**СЛАЙД 1**

Передача информации в мобильных сетях является основным методом коммуникации в нашем современном мире. Но этот процесс также сопровождается рисками для безопасности данных. Поэтому методы и алгоритмы шифрования стали одними из важнейших средств защиты информации в мобильных сетях.

**СЛАЙД 2**

Если есть радиотехническая система (РТС) включающая в себя множество устройств и между этими устройствами необходимо выполнять обмен информацией, необходимо разделять каналы.

Для примера рассмотрим сотовую связь.

Есть базовая станция (БС) и множество абонентских устройств. Между БС и мобильными телефонами образуется канал, сколько мобильных устройств столько и каналов. Задача — организовать разделение каналов таким образом, чтобы работа одного устройства, не создавала помех для другого устройства.

**СЛАЙД 3**

При кодовом разделении каналов на одной фиксированной частоте все абоненты передают информацию одновременно.  Они пересекаются по частоте и по времени. Тогда почему они друг другу не мешают?

CDMA (Code Division Multiple Access) - это метод множественного доступа, используемый в сотовых и беспроводных сетях связи, который позволяет нескольким пользователям использовать одну и ту же частоту одновременно, используя разные коды для кодирования своих данных.

Каждый пользователь в сети CDMA имеет свой собственный уникальный код, который используется для передачи его данных через сеть. Это позволяет многим пользователям использовать одну и ту же частоту одновременно, не мешая друг другу.

Одним из преимуществ CDMA является возможность использования более эффективного использования частотного спектра, что позволяет увеличить количество пользователей, которых можно обслуживать одновременно.

**СЛАЙД 4**

Метод шифрования кодами Уолша - это один из методов шифрования, используемых в сотовых сетях связи, который позволяет передавать данные через общий канал, используя уникальные коды Уолша для каждого пользователя.

Коды Уолша - это наборы последовательностей из 1 и -1, которые используются для кодирования данных перед их передачей по сети. Каждый пользователь в сети имеет свой собственный уникальный код Уолша, который используется для кодирования и декодирования его данных. Это позволяет многим пользователям использовать один и тот же канал связи одновременно, не мешая друг другу.

Одним из преимуществ метода шифрования кодами Уолша является возможность передачи большего количества данных через общий канал связи, что позволяет увеличить количество пользователей, которых можно обслуживать одновременно.

На осциллограмме (1) присутствует информационный сигнал, т.е. полезная информация. Информационный сигнал (1) перемножаем с кодовой последовательностью Уолша (2). У последовательности Уолша есть длина, у нее 8 импульсов на последовательности. Вся длина последовательности должна уложиться в длину символа. Длительность последовательности = длительности символа.

Когда начинает передаваться следующий символ, кодовая последовательность начинает опять циклически повторяться от символа к символу. Когда символы “1” и “2” перемножаем с кодовой последовательностью Уолша получаем модулирующую последовательность (3).

Осциллограмму (3) и будем подавать на модулятор. Если символ “1”, тогда кодовая последовательность какая была, такая и осталась. Если символ “0”, тогда последовательность перевернулась.

Когда осциллограмму (3) подаем на модулятор формируется сигнал с двоичной фазовой модуляцией (2-ФМн), но фаза здесь меняется не каждый информационный символ, а будет определяться частотой следования импульсов кодовой последовательности. Скорость манипуляции — как часто меняется параметра гармонического сигнала. В данном случае фаза. Здесь скорость манипуляции в 8 раз больше, чем символьная скорость.

**СЛАЙД 5**

На рисунке выше (способ 1) есть последовательно Уолша, Ts — это длительность информационного символа, а Tch — длительность чипа. N — длина кодовой последовательности (КП). Длительность чипа будем 8 раз меньше длительности символа.

**СЛАЙД 6**

Второй пример формирования cdma. Изменен порядок перемножения. Один импульс кодовой последовательности называется чипом. В примере последовательность включает 8 чипов.

Информационный символы (1) подаем на фазовый модулятор и уже сигнал (2) перемножаем с кодовой последовательностью Уолша (3). В этом примере переставили порядок действий, но результат получился тот же самый.

**СЛАЙД 7**

Во втором способе сначала подали сигнал на модулятор, а затем перемножили с последовательность Уолша.

Когда сигналы доходят до приемника, используя уникальный код, применяемый на приемной стороне, можно извлечь сигнал только одного абонента, тогда как сигналы других абонентов остаются зашифрованными. Это позволяет достичь высокой емкости и надежности передачи данных.

**СЛАЙД 8**

В качестве алгоритма шифрования в GSM используются алгоритмы из семейства A5.  
GSM - это стандарт цифровой сотовой связи, который используется для передачи данных в мобильных сетях. (Сокращение GSM означает Global System for Mobile Communications.) Он поддерживает передачу голоса и данных, а также обеспечивает безопасность передачи данных при помощи шифрования.

Рассмотрим подробнее алгоритм A5/1.

Метод шифрования A5/1 (или A5/2) - это алгоритм шифрования, который используется для защиты данных в сетях мобильной связи. Он был разработан в конце 1980-х годов и до сих пор используется в GSM-сетях.

Алгоритм A5/1 является поточным.

**СЛАЙД 9**

Поточный шифр - это один из типов шифров, который шифрует данные путем генерации последовательности случайных битов.

Формирование выходной последовательности происходит путём сложения потока исходного текста с генерируемой последовательностью.

**СЛАЙД 10**

Регистр сдвига с линейной обратной связью состоит из собственно регистра (последовательности бит заданной длины) и обратной связи. На каждом такте происходит следующие действия: крайний левый бит (старший бит) извлекается, последовательность сдвигается влево и в опустевшую правую ячейку (младший бит) записывается значение функции обратной связи. Эта функция является суммированием по модулю два определённых битов регистра и записывается в виде многочлена, где степень указывает номер бита. Извлечённые биты формируют выходную последовательность.

**СЛАЙД 11**

Структура алгоритма А5 выглядит следующим образом:

* Три регистра(R1, R2, R3) имеют длины 19, 22 и 23 бита,
* Многочлены обратных связей:
  + X19 + X18 + X17 + X14 + 1 для R1,
  + X22 + X21 + 1 для R2 и
  + X23 + X22 + X21 + X8 + 1 для R3,
* Управление тактированием осуществляется специальным механизмом:
  + в каждом регистре есть биты синхронизации: 8 (R1), 10 (R2), 10 (R3),
  + вычисляется функция F = x&y|x&z|y&z, где & — булево AND, | - булево OR, а x, y и z — биты синхронизации R1, R2 и R3 соответственно,
  + сдвигаются только те регистры, у которых бит синхронизации равен F,
  + фактически, сдвигаются регистры, синхробит которых принадлежит большинству,
* Выходной бит системы — результат операции XOR над выходными битами регистров.

А5/1 использует последовательность ключей, которая генерируется на основе трех регистров сдвига. Каждый регистр имеет различную длину и заполняется случайными битами из ключа, который задается при инициализации алгоритма. Ключ длиной 64 бита состоит из двух частей: 54 бита используются для генерации последовательности ключей, а оставшиеся 10 бит являются битами идентификатора абонента.

Генерация последовательности ключей происходит путем сдвига битов в каждом регистре в зависимости от значений его внутренних битов. В процессе работы алгоритма биты каждого регистра соединяются логическим "И" для создания выходного бита, который используется для шифрования передаваемых данных.