УДК 681.327

А.Г.Ткаченко (6 курс, каф. ПМ), С.В.Стахов, к.ф.-м.н., доц.

МАТЕМАТИЧЕСКОЕ ОПИСАНИЕ И АНАЛИЗ ШИФРА GSM.A5/2

Цель работы — построение математической модели и алгоритма взлома шифра A5/2 в протоколе GSM.

В основу алгоритма взлома шифра A5/2 взят метод, предложенный в работе [1] и описанный на уровне математических идей. Их явная реализация — цель нашей работы.

В ходе теоретических исследований нами построено математическое описание зависимости результата алгоритма шифрования от сеансового ключа, номера кадра и его кода.

При построении и анализе модели шифра получены следующие результаты:

1. Процесс инициализации алгоритма шифрования сеансовым ключом и номером кадра явно выражен линейным обратимым преобразованием.
2. При одном значении сеансового ключа после инициализации разными номерами кадров состояния регистров явно, линейно выражены друг через друга и известную побитную сумму номеров.
3. Значения битов гаммы шифра явно, квадратично выражены через начальные состояния регистров после инициализации.
4. Выведены явные формулы матриц линеаризованных систем уравнений, связывающих ключ с отрезком известной гаммы шифра.
5. Выведены линеаризованные системы уравнений, связывающих ключ с несколькими кадрами шифра. Они используют линейный инвариант кода, корректирующего ошибки в GSM.

На основе математической модели и анализа шифра разработан алгоритм его взлома по нескольким известным открытым кадрам и получены следующие результаты:

1. Реализован алгоритм этой атаки;
2. Рассчитаны данные, позволяющие снизить вычислительную сложность алгоритма на основе предварительных вычислений.

ЛИТЕРАТУРА:

1. Elad Barkan, Eli Biham, Nathan Keller «Instant Ciphertext-Only Cryptanalysis of GSM Encrypted Communication», 2006 г.