(12) UK Patent Application (19) GB (11) 2501315 (13) A

(43) Date of A Publication 23.10.2013

(21) Application No: 1206995.1

(22) Date of Filing: 20.04.2012

(71) Applicant(s):
**David Sallis**
**42 Sheen Park, Richmond, LONDON, Greater London,**
**TW9 1UW, United Kingdom**

(72) Inventor(s):
**David Sallis**

(74) Agent and/or Address for Service:
**Withers & Rogers LLP**
**4 More London Riverside, LONDON, SE1 2AU,**
**United Kingdom**

(51) INT CL:
***H04L 9/06*** (2006.01)

(56) Documents Cited:

| | |
|---|---|
| **EP 0625845 A1** | **WO 2008/023881 A1** |
| **US 20070092076 A1** | **US 20030231765 A1** |

**Wikipedia article "Padding (cryptography)", obtained from the Internet: http://en.wikipedia.org/wiki/Padding_(cryptography) (retrieved on the 7/11/12)**
**Paterson et al, "Immunising CBC mode against padding oracle attacks: A formal security treatment", 6th International Conference on Security and Cryptography for Networks, 10-12 Sept. 2008, Springer-Verlag.**
**Journal of Discrete Mathematical Sciences & Cryptography, August 2008, Vol. 11, No. 4, pages 385-391, Chuan-Chi Wang et al, "Low information leakage random padding scheme for block encryption"**

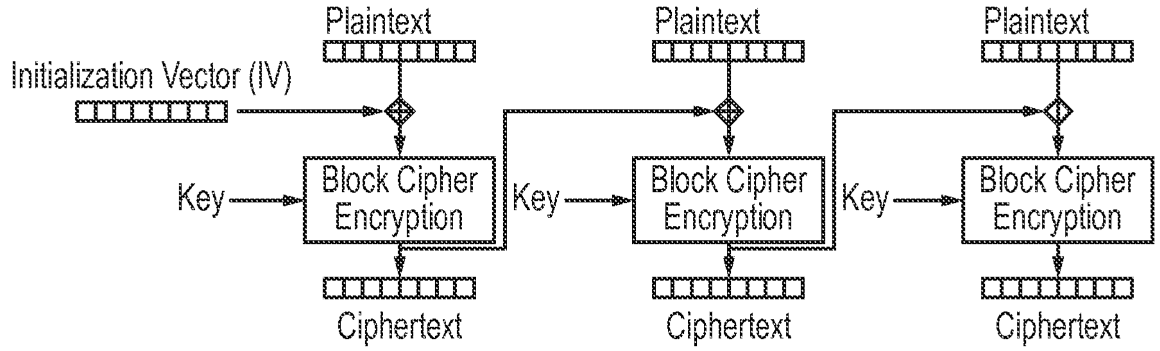
(58) Field of Search:
INT CL **H04L**
Other: **Online: WPI, EPODOC, INSPEC, TXTE**

(54) Title of the Invention: **Methods for generating and decrypting ciphertext**
Abstract Title: **Generation of ciphertext using cipher block chaining (CBC) with padding**

(57) A method of generating a ciphertext sequence from a first key and plaintext comprises generating a first initialisation vector (IV1) and a padding sequence, combining the plaintext and the padding sequence to generate a first intermediate sequence, and generating ciphertext by encrypting the first intermediate sequence using the key and the initialisation vector in a standard cipher-block chaining (CBC) process having a block length of M bytes. The ciphertext is decrypted by generating a second initialisation vector (IV2), decrypting the ciphertext using the first key and the second initialisation vector, and then removing the first N bytes. The padding sequence and initialisation vectors may be randomly generated. The padding sequence may have a length of M bytes and may be added to the beginning of the plaintext. The decryption does not require any knowledge of IV1 (IV2 being unrelated to IV1), or the padding.

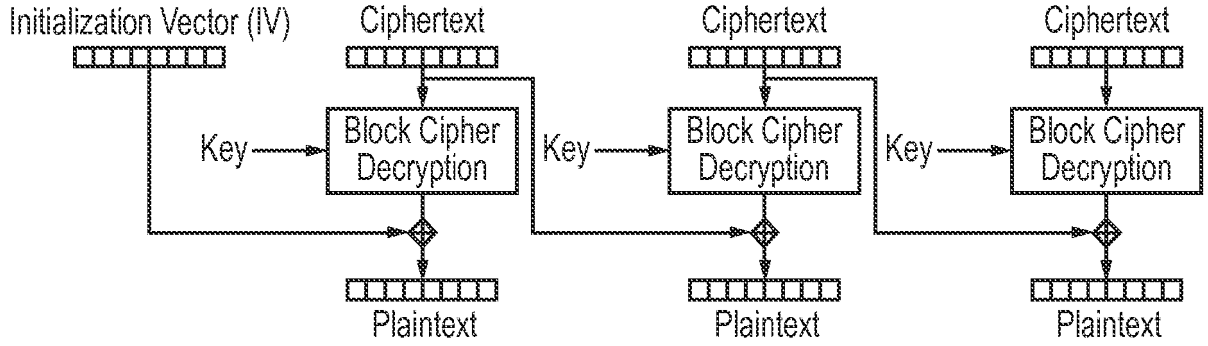
GB 2501315 A

At least one drawing originally filed was informal and the print reproduced here is taken from a later filed formal copy.



