СЛАЙДОВАЯ АТАКА

Алгоритм шифрования на основе сети Фейстеля

Li

Ri

Li+1

Ri+1

P4

К

E/P

S1

S2

F

Таблица перестановки с расширением E/P

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| 4 | 1 | 2 | 3 | 2 | 3 | 4 | 1 |

Значение в ячейке таблицы означает, что в данную позицию становится бит исходной строки с указанным номером.

Исходная 4 битная строка (b1, b2, b3, b4) преобразуется к виду:

(b4, b1, b2, b3, b2, b3, b4. b1).

Таблицы замен

|  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| S1 | 00 | 01 | 10 | 11 |  | S2 | 00 | 01 | 10 | 11 |
| 00 | 01 | 00 | 11 | 10 |  | 00 | 01 | 01 | 10 | 11 |
| 01 | 11 | 10 | 01 | 00 |  | 01 | 10 | 00 | 01 | 11 |
| 10 | 00 | 10 | 01 | 11 |  | 10 | 11 | 00 | 01 | 00 |
| 11 | 11 | 01 | 11 | 01 |  | 11 | 10 | 01 | 00 | 11 |

S-блоки формируют следующим образом: 1 и 4 биты входной последовательности рассматриваются как 2 битные числа, определяющие строку, 2 и 3 определяют столбец преобразования S-блока. Элемент, находящийся на пересечении соответсвующих строки и столбца, является выходом S-блока.

Таблица входов и выходов S-блока.

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Вход | Выход S1 | Выход S2 | Вход | Выход S1 | Выход S2 |
| 0000 | 01 | 01 | 1000 | 00 | 11 |
| 0001 | 11 | 10 | 1001 | 11 | 10 |
| 0010 | 00 | 01 | 1010 | 10 | 00 |
| 0011 | 10 | 00 | 1011 | 01 | 01 |
| 0100 | 11 | 10 | 1100 | 01 | 01 |
| 0101 | 01 | 01 | 1101 | 11 | 00 |
| 0110 | 10 | 11 | 1110 | 11 | 00 |
| 0111 | 00 | 11 | 1111 | 01 | 11 |

Таблица перестановки P4

|  |  |  |  |
| --- | --- | --- | --- |
| 2 | 4 | 3 | 1 |

Идея слайдовой атаки заключается в сопоставлении одного процесса шифрования с другим таким образом, что один из них будет "отставать" от другого на раунд.

Пусть X, Y и X', Y' -- слайдовые пары пара открытый текст -- шифротекст. Для таких пар должно выполнятся условие:

X=F(X') Y=F(Y')

В алгоритмах шифрования на основе сети Фейстеля раундовая функция F преобразует только одну половину текста. Поэтому условие нахождения потенциальной слайдовой пары может быть сформулировано: (X, Y) образует слайдовую пару совместно с (X', Y'), если левые половины тестов X и Y' равны соответственно правым половинам X' и Y.

X\_L=X'\_R, Y'\_L=Y\_R

Для поиска слайдовой пары выбирается:

- маска -- произвольное n/2 битовое значение m (где n -- размер входного блока алгоритма в битах),

- подбирается массив открытых текстов Xi=(m, Xi\_R), которые будут различаться только случайно выбранной правой частью, и массив Xj'=(Xj\_L, m), которые будут различаться только случайно выбранной левой частью.

В качестве слайдовых отбирают пары, для которых выполняется условие:

Yi\_R=Yj'\_L.

Пусть m=1101,

Таблица. Отбор по левой половине входного текста (Xi, Yi)

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Xi, Yi | Исходный текст | | Шифротекст | |
| № | X\_L | X\_R | Y\_L | Y\_R |
| 11 | 1101 | 1010 | 1110 | 0010 |
| 12 | 1101 | 1011 | 0101 | 0011 |
| 13 | 1101 | 1100 | 1000 | 1110 |
| 14 | 1101 | 1101 | 1101 | 1101 |
| 15 | 1101 | 1110 | 0110 | 1010 |
| 16 | 1101 | 1111 | 1100 | 1011 |

Таблица. Отбор по правой половине входного текста (Xj', Yj')

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Xi, Yi | Исходный текст | | Шифротекст | |
| № | X'\_L | X'\_R | Y'\_L | Y'\_R |
| 1 | 0000 | 1101 | 0000 | 1000 |
| 2 | 0001 | 1101 | 0010 | 1000 |
| 3 | 0011 | 1101 | 0011 | 1101 |
| 4 | 0100 | 1101 | 1110 | 0110 |
| 5 | 0101 | 1101 | 1101 | 0101 |
| 6 | 0110 | 1101 | 1010 | 0010 |

Требуется найти ключ алгоритма шифрования.

