Алгоритм IDEA

Алгоритм ***IDEA*** (***International Data Encryption Algorithm***) является блочным шифром. Он оперирует 64-битовыми блоками открытого текста. Несомненным достоинством алгоритма IDEA является то, что его ключ имеет длину 128 бит. Один и тот же алгоритм используется и для шифрования, и для дешифрования.

Первая версия алгоритма IDEA была предложена в 1990 г., ее авторы - Х.Лей и Дж.Мэсси. Первоначальное алгоритм назывался ***PES*** (Proposed Encryption Standard). Улучшенный вариант этого алгоритма, разработанный в 1991 г., получил название ***IPES*** (Improved Proposed Encryption Standard). В 1992 г. IPES изменил свое имя на IDEA. Алгоритм IDEA использует при шифровании процессы смешивания и рассеивания, которые легко реализуются аппаратными и программными средствами.

В IDEA используются следующие математические операции:

- поразрядное сложение по модулю 2 (операция "исключающее ИЛИ"); операция обозначается как (+);
- сложение беззнаковых целых по модулю 2^{16}; операция обозначается как [+];
- умножение беззнаковых целых по модулю (2^{16}+1), причем блок из 16 нулей рассматривается как 2^{16}; операция обозначается как (·).

Все операции выполняются над 16-битовыми субблоками.

Эти три операции несовместимы в том смысле, что:

- никакая пара из этих трех операций не удовлетворяет ассоциативному закону, например a[+](b(+)c)#(a[+]b)(+)c;
- никакая пара из этих трех операций не удовлетворяет дистрибутивному закону, например a[+](b(·)c)#(a[+]b)(·)(a[+]c).

Комбинирование этих трех операций обеспечивает комплексное преобразование входных данных, существенно затрудняя крипто-анализ IDEA по сравнению с DES, который базируется исключительно на операции "исключающее ИЛИ".

Общая схема алгоритма IDEA приведена на рис.1. 64-битовый блок данных делится на четыре 16-битовых субблока. Эти четыре субблока становятся входом в первый цикл алгоритма. Всего выполняется восемь циклов. Между циклами второй и третий субблоки меняются местами. В каждом цикле выполняется следующая последовательность операций:

1. (·) - умножение субблока X_1 и первого подключа.
2. [+] - сложение субблока X_2 и второго подключа.
3. [+] - сложение субблока X_3 и третьего подключа.
4. (·) - умножение субблока X_4 и четвертого подключа.
5. (+) - сложение результатов шагов 1 и 3.
6. (+) - сложение результатов шагов 2 и 4.

7. (·) - умножение результата шага 5 и пятого подключа.
8. [+] - сложение результатов шагов 6 и 7.
9. (·) - умножение результата шага 8 и шестого подключа.
10. [+] - сложение результатов шагов 7 и 9.
11. (+) - сложение результатов шагов 1 и 9.
12. (+) - сложение результатов шагов 3 и 9.
13. (+) - сложение результатов шагов 2 и 10.
14. (+) - сложение результатов шагов 4 и 10.

