Дан зашифрованы файл и ключ для расшифрования k. С помощью алгоритма пороговой схемы ключ можно разделить на n частей, а для расшифрования файла нужны t частей из n (порог t определяется при разделении ключа k).  
Доказать, что пороговая схема уменьшает вероятность компрометации ключа.