphi(N_m)$ is sourced from a "seed value" N, but is "doubly diversified" to prevent calculation by any person or entity other than the member owner, who may only derive a legitimate $\varphi(N_m)$ and thus a legitimate d_m by utilizing the values supplied by the parent.

Returning now to Fig. 5, at box 156, the values N_m, d_m, e, N, and N_{mv} are stored in the secure nonvolatile memory 120. Finally, at box 158, the member variant value N_{mv} is supplied as an output, for printing, display and/or remote transmission. This member variant value is "published" or made available upon request, and the member's public key modulus can be readily derived by multiplying N_{mv} by N:

$$N_m = N_{mv}.N.$$

Thus, the member has the public key (e, N_m), with the corresponding secret key counterpart being d_m. However, the member variant value N_{mv} rather than N_m itself is published by the member.

With the above in mind, it will be appreciated that the authenticity of data Y emanating from the member may be established by the member digitally signing the data with d_m, such that

$$X = Y^{dm} \pmod{N_m}$$

and that such signature X may be verified by any entity (whether a member of the group or not) by calculating

$$Y = X^{e} \pmod{N, N_{mv}}$$

This procedure not only determines the validity of the signature supplied by the member via N_{mv}, but also determines valid membership of the group via N. Consequently, if proof of group membership is established, then the value N_{mv} may be trusted, even though it may be unknown immediately prior to the authenticity test. It can therefore be delivered with the digital signature, obviating the need for any prior knowledge by the signature verifier except for the published group N and e values.

Furthermore, enciphered data Y can be feasibly deciphered only by the member by utilizing mod N_m exponentiation to the power d_m provided that the transmitter of such enciphered data ultilizes the group public e value and the N value modified by the member variant N_{mv}.

Referring now to Fig. 6, there is shown a flowchart for the operational phase of the member security processor 110. Thus, as shown at box 170, there is input a decipher command, together with enciphered data or cleartext. As shown at box 172, the input data is raised to the exponent power d_m, using the member's stored secret key d_m, and the result expressed as a residue, mod N_m, using

the member's public key modulus value N_m, thereby providing cleartext or a digital signature. Finally, as shown at box 174, the provided cleartext or digital signature is made available as an output signal for printing, display or remote transmission, together with the member variant value N_{mv}.

It will be appreciated from the above that communication with a group member can be established by an entity which is not a group member. Communication by such an entity is illustrated in the flowchart shown in Fig. 7, it being understood that the entity has a conventional processor, such as a PC (personal computer), including computing and storage facilities. Thus, box 180 shows an input as comprising an encipher command, the values N and e, which are supplied by the group parent, or derived from published lists, input data in the form of cleartext or a signature, and a member variant value N_{mv} corresponding to the member with which the entity desires to communicate. Next, as shown at box 182, the product of N_{mv} and N is computed to produce N_m, which is the public key modulus of the communicating group member. Then, the input data (cleartext or signature) is subject to exponentiation to the power e, modulo N_m to produce enciphered data or cleartext, such computed data being stored if desired, as shown at box 184. The enciphered data o- cleartext are then available to be provided as output signals, as shown at box 186.

An advantage of the arrangement described herein is that a forger knowing N cannot feasibly calculate a suitable N_{mv} and matching d_m to produce a valid signature without knowledge of a suitable $\varphi(N_m)$. Note that:

$$d_m = \frac{1 + K\varphi(N_m)}{e}$$

$$\varphi(N_m) = \varphi(N) \cdot \varphi(N_{mv}).$$

Although $\varphi(N_{mv})$ can be determined by a forger selecting his own N_{mv}, to calculate $\varphi(N)$ requires a knowledge of P and Q. These values are known only to the parent, and are kept secret. Thus, provided that the secrecy of P and Q can be maintained, a forger can be defeated.

As a further safeguard, to protect against the accidental disclosure of a member's $\varphi(N_{mi})$, the parent or group may decide to publish or make readily available the N_{mv} values of all the group members, thus precluding fraudulent N_{mv} values from being used.

Further, one member cannot masquerade as another member because the correct d_m requires knowledge of $\varphi(N_{mi})$ and it is not possible to determine another member's $\varphi(N_{mi})$ without knowledge of $\varphi(N)$ and the member's R and S values. All these values are kept secret by the parent.

