**Блочные шифры**

**СЛАЙД 2** – Цель и задачи

Цель: ознакомление с понятием блочный шифр, его принципом работы и видами.

Задачи:

* Изучить основную идею работы блочного шифра
* Рассмотреть виды блочных шифров
* Ознакомиться с режимами шифрования

**СЛАЙД 3** – Блочный шифр

Современный блочный шифр – это шифр с симметричным ключом, разбивающий перед шифрованием открытый текст на n-битовые блоки и далее шифрующий сообщение блоками, т.е.

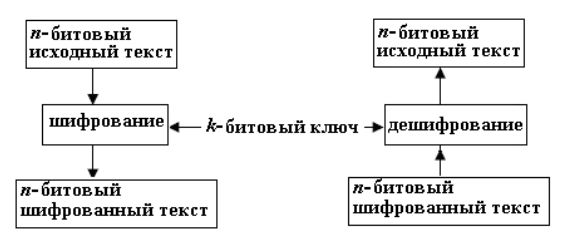


где x , y – блоки открытого и шифрованного текстов; k – секретный ключ шифра; E , D – функции шифрования и дешифрования (другими словами, блоковый алгоритм – это алгоритм простой замены блоков текста фиксированной длины).

**СЛАЙД 4** – Шифрование и дешифрование

Алгоритмы дешифрования и шифрования – инверсные, оба работают на одном и том же секретном ключе.

Общая идея шифрования и дешифрования с помощью блочного шифра:



Если сообщение содержит менее n битов, то его дополняют дополнительными данными (чаще нулями) до n-битового размера; если текст имеет больше, чем n бит, то его делят на n-битовые блоки.

Чаще всего блочные шифры обрабатывают блоки длиной n = 64, 128, 256, 512 бит.

**СЛАЙД 5** – Виды блочных шифров

Блочные шифры бывают двух основных видов:

* шифры перестановки (transposition, permutation, P-блоки);
* шифры замены (подстановки, substitution, S-блоки).

Шифры перестановок переставляют элементы открытых данных (биты, буквы, символы) в некотором новом порядке. Различают шифры горизонтальной, вертикальной, двойной перестановки, решетки, лабиринты, лозунговые и др.

Шифры замены заменяют элементы открытых данных на другие элементы по определенному правилу. Paзличают шифры простой, сложной, парной замены, буквенно-слоговое шифрование и шифры колонной замены.

**СЛАЙД 6** – Виды шифра замены

Шифры замены делятся на две группы:

* моноалфавитные (код Цезаря);
* полиалфавитные (шифр Видженера, цилиндр Джефферсона, диск Уэтстоуна, Enigma).

В моноалфавитных шифрах замены буква исходного текста заменяется на другую, заранее определенную букву. Например, в коде Цезаря буква заменяется на букву, отстоящую от нее в латинском алфавите на некоторое число позиций. Очевидно, что такой шифр взламывается совсем просто. Нужно подсчитать, как часто встречаются буквы в зашифрованном тексте, и сопоставить результат с известной для каждого языка частотой встречаемости букв.

В полиалфавитных подстановках для замены некоторого символа исходного сообщения в каждом случае его появления последовательно используются различные символы из некоторого набора. Понятно, что этот набор не бесконечен, через какое-то количество символов его нужно использовать снова. В этом слабость чисто полиалфавитных шифров.

**СЛАЙД 7** – Режимы шифрования

Режим шифрования – метод применения блочного шифра, позволяющий преобразовать последовательность блоков открытых данных в последовательность блоков зашифрованных данных. При этом для шифрации одного блока могут использоваться данные другого блока. Обычно режимы шифрования используются для модификации процесса шифрования так, чтобы результат шифрования каждого блока был уникальным вне зависимости от шифруемых данных и не позволял сделать какие-либо выводы об их структуре. Это обусловлено, прежде всего, тем, что блочные шифры шифруют данные блоками фиксированного размера, и поэтому существует потенциальная возможность утечки информации о повторяющихся частях данных шифруемых на одном и том же ключе. Существует несколько стандартных режимов шифрования.

**СЛАЙД 8** – Electronic Codebook (ECB) – режим простой замены

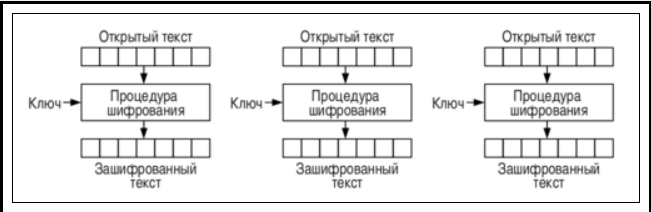
Сообщение делится на блоки. Каждый блок шифруется отдельно (независимо от других и на одном ключе). Этот режим называется режимом электронной кодовой книги, так как существует возможность создать книгу, в которой каждому блоку открытого текста будет сопоставлен блок зашифрованного текста. Однако создать книгу – нетривиальная задача. Если размер блока равен x бит, то в книге будет содержаться 2x записей, и каждая книга будет соответствовать одному ключу.

