Шифрование, алгоритмы симметричного шифрования.

Шифрование — это процесс преобразования исходного сообщения M (называемого

*открытым текстом) в форму M' (зашифрованный текст или шифртекст). При этом провести обратное преобразование M' в M возможно только обладая некоторой дополнительной информацией, называемой ключом.*

## *Симметричное шифрование*

Всимметричных алгоритмах шифрования *один и тот же ключ*K используется для того, чтобы зашифровать сообщение и для его последующей расшифровки. Таким образом, и *отправитель*и *получатель*сообщения должны располагать одним и тем же ключом. Схематично это можно записать в виде:

M' = E(M, K) M = D(M', K),

где Е — функция шифрования (encrypt), а D — функция дешифрования (decrypt), обе используют ключ K в качестве одного из параметров.

Исторически симметричное шифрование появилось первым. Более того, до середины XX века это была единственная разновидность шифрования. Симметричные алгоритмы широко применяются и в настоящее время.

Алгоритм IDEA (International Data Encryption Algorithm) (на данный момент практически не используется ввиду устаревания технологии). В течении долгого времени рассматривался как замена тогда активно используемого DES ввиду большей скорости шифрования и большей устойчивости к взломам, так же в виде ряда других причин (например длина ключа des была всего 56 бит, что даже в 90е годы было довольно легкой переборной задачей). Однако так как технология была запатентована, то существовали проблемы с её повсеместным использованием, и в финале более широкое распространение получил алгоритм Rijdael, используемый в AES.

Алгоритм блочного шифрования, разработанный в Швейцарии в 91-92х годах.

Довольно долго рассматривался как высокий международный стандарт государственного шифрования.

Длина ключа 128 бит

Длина ключевого материала 6 \* 8 \* 16 + 4 \* 16

Первые подключи нарезаются из 128ми битного ключа.

Затем выполняется циклический сдвиг на 25 бит и нарезаются новые ключи по 16 бит

25 бит выбраны таким образом, что бы первый ключ в каждом раунде брался из своей области исходного ключа.

Длина блока 64 бита

Перемешивание 1го целого блока за 1 раунд.

8 раундов перемешивание + заключительное преобразование (1)

Операции не самые характерные для симметричного шифрования

1. XOR (сложение по модулю 2)
2. + mod (2 ^ 16) (сложение по модулю 2 ^16)
3. \* mod (2 ^ 16 + 1) (умножение по модулю 2 ^ 16 + 1) – довольно долгая операция где 2 ^ 16 + 1 – p (простое число)

Между этими операциями не действует ни дистрибутивный, ни ассоциативный законы

В результате можно получить хорошую диффузию

В основе лежит блок MA (multiply addition)

64 битный блок будет поделен на 4 части, и работа производятся операции над 16ти битными блоками.

На вход подаются два 16ти битных значения (P1 и P2)

