DES – симетричний, блочний шифр. Тому для початку потрібно сказати що таке блочні шифри.

Блочні шифри влаштовані досить просто. Для початку потрібно встановити вектор ініціалізації та ключ. За допомогою ключа та вектору ініціалізації формується вектор ініціалізації для наступного блоку, тобто виходить лавинний ефект. І при зміненні будь якого символу зміниться й усе, що йде після нього в кінцевому шифротексті.

Як вже було сказано DES – блочний шифр. Його дані шифруються блоками по 64 біти. Алгоритм працює із кожним 64-бітним блоком явного тексту, а в результаті повертає 64-бітний блок шифрограми. Більше того, як для шифруванн, так і для шифрації кожен раз використовується один й той самий алгоритм(за винятком дещо іншої генерації робочих ключів).

Довжина ключа кожен раз однакова – 56 біт(в джерельному варіанті використовується 64-бітний ключ, тому що кожний восьмий біт – біт паритету, вони можуть бути винесені в останній байт ключа). Ключем може бути довільна 64-бітна комбінація, яка може бути змінена в будь-який момент часу. Деякі з цих комбінацій вважаються слабкими ключами, оскільки можуть бути легко визначені. Безпечність алгоритму на пряму залежить від безпечності ключа.

Перейдемо до алгоритму. На вході подаються 64-бітний блок даних, які переставляються згідно з таблицею:

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | 13 | 14 | 15 | 16 |
| 58 | 50 | 42 | 34 | 26 | 18 | 10 | 2 | 60 | 52 | 44 | 36 | 28 | 20 | 12 | 4 |

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 17 | 18 | 19 | 20 | 21 | 22 | 23 | 24 | 25 | 26 | 27 | 28 | 29 | 30 | 31 | 32 |
| 62 | 54 | 46 | 38 | 30 | 22 | 14 | 6 | 64 | 56 | 48 | 40 | 32 | 24 | 16 | 8 |

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 33 | 34 | 35 | 36 | 37 | 38 | 39 | 40 | 41 | 42 | 43 | 44 | 45 | 46 | 47 | 48 |
| 47 | 49 | 41 | 33 | 25 | 17 | 9 | 1 | 59 | 51 | 43 | 35 | 27 | 19 | 11 | 3 |

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 49 | 50 | 51 | 52 | 53 | 54 | 55 | 56 | 57 | 58 | 59 | 60 | 61 | 62 | 63 | 64 |
| 61 | 53 | 45 | 37 | 29 | 21 | 13 | 5 | 63 | 55 | 47 | 39 | 31 | 23 | 15 | 7 |

Далі йде повторюється наступні операції шістнадцять разів.

Функція розширює 32-бітовий вектор до 48-бітового вектору шляхом повторення деяких біт з згідно з таблицею:

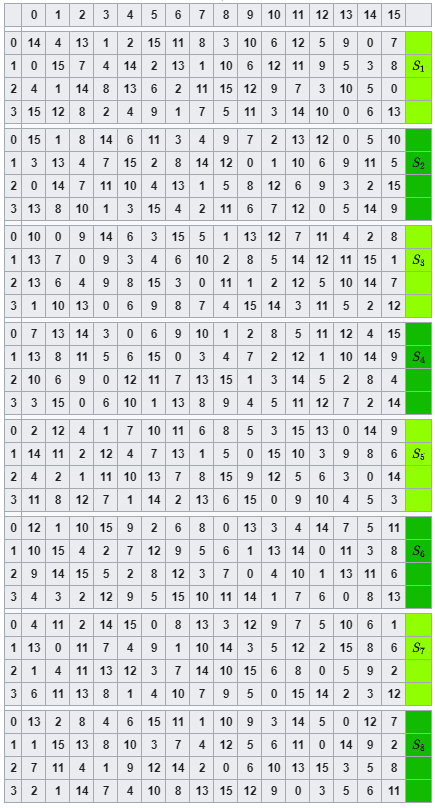
|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| \_ | 1 | 2 | 3 | 4 | \_ | \_ | 5 | 6 | 7 | 8 | \_ | \_ | 9 | 10 | 11 | 12 |
| 32 | 1 | 2 | 3 | 4 | 5 | 4 | 5 | 6 | 7 | 8 | 9 | 8 | 9 | 10 | 11 | 12 |

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| \_ | \_ | 13 | 14 | 15 | 16 | \_ | \_ | 17 | 18 | 19 | 20 | \_ | \_ | 21 | 22 | 23 |
| 13 | 12 | 13 | 14 | 15 | 16 | 17 | 16 | 17 | 18 | 19 | 20 | 21 | 20 | 21 | 22 | 23 |

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 24 | \_ | \_ | 25 | 26 | 27 | 28 | \_ | \_ | 29 | 30 | 31 | 32 | \_ |
| 24 | 25 | 24 | 25 | 26 | 27 | 28 | 29 | 28 | 29 | 30 | 31 | 32 | 1 |

Перший рядок – номера вхідних біт, другий рядок – вхідні біти. Повторення номерів означає повторення біт.