Thus, by virtue of the present invention, each group member is protected from other members, yet can prove both himself specifically and his membership of the group generally. Even the group parent cannot masquerade as another member.

The invention is therefore suitable in environments such as an international transaction card association which may have many thousands of card issuing members. Each of these card issuers could secure himself from forgery of his cards without the need to previously disclose the information required to establish the authenticity of his cards to various authenticators such as card accepting merchants. The card acceptor need only have prior knowledge of the association's global values N and e in order to readily determine the authenticity of the card. The card would need to carry and disclose as required the member's variant N_{mv} and a value which may be determined as having been produced by the utilization of the

member's specific secret key d_m. The card acceptor could then un-sign that value and compare it to a known value appropriate for that card or transaction.

CLAIMS

1. A method of diversifying a key pair for use in public key cryptography by a requesting entity, including the step of generating at a parent entity, a public key N, e, where the modulus N is the product of first and second prime numbers P,Q and e is a corresponding public key integer value, characterized by the steps of: selecting third and fourth prime numbers R,S and transmitting to said requesting entity a first value N_{mi} and a second value $\varphi(N_{mi})$ where said first value N_{mi} = N.R.S and where said second value $\varphi(N_{mi}) = \varphi(N).(R-1).(S-1)$, wherein the symbol φ represents Euler's totient function; selecting, at said requesting entity, fifth and sixth prime numbers T,U; and computing, at said requesting entity a third value N_m and a fourth value d_m, where $N_m = N_{mi}.T.U$, and where

$$d_m = \frac{1+K\varphi(N_m)}{e}$$

wherein

$$\varphi(N_m) = \varphi(N_{mi}).(T-1).(U-1)$$

and wherein K and d_m are integers, whereby d_m is adapted to be used by said requesting entity as the secret key counterpart of the public key value e with respect to the modulus N_m.

2. A method according to claim 1, characterized by the steps of: storing the values of N, $\varphi(N)$ and e in storage means (20) at said first entity.

3. A method according to claim 2, characterized by the step of storing in said storage means (20) an identification code identifying said requesting entity, said first value N_{mi} and said second value $\varphi(N_{mi})$.

4. A method according to claim 3, characterized by the step of computing, at said requesting entity,

a fifth value N_{mv}, where

$$N_{mv} = \frac{N_m}{N}$$

and storing said fifth value in further storage means (20) at said requesting entity.

5. A method according to any one of the preceding claims, characterized in that the value of said public key integer value e is a prime number.

6. A method according to claim 4 or claim 5, characterized by the step of multiplying the value N_{mv} by the value N to yield the value N_m, utilization of which, with the value e, enables the verification of digital signatures or the enciphering of data sent from or to said requesting entity.

