МИНОБРНАУКИ РОССИИ

РГУ нефти и газа (НИУ) имени И.М. Губкина

|  |  |
| --- | --- |
| Факультет | **Комплексной безопасности ТЭК** |
| Кафедра | **Управления безопасностью сложных систем** |

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Оценка комиссии: |  | | | Рейтинг: |  |
| Подписи членов комиссии: | | | | | |
|  | |  |  | | |
| (подпись) | |  | (фамилия, имя, отчество) | | |
|  | |  |  | | |
| (подпись) | |  | (фамилия, имя, отчество) | | |
|  | | | | | |
| (дата) | | | | | |
|  | |  |  | | |

**КУРСОВАЯ РАБОТА**

|  |  |
| --- | --- |
| по дисциплине | Методы программирования |
|  | |

|  |  |
| --- | --- |
| На тему | Разработка программного приложения «алгоритм шифрования IDEA» |
|  | |
|  | |

|  |  |  |  |
| --- | --- | --- | --- |
| «К ЗАЩИТЕ» |  | ВЫПОЛНИЛИ: |  |
|  |  | Студенты группы |  |
|  |  |  | (номер группы) |
| стар. преподаватель Гизатуллин М.Р.. |  | Батышкин В. А. | |
| (должность, ученая степень; фамилия, и.о.) |  | Крыжановский В. В. | |
|  |
| (подпись) |  | (фамилия, имя, отчество) (подпись) | |
|  |  |  | |
| (дата) |  | (дата) | |

|  |
| --- |
| Москва, 2022 |

Содержание

Введение

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. По техническим причинам схема шифрования обычно использует псевдослучайный ключ шифрования, сгенерированный алгоритмом. Возможно расшифровать сообщение, не имея ключа, но для хорошо разработанной схемы шифрования требуются значительные вычислительные ресурсы и навыки. Авторизованный получатель может легко расшифровать сообщение с помощью ключа, предоставленного отправителем получателям, но не неавторизованным пользователям.

Симметричное шифрование

В симметричных 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

IDEA (англ. International Data Encryption Algorithm, международный алгоритм шифрования данных) — симметричный блочный алгоритм шифрования данных, запатентованный швейцарской фирмой Ascom. Известен тем, что применялся в пакете программ шифрования PGP. В ноябре 2000 года IDEA был представлен в качестве кандидата в проекте NESSIE в рамках программы Европейской комиссии IST (англ. Information Societies Technology, информационные общественные технологии).

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.

IDEA использует 128-битный ключ и 64-битный размер блока, открытый текст разбивается на блоки по 64 бит. Если такое разбиение невозможно, то последний блок дополняется определённой последовательностью бит. Во избежание утечки информации о каждом отдельном блоке используются различные режимы шифрования. Каждый исходный незашифрованный 64-битный блок делится на четыре подблока по 16 бит каждый, так как все алгебраические операции, использующиеся в процессе шифрования, совершаются над 16-битными числами. Для шифрования и расшифрования IDEA использует один и тот же алгоритм.

Фундаментальным нововведением в алгоритме является использование операций из разных алгебраических групп, а именно:

* сложение по модулю 216
* умножение по модулю 216 + 1
* побитовое исключающее ИЛИ (XOR).

Между данными операциями не действует ни дистрибутивный, ни ассоциативный законы. В результате можно получить устойчивую диффузию.

В основе Алгоритма лежит блок MA (multiply addition)

