**Лекция 10. Дифференциальный криптоанализ. Дифференциальный криптоанализ**

 **DES.**

**Дифференциальный криптоанализ.**

 При анализе предполагается, что на каждом цикле используется свой подключ шифрования.ДКА может использовать как выбранные, так и известные открытые тексты . Успех таких попыток вскрытия r-циклического шифра зависит от существования дифференциалов (r-1)-го цикла, которые имеют большую вероятность. Дифференциал i-го цикла определяется как пара ( a , b) i такая, что пара различных открытых текстов x, x\* c разностью a может привести к паре выходных текстов y, y\* после i-ого цикла, имеющих разность b (для соответствующего понятия разности ). Вероятность i-циклового дифференциала (a ,b )i - это условная вероятность P(D y(i)=b | D x= a ) того, что разность D y(i) пары шифротекстов( y, y\*) после i-ого цикла равна b при условии, что пара текстов (x, x\*) имеет разность D x=a ; открытый текст x и подключи циклов к(1) , к(2) ,...., к(i) независимыми и равновероятными. Основная процедура ДКА r-циклического шифра
**с использованием выбранных открытых текстов может быть следующей :**

**1.** На этапе предвычислений ищем множество (r-1)-цикловых дифференциалов (a 1,b 1) r-1, (a 2,b 2) r-1 ,.... (a s,b s)r-1 . Упорядочиваем это множество дифференциалов по величине их вероятности.

**2**. Выбираем открытый текст x произвольным образом и вычисляем x\* так, чтобы разность между x и x\* была равна a 1. Тексты x и x\* шифруется на подлинном ключе и после r циклов получаем пару шифртекстов y(r) , y\*(r). Предполагаем, что на выходе предпоследнего (r-1)-ого цикла разность шифртекстов равна наиболее вероятной: D y(r-1)=b 1. Для тройки (D y(r-1), y(r) , y\*(r)) находим каждое возможное (если их несколько) значение подключа последнего цикла к(r). Добавляем его к количеству появлений каждого такого значения подключа к(r).

**3**. Повторяем п.2 до тех пор, пока одно или несколько значений под ключа к(r) не станет появляться чаще других. Берем этот под ключ или множество таких под ключей в качестве криптографического решения для под ключа к(r).

**4**. Повторяем пп.1-3 для предпоследнего цикла, при этом значения y(r-1) вычисляются расшифрованием шифртекстов на найденном под ключе последнего цикла к(r). Далее действуем аналогично, пока не будут раскрыты ключи всех циклов шифрования.

Предложенный впервые для анализа конкретного шифра, ДКА оказался применимым для анализа широкого класса марковских шифров. Марковским называется шифр, у которого уравнение шифрования на одном цикле удовлетворяет условию: вероятность дифференциала не зависит от выбора открытых текстов. Тогда, если подключи циклов независимы, то последовательность разностей после каждого цикла образует марковскую цепь, где последующее состояние определяется только предыдущим. Примерами марковских шифров являютс DES и FEAL . Можно показать, что марковский r-цикловый шифр с независимыми подключами является уязвимым для ДКА тогда и только тогда, когда для одного цикла шифрования ключ по известной тройке (y,y\*,D x) может быть легко вычислен, и существует (r-1)-цикловый дифференциал (a ,b )к-1 такой, что его вероятность удовлетворяет условию

P(D y(r-1)=b | D x=a )>>2-n ,

где n-количество бит в блоке шифруемого текста.

Сложность раскрытия ключа r-циклического шифра Q(r) определяется как число используемых шифрований с последующим вычислением ключа:

Q(r)- 2/ (Pmax - 1/(2n-1)),

где Pmax=max(a )max(b )(P(D y(r-1)=b | D x=a )). В частности, если Pmax ё 1/(2n-1), то атака не будет успешной. Поскольку вычисление под ключа - более трудоемкая операция, чем шифрование, то единицей измерения сложности является сложность нахождения возможных подключей одного цикла по известным (D y(r-1),y(r),y\*(r)).

Отличительной чертой дифференциального анализа является то, что он практически не использует алгебраические свойства шифра (линейность, аффинность, транзитивность, замкнутость и т.п.), а основан лишь на неравномерности распределения вероятности дифференциалов.