**МИНИСТЕРСТВО ОБРАЗОВАНИЯ РЕСПУБЛИКИ БЕЛАРУСЬ**

**БЕЛОРУССКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ**

**Факультет прикладной математики и информатики**

**ВИКТОР ИВАНОВИЧ ГРАСЬКОВ**

**Лабораторная работа №3**

Отчет по лабораторной работе № 3

вариант 1

(“Методы криптографии”)

студента 2-го курса 13-ой группы

|  |
| --- |
| **Преподаватель** |
| **Ярошеня Ю.С.** |

2020 год

Криптосистема Des

Рассмотрим результаты, полученные с помощью проведения тестов NIST

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
|  | Сценарий 1 | Сценарий 2 | Сценарий 3 | Сценарий 4 | Сценарий 5 | Сценарий 6 |
| Тест 1 | + | - | + | + | + | + |
| Тест 2 | + | + | + | + | + | + |
| Тест 3 | + | + | - | + | + | + |
| Тест 4 | + | + | + | + | + | + |
| Тест 5 | + | + | + | + | + | + |
| Тест 6 | + | + | + | + | + | + |
| Тест 7 | + | + | - | + | + | + |
| Тест 8 | + | - | - | - | - | - |
| Тест 9 | + | + | - | + | + | + |
| Тест 10 | + | + | + | + | - | + |

|  |  |
| --- | --- |
| Тест 1 | FREQUENCY MONOBITS TEST |
| Тест 2 | BINARY MATRIX RANK TEST |
| Тест 3 | CUMULATIVE SUMS TEST |
| Тест 4 | FREQUENCY MONOBITS TEST |
| Тест 5 | LINEAR COMPLEXITY TEST |
| Тест 6 | LONGEST RUN OF ONES TEST |
| Тест 7 | MAURER'S UNIVERSAL STATISTICAL TEST |
| Тест 8 | RANDOM EXCURSION TEST |
| Тест 9 | RUNS TEST |
| Тест 10 | SERIAL TEST |

Сценарии:

1. Исследование вероятностных свойств выходной последовательности режима простой замены при произвольном выборе открытого текста и ключа
2. Исследование вероятностных свойств выходной последовательности режима простой замены при специальном выборе открытого текста и ключа.
3. Исследование размножения ошибки при изменении ключа в режиме простой замены.
4. Исследование размножения ошибки при изменении открытого текста в режиме простой замены.
5. Исследование корреляции открытого текста и зашифрованного текста в режиме простой замены.
6. Исследование вероятностных свойств выходной последовательности в режиме цепочной обработки.

**Итого: 50/60 пройдено, что составляет 83,(3)%**

Можно сделать вывод, что у криптосистемы есть некоторые трудности с прохождением теста на произвольные отклонения (Random Excursions Test). Этот тест подсчитывает число циклов, имеющих строго k посещений при произвольном обходе кумулятивной суммы. Произвольный обход кумулятивной суммы начинается с частичных сумм после последовательности (0,1), переведённой в соответствующую последовательность (-1, +1). Цикл произвольного обхода состоит из серии шагов единичной длины, совершаемых в случайном порядке. Кроме того, такой обход начинается и заканчивается на одном и том же элементе. Цель данного теста – определить, отличается ли число посещений определённого состояния внутри цикла от аналогичного числа в случае абсолютно случайной входной последовательности. Фактически данный тест есть набор, состоящий из восьми тестов, проводимых для каждого из восьми состояний цикла: -4, -3, -2, -1 и +1, +2, +3, +4.

Статистикой теста является мера согласованности наблюдаемого количества визитов при случайном блуждании с заданным состоянием в середине цикла, в сравнении с тем, что ожидается теоретически

С помощью этого теста определяется отклонение от теоретического закона распределения визитов в конкретное состояние при случайном блуждании

На мой взгляд на данный момент шифр уже неплохо так устарел и не соответствует требованиям современных норм безопасности. При этом всем поведение шифра за столько лет криптоанализа достаточно хорошо изучено. Известны его уязвимости и сильные стороны. Шифр дал начало целом направления криптоанализа такие как:

Линейный криптоанализ – анализ зависимостей между открытым текстом и шифротекстом.

Дифференциальный криптоанализ – анализ зависимостей между соотношениями двух или более открытых текстов и соответствующих им шифротекстов.

Криптоанализ на связанных ключах – поиск и анализ зависимостей между шифротекстами, полученными на искомом ключе и ключах, связанных предполагаемым соотношением с искомым ключом

Des удовлетворяет лавинному критерию, если при изменении одного бита на входе алгоритма изменяется в среднем половина битов на выходе алгоритма. Если же при изменении одного бита на входе каждый бит на выходе изменяется с вероятностью ½, то криптоалгоритм удовлетворяет строгому лавинному критерию. В DES лавинный эффект проявляется уже на 4-5 раунде. Так, если зашифровать на одном ключе с помощью DES, 2 блока открытого текста, отличающиеся одним битом, то блоки шифротекстов будут отличаться на 29 бит, т.е. изменение открытого текста на 1,5% вызывает 45% изменений шифротекста.

DES стойко выдержал 20 лет массового всемирного криптоанализа – десятилетия криптоанализа не привели к обнаружению серьезных уязвимостей в алгоритме. При этом существуют различные атаки, основанные не на переборе ключей, но для их проведения необходимо иметь дополнительные данные, например, 2^47 пар открытых текстов и шифротекстов. Что является сложной задачей на практике, и самый эффективным способом и по сегодняшний день остается полный перебор. Проблемой для des стало то, что технический прогресс развился до такой степени, что компьютер за вполне приличное время теперь способен сделать даже полный перебор всех его ключей, а с помощью различных алгоритмов его возможно уменьшить еще на несколько порядков.

Самая серьезная проблема DES –размер ключа (56 битов). Чтобы предпринять атаку грубой силы, надо проверить 2^56 ключей. Если проверять 6 10 ключей/сек., то потребуется 2000 лет, чтобы выполнить атаку грубой силы на DES на одном процессоре. Если сделать компьютер с миллионом крипточипов, то все множество ключей проверится за 20 часов. Когда был введен DES, стоимость такого компьютера была немного более миллиона долларов, но она быстро снизилась. Такой специальный компьютер был создан в 1998 году и нашел ключ за 56 часов. А с помощью компьютерных сетей можно моделировать параллельный поиск ключей, что также ускоряет вскрытие.

Однако это нельзя назвать приговором для des, так как на данный момент существует его модернизированный вариант triple des, в котором как следует из названия des применяется трижды, что обеспечивает длину ключа, недоступную для перебора на современных устройствах, что тем самым дарует des вторую жизнь.

DES был национальным стандартом США в 1977—1980 гг., но в настоящее время DES используется (с ключом длины 56 бит) только для устаревших систем, чаще всего используют его более криптоустойчивый вид (3DES, DESX). 3DES является простой эффективной заменой DES, и сейчас он рассмотрен как стандарт. В ближайшее время планируется замена DES и Triple DES алгоритмом AES, однако это очень дорогое удовольствие, учитывая что в некоторых системах des имеет поддержку на физическом уровне, и с большой уверенностью можно сказать,что des будет однозначно жив до тех пор, пока живы подобные системы. Алгоритм DES широко применяется для защиты финансовой информации: так, модуль THALES (Racal) HSM RG7000 полностью поддерживает операции TripleDES для эмиссии и обработки кредитных карт VISA, EuroPay и прочие. Канальные шифраторы THALES (Racal) DataDryptor 2000 используют TripleDES для прозрачного шифрования потоков информации. Также алгоритм DES используется во многих других устройствах и решениях THALES-eSECURITY.