МИНОБРНАУКИ РОССИИ

федеральное государственное бюджетное образовательное учреждение

высшего профессионального образования

«Череповецкий государственный университет»

**Лабораторная работа № 4**

**«Алгоритмы создания цепочек в симметричных криптосистемах»**

**Выполнил:**

студент гр. 1ИВТпб-01-41оп

Климов А.Г.  
**Проверил:** преподаватель

Юдина О.В.  
Отметка о зачете:

Череповец

2018 год

**Задание:**

1. Закодировать сообщение, используя блочный алгоритм из лабораторной работы № 1.
2. Получить ключ из парольной фразы с помощью хэш-преобразований из лабораторной работы № 2.
3. Реализовать 4 цепочки кодирования.

Схемы шифрования:

* + ECB



* + CBC



* + CFB



* + IGE

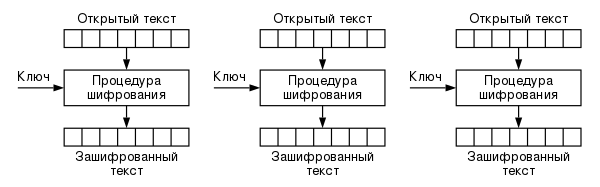


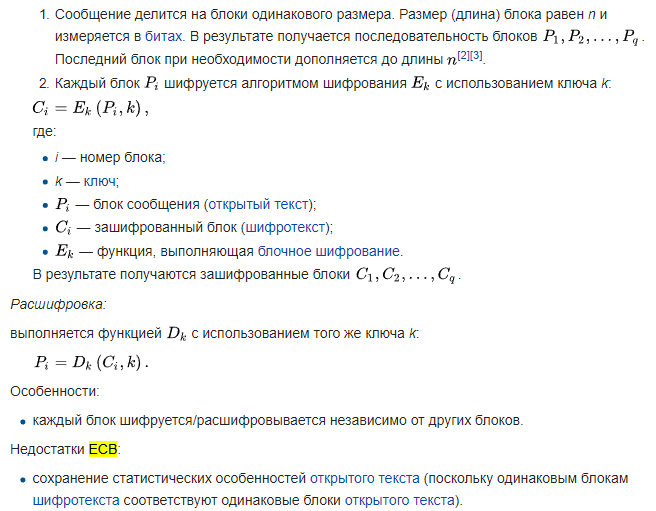
**Выполнение:**

Electronic Codebook (ECB)

Пусть дано сообщение P (открытый текст, последовательность бит, данные).

Во время шифрования выполняются следующие действия:





Достоинства ECB:

постоянная скорость обработки блоков (скорость определяется эффективностью реализации шифра);

возможно распараллеливание вычислений (так как блоки не связаны между собой).

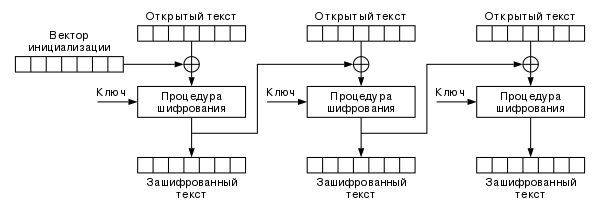
Этот режим называется режимом электронной кодовой книги, так как существует возможность создать книгу, в которой каждому блоку открытого текста будет сопоставлен блок зашифрованного текста. Однако создать книгу — нетривиальная задача. Если размер блока равен x бит, то в книге будет содержаться 2x записей, и каждая книга будет соответствовать одному ключу.

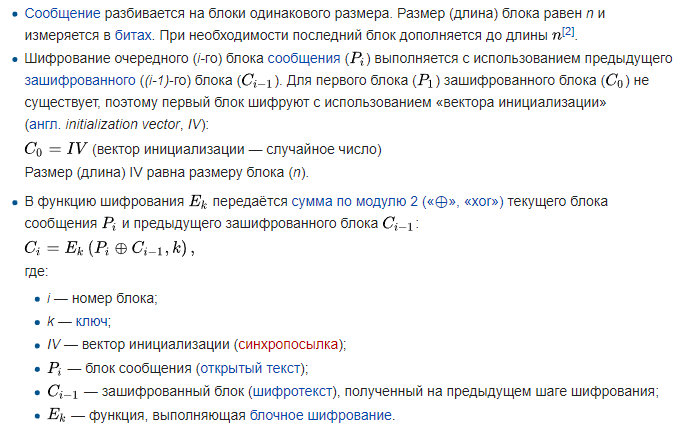
Результат:

