Семин Владислав ККСО-01-20 КПЗИ лаб. 4 в-21

Предложить вариант криптографической схемы, отвечающей следующим требованиям.

Алгоритм шифрования с любым типом зацепления блоков и проверкой целостности сообщения, с выработкой ключа через функцию, использующую дополнительную память.

Длина ОТ 2211 байтов

Параметры криптографических примитивов:

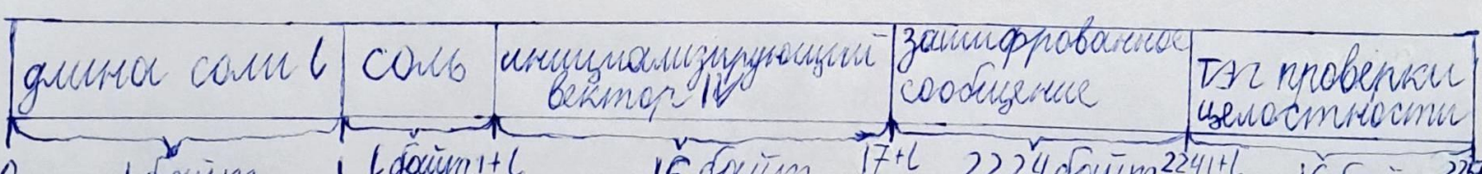
scrypt: степень параллельности $p=1$, размер блока $r=32$, сложность $N=4096$

Согласно открытым источникам минимальные требования по памяти для scrypt $128 \cdot N \cdot r$ байт

В данном случае $128 \cdot 4096 \cdot 32$ байт $= 16$ Мбайт

OMAC: для выработки подключей используется рекомендуемая NIST для шифров с 128-битными блоками константа 0x87

Протокол сообщения:



Что подаётся на вход схеме зашифрования:

соль – последовательность байт произвольной длины менее 256,
инициализирующий вектор IV – последовательность байт длиной 16, парольная фраза,
открытый текст длиной 2211 байт

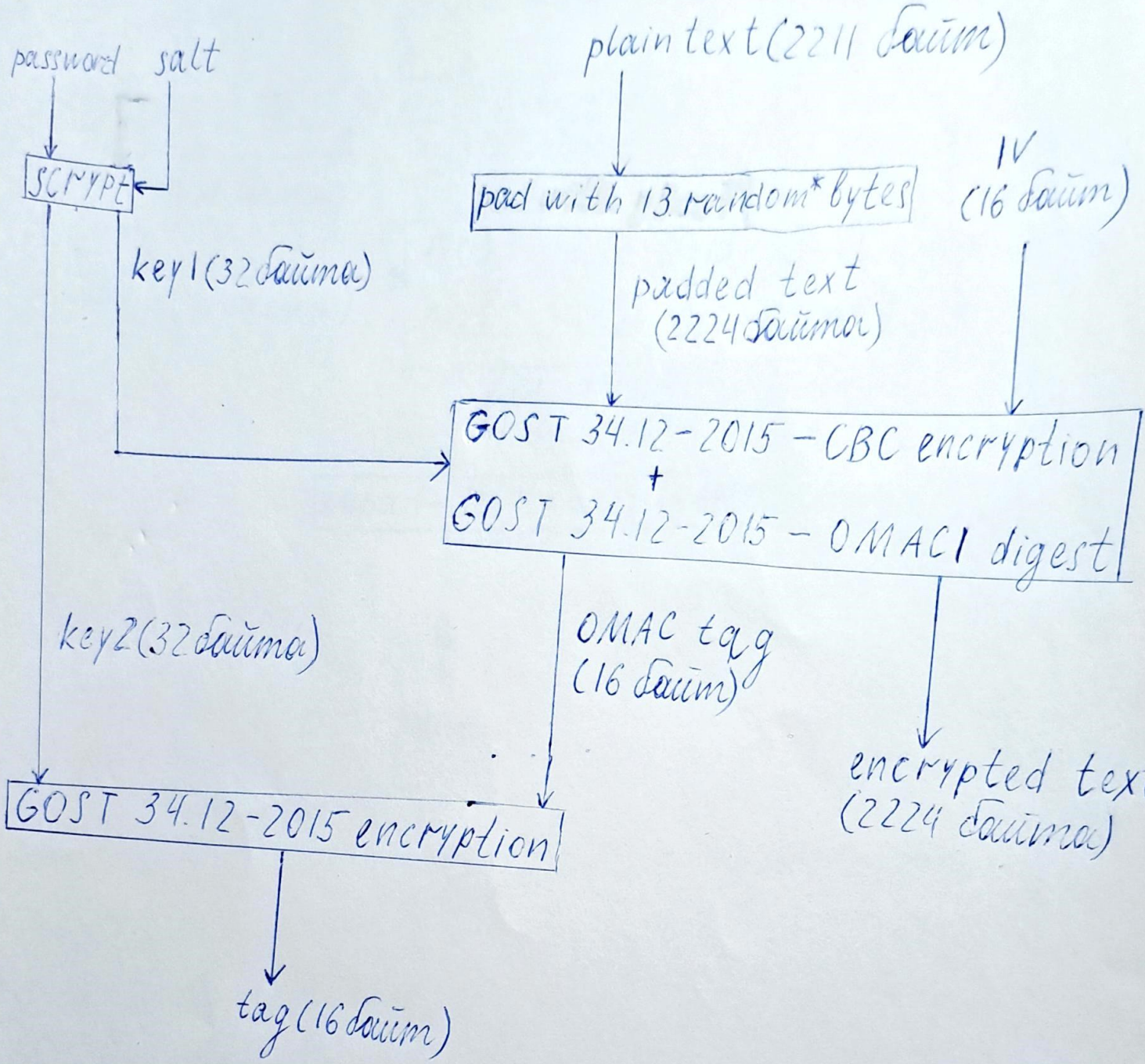
Схема шифрования выдаёт сообщение по вышеописанному протоколу

Схеме дешифрования на вход подаётся сообщение по вышеописанному протоколу и парольная фраза
Возможны три исхода работы схемы дешифрования:

- дешифрованное сообщение
- сообщение о ошибке проверки MAC
- сообщение о ошибке в протоколе принятого сообщения (в случае, если длина сообщения больше или меньше 2257 + L)

Семин Владислав ККСО-01-20 КПЗИ лаб 4 в-21

Схема зашифрования:



*В ISO 10126 используется паддинг случайными байтами, однако последний байт тоже длина паддинга. Так как данная схема предполагает фиксированный размер OT, то предлагается не вписывать в конец размер паддинга, а сделать все байты случайными

Семин Владислав ККСО-01-20 КПЗИ лаб. 4 в-21

Схема дешифрования: