УДК 004.021(043.2)

Швец А. В., Швец В. В.
Национальный авиационный университет, Киев

ИСПОЛЬЗОВАНИЕ ТАБЛИЧНОГО ПРОЦЕССОРА MS EXCEL В МОДЕЛИРОВАНИИ КРИПТОАЛГОРИТМА DES

DES (*Data Encryption Standard*) — симметричный алгоритм шифрования, разработанный фирмой IBM и утвержденный правительством США в 1977 году как официальный стандарт (FIPS 46-3). DES имеет блоки по 64 бита и 16 цикловую структуру сети Фейстеля, для шифрования использует ключ с длиной 56 бит. Алгоритм использует комбинацию нелинейных (S-блоки) и линейных (перестановки E, IP, IP-1) преобразований. DES является блочным шифром. Входными данными для блочного шифра служат блок размером n бит и k-битный ключ. На выходе, после применения шифрующего преобразования, получается n-битный зашифрованный блок, причём незначительные различия входных данных, как правило, приводят к существенному изменению результата. Блочные шифры реализуются путём многократного применения к блокам исходного текста некоторых базовых преобразований.

Моделирование алгоритма DES позволяет глубже понять его работу. В качестве платформы, в которой можно реализовать модель алгоритма DES очень удобно использовать табличный процессор MS Excel, потому, что он работает с отдельными ячейками и имеет мощную надстройку функций обработки символов, целочисленных данных, преобразований символов в двоичный код. Табличный процессор MS Excel имеет развитую систему меж ячеечных связей и их визуализацию (рис. 1). В предлагаемой реализации алгоритма моделируется все

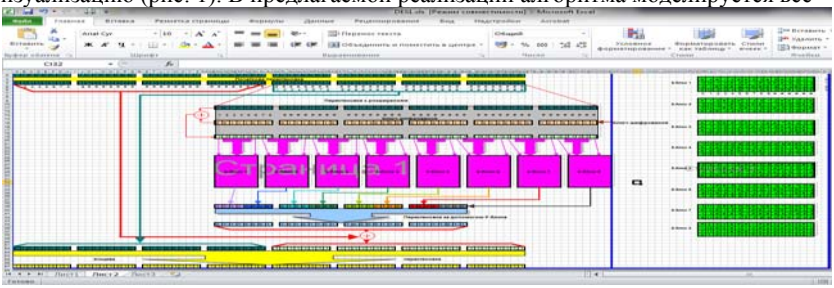

Рис. 1 Модель алгоритма DES

этапы работы одного раунда: перестановки в S и P блоках, работа сети Фейстеля, а также разворачивание и генерирование ключа, получение зашифрованного кода. Данная разработка предлагается, как лабораторная работа по предмету "Криптография и стеганография" для студентов направления 6.170102.

Научный руководитель – Швец В.А., канд. техн. наук, доцент