

What is claimed is:

1. A digital radio comprising;
 - a RF transmitter for transmitting digital signals over a radio frequency link;
 - a RF receiver for receiving digital signals transmitted over said radio frequency link;
 - a non-volatile memory device;
 - an encryptor/decryptor coupled to said memory device for cryptographically transforming said transmitted and/or received digital signals based on at least one cryptographic key stored within said memory device; and
 - a further arrangement coupled to said memory device, said further arrangement writing, into said memory device, said cryptographic key within a field of randomized data, said further arrangement hiding said stored cryptographic key within said stored randomized data field, said further arrangement ensuring that said cryptographic key is transformed before said cryptographic key is stored within said memory device and for ensuring that said stored cryptographic key is inversely transformed before it is used by said encryptor/decryptor to cryptographically transform said transmitted and/or received digital signals.

Wherein said farther arrangement repetitively applies different transformations to said cryptographic key.
2. A radio as in claim 1 wherein said further arrangement stores said cryptographic key into said memory device in one of a plurality of key banks.
3. A radio as in claim 1 wherein said further arrangement includes means for storing pseudo-random data into said memory device, and wherein said further arrangement transforms said cryptographic key at least in part in response to said stored pseudo-random data.
4. A digital radio as in claim 1 wherein said further arrangement overwrites portions of said field of randomized data with said cryptographic key, said overwritten cryptographic key disposed entirely within said field of randomized data.

5. A digital radio as in claim 1 wherein said transformation and said inverse transformation are based at least in part on portions of said randomized data field.

6. A digital radio as in claim 1 wherein said further arrangement includes means for exclusive-ORing said cryptographic key with portions of said randomized data to provide a result, and for storing said result in said memory device within said randomized data field.

7. A digital radio as in claim 1 wherein said further arrangement stores at least one pseudo-random value within said randomized data field, and wherein said further arrangement includes means for calculating a starting address within said randomized data field based on said pseudo-random value and for storing said cryptographic key within a key bank beginning at said starting address.

8. A method of communicating securely between first and second radio frequency transceivers over an insecure radio frequency channel, said method including the following steps performed by each of said first and second transceivers:-

- a) storing cryptographic key information in first and second key banks;
- b) selecting one of said first key bank and said second key bank, and also selecting personality data defining at least one further operating characteristic of said transceiver; and
- c) using cryptographic key information from said selected key bank to encrypt and/or decrypt radio frequency transmissions communicated at least in part in accordance with said further operating characteristic, wherein;

said step (c) includes selecting a discrete cryptographic key based on a key bank selector and a key selector; and

said method further includes changing said key bank selector without changing said key selector in order to select any of plural cryptographic keys associated with the same communicating first and second radio frequency transceivers.

9. A method as in claim 8 wherein said step (c) includes the following steps:
i) reading said cryptographic key information from said selected key bank;

- ii) decrypting said cryptographic key information to produce a "clear" key code; and
- iii) encrypting a digitized voice data stream based on said "clear" key code.

10. A method as in claim 8 wherein said step (a) includes encrypting a plurality of discrete cryptographic keys, storing at least one of said encrypted keys in said first key bank, and storing at least another of said encrypted keys in said second key bank, said first and second radio frequency transceivers alternatively selecting from said first bank encrypted keys and said second bank encrypted keys for communicating therebetween.

11. A method as in claim 8 wherein said storing step (a) includes:

- 1) storing pseudo-random data into a non-volatile memory, and
- 2) overwriting only some of said stored pseudo-random data with said cryptographic key information.

12. A method as in claim 8 wherein said storing step (a) includes:

- 1) storing pseudo-random data into a non-volatile memory, and
- 2) hiding said cryptographic key information within said stored pseudo-random data.

13. A method as in claim 8 wherein said storing step (a) includes:

- 1) generating a pseudo-random value; and
- 2) storing said cryptographic key information into a non-volatile memory beginning at a starting address determined at least in part in response to said pseudo-random value.

