**Лабораторная работа №3**

**«Изучение математических методов анализа стойкости парольных систем»**

    Учебные и воспитательные цели:

    1.Рассмотреть принципы использования математических методов при анализе стойкости парольных систем.

    2. Изучить обобщенный алгоритм подбора пароля.

Вступительная часть  
     В практических задачах защиты информации большое внимание уделяется парольной защите информационных ресурсов. Все современные операционные системы и многие прикладные программы имеют гибкие и мощные механизмы осуществления парольной защиты. Любая парольная система защиты является в определенной степени уязвимой. Оценить стойкость парольных систем, указать на необходимые требования по повышению ее защищенности – достаточно сложная задача, не всегда имеющая строгое математическое решение.

**Принципы использования математических методов при анализе стойкости парольных систем**

    Стойкость парольной системы оценивается для того, чтобы сделать вывод о возможности и целесообразности ее взлома, так как время взлома может быть настолько велико, что знание парольной информации может потерять ценность.  
    Известно, что основными методами взлома паролей являются:

* метод атаки по словарю (перебираются пароли, являющиеся осмысленными комбинациями символов или наиболее распространенные парольные комбинации);
* гибридные атаки (перебираются пароли из словаря, но некоторым образом дополненные). Так, например, гибридная атака может проверять не только пароли из словаря, но и их объединения, слова из словаря, записанные в транслитеративной форме, пароли, полученные из паролей словаря изменением символов;
* метод полного перебора (генерируются все возможные комбинации символов некоторого алфавита и подставляются в качестве паролей).

    Основными объектами исследования являются пароли – комбинации определенных символов. Поскольку наибольший интерес представляет метод полного перебора, так как он дает гарантированный успех, то в основном задачи определения стойкости паролей сводятся к комбинаторным задачам. В связи с этим целесообразно привести основные формулы комбинаторики.

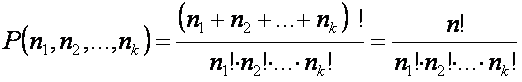
**Применение формул комбинаторики для анализа стойкости парольных систем**

***Перестановки без повторений***

     Пусть имеется множество М, состоящее из n элементов любой природы. Если упорядочить это множество, пронумеровав некоторым образом его элементы, то получим кортеж длины n с попарно различными элементами, который называют - *перестановкой из n  элементов*.  
***Определение****.* Всякое упорядоченное n-элементное множество называется перестановкой из n элементов.  
***Теорема.*** Число всех перестановок из n элементов равно произведению последовательных натуральных чисел от 1 до n включительно, то есть                                 
*Pn=1\*2\*3\*…\*n=n!*

***Перестановки с повторениями***

    Пусть α – кортеж длины n, составленный из элементов m-множества X. Перенумеруем элементы множества *X: X={x1,x2,…,xm}.* Тогда каждому числу k, где *1≤k≤m*, соответствует число *nk*, показывающее сколько раз элемент xk встречается среди компонент кортежа α. Выписывая по порядку эти числа, получаем новый кортеж *(n1,…,m)*, который и называют составом кортежа α. Два кортежа, имеющие один и тот же состав, могут отличаться друг от друга порядком компонент. Их называют перестановками с повторениями данного состава.  
***Определение.*** Перестановками с повторениями из элементов *a,b,…,r* , в которой эти элементы повторяются соответственно *n1,n2,..,nk* раз, называется кортеж длины *n=n1+n2+..+nk*, среди компонент которого a встречается n1 раз, *b – n2* раз и так далее, *r – nk* раз.  
Обозначим число перестановок с повторениями символом*P(* *n1+n2+..+nk*)  
***Теорема****.* Число различных перестановок с повторениями из элементов a,b,…,r , в которых эти элементы повторяются соответственно *n1+n2+..+nk* раз, определяется по формуле:

.

***Размещения без повторений***

    Множество вместе с заданным порядком расположения его элементов называют упорядоченным множеством. Рассмотрим комбинаторную задачу, связанную с выбором упорядоченных подмножеств некоторого конечного множества. Общая формулировка этой задачи такова: имеется множество, состоящее из n элементов. Сколько можно составить упорядоченных подмножеств, содержащих k его элементов?  
Для решения этой задачи необходимо узнать число различных размещений из n элементов по k элементов.  
***Определение****.*Всякое упорядоченное k-элементное подмножество n­элементного множества при k*≤*n называется размещением из n элементов по k.    
Как следует из определения, два размещения считаются различными, если они отличаются друг от друга хотя бы одним элементом или состоят из одних и тех же элементов, но расположенных в разном порядке. Число таких размещений из n элементов по k элементов обозначают символом.Akn   
***Теорема.*** Число различных размещений из n элементов по k равно произведению k последовательных натуральных чисел, наибольшим из которых является n, то есть

Akn  = *n·(n-1)\*(n-2)\*…\*(n-k+1)* или Akn=http://stavkombez.ru/method/TOKB/index.files/lab/lab_3_clip_image008.gif.

