# **СРСП 14.** Криптоанализ IDEA.

**Форма и содержание отчета**

Отчет должен содержать:

1. Титульный лист установленного образца.
2. Описание комплексного поиск возможных методов доступа.
3. Сравнительный анализ рассмотренных терминалов защищенной информационной системы.
4. Перечень использованных информационных источников.

Отчет выполняется на листах формата А4 рукописным или печатным способом. При рукописном оформлении отчета текст следует излагать четким почерком чернилами черного цвета.

Длина ключа IDEA равна 128 битам - более чем в два раза длиннее ключа DES. При условии, что наиболее эффективным является вскрытие грубой силой, для вскрытия ключа потребуется 2128 (1038) шифрований. Создайте микросхему, которая может проверять миллиард ключей в секунду, объедините миллиард таких микросхем, и вам потребуется 1013 лет для решения проблемы - это больше, чем возраст вселенной. 1024 таких микросхем могут найти ключ за день, но во вселенной не найдется столько атомов кремния, чтобы построить такую машину. Наконец мы чего-то достигли, хотя в некоторых темных вопросах я лучше останусь сторонним наблюдателем.

Может быть вскрытие грубой силой - не лучший способ вскрытия IDEA. Алгоритм все еще слишком нов, чтобы можно было говорить о каких-то конкретных криптографических результатах. Разработчики сделали все возможное, чтобы сделать алгоритм устойчивым к дифференциальному криптоанализу. Они определили понятие марковского шифра и продемонстрировали, что устойчивость к дифференциальному криптоанализу может быть промоделирована и оценена количественно. (Для сравнения с алгоритмом IDEA, устойчивость которого к дифференциальному криптоанализу была усилена. На рис. 1 приведен первоначальный алгоритм PES. Незначительные изменения могут привести к столь большим различиям.) Лай (Lai) утверждал (он привел подтверждение, но не доказательство), что IDEA устойчив к дифференциальному криптоанализ уже после 4 из 8 этапов. Согласно Бихаму, его попытка вскрыть IDEA с помощью криптоанализа со связанными ключами также не увенчалась успехом.

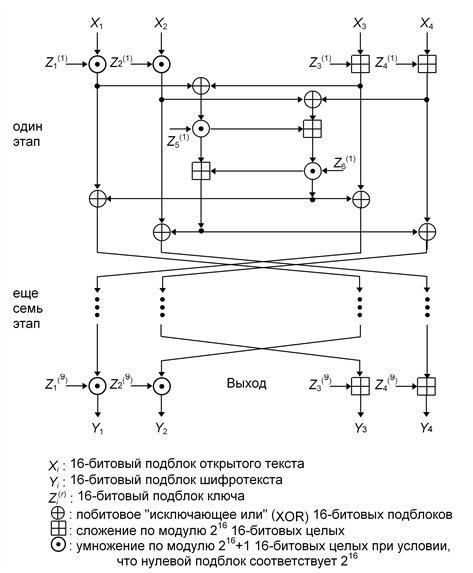


Рис. 1. PES.

Вилли Майер (Willi Meier) исследовал три алгебраических операции IDEA и показал, что, хотя они несовместимы, есть случаи, когда эти операции можно упростить так, чтобы в некоторой степени облегчить. Его вскрытие 2-этапного IDEA оказалось эффективнее вскрытия грубой силой (242 операций), но для IDEA с 3 и более этапами эффективность этого вскрытия была ниже вскрытия грубой силой. Безопасность полного 8-этапного IDEA осталась непоколебимой.

Джоан Дэймен (Joan Daemen) открыла класс слабых ключей IDEA. Эти ключи не являются слабыми в том смысле, в котором слабы некоторые ключи DES, для которых функция шифрования обратна самой себе. Слабость этих ключей состоит в том, что взломщик может легко определить их с помощью вскрытия с выбранным открытым текстом. Например, слабым является следующий ключ (в шестнадцатиричной записи):

0000,0000,0x00,0000,0000,000x,xxxx,x000

В позиции "x" может стоять любая цифра. При использовании такого ключа побитовое XOR определенных пар открытых текстов равно побитовому XOR получившихся пар шифротекстов.

В любом случае вероятность случайной генерации одного из таких слабых ключей очень мала: 1/296. Опасность случайно выбрать такой ключ практически не существует. К тому же, несложно модифицировать IDEA так, чтобы исключить наличие слабых ключей - достаточно выполнить XOR каждого подключа с числом 0x0dae.

Хотя попыток выполнить криптоанализ IDEA было много, мне неизвестно ни об одной успешной.