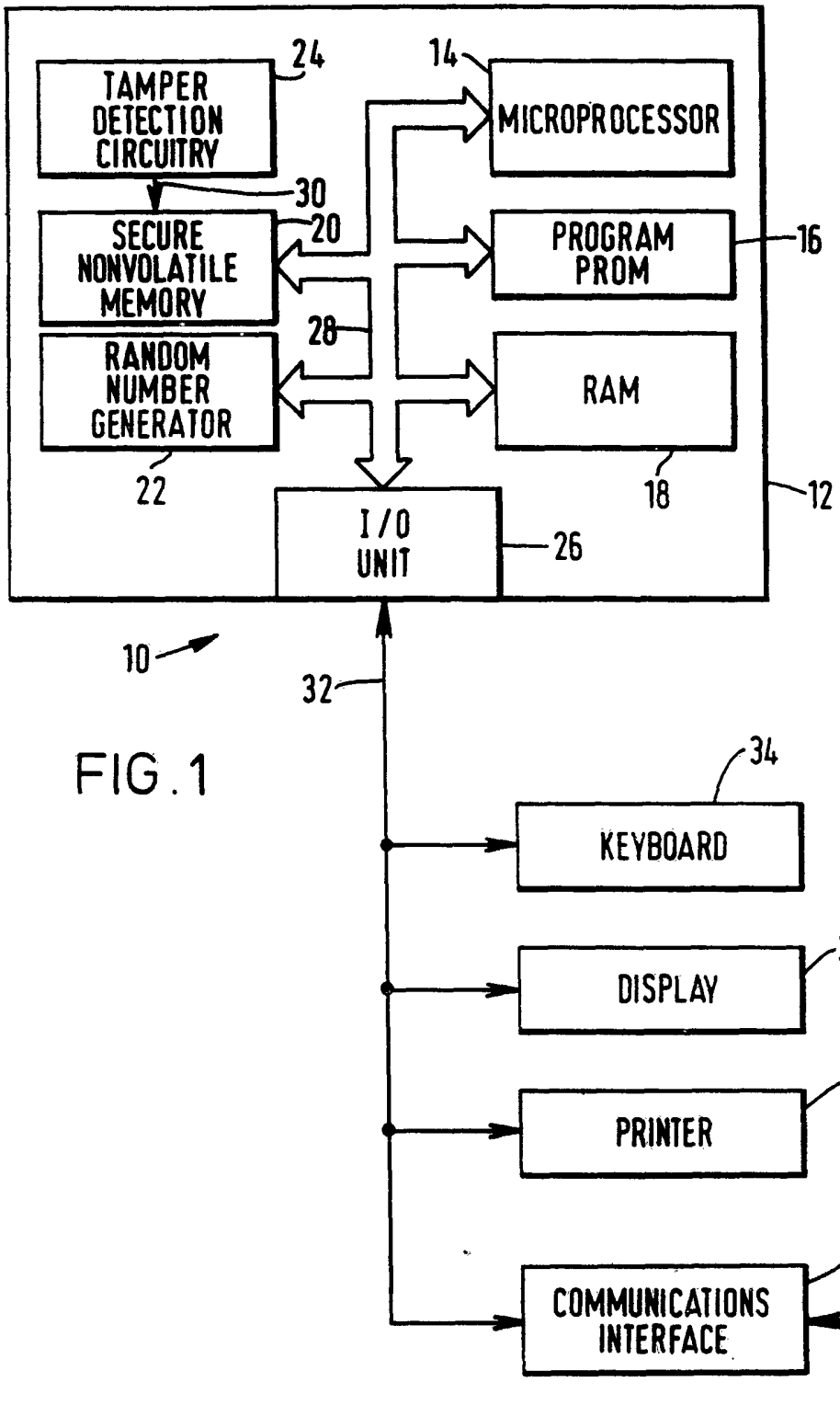

TAMPER DETECTION CIRCUITRY
24
MICROPROCESSOR
14
30
SECURE NONVOLATILE MEMORY
20
PROGRAM PROM
16
28
RANDOM NUMBER GENERATOR
RAM
22
18
12
I/O UNIT
26
10
32
34
KEYBOARD
DISPLAY
36
PRINTER
38
40
COMMUNICATIONS INTERFACE
42