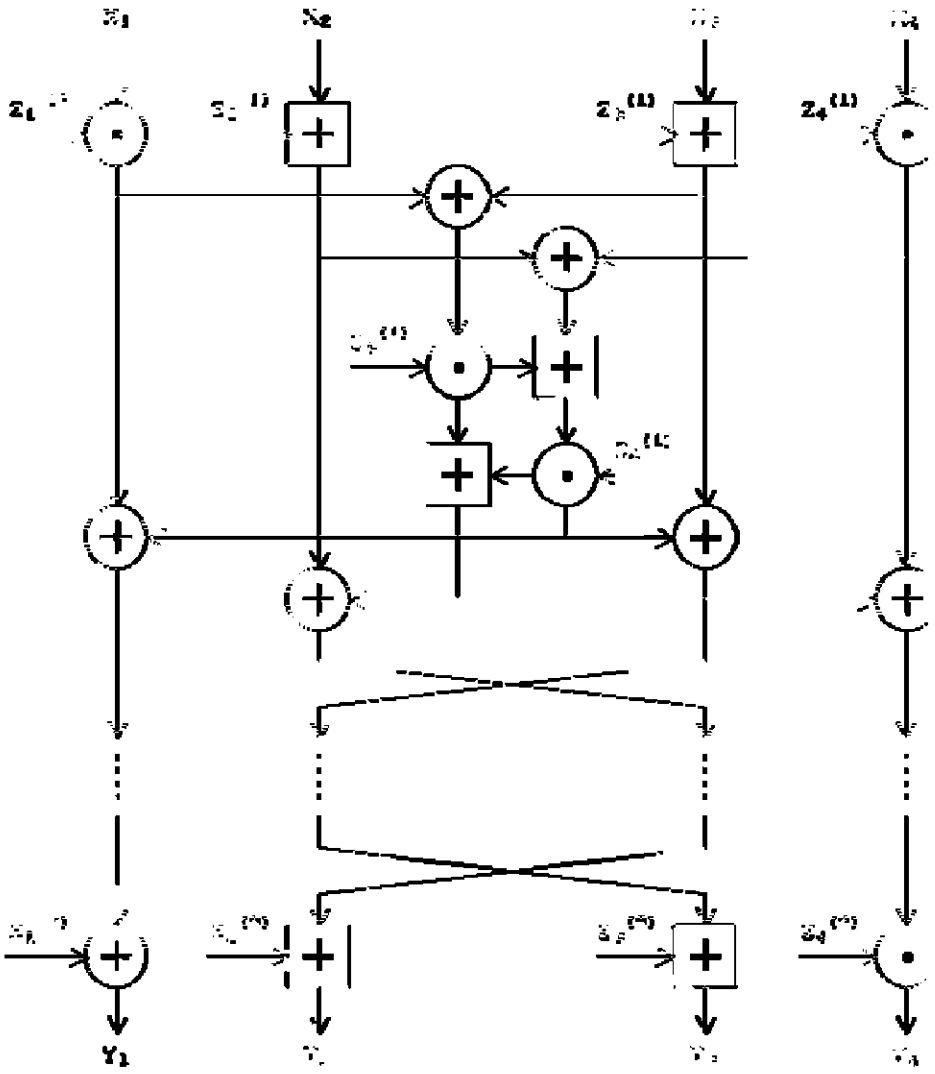

Рис. 1. Схема алгоритма IDEA (режим шифрования)

Выходом цикла являются четыре субблока, которые получаются как результаты выполнения шагов 11, 12, 13 и 14. В завершение цикла второй и третий субблоки меняются местами (за исключением последнего цикла). В результате формируется вход для следующего цикла.

После восьмого цикла осуществляется заключительное преобразование выхода:

1. (·) - умножение субблока X_1 и первого подключа.
2. [+] - сложение субблока X_2 и второго подключа.
3. [+] - сложение субблока X_3 и третьего подключа.

4. (·) - умножение субблока X_4 и четвертого подключа.

Полученные четыре субблока $Y_1,\ldots, Y_4$ объединяют в блок шифртекста.

Создание подключей $Z_1 \ldots Z_6$ также относительно несложно. Алгоритм использует всего 52 подключа (по шесть для каждого из восьми циклов и еще четыре для преобразования выхода). Сначала 128-битовый ключ делится на восемь 16-битовых подключей. Это - первые восемь подключей для алгоритма (шесть подключей - для первого цикла и первые два подключа - для второго). Затем 128-битовый ключ циклически сдвигается влево на 25 бит и снова делится на восемь подключей (четыре подключа - для второго цикла и четыре подключа - для третьего). Ключ снова циклически сдвигается влево на 25 бит для получения следующих восьми подключей и т.д., пока выполнение алгоритма не завершится.

Дешифрование осуществляется аналогичным образом, за исключением того, что порядок использования подключей становится обратным, причем ряд подключей дешифрования являются или аддитивными (-x), или мультипликативными (1/x) обратными величинами подключей шифрования (табл. 1).