14. A method as in claim 13 wherein said storing step (a) further includes storing said pseudo-random value within said non-volatile memory.

15. A method as in claim 8 wherein said storing step (a) includes:

- 1) storing pseudo-random data into a non-volatile memory;
- 2) transforming said cryptographic key information at least in part based on said stored pseudo-random data; and
- 3) storing said transformed cryptographic key information into said non-volatile memory.

16. A method as in claim 15 wherein;

said storing step (1) includes writing first and second pseudo-random data into said non-volatile memory;

said transforming step (2) comprises transforming said cryptographic key information based on said first stored pseudo-random data; and

said storing step (3) comprises overwriting said second stored pseudo-random data with said transformed cryptographic key information.

17. A method of operating a digital two-way radio frequency transceiver of the type having a non-volatile memory comprising the following steps:

- a) defining first and second key banks;
- b) defining a variable value;
- c) storing a first plurality of cryptographic keys into said first key bank at a variable location within said non-volatile memory, including the step of selecting said variable location based on said defined variable value;
- d) storing a second plurality of cryptographic keys into said second key bank at a variable location within said non-volatile memory, including the step of selecting said variable location based on said defined variable value;
- e) selecting between said first key bank and said second key bank;
- f) selecting a cryptographic key stored within said selected key bank;
- g) converting analog speech signals into digitized data;
- h) encrypting said digitized data using said selected cryptographic key to provide encrypted digitized data;
- i) generating a radio frequency carrier signal;
- j) modulating said radio frequency carrier signal with said encrypted digitized data;
- k) transmitting said modulated radio frequency carrier signal over the air;
- l) repeating said step (b) to define a further variable value; and
- m) repeating said steps (c) and (d) to store said first and second key bank at variable locations different from said first-mentioned variable locations based on said defined further variable value.

18. A method as in claim 17 wherein said steps (c) and (d) include the step

of encrypting cryptographic keys before storing them, and said method further includes the step of decrypting said encrypted selected cryptographic key before performing said encrypting step (h) with said decrypted selected cryptographic key.

19. A method as in claim 17 wherein:
 - said defining step (b) comprises;
 - generating a pseudo-random value constrained within a range, and
 - providing a second, fixed value; and
 - said storing steps (c) and (d) each include the step of calculating at least one address based at least in part on said pseudo-random value and said second, fixed value.
20. A method as in claim 17 wherein:
 - said method further includes storing a field of pseudo-random data within said non-volatile memory; and
 - said storing steps (b), (c) result in overwriting less than all of said stored pseudo-random data field with said first and second key banks.
21. A method as in claim 17 wherein said storing steps (b), (c) include encrypting said first and second plurality of cryptographic keys prior to storing said keys in said memory.
22. A method as in claim 21 wherein said cryptographic keys encrypting step comprises transforming said cryptographic keys based at least in part on data stored in said non-volatile memory.
23. A method as in claim 22 further including storing randomized data in said memory, and wherein said transforming step comprises transforming said cryptographic keys based at least in part on said stored pseudo-random data.
24. A method of protecting cryptographic keys retained by a radio transceiver comprising:
 - a) connecting a keyloader to a radio transceiver; and
 - b) performing the following steps in response to said connecting step (a);
 - 1) reading, from said radio, stored cryptographic key

information encrypted using a first encryption transformation;

2) decrypting said read cryptographic key information;

3) encrypting said decrypted cryptographic key information using a second encryption transformation different from said first encryption transformation;

4) storing a field of randomized data within said radio, and

5) storing and hiding within said stored randomized data field said key information encrypted by said step (3).

25. A method as in claim 24 wherein said storing and hiding step (5) includes the step of storing said encrypted key information into said radio beginning at a variable location within a non-volatile memory device.

