УДК 519.63

Криптоанализ алгоритмов шифрования

Харма Укба
Белорусский национальный технический университет

Криптоанализ — Это наука о методах получения исходного значения зашифрованной информации, не имея доступа к секретной информации (ключу), необходимой для этого.

Появление новых криптографических алгоритмов приводит к разработке способов их взлома. Результатом возникновения каждого нового метода криптоанализа является пересмотр оценок безопасности шифров, что в свою очередь влечет за собой необходимость создания более стойких шифров.

Результаты криптоанализа конкретного шифра называют **криптографической атакой** на этот шифр. Успешную криптографическую атаку, дискредитирующую атакуемый шифр, называют **взломом** или **вскрытием** (рис. 1).

В диссертационной работе анализируются 4 основных метода криптоанализа, предполагая знание криптоаналитиком алгоритма шифра:

1. Атака на основе шифротекста.
2. Атака на основе открытых текстов и соответствующих шифротекстов.
3. Атака на основе подобранного открытого текста (возможность выбрать текст для шифрования).
4. Атака на основе адаптивно подобранного открытого текста.

Рис. 1 Атаки криптоанализа

А также проводится анализ дополнительных методов криптоанализа

- атака на основе подобранного шифротекста;
- атака на основе подобранного ключа;
- бандитский криптоанализ.