Математические и алгоритмические основы безусловно стойких шифров

Фионов Андрей Николаевич
Институт вычислительных технологий СО РАН (Новосибирск), Россия

Большинство шифров, которые сегодня практически используются в системах защиты информации, имеют одну неприятную особенность: их стойкость не доказана математически строго. Точнее говоря, не показано, что для взлома шифра не существует более быстрого алгоритма, чем прямой перебор ключей. Не исключено, что со временем такой алгоритм может быть найден. Но можно ли построить шифр, который невозможно взломать? В докладе будет дан ответ на этот вопрос. Будут представлен обзор методов построения безусловно стойких шифров и условия применимости этих методов.