We are here to save the world

Приветствуем вас на нашем хакатоне. Без лишних слов перейдем сразу к делу.

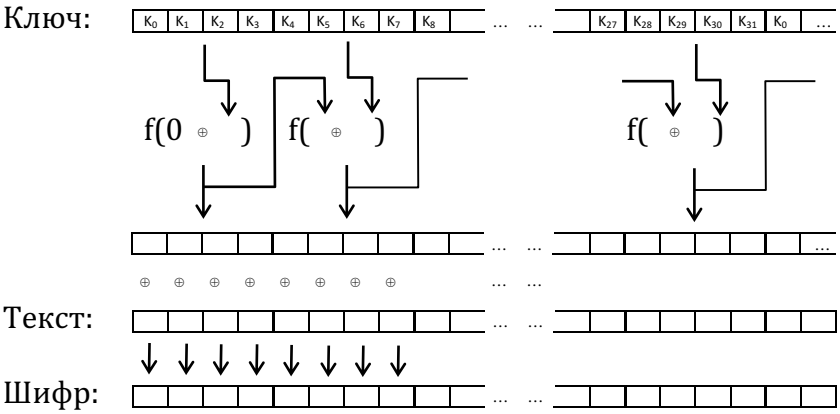
На первом этапе вам необходимо реализовать алгоритм, которым зашифрованы все остальные задания.

Описание алгоритма

Алгоритм параметризуется 256-битным ключом. Ключ разбивается на 8 блоков по 4 байта. Исходный текст также разбивается на блоки по 4 байта, и один раунд алгоритма производится над одним блоком текста и одним блоком ключа.

1) Берется очередной блок ключа как беззнаковое 32-битное число (после 8-го блока берется снова 1-й и так далее).
2) Блок складывается по модулю 2 с результатом работы раунда алгоритма на предыдущем этапе (или 0 в случае, если это первый раунд)
3) Над результатом выполняется функция f(x) = x*134775813+ 1, где все числа – 32-битные беззнаковые.
4) Получившийся результат является результатом работы раунда алгоритма, который будет использован на следующем раунде
5) Этот же результат складывается по модулю 2 с очередным блоком исходного текста, представленным как беззнаковое 32-битное число
6) Результат этого сложения и есть очередные 4 байта зашифрованного текста. Если в последнем блоке текста меньше четырех байт (размер текста не кратен четырем), то лишние байты отбрасываются, таким образом длина зашифрованного текста всегда равна длине исходного текста.
7) Далее происходит переход к следующему раунду

Графически алгоритм можно представить следующим образом:



Алгоритм симметричный, поэтому расшифрование устроено в точности также, как и шифрование (текст и шифр меняются местами: на входе будет шифр, а на выходе – текст).

Сложение по модулю 2 (обозначается как $\oplus$)есть побитовая операция, где над каждой парой бит из двух чисел выполняется следующая бинарная функция:

a	b	$a \oplus b$
0	0	0
0	1	1
1	0	1
1	1	0

Пример

Если зашифровать ASCII-строчку "The power to protect what matters most" (без кавычек), которая в шестнадцатеричном представлении будет следующей последовательностью байт:

54 68 65 20 70 6F 77 65 72 20 74 6F 20 70 72 6F 74 65 63 74 20 77 68 61 74 20 6D 61 74 74 65 72 73 20 6D 6F 73 74

и в качестве ключа использовать ASCII-строчку "Kaspersky Lab" (без кавычек), дополненную до 256 бит нулями, которая в шестнадцатеричном представлении будет следующей последовательностью байт:

4B 61 73 70 65 72 73 6B 79 20 4C 61 62 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00

то в результате получится следующая последовательность байт (в шестнадцатеричном представлении):

2C FA A6 32 E2 3B 9C 19 EA 54 92 84 C3 40 D3 88 04 65 10 36 11 B5 90 7A 82 2E E8 08 BB 56 65 A1 E6 41 5D B3 C2 57

Результат

С помощью этого алгоритма вы сможете расшифровать файл encrypted. Но вам еще нужен ключ, который вы уже видели в этом задании...