Зашифрование может быть описано следующим образом:

Ci = F(Pi) для любых i от 1 до N.

Здесь Ci и Pi – блоки зашифрованного и открытого текстов соответственно, а F – функция блочного шифрования. Расшифровка по той же схеме.

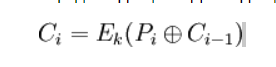
То есть Pi = F-1(Ci).



**СЛАЙД 9** – Cipher Block Chaining (CBC) – режим сцепления блоков шифртекста

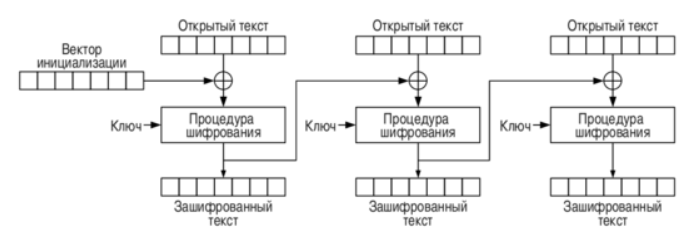
Для сцепления используется механизм обратной связи, поскольку результат шифрации предыдущих блоков используется для шифрации текущего блока. Таким образом любой блок шифра зависит не только от исходного текста, но и от всех предыдущих блоков текста. В Cipher Block Chaining (CBC) текст XOR’ится с предыдущим зашифрованным блоком перед шифрацией. Дешифрация проводится аналогично.

Математическая запись:





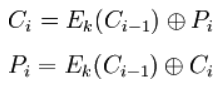
C0 = IV



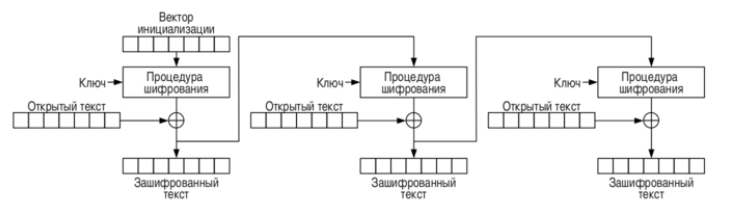
При этом в начале кодирования используется вектор инициализации для того, чтобы любое сообщение было по – настоящему уникальным (иначе будут трудности со стандартным заголовком). Вектор инициализации должен быть случайным числом. Его не обязательно хранить в секрете, можно передавать его вместе с сообщением.

**СЛАЙД 10** – Cipher Feedback (CFB) – режим обратной связи по шифртексту

Режим (CFB) обратной связи шифра, близкий родственник CBC, превращает блочный шифр в самосинхронизирующийся шифр потока. Операция очень похожа на предыдущую; в частности, расшифровка CFB почти идентична расшифровке CBC, выполненной наоборот:



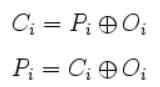
C0 = IV, где IV – вектор инициализации



**СЛАЙД 11** – Output Feedback (OFB) – режим обратной связи по выходу

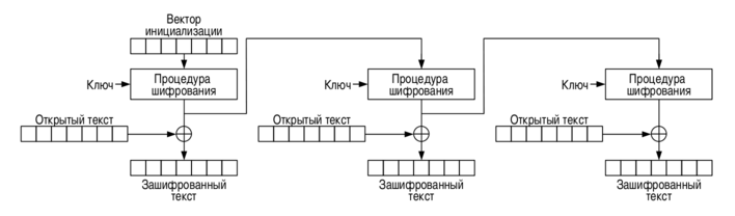
Режим (OFB) обратной связи вывода превращает блочный шифр в синхронный шифрпоток: это генерирует ключевые блоки, которые являются результатом сложения с блоками открытого текста, чтобы получить зашифрованный текст. Так же, как с другими шифрами потока, зеркальное отражение в зашифрованном тексте производит зеркально отраженный бит в открытом тексте в том же самом местоположении. Это свойство позволяет многим кодам с исправлением ошибок функционировать как обычно, даже когда исправление ошибок применено перед кодированием.

Из-за симметрии операции сложения, шифрование и расшифрование похожи:



Oi = Ek (Oi – 1)

O0 = IV

  
**СЛАЙД 12** – Выводы

Выводы:

* Изучена основная идея работы блочного шифра
* Рассмотрены виды блочных шифров
* Ознакомлены с режимами шифрования и принципов их работы

**СЛАЙД 13** – Список использованных источников

Сушко С.А., Практическая криптология – Блочные шрифты

<https://bit.nmu.org.ua/ua/student/metod/cryptology/%D0%BB%D0%B5%D0%BA%D1%86%D0%B8%D1%8F%205.pdf>

Криптография – Блочные шрифты

<http://kryptography.narod.ru/block.html>

CodeNet – Блочные шрифты

<http://www.codenet.ru/progr/alg/enc/7.php>