Блок 48 біт -иться з раундовим ключем .



«Розширені» біти використовуються для визначення номера 0-1-2-3 таблиці (ліва колонка).

Далі виконується перестановка.

Перестановка

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | 13 | 14 | 15 | 16 |
| 16 | 7 | 20 | 21 | 29 | 12 | 28 | 17 | 1 | 15 | 23 | 26 | 5 | 18 | 31 | 10 |

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 17 | 18 | 19 | 20 | 21 | 22 | 23 | 24 | 25 | 26 | 27 | 28 | 29 | 30 | 31 | 32 |
| 2 | 8 | 24 | 14 | 32 | 27 | 3 | 9 | 19 | 13 | 30 | 6 | 22 | 11 | 4 | 25 |

За формулою отримуємо значення .

Після 16 раундів перестановка біт виглядає ось так:

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | 13 | 14 | 15 | 16 |
| 40 | 8 | 48 | 16 | 56 | 24 | 64 | 32 | 39 | 7 | 47 | 15 | 55 | 23 | 63 | 31 |

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 17 | 18 | 19 | 20 | 21 | 22 | 23 | 24 | 25 | 26 | 27 | 28 | 29 | 30 | 31 | 32 |
| 38 | 6 | 46 | 14 | 54 | 22 | 62 | 30 | 37 | 5 | 45 | 13 | 53 | 21 | 61 | 29 |

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 33 | 34 | 35 | 36 | 37 | 38 | 39 | 40 | 41 | 42 | 43 | 44 | 45 | 46 | 47 | 48 |
| 36 | 4 | 44 | 12 | 52 | 20 | 60 | 28 | 35 | 3 | 43 | 11 | 51 | 19 | 59 | 27 |

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 49 | 50 | 51 | 52 | 53 | 54 | 55 | 56 | 57 | 58 | 59 | 60 | 61 | 62 | 63 | 64 |
| 34 | 2 | 42 | 10 | 50 | 18 | 58 | 26 | 33 | 1 | 41 | 9 | 49 | 17 | 57 | 25 |

Вхідний біт ставить на місце номер 40, другий номер 8 і.т.д.

В DES використовується 16 циклів вихідними даними для кожного з них є біти відкритого тексту(на вході першого раунду), чи 64 біти результату роботи попереднього раунду(у всіх наступних).

Для роботи алгоритму потрібно згенерувати раундові ключі. Ключі отримують з початкового ключа (один символ ASII 8 байтів 64 біт) наступним чином. Вісім бітів, що знаходяться в позиціях 8, 16, 24, 32, 40, 48, 56, 64 додаються в ключ таким чином, щоб кожен байт містив непарне число одиниць.

Початкова перестановка біт ключа



Ця перестановка визначається двома блоками і по 28 біт кожен. Перші 3 біта є біти 57, 49, 41 розширеного ключа. А перші 3 біта є біти 63, 55, 47 розширеного ключа. Для раундів , отримують з одним або двома лівими циклічними зрушеннями згідно з таблицею:

Циклічний зсув

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| -й раунд | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | 13 | 14 | 15 | 16 |
| Число зсувів | 1 | 1 | 2 | 2 | 2 | 2 | 2 | 2 | 1 | 2 | 2 | 2 | 2 | 2 | 2 | 1 |

Ключ складається з 48 біт, вибраних з бітів вектору (56 біт) згідно з приведеною нижче таблицею. Перший і другий біти є біти 14, 17 вектору .

|  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| -й біт раундового ключа | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 |
| Номери біт 3 векторів | 14 | 17 | 11 | 24 | 1 | 5 | 3 | 28 | 15 |

|  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| -й біт раундового ключа | 10 | 11 | 12 | 13 | 14 | 15 | 16 | 17 | 18 |
| Номери біт 3 векторів | 6 | 21 | 10 | 23 | 19 | 12 | 4 | 26 | 8 |

|  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| -й біт раундового ключа | 19 | 20 | 21 | 22 | 23 | 24 | 25 | 26 | 27 |
| Номери біт 3 векторів | 16 | 7 | 27 | 20 | 13 | 2 | 41 | 52 | 31 |

|  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| -й біт раундового ключа | 28 | 29 | 30 | 31 | 32 | 33 | 34 | 35 | 36 |
| Номери біт 3 векторів | 37 | 47 | 55 | 30 | 40 | 51 | 45 | 33 | 48 |

|  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| -й біт раундового ключа | 37 | 38 | 39 | 40 | 41 | 42 | 43 | 44 | 45 |
| Номери біт 3 векторів | 44 | 49 | 39 | 56 | 34 | 53 | 46 | 42 | 50 |

|  |  |  |  |
| --- | --- | --- | --- |
| -й біт раундового ключа | 46 | 47 | 48 |
| Номери біт 3 векторів | 36 | 29 | 32 |

Біти 1-48 використовують для раундового -у.

В цього алгоритму є недолік. Він нестійкий до «лобової» атаки, тобто ключ можна просто підібрати, бо його розмір лише бітів.