WHAT IS CLAIMED IS:

1. A method comprising:

obtaining, by a key management computer, a key rotation period based on at least an adversarial storage limit;

generating, by the key management computer, a first cryptographic key; and

generating, by the key management computer, 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:

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

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

2. The method of claim 1 further comprising:

providing, by the key management computer, the first cryptographic key to a key recipient computer, wherein the key recipient computer encrypts data with the first cryptographic key.

3. The method of claim 2 further comprising:

receiving, by the key management computer, a cryptographic key request message from the key recipient computer; and

providing, by the key management computer, a cryptographic key response message comprising the second cryptographic key to the key recipient computer, wherein the key recipient computer encrypts additional data with the second cryptographic key.

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

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

6. The method of claim 1, wherein obtaining the key rotation period based on at least the adversarial storage limit further comprises:

obtaining, by the key management computer, the key rotation period based on at least the adversarial storage limit from a memory of the key management computer.

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 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.

9. The method of claim 1 further comprising:

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

10. 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:

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

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

11. The key management computer of claim 10 further comprising:

an adversarial storage limit determination module;

a key rotation period determination module; and

a cryptographic key generation module.

12. The key management computer of claim 10 further comprising:

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

obtaining the key rotation period from the memory.

13. The key management computer of claim 12, wherein the method further comprises:

obtaining the adversarial storage limit;

determining the key rotation period based on at least the adversarial storage limit; and

storing the key rotation period in the memory.

14. The key management computer of claim 10, wherein the method further comprises:

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

15. The key management computer of claim 10, wherein the key rotation period specifies an encryption data limit for the first cryptographic key.

16. The key management computer of claim 10, wherein the key rotation period specifies a cipher call limit for the first cryptographic key.

17. The key management computer of claim 10, wherein the first cryptographic key is a first symmetric key and wherein the second cryptographic key is a second symmetric key.

18. The key management computer of claim 10, wherein the method further comprises:

storing the first cryptographic key and the second cryptographic key in a cryptographic key database.

19. 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:

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

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