FIG. 1

FIG. 2

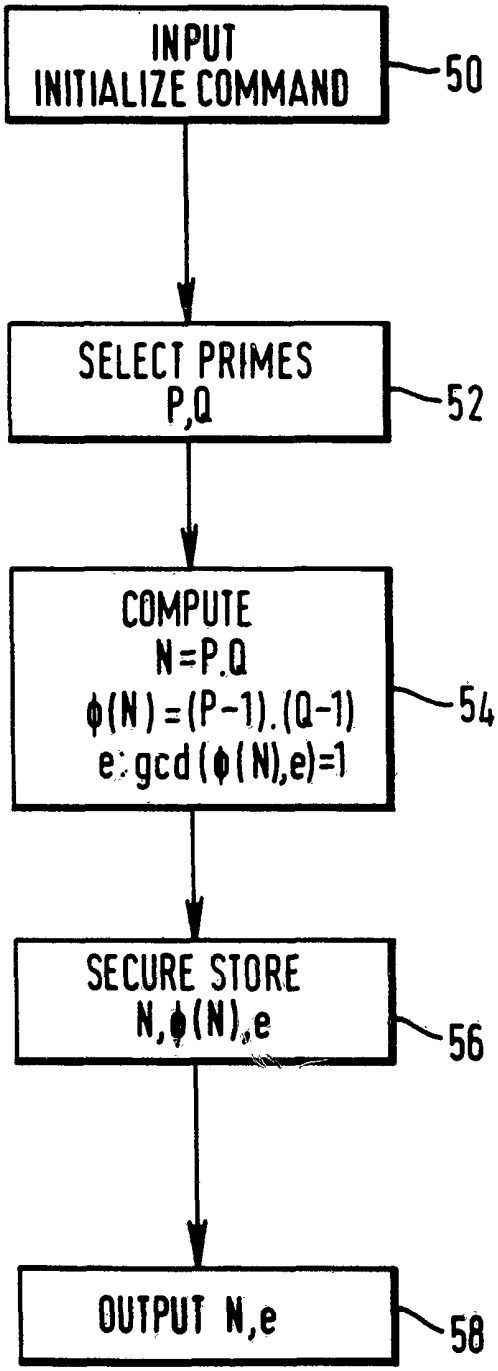
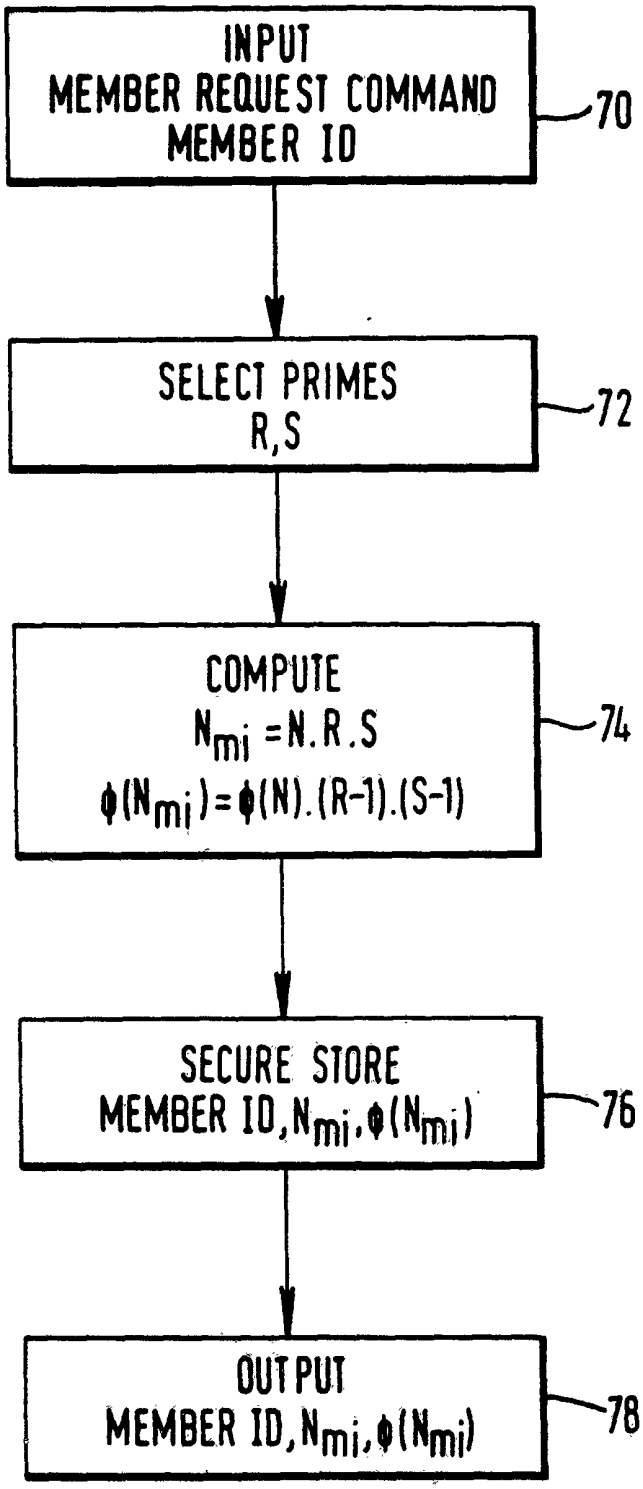

INPUT
INITIALIZE COMMAND
50
SELECT PRIMES
P,Q
52
COMPUTE
N=P.Q
φ(N)=(P-1).(Q-1)
e: gcd(φ(N),e)=1
54
SECURE STORE
N,φ(N),e
56
OUTPUT N,e
58

FIG. 3


INPUT
MEMBER REQUEST COMMAND
MEMBER ID
70
SELECT PRIMES
R,S
72
COMPUTE
$N_{mi} = N.R.S$
$\phi(N_{mi}) = \phi(N).(R-1).(S-1)$
74
SECURE STORE
MEMBER ID, N_{mi}, $\phi(N_{mi})$
76
OUTPUT
MEMBER ID, N_{mi}, $\phi(N_{mi})$
78

