

WHAT IS CLAIMED IS:

1                   1.     A method comprising:  
2                   obtaining, by a key management computer, a key rotation period based  
3                   on at least an adversarial storage limit;  
4                   generating, by the key management computer, a first cryptographic  
5                   key; and  
6                   generating, by the key management computer, a second cryptographic  
7                   key to replace the first cryptographic key according to the key rotation period,  
8                   wherein the key rotation period is determined according to the following  
9                   formula:

$$q = \frac{\varepsilon * 2^n}{n * m}$$

10                   where  $q$  is the key rotation period,  $\varepsilon$  is a security value,  $n$  is a block  
11                   size of a corresponding block cipher, and  $m$  is the adversarial storage limit.

1                   2.     The method of claim 1 further comprising:  
2                   providing, by the key management computer, the first cryptographic  
3                   key to a key recipient computer, wherein the key recipient computer encrypts data  
4                   with the first cryptographic key.

1                   3.     The method of claim 2 further comprising:  
2                   receiving, by the key management computer, a cryptographic key  
3                   request message from the key recipient computer; and  
4                   providing, by the key management computer, a cryptographic key  
5                   response message comprising the second cryptographic key to the key recipient  
6                   computer, wherein the key recipient computer encrypts additional data with the  
7                   second cryptographic key.

1                   4.     The method of claim 1, wherein the key rotation period specifies  
2                   an encryption data limit for the first cryptographic key.

1                   5.     The method of claim 1, wherein the key rotation period specifies  
2                   a cipher call limit for the first cryptographic key.

1                    6.        The method of claim 1, wherein obtaining the key rotation period  
2 based on at least the adversarial storage limit further comprises:  
3                    obtaining, by the key management computer, the key rotation period  
4 based on at least the adversarial storage limit from a memory of the key  
5 management computer.

1                    7.        The method of claim 6 further comprising:

obtaining, by the key management computer, the adversarial storage limit;

determining, by the key management computer, the key rotation period based on at least the adversarial storage limit; and

storing, by the key management computer, the key rotation period in the memory.

~~8. The method of claim 7, wherein determining the key rotation period based on at least the adversarial storage limit further comprises:~~

~~determining, by the key management computer, the key rotation period based on at least the adversarial storage limit, a security value, and a block cipher block size.~~

89. The method of claim 1 further comprising:

storing, by the key management computer, the first cryptographic key and the second cryptographic key in a cryptographic key database, wherein a key recipient computer retrieves the first cryptographic key and/or the second cryptographic key from the cryptographic key database.

910. The method of claim 1 further comprising:

updating, by the key management computer, the adversarial storage limit after a predetermined amount of time.

1011. A key management computer comprising:

a processor; and

a computer-readable medium coupled to the processor, the computer-readable medium comprising code executable by the processor for implementing a method comprising:

obtaining a key rotation period based on at least an adversarial storage limit;

generating a first cryptographic key; and

generating a second cryptographic key to replace the first cryptographic key according to the key rotation period.

wherein the key rotation period is determined according to the following formula:

13  $q = \frac{\varepsilon * 2^n}{n * m}$

14 where  $q$  is the key rotation period,  $\varepsilon$  is a security value,  $n$  is a

15 block size of a corresponding block cipher, and  $m$  is the adversarial storage

16 limit.

1                    1112. The key management computer of claim 1011 further  
2 comprising, wherein the method further comprises:

3                    an adversarial storage limit determination module;  
4                    a key rotation period determination module; and  
5                    a cryptographic key generation module.

1                    1213. The key management computer of claim 1011 further  
2 comprising:

3                    a memory coupled to the processor, and wherein obtaining the key  
4 rotation period based on at least the adversarial storage limit further comprises:  
5                    obtaining the key rotation period from the memory.

1                    1314. The key management computer of claim 1213, wherein the  
2 method further comprises:

3                    obtaining the adversarial storage limit;  
4                    determining the key rotation period based on at least the adversarial  
5 storage limit; and  
6                    storing the key rotation period in the memory.

1                    ~~15. The key management computer of claim 14, wherein~~  
2 ~~determining the key rotation period based on at least the adversarial storage limit~~  
3 ~~further comprises:~~

4                    ~~determining the key rotation period based on at least the adversarial~~  
5 ~~storage limit, a security value, and a block cipher block size.~~

1                    1416. The key management computer of claim 1011, wherein the  
2 method further comprises:

3                    updating the adversarial storage limit after a predetermined amount of  
4 time.

1                    1517. The key management computer of claim 1011, wherein the key  
2 rotation period specifies an encryption data limit for the first cryptographic key.

1                    1618. The key management computer of claim 1011, wherein the key  
2 rotation period specifies a cipher call limit for the first cryptographic key.

1719. The key management computer of claim 1011, wherein the first cryptographic key is a first symmetric key and wherein the second cryptographic key is a second symmetric key.

1820. The key management computer of claim 1011, wherein the method further comprises:  
storing the first cryptographic key and the second cryptographic key in a cryptographic key database.

~~21. The key management computer of claim 11, wherein the key rotation period is determined according to the following formula:~~

$$q = \frac{\epsilon * 2^n}{n * m}$$

~~where  $q$  is the key rotation period,  $\epsilon$  is a security value,  $n$  is a block size of a corresponding block cipher, and  $m$  is the adversarial storage limit.~~

1922. A key management computer comprising:  
a processor; and  
a computer-readable medium coupled to the processor, the computer-readable medium comprising code executable by the processor for implementing a method comprising:

obtaining a key rotation period based on at least an adversarial storage limit;

generating a first cryptographic key; and

generating a second cryptographic key to replace the first cryptographic key according to the key rotation period  
~~The key management computer of claim 11,~~

wherein the key rotation period is determined according to the following formula:

$$q' = \frac{\epsilon * 2^n}{m}$$

where  $q'$  is the key rotation period,  $\epsilon$  is a security value,  $n$  is a block size of a corresponding block cipher, and  $m$  is the adversarial storage limit.