1. Отобрать из генерированных текстов несколько слайдовых пар. Подойдут пары, для которых выполняется условие Yi\_R=Yj'\_L.

Отобранные слайдовые пары

|  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| № | X\_L | X\_R | Y\_L | Y\_R |  | № | X'\_L | X'\_R | Y'\_L | Y'\_R |
| 2 | 1101 | 1011 | 0101 | 0011 |  | 3 | 0011 | 1101 | 0011 | 1101 |
| 3 | 1101 | 1100 | 1000 | 1110 |  | 4 | 0100 | 1101 | 1110 | 0110 |
| 5 | 1101 | 1110 | 0110 | 1010 |  | 6 | 0110 | 1101 | 1010 | 0010 |

2. Провести анализ первых раундов для первой слайдовой пары.

Рассмотрим 1-ю пару (2 и 3). Сопоставим процессы шифрования первых раундов для элементов слайдовой пары X=F(X')

X'\_L=0011

X'\_R =1101

X\_L=1101

X\_R =1011

F

К

Рис. 2 Сопоставление первых раундов первой слайдовой пары.

3. Получить значение на выходе функции F.

Т.к. XOR обратная сама по себе, тогда

F(X'\_R)= X'\_L XOR X\_R= 0011 XOR 1011=**1000**

Применить обратное преобразование по таблице P4

Прямое преобразование 2431

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Вход | b1 | b2 | b3 | b4 |
| Преобразование | 2 | 4 | 3 | 1 |
| Выход | b2 | b4 | b3 | b1 |

Обратное преобразование 4132

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Вход | b2 | b4 | b3 | b1 |
| Преобразование | 4 | 1 | 3 | 2 |
| Выход | b1 | b2 | b3 | b4 |
|  |  |  |  |  |
| Вход | 1 | 0 | 0 | 0 |
| **Выход** | **0** | **1** | **0** | **0** |

Таким образом, результат преобразования P4-1 0100.

Следовательно, при шифровании на блок перестановки поступило значение 0100.

Тогда из блока S1 поступило значение 01, а из блока S2 поступило значение 00.

4. Установить возможные входы блока S1, дающие выход 01. Из таблицы входов и выходов S-блоков находим все возможные входы: 0000, 0101, 1011, 1100, 1111. Эти значения при шифровании могли быть получены в результате наложения первой части ключа К1.

5. Установить возможные входы блока S2, дающие выход 00. Из таблицы входов и выходов S-блоков находим все возможные входы: 0011, 1010, 1101, 1110. Эти значения при шифровании могли быть получены в результате наложения второй части ключа К2.

6. Получить значение входа функции F. Согласно рис.2 вход функции F равен значению X'\_R =1101.

7. Получить результат первого преобразования раундовой функции перестановки с расширением E/P.

Согласно таблице перестановки результат E/P для входа 1101 равен 11101011. При шифровании это значение было сложено побитно по модулю 2 с ключом К=(К1, К2).

Таким образом на вход блока S1 подано значение 1110 XOR К1;

на вход блока S2 подано значение 1011 XOR К2;

Зная возможные значения входов S1 и S2 можно получить все возможные значения ключа К1 и К2.