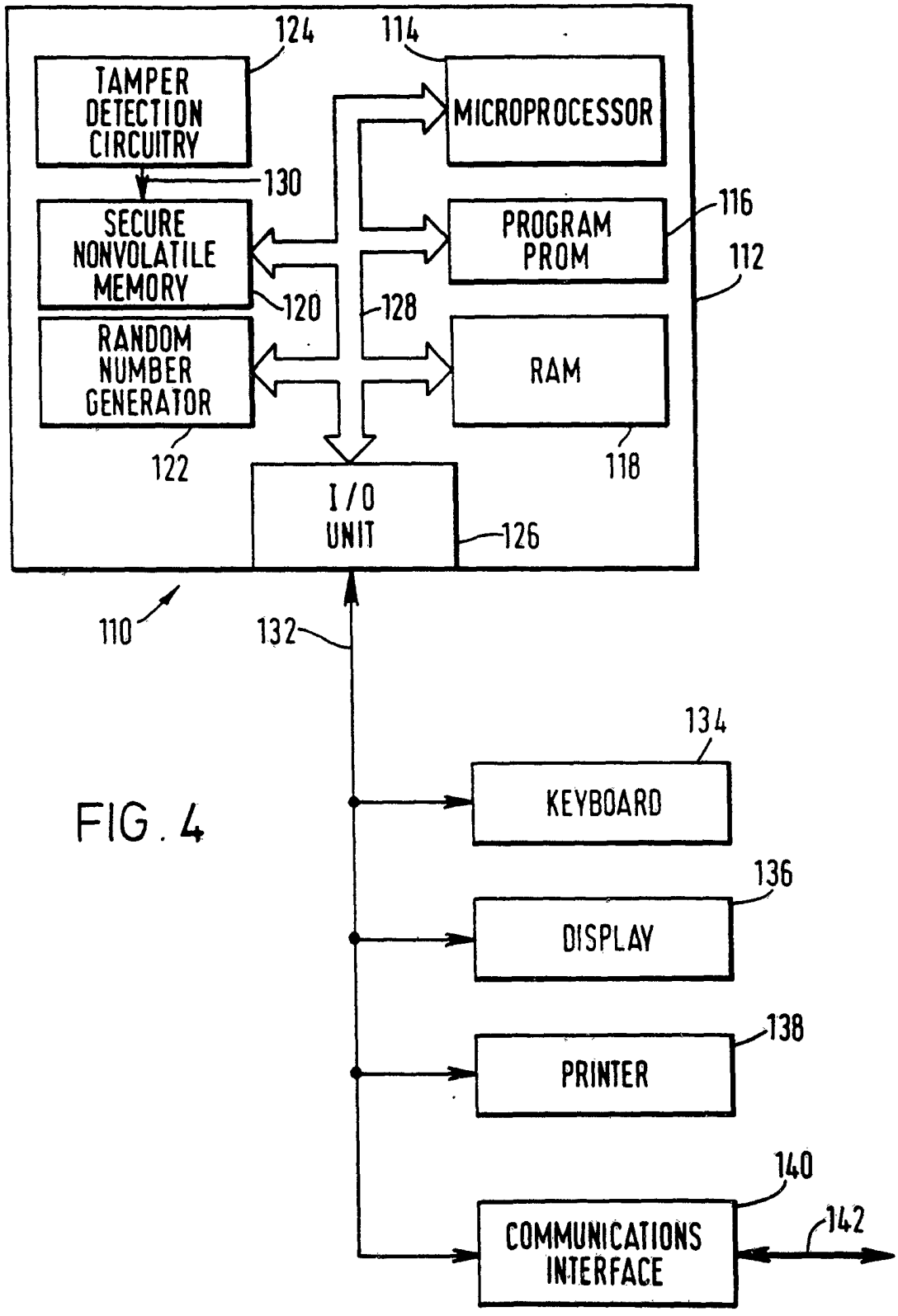

TAMPER DETECTION CIRCUITRY
124
MICROPROCESSOR
114
130
SECURE NONVOLATILE MEMORY
PROGRAM PROM
116
112
120
128
RANDOM NUMBER GENERATOR
RAM
122
118
I/O UNIT
126
110
132
134
KEYBOARD
136
DISPLAY
138
PRINTER
140
COMMUNICATIONS INTERFACE
142