26. A method as in claim 24 wherein said storing and hiding step (5) includes the step of storing said encrypted key information into said radio beginning at a random location within a radio non-volatile memory device.

27. A method as in claim 24 wherein said storage and hiding step (5) includes the step of storing said encrypted key information into said radio within a portion of a radio non-volatile memory device that contains shrouding data.

28. A method as in claim 24 wherein said storing and hiding step (5) includes the step of storing said encrypted key information into said radio beginning at a random location within a portion of a radio non-volatile memory device that contains random data.

29. A method as in claim 24 wherein said encrypting step (3) comprises transforming said cryptographic key information based at least in part on randomized data stored by said storing step (4).

30. A method as in claim 24 wherein said storage and hiding step (5) comprises storing said key information beginning at an address calculated based on at least some of said stored randomized data.

31. A secure method for storing cryptographic keys within the non-volatile memory of a radio device, said method comprising:

a) storing shrouding data within said radio device non-volatile memory,

said shrouding data occupying a block of memory addresses;

- b) providing a variable value;
- c) generating a memory address within said block based at least in part on said variable value; and
- d) hiding said cryptographic keys within said stored randomized data by storing said cryptographic keys within said shrouding data beginning at said generated memory address.

32. A secure method as in claim 31 further including the following steps performed subsequently to said step (d);

- e) providing a further variable value different from said first-mentioned variable value;
- f) generating a further memory address within said block based at least in part on said further variable value; and
- g) overwriting the copy of said cryptographic keys stored beginning at said first-mentioned memory address with shrouding data, and re-storing said cryptographic keys within shrouding data beginning at said further generated memory address.

33. A secure method as in claim 32 wherein said steps (e) - (g) are performed each time a keyloader is connected to said radio device.

34. A secure method as in claim 31 further including encrypting said cryptographic keys at least in part in response to said stored shrouding data before storing said keys within said non-volatile memory.

35. A method as in claim 31 wherein said hiding step (d) comprises overwriting less than all of said shrouding data with said keys.

36. A method as in claim 31 wherein said hiding step (d) comprises encrypting said keys using a process responsive to said stored shrouding data.

37. A method of programming encryption key information into a digital radio communications device non-volatile memory comprising.

- a) writing a block of pseudo-random characters into a portion of said non-volatile memory;
- b) selecting, based at least in part on a pseudo-random process, a

location within said block; and

c) writing at least one cryptographic key into said memory portion at a place corresponding to said selected location, said pseudo-random characters shrouding said written key.

38. A method as in claim 37 further including:

d) selecting a further location based at least in part on said pseudo-random process; and

e) writing said key into said memory portion at a different place corresponding to said further location.

39. A method as in claim 37 further including transforming said encryption key at least in part in response to at least some of said pseudo-random characters, and wherein said writing step (e) comprises writing said transformed encryption key into said memory portion.

40. A method as in claim 39 further including reading said transformed key from said memory portion, and inversely transforming said read transformed key in response to said at least some pseudo-random characters.

41. A method as in claim 37 further including reading said key from said memory portion, and transforming said read key in response to at least some of said pseudo-random characters.

42. A radio communications device comprising:

a non-volatile memory;

means for providing variable data;

address selecting means coupled to receive said variable data for selecting a memory address based at least in part on said variable data; and

shrouding means coupled to said non-volatile memory and also coupled to said address selecting means, for storing shrouding data within said non-volatile memory and for storing at least one cryptographic key within said stored shrouding data beginning at said generated memory address.

43. An arrangement for programming encryption key information into a digital

radio communications device non-volatile memory comprising:

means for writing shrouding characters into a portion of said memory;

means for pseudo-randomly selecting a location within said memory portion;

key encrypting means for encrypting a cryptographic key; and

means coupled to said selecting means and to said key encrypting means for writing said encrypted cryptographic key into said memory portion at a place corresponding to said selected location and surrounded by said shrouding characters, said shrouding characters hiding said encrypted cryptographic key.