Таблица 1

Подключи шифрования и дешифрования алгоритма IDEA

Цикл	Подключи шифрования	Подключи дешифрования
1	Z1(1 Z2(1) Z3(1) Z4(1) Z5(1) Z6(1)	Z1(9)–1 -Z2(9) –Z3(9) Z4(9)–1 Z5(8) Z6(8)
2	Z1(2) Z2(2) Z3(2) Z4(2) Z5(2) Z6(2)	Z1(8)–1 –Z3(8) –Z2(8) Z4(8) –1 Z5(7) Z6(7)
3	Z1(3) Z2(3) Z3(3) Z4(3) Z5(3) Z6(3)	Z1(7)–1 -Z2(7) –Z3(7) Z4(7)–1 Z5(6) Z6(6)
4	Z1(4) Z2(4) Z3(4) Z4(4) Z5(4) Z6(4)	Z1(6)–1 –Z3(6) -Z2(6) Z4(6)–1 Z5(5) Z6(5)
5	Z1(5) Z2(5) Z3(5) Z4(5) Z5(5) Z6(5)	Z1(5)–1 -Z2(5) –Z3(5) Z4(5)–1 Z5(4) Z6(4)
6	Z1(6) Z2(6) Z3(6) Z4(6) Z5(6) Z6(6)	Z1(4)–1 –Z3(4) –Z2(4) Z4(4)–1 Z5(3) Z6(3)
7	Z1(7) Z2(7) Z3(7) Z4(7) Z5(7) Z6(7)	Z1(3)–1 -Z2(3) –Z3(3) Z4(3)–1 Z5(2) Z6(2)
8	Z1(8) Z2(8) Z3(8) Z4(8) Z5(8) Z6(8)	Z1(2)–1 –Z3(2) –Z2(2) Z4(2)–1 Z5(1) Z6(1)
Преобразование выхода	Z1(9) Z2(9) Z3(9) Z4(9)	Z1(1)–1 –Z2(1) –Z3(1) Z4(1) –1

Для реализации алгоритма IDEA было принято соглашение, что мультипликативная обратная величина (1/x) от 0 равна 0.

Алгоритм IDEA обладает рядом преимуществ перед алгоритмом DES. Он зачительно безопаснее алгоритма DES, поскольку 128-битовый ключ алгоритма IDEA вдвое больше ключа DES. Внутренняя структура алгоритма IDEA обеспечивает лучшую устойчивость к ***криптоанализ***у. Существующие программные реализации примерно вдвое быстрее реализаций алгоритма DES. Алгоритм IDEA запатентован в Европе и США.

Литература

1 Тимофеев, А. М. Криптографическая защита информации : учеб.-метод. пособие / А. М. Тимофеев. – Минск : БГУИР, 2020. – 112 с.

2 Тимофеев, А. М. Криптографическая защита информации : пособие / А. М. Тимофеев. – Минск : БГУИР, 2018. – 44 с.

3 Рябко Б. Я. Криптографические методы защиты информации / Б. Я. Рябко, А. Н. Фионов. – М. : Горячая линия-Телеком, 2017. – 230 с.

4 Лапонина, О. Р. Основы сетевой безопасности: криптографические алгоритмы и протоколы взаимодействия / О. Р. Лапонина. – М. : НОУ «Интуит», 2016. – 244 с.

5 Словарь основных терминов по криптологии / сост. Ю. С. Харин [и др.]. – Мн. : БГУ, 2014. – 92 с.

6 Бузов, Г. А. Защита информации ограниченного доступа от утечки по техническим каналам / Г. А. Бузов. – М. : Горячая линия-Телеком, 2017. – 586 с.

7 Введение в теоретико-числовые методы криптографии / М. М. Глухов [и др.]. – Санкт-Петербург : Лань, 2011. – 400 с.

8 Криптографические методы защиты информации. Кн. 4 / под ред. Е. М. Сухарева. – М. : Радиотехника, 2007. – 312 с.

9 Смарт Н. Криптография / Н. Смарт . – М. : Техносфера, 2005. – 528 с.

10 Мао В. Современная криптография : теория и практика / В. Мао. – М. : Вильямс, 2005. – 768 с.

11 Вельшенбах М. Криптография на Си и С++ в действии / М. Вельшенбах. – М. : Триумф, 2004. – 464 с.

12 Левин М. Криптография / М. Левин. – М. : Познавательная книга плюс, 2001. – 320 с.

13 Основы криптографии : учебное пособие для студентов вузов / А. П. Алферов [и др.]. – М. : Гелиос АРВ, 2001. – 480 с.

14 Криптографическая защита информации [Электронный ресурс]. – Режим доступа : https://erud.bsuir.by/?PageID=83978&menuItemID=null&prop_id=21721%3B217. – Дата доступа: 1.09.2021.

15 Деятельность ОАЦ в сфере защиты информации. Техническая и криптографическая защита информации. Лицензирование [Электронный ресурс]. – Режим доступа : https://oac.gov.by/activity/technical-and-cryptographic--information-protection/licensing. – Дата доступа: 1.09.2021.