FIG. 4

FIG. 5

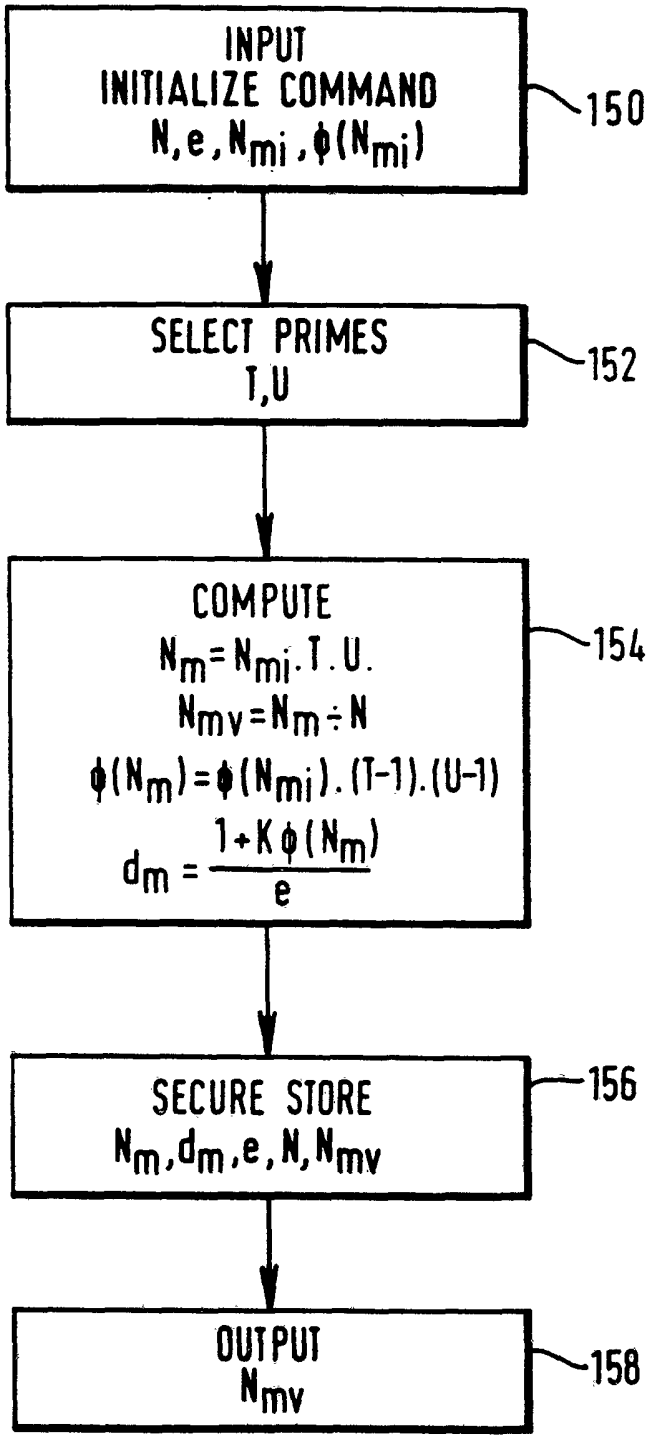

INPUT
INITIALIZE COMMAND
N, e, N_{mi}, $\phi(N_{mi})$
150
SELECT PRIMES
T, U
152
COMPUTE
$N_m = N_{mi} . T . U .$
$N_{mv} = N_m \div N$
$\phi(N_m) = \phi(N_{mi}) . (T-1) . (U-1)$
$d_m = \frac{1 + K\phi(N_m)}{e}$
154
SECURE STORE
N_m, d_m, e, N, N_{mv}
156
OUTPUT
N_{mv}
158

