Математический анализ двух шифров Шеннона

АВТОРЫ: д.т.н. Рябко Б.Я.

В 1949 году К. Шеннон опубликовал знаменитую работу «Communication theory of secrecy systems», в которой были заложены основы современной криптографии. В этой работе он описал два простых шифра, представляющих практический интерес, но не дал строгого доказательства их свойств.

Шеннон рассматривал так называемые шифры с бегущим ключом и следующую схему их применения: есть два участника – отправитель и получатель, которые хранят один и тот же текст $K = k1\ k2\ \dots\ kt$, состоящий из t букв (например, книгу). В случае, когда отправителю надо секретно передать получателю некоторое сообщение $Y= y1\ y2\ \dots\ ys\ (s<t)$, он его шифрует (надеясь скрыть его содержание от любопытных). Для этого он сначала заменяет буквы $y1\ y2\ \dots\ ys$ и $k1\ k2\ \dots\ ks$ на целые числа, соответствующие их номерам в алфавите, затем побуквенно складывает: $z1= (x1+k1) \bmod A$, $z2= (x2+k2) \bmod A$,...$zs= (xs+ks) \bmod A$, где A – число букв в алфавите (считаем, что маленькие и большие буквы отождествляются и пробелы удалены, хотя все без труда переносится и на общий случай). Затем отправитель пересылает сообщение $z1\ z2\ \dots\ zs$ получателю, скажем, по почте, где его могут скопировать любопытные. Получатель дешифрирует, то есть проводит обратные вычисления: $u1 = (z1-k1) \bmod A$, $u2 = (z2 - k2) \bmod 2$,...$us = (zs-ks) \bmod A$ и находит исходное сообщение, так как $u1\ \dots\ us = y1\ \dots\ ys$. Оказалось, что этот шифр ненадежен: в случае английского языка любопытные по $z1\ z2\ \dots\ zs$ могут найти исходное сообщение $y1\ y2\ \dots\ ys$ (даже без знания $k1\ k2\ \dots\ ks$!) Отметим, что в этой схеме текст $k1\ k2\ \dots\ ks$ называется “ключ” – key.

Шеннон в своей статье рассмотрел этот шифр и строго показал, почему он ненадежен. Он предложил два естественных и просто реализуемых обобщения, но не провел их математического анализа из-за отсутствия в то время соответствующих методов. В последующие годы эти шифры рассматривались несколькими авторами, но также без строгих доказательств (Hellman M.E. «An extension of the Shannon theory approach to cryptography», 1977).

Важно отметить, что, по очевидным причинам, методы со строго доказанным (математически) уровнем надежности (или «стойкости») представляют для криптографии наибольшую ценность. Кроме того, с появлением компьютеров и Интернета, где хранится гигантское количество общедоступных текстов, предложенные Шенноном методы стали просто реализуемыми и, как следствие, их практическая ценность возросла.

В 2017 году (через 67 лет после публикации Шеннона) задача строгого математического доказательства свойств этих двух шифров была решена в работе [1].

ПУБЛИКАЦИИ:

1. Ryabko B. Properties of two Shannon’s ciphers // Designs, Codes and Cryptography. - 2017. - P.1-7.