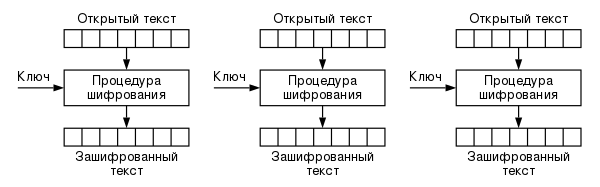
Требуется создать консольное приложение на любом языке, позволяющее защитить файл от шифрования AES в режиме электронной кодовой книги.

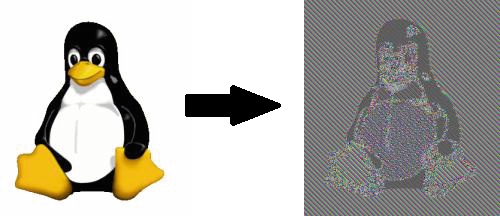
**Режим электронной кодовой книги.**

В этом режиме данные делятся на блоки и каждый блок шифруется независимо от других: Ci=F(Bi, Ki), как представлено на рис.1.



**Защита в режиме электронной кодовой книги.**

В криптографии у режима электронной кодовой книги есть большой недостаток. Идентичные блоки исходного текста превращаются в идентичные блоки зашифрованного текста, таким образом он некорректно скрывает форму данных, как представлено на рис.3.



Первый шаг – расширение данных. Каждый байт данных дополняется нулевыми байтами до получения блока размера n. В случае шифра AES, n=16. Таким образом, файл T размером m байт: T = B0, B1, … Bm, превращается в расширенный файл: eT = B0,0…0, B1,0…0,… Bm,0…0(1),  
где между ненулевыми символами располагается n-1 нулей.  
Дополнительно создается словарь: dic = 0,0…0,1,0…0,…,255,0…0, где между ненулевыми символами располагается n-1 нулей.

Если программа-вымогатель использует один и тот же ключ для шифрования всех файлов, она также шифрует файл словаря. Пользователь может восстановить все файлы путем соотнесения зашифрованных блоков из файлов с зашифрованными блоками из словаря, для которых известно незашифрованное значение.

Если программа-вымогатель использует индивидуальный ключ для каждого файла, то словарь может быть создан в начале каждого файла. Таким образом файл T расширяется в dic+eT: dic+eT=0,0…0,1,0…0,…,255,0…0, B0,0…0, B1,0…0,… Bm,0…0 ,где между ненулевыми символами располагается n-1 нулей.

После чего, основываясь на словаре мы можем однозначно сопоставить любой блок шифртекста с соответствующим ему блоком исходного текста

Соответственно, требуемый функционал. Для первого варианта – словарь располагается отдельно от исходного файла, для второго варианта словарь создаётся в начале файла.  
  
Ключ prepare – расширяет указанный исходный файл с данными и создаёт файл словаря .

Ключ encode – шифрует указанный расширенный файл и файл словаря AES со случайным ключом  
Ключ translate – выводит в отдельный файл таблицу сопоставления блоков шифртекста и блоков исходного текста, основываясь на словаре  
Ключ decode – на основании таблицы сопоставления расшифровывает наш файл с данными, после чего убирает из него расширение и словарь, если это необходимо.