FIG. 6

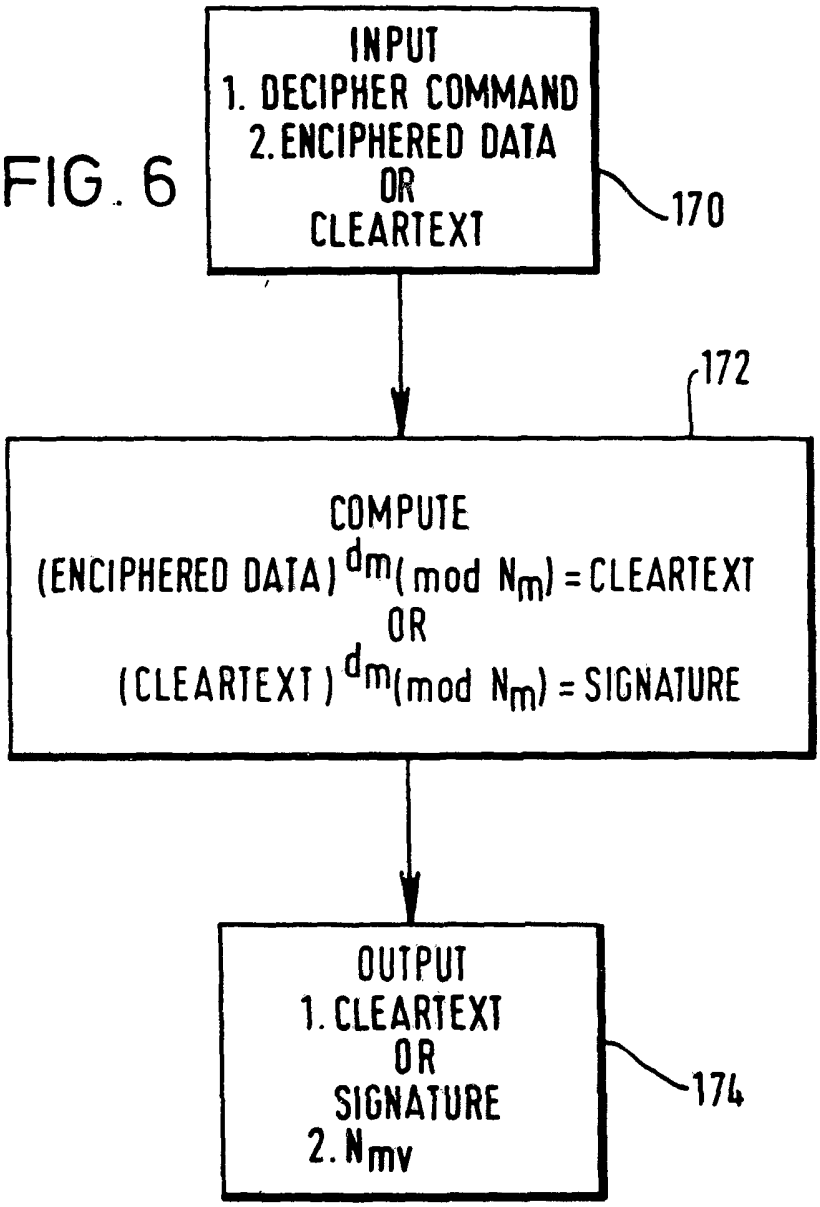
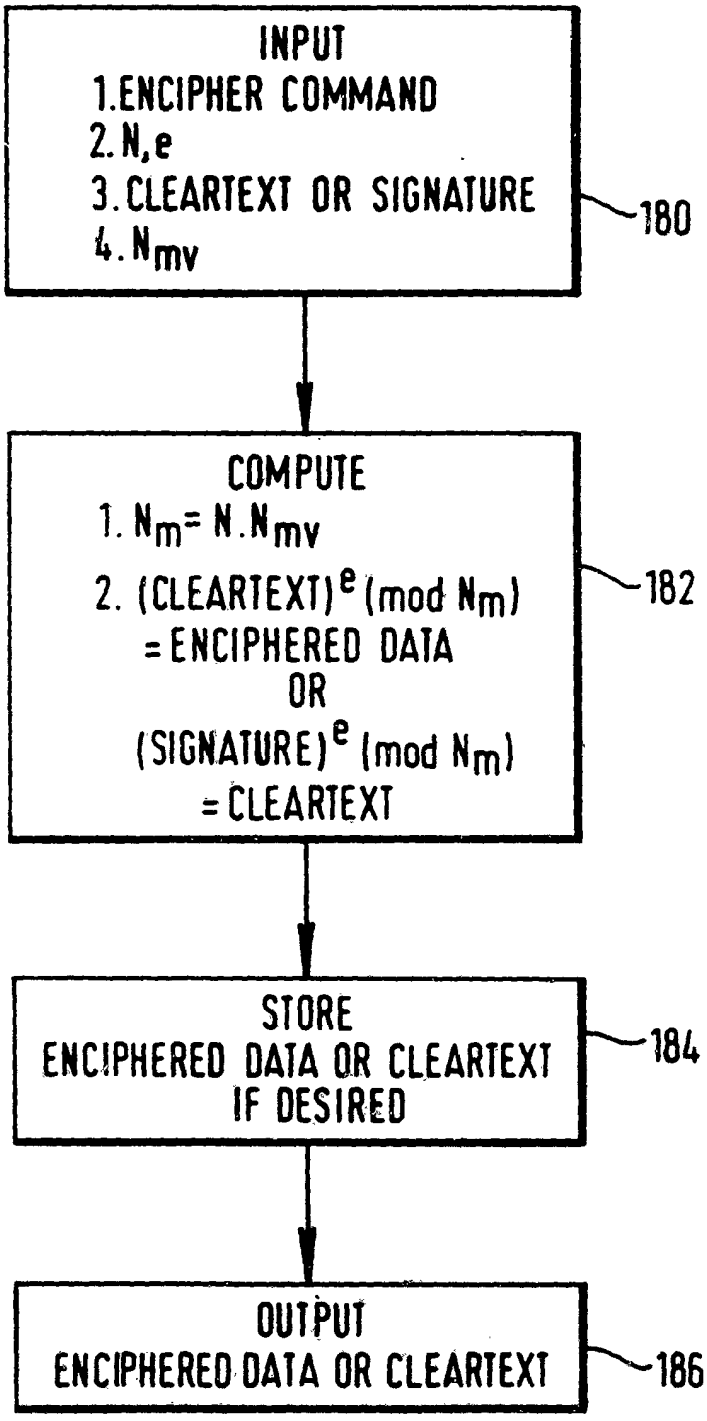