Cipher Block Chaining (CBC) mode encryption

FIG. 1



Cipher Block Chaining (CBC) mode decryption

FIG. 2

# Methods for Generating and Decrypting Ciphertext

## Field of the Invention

The present invention relates to an enhancement of the Cipher Block Chaining (CBC) cryptography method patented by IBM ("Message verification and transmission error detection by block chaining", US Patent 4074066, 1976), and subsequent enhancements to the CBC method.

## Background to the Invention

As is well known to those skilled in the art, the CBC algorithm requires, in addition to a key (Key) for encryption and decryption of a message, an Initialisation Vector (IV). It is also well known that for a constant Key, known to both the sender and receiver of the message, the IV must be different for each message if the security of the cipher is to be reasonably safe from attempts to decrypt the encrypted message (Ciphertext) by a third party (Attacker). This necessitates the generation and sending of a new IV along with each Ciphertext, and if the Ciphertext is to be stored, necessitates storing the IV in addition to the Ciphertext. These necessities are an inconvenience in computer systems that transmit and/or store messages encrypted using the CBC algorithm and its variants.

## Summary of the Invention

In a first aspect, the present invention provides a method of generating a ciphertext sequence from a first key and a plaintext sequence, the method comprising: generating a first initialisation vector and a padding sequence; combining the plaintext sequence and padding sequence to generate a first intermediate sequence; generating the ciphertext sequence by encrypting the first intermediate sequence using a cipher-block chaining process having a cipher block length of M bytes, the first key and the first initialisation vector.

In a preferred embodiment, the present invention provides a method of encrypting a message using a CBC method, transmitting or otherwise sharing the Ciphertext, and decrypting the Ciphertext, all without any knowledge by the decrypting party of the IV, nor any requirement of the encrypting party to retain the IV used for the encryption of the message. This is all without any prejudice to the security of the method with respect to decryption by an Attacker.

In further preferred embodiments, the method results in a Ciphertext that is in general different for each instance of encryption of the same message with the same Key, save for accidental cases that will in practice be extremely rare provided a reasonably long Cipher Block size is employed, for example less than one chance in 300,000,000,000,000,000,000,000,000,000,000,000,000 of two successive Ciphertexts being the same for a Cipher Block size of 16 bytes. This aspect is of considerable utility, for example where a commonly occurring message such a person's name appears encrypted in multiple records within a database, in which case the method prevents the association of one record with another by the observation of a common Ciphertext. Note that this aspect is possessed by the standard CBC method provided a different IV is used for each encryption using the same key, but in practice this requirement for a different IV is often not properly observed because of the inconvenience of generation, transmission and/or storage of the different IV for each case.

In a second aspect, the present invention provides a method of generating a plaintext sequence by decrypting a ciphertext sequence using a first key, the method comprising: generating a second initialisation vector; generating a second intermediate sequence by decrypting the ciphertext sequence using the a cipher-block chaining process, the first key and the second initialisation vector; and generating the plaintext sequence by removing the first N bytes from the second intermediate sequence.

## Brief Description of the Drawings

The present invention will now be described by way of example only, and with reference to the accompanying drawings, in which:

Figure 1 shows the standard CBC encryption method known from the prior art; and

Figure 2 shows the standard CBC decryption method known from the prior art.

## Detailed Description of Embodiments of the Invention

### Encryption

A Key, known both to the sender and the receiver but to no other party, and a message (Plaintext) known initially only to the sender, are given.

To encrypt the Plaintext the sender first generates an IV at random (IV1) using one of the secure random string generation algorithms that will be known to those skilled in the art.

A second independent random string (the Padding) equal in length to that of the Cipher Block is similarly generated by the sender.

The sender creates a Padded Message by concatenating the Padding and the Plaintext.

A Ciphertext is created by encrypting the Padded Message using the standard CBC method with IV1 and the Key.

The sender transmits or otherwise shares the Ciphertext with the receiver. The sender does not retain any knowledge of IV1 or the Padding, nor does the sender transmit or otherwise share with the receiver the IV1 or the Padding.

### Decryption

To decrypt the Ciphertext the receiver first generates an IV at random (IV2) using one of the secure random string generation algorithms that will be known to those skilled in the art. IV2 is necessarily unrelated to IV1 since IV1 is unknown to the receiver.