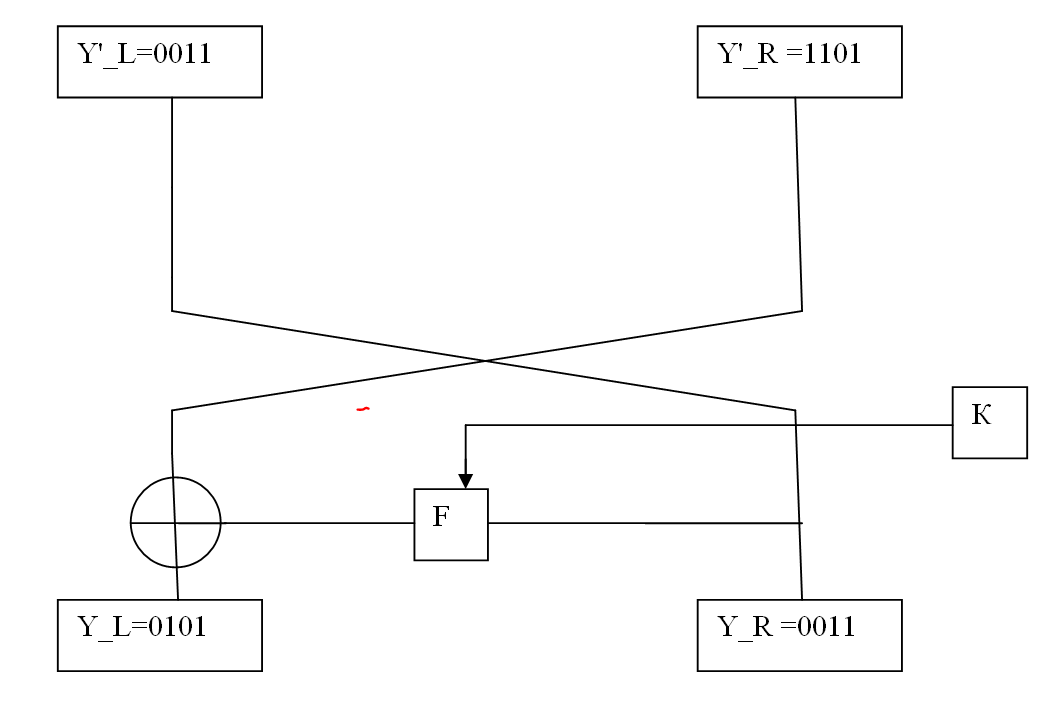
8. Получить возможные значения ключа К1 и К2. Для каждого значения, определенного как вход S1 блока, следует провести побитную XOR операцию со значением 1110, что даст возможные значения К1.

Для каждого значения, определенного как вход S2 блока, следует провести побитную XOR операцию со значением 1011, что даст возможные значения К2.

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Вход S1 | | К1 | Вход S2 | | К2 |
| 0000 | XOR 1110 | =1110 | 0011 | XOR 1011 | =1000 |
| 0101 | XOR 1110 | =1011 | 1010 | XOR 1011 | =0001 |
| 1011 | XOR 1110 | =0101 | 1101 | XOR 1011 | =0110 |
| 1100 | XOR 1110 | =0010 | 1110 | XOR 1011 | =0101 |
| 1111 | XOR 1110 | =0001 |  | | |

9. Провести анализ последних раундов шифрования для первой отобранной слайдовой пары (2,3).

Сопоставить процессы шифрования первых раундов для элементов слайдовой пары Y=F(Y') (рис. 2).



10. Зная значения Y\_L и Y'\_R можно вычислить значение выхода F функции -- 1000. Анализ этого значения аналогичен проведенному выше.

Все возможные входы S1: 0000, 0101, 1011, 1100, 1111.

Все возможные входы S2: 0011, 1010, 1101, 1110.

11. Значение Y'\_L определяет значение входа F функции 0011. Согласно таблице перестановки результат E/P для входа 0011 равен 10010110.

Таким образом на вход блока S1 подано значение 1001 XOR К1;

на вход блока S2 подано значение 0110 XOR К2.

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Вход S1 | | К1 | Вход S2 | | К2 |
| 0000 | XOR 1001 | =1001 | 0011 | XOR 0110 | =0101 |
| 0101 | XOR 1001 | =1100 | 1010 | XOR 0110 | =1100 |
| 1011 | XOR 1001 | =0010 | 1101 | XOR 0110 | =1011 |
| 1100 | XOR 1001 | =0101 | 1110 | XOR 0110 | =1000 |
| 1111 | XOR 1001 | =0111 |  | | |

12. Сравнить возможные значения подключей К1 и К2, полученные в ходе анализа первой слайдовой пары:

|  |  |  |  |
| --- | --- | --- | --- |
| К1 | | К2 | |
| Первые раунды | Последние раунды | Первые раунды | Последние раунды |
| 1110 | 1001 | 1000 | 0101 |
| 1011 | 1100 | 0001 | 1100 |
| 0101 | 0010 | 0110 | 1011 |
| 0010 | 0101 | 0101 | 1000 |
| 0001 | 0111 |  |  |

Полученные совпадения (выделены серым) сужают возможные варианты ключей К1 и К2.

К1 может принимать два значения 0101 и 0010, К2 1000 и 0101.

Всего имеет 2\*2=4 варианта ключей.

Для дальнейшего уменьшения вариантов ключей необходимо проанализировать оставшиеся слайдовые пары.

Если при анализе не найдено совпадений между вариантами значений К1 или К2, полученных при анализе первых и последних раундов, значит отобранная пара не является слайдовой, ее следует исключить из рассмотренных и перейти к анализу следующей.