INPUT
1. DECIPHER COMMAND
2. ENCIPHERED DATA
OR
CLEARTEXT
170
172
COMPUTE
(ENCIPHERED DATA) ^{d_m} (mod N_m) = CLEARTEXT
OR
(CLEARTEXT) ^{d_m} (mod N_m) = SIGNATURE
OUTPUT
1. CLEARTEXT
OR
SIGNATURE
2. N_{mv}
174

FIG. 7


INPUT
1. ENCIPHER COMMAND
2. N, e
3. CLEARTEXT OR SIGNATURE
4. N_{mv}
180
COMPUTE
1. $N_m = N . N_{mv}$
2. $(CLEARTEXT)^e \pmod{N_m}$
= ENCIPHERED DATA
OR
$(SIGNATURE)^e \pmod{N_m}$
= CLEARTEXT
182
STORE
ENCIPHERED DATA OR CLEARTEXT
IF DESIRED
184
OUTPUT
ENCIPHERED DATA OR CLEARTEXT
186

INTERNATIONAL SEARCH REPORT

International Application No PCT/US 89/03253

I. CLASSIFICATION OF SUBJECT MATTER (if several classification symbols apply, indicate all) *

According to International Patent Classification (IPC) or to both National Classification and IPC

IPC[5]: H 04 L 9/30

II. FIELDS SEARCHED

Minimum Documentation Searched 7

Classification System	Classification Symbols
IPC[5]	H 04 L

Documentation Searched other than Minimum Documentation to the Extent that such Documents are Included in the Fields Searched 8

III. DOCUMENTS CONSIDERED TO BE RELEVANT 9

Category *	Citation of Document, 11 with indication, where appropriate, of the relevant passages 12	Relevant to Claim No. 13
A	N.E.C. Research & Development, no. 71, October 1983, (Tokyo, JP) K. Itakura et al.: "A public-key cryptosystem suitable for digital multisignatures", pages 1-8, see page 4, left-hand column, line 7 - last line; right-hand column, lines 10-12, line 28 - last line; page 5, left-hand column, line 31 - last line --	1,5
A	Review of the Electrical Communication Laboratories, vol. 32, no. 5, September 1984, (Tokyo, JP) K. Koyama: "Encrypted broadcast communication using public master key", pages 869-876, see page 872, right-hand column, line 7 - page 873, left-hand column, line 6	1

---

* Special categories of cited documents: 10

"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 citation or other 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

"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.

"&" document member of the same patent family

IV. CERTIFICATION

Date of the Actual Completion of the International Search	Date of Mailing of this International Search Report
13th November 1989	08 DEC 1989
International Searching Authority	**Signature of Authorized Officer**
EUROPEAN PATENT OFFICE	T.K. WILLIS