# О ВЕРОЯТНОСТНОМ ШИФРОВАНИИ

В.А. Молчанов, А.К. Минуситов

В работе рассматриваются криптосистемы на основе вероятностного шифрования. Главная особенность вероятностного шифрования заключается в том, что один и тот же открытый текст, зашифрованный на одном и том же ключе, порождает различные шифротексты.

Первой схемой вероятностного шифрования с открытым ключом является хорошо известный алгоритм Гольдвассера-Микали [1]. В стандартной реализации данного алгоритма при генерации ключей выбираются два случайных числа, удовлетворяющих лишь условию, что они в двоичном представлении имеют одинаковую длину. В нашей работе предлагается выбирать в качестве закрытого ключа пару простых чисел $p, q$, удовлетворяющих условию $p, q \equiv 3 \pmod 4$, чтобы использовать их также в генераторе псевдослучайных чисел BBS [1, с. 524–528.].

Предлагается также введение в зашифрованный текст случайных данных, которые затруднят использование методов выявления статистических закономерностей путем подбора открытых или шифрованных сообщений. Случайные данные генерируются с помощью генератора псевдослучайных чисел BBS, причем выходные данные будут зависеть от $N$-части открытого ключа, чтобы их присутствие в зашифрованном тексте нельзя было выявить.

Была разработана программа, реализующая предлагаемый алгоритм и имеющая пользовательский интерфейс. Программа позволяет сгенерировать пары открытого и закрытого ключей, помещая их в текстовые файлы, шифровать и расшифровывать данные из выбранных пользователем файлов.

**Литература**

1. Мао В. Современная криптография: Теория и практика. М.: Вильямс, 2005. 768 с.