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

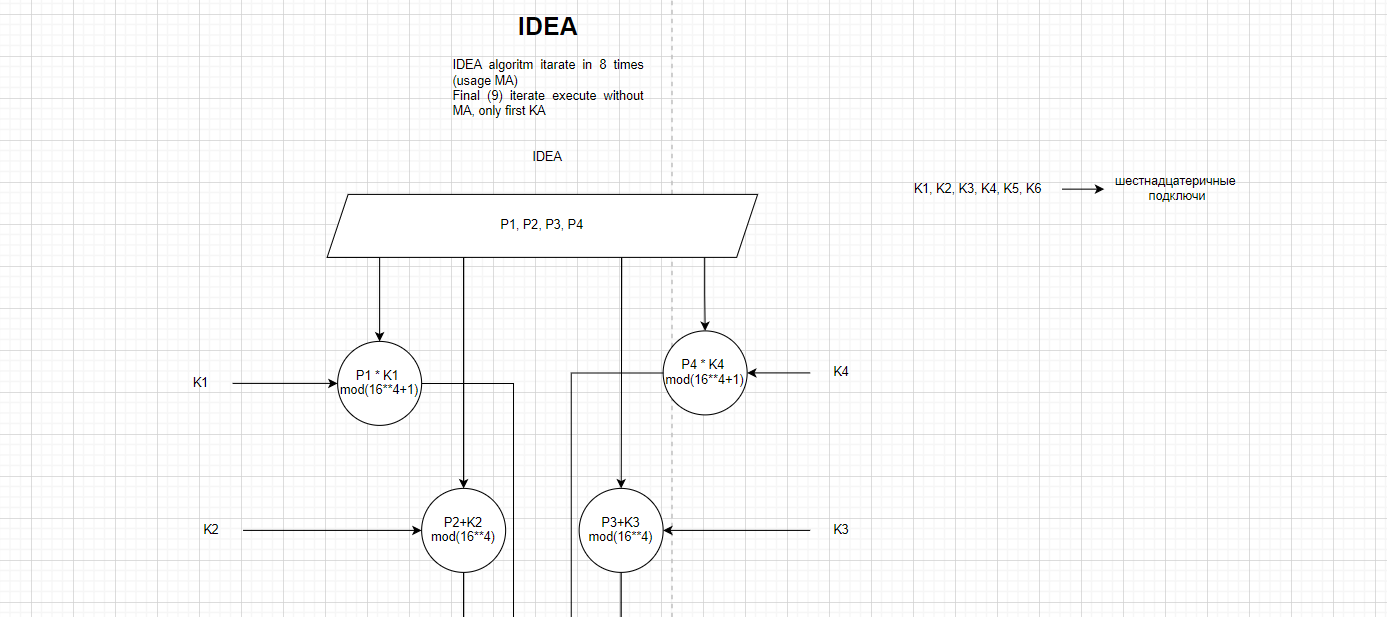
Заключение

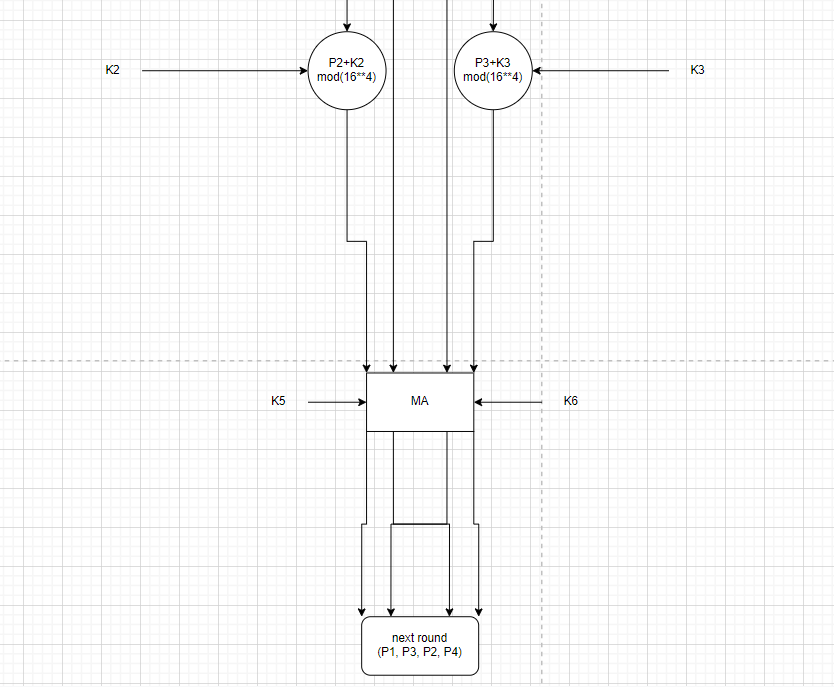
Литература

Приложение 1

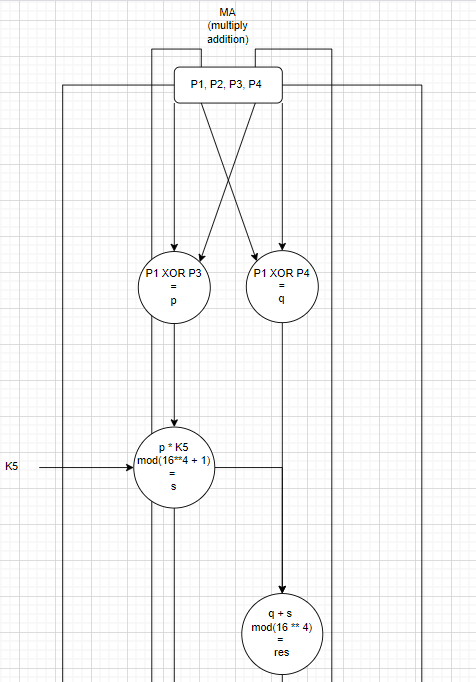
Схемы

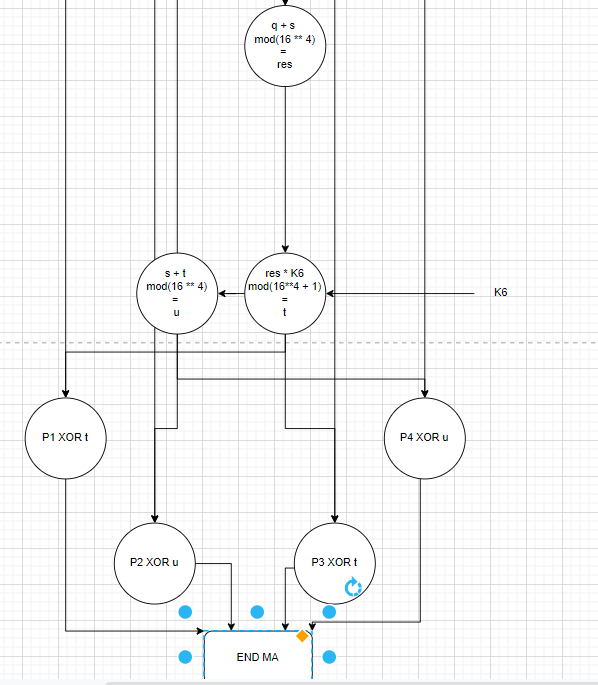
IDEA





Multiply addition





Приложение 2

Код

<https://github.com/Vladislav1809/IDEA_course_work>

(листинг будет реализован в финальном варианте работы)