Using the Key, known to the receiver, and IV2, the receiver uses the standard CBC method to decrypt the Ciphertext, resulting in a string (Padded Message 2). The receiver removes a certain number (N) bytes from the beginning of Padded Message 2, resulting in the original Plaintext.

The number N will in general depend on the Cipher Block size employed and the particular implementation of the CBC method and the underlying cipher employed. The number N is easy to determine by examination of an example Plaintext and Padded Message 2 resulting from the particular combination of Block size and underlying cipher employed. For example, in the present embodiment with a Block size of 16 bytes and the commonly used AES256 cipher, then N is equal to 24.

## Claims

1. A method of generating a ciphertext sequence from a first key and a plaintext sequence, the method comprising:

generating a first initialisation vector and a padding sequence;

combining the plaintext sequence and padding sequence to generate a first intermediate sequence;

generating the ciphertext sequence by encrypting the first intermediate sequence using a cipher-block chaining process having a cipher block length of M bytes, the first key and the first initialisation vector.

2. A method of generating a ciphertext sequence according to claim 1, wherein the length of the padding sequence is M bytes.

3. A method according to claims 1 or 2, wherein the first initialisation vector and the padding sequence are generated at random.

4. A method according to any of claims 1 to 3, wherein the cipher-block chaining process is a standard cipher-block chaining process.

5. A method according to any preceding claim, wherein the padding sequence is combined with the plaintext sequence by adding the padding sequence to the beginning of the plaintext sequence.

6. A method of generating a plaintext sequence by decrypting a ciphertext sequence using a first key, the method comprising:

generating a second initialisation vector;

generating a second intermediate sequence by decrypting the ciphertext sequence using the a cipher-block chaining process, the first key and the second initialisation vector; and

generating the plaintext sequence by removing the first N bytes from the second intermediate sequence.

7. A method according to claim 6, wherein the ciphertext sequence is generated according to the method of any of claims 1 to 5.

8. A computer implemented method according to any of claims 1 to 7.

9. A computer program or a suite of computer programs configured to carry out the method of any of claims 1 to 7.

10. A computer-readable medium having the computer program or suite of computer programs according to claim 9 stored thereon.

11. A computing device configured to carry out the steps of any of claims 1 to 7.

| | | | |
|---|---|---|---|
| **Application No:** | GB1206995.1 | **Examiner:** | Matthew Nelson |
| **Claims searched:** | 1-11 | **Date of search:** | 7 November 2012 |

## Patents Act 1977: Search Report under Section 17

**Documents considered to be relevant:**

| Category | Relevant to claims | Identity of document and passage or figure of particular relevance |
|---|---|---|
| X | 1-11 | Wikipedia article "Padding (cryptography)", obtained from the Internet: http://en.wikipedia.org/wiki/Padding_(cryptography) (retrieved on the 7/11/12)<br>See whole document. |
| X | 1, 3, 4, 6-11 | WO 2008/023881 A1<br>(SAMSUNG) See e.g. paragraphs 47-52. |
| X | 1, 3, 4, 6-11 | EP 0625845 A1<br>(MITA INDUSTRIAL) See whole document. |
| X | 1, 3, 4, 6-11 | US 2007/0092076 A1<br>(FU et al) See e.g. paragraphs 4, 5, 40 and 48. |
| X | 1, 3, 4, 6-11 | US 2003/0231765 A1<br>(TARDO) See e.g. paragraphs 49-54 and claim 9. |
| X | 1, 3, 4, 6-11 | Paterson et al, "Immunising CBC mode against padding oracle attacks: A formal security treatment", 6th International Conference on Security and Cryptography for Networks, 10-12 Sept. 2008, Springer-Verlag.<br>See e.g. Definition 9 [Abyte Pad] on page 352 |
| X | 1, 3, 4, 6-11 | Journal of Discrete Mathematical Sciences & Cryptography, August 2008, Vol. 11, No. 4, pages 385-391, Chuan-Chi Wang et al, "Low information leakage random padding scheme for block encryption"<br>See Inspec abstract accession no. 10529204 |

Categories:

| | | | |
|---|---|---|---|
| X | Document indicating lack of novelty or inventive step | A | Document indicating technological background and/or state of the art. |
| Y | Document indicating lack of inventive step if combined with one or more other documents of same category. | P | Document published on or after the declared priority date but before the filing date of this invention. |
| & | Member of the same patent family | E | Patent document published on or after, but with priority date earlier than, the filing date of this application. |

### Field of Search:

Search of GB, EP, WO & US patent documents classified in the following areas of the UKC$^{X}$ :

Worldwide search of patent documents classified in the following areas of the IPC

H04L

The following online and other databases have been used in the preparation of this search report

Online: WPI, EPODOC, INSPEC, TXTE

**International Classification:**

| Subclass | Subgroup | Valid From |
|---|---|---|
| H04L | 0009/06 | 01/01/2006 |