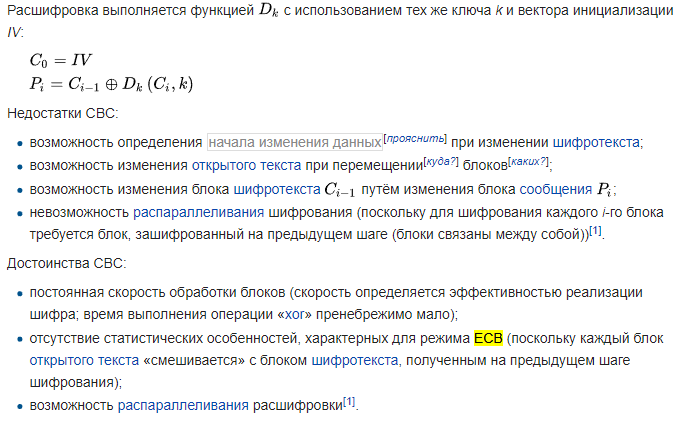
|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| № блока | Открытый текст | Парольная фраза | Ключ шифрования | Зашифрованный текст | Ключ расшифровки |
| 1 | qqq | zzzq | 3092 | GÉµþÓ |  |
| 2 | www | zzzq | 3092 | ~WWÑå\_ |  |
| 3 | eee | zzzq | 3092 | iPF¬\_~\_+ |  |

Cipher Block Chaining (CBC)

Для шифрования некоторого сообщения P выполняются следующие действия:







Результат:

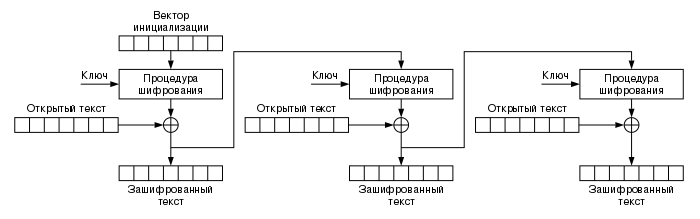
Вектор инициализации = 25.

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| № блока | Открытый текст | Парольная фраза | Ключ шифрования | Зашифрованный текст | Ключ расшифровки |
| 1 | qqq | 0025 | 3059 | /ëþ¸ |  |
| 2 | www | zzzq | 3092 | ¯!«»æ± |  |
| 3 | eee | zzzq | 3092 | O$^÷\_$\_\_\_\_µ¿\_é0 |  |

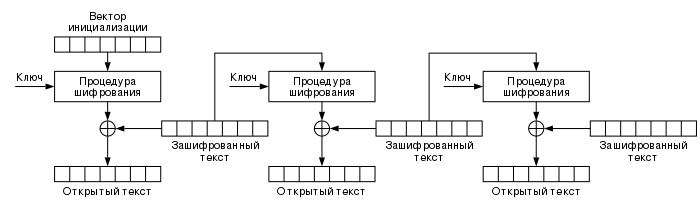
Cipher Feedback Mode (CFB)

Режим обратной связи по шифротексту, режим гаммирования с обратной связью (англ. Cipher Feedback Mode, CFB) — один из вариантов использования симметричного блочного шифра, при котором для шифрования следующего блока открытого текста он складывается по модулю 2 с перешифрованным (блочным шифром) результатом шифрования предыдущего блока.

Шифрование может быть описано следующим образом:



Расшифрование может быть описано следующим образом:



Вектор инициализации IV, как и в режиме сцепления блоков шифротекста, можно делать известным, однако он должен быть уникальным.

Ошибка, которая возникает в шифротексте при передаче (например, из-за помех), сделает невозможным расшифровку как блока, в котором ошибка произошла, так и следующего за ним, однако не распространяется на последующие блоки.

Существует более сложный вариант использования режима, когда размер блока CFB не совпадет с размером блока шифра.

Результат:

Вектор инициализации = 25.

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| № блока | Открытый текст | Парольная фраза | Ключ шифрования | Зашифрованный текст | Ключ расшифровки |
| 1 | qqq | 0025 | 3059 | mZ¼ |  |
| 2 | www | zzzq | 3092 | ú;©\_¤Ãr! |  |
| 3 | eee | zzzq | 3092 | À1(ÆÆïµ¿é0 |  |

IGE



Результат:

Вектор инициализации = 25.

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| № блока | Открытый текст | Парольная фраза | Ключ шифрования | Зашифрованный текст | Ключ расшифровки |
| 1 | qqq | 0025 | 3059 | ûS¨mrmÆ\_ |  |
| 2 | www | zzzq | 3092 | >Þ\_RØÃ¤ê?§F\_Ëù&! |  |
| 3 | eee | zzzq | 3092 | +j #\_3\_èB\_\_ø\_6Åj´Ô |  |