***Размещения с повторениями***

    Пусть имеем множество, состоящее из n элементов любой природы. Кортеж длины k, составленный из n элементов этого множества, называется размещением с повторениями. Здесь необязательно  n*≤*k.  
***Определение****.*Кортеж длины k, составленный из n-элементного множества, называется размещением с повторениями из n элементов по k. Число всевозможных размещением с повторениями из n элементов по k обозначают символом http://stavkombez.ru/method/TOKB/index.files/lab/lab_3_clip_image010.gif.  
***Теорема.*** Число различных размещений с повторениями из n элементов по k определяется по формуле:

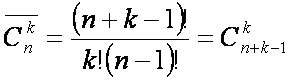
http://stavkombez.ru/method/TOKB/index.files/lab/lab_3_clip_image012.gif- Сочетания без повторений

    При составлении k-элементных подмножеств n-элементного множества нас не всегда интересует порядок, в котором располагаются элементы. В таком случае речь идет о подмножествах, не являющихся упорядоченными.  
***Определение****.* Всякое k-элементное подмножество n-элементного множества при k*≤*n называется сочетанием из n элементов по k.  
     Другими словами, сочетания из n элементов по k в каждом называются такие соединения, из которых каждое содержит k элементов, взятых из числа данных n элементов, и которые отличаются друг от друга по крайней мере одним элементом. Порядок элементов в сочетании значения не имеет. Число различных сочетаний из n элементов по k обозначаются символом Ckn .  
***Теорема.*** Число сочетаний из n элементов по k определяется по формуле:

http://stavkombez.ru/method/TOKB/index.files/lab/lab_3_clip_image016.gif=.

***Сочетания с повторениями***

Имеются элементы n различных типов. Сколько совокупностей, содержащих по k элементов каждая, можно составить из них, если не принимать во внимание порядок расположения элементов в совокупности? Задачи такого типа называют задачами на сочетания с повторениями.  
***Определение.*** Сочетанием с повторениями из данных n различных типов элементов по k элементов называется всякая совокупность, содержащая k элементов, каждый из которых  является одним из элементов указанных типов.  
Как видно из определения, сочетания с повторениями являются неупорядоченными множествами, а различные сочетания отличаются друг от друга входящими в них элементами, причем каждый элемент может входить в сочетание несколько раз. Для сочетаний с повторениями возможен случай, когда  n < k. Число различных сочетаний с повторениями из n элементов по k будем обозначать символом  http://stavkombez.ru/method/TOKB/index.files/lab/lab_3_clip_image020.gif.  
***Теорема.*** Число различных сочетаний с повторениями из n типов элементов по k элементов определяется по формуле:

.

**Изучение обобщенного алгоритма подбора пароля**  
Анализ уязвимости парольной системы требует использования ряда математических формул для определения параметров уязвимости.   
Будем использовать следующие условные обозначения:  
*M* – множество символов алфавита, используемого при переборе;  
*m = |M|* - мощность алфавита;  
*t1* – время, затрачиваемое на генерирование одного хэш-значения;  
*t2* – время сравнения двух хэш-значений;  
*n* – число символов пароля.

*В общем виде алгоритм подбора пароля выглядит следующим образом:*

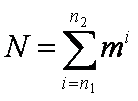
* Получение таблицы хэш-значений паролей;
* Получение очередного пароля (либо из словаря, либо гибридным методом) или генерация очередной комбинации;
* Подстановка нового пароля в алгоритм получения хэш-значения (время *t1*);
* Поочередное сравнение полученного на 3-ем шаге хэш-значение с имеющимися (после п.1) значениями в таблице. В случае совпадения данная комбинация есть действительный пароль указанного в хэш-таблице пользователя;
* Если возможна генерация (получение) нового пароля, то осуществляется переход к п. 2;
* Выход.

Таким образом, стойкость парольной системы определяется рядом факторов, поддающихся вполне конкретной оценке – общим числом парольных комбинаций, временем генерации хэш-значения, временем сверки хэш-значений. Для определения стойкости основным параметром выделим *t* - общее время полного перебора паролей.   
Приведем основные производные комбинаторные формулы применительно к задаче анализа стойкости парольной системы:  
*Формула определения общего числа парольных комбинаций:*

* + если известна длина пароля *n*:

http://stavkombez.ru/method/TOKB/index.files/lab/lab_3_clip_image024.gif

* + если известно, что длина пароля от *n1* до *n2* символов:



* + если известны *l* символов пароля и известны их места:

http://stavkombez.ru/method/TOKB/index.files/lab/lab_3_clip_image028.gif

*Формула определения времени перебора:*

http://stavkombez.ru/method/TOKB/index.files/lab/lab_3_clip_image030.gif

**Задание студентам для самостоятельной работы**

1. Определить время подбора 5 паролей, если известно, что длина каждого из них не превосходит *n2* символов, пароли набираются на алфавитно-цифровой клавиатуре (без использования «Shift») (учесть возможность сверки всех 5 паролей для одного хэш-значения) (параметры *n2 ,* *t1,* *t2* см. в приложении у преподавателя, в соответствии с номером своего варианта).  
2. Рассчитать вероятность успешной гибридной атаки по n-символьному словарю с использованием возможности замены 2 символов слева и справа, если длина пароля n символов, а в словаре *H* слов, используется *m*=26. (параметры n,H см. в приложении у преподавателя, в соответствии с номером своего варианта).  
3. Определить формулу для расчета общего числа парольных комбинаций, если известно, что в пароле от *n1* до *n2* символов, а также известно, что из *m* символов алфавита *M=*{*M1,M2,..Mm*} символы{*M1,M2,..Mm*} встречаются в пароле точно и:  
А) известно, что каждый из этих символов встречается только один раз;  
Б) известно, что каждый символ может встречаться несколько раз.  
4. Найти минимальную длину пароля *n*, при которой пароль не будет взломан в течение 1 года (при постоянном переборе) при количестве символов алфавита *m*, и скорости перебора 500000 пар/сек. (параметр *m* см. в приложении у преподавателя, в соответствии с номером своего варианта).  
5. Определить минимальную мощность множества символов алфавита *m*, при котором пароль длиной *n* не будет взломан в течение 3 мес. скорости перебора 300000 пар/сек. (параметр n см. в приложении у преподавателя, в соответствии с номером своего варианта).   
6. Определить время подбора пароля, если известно, что его длина не превосходит *n2* символов, пароль набирается на алфавитно-цифровой клавиатуре (с использованием Shift), а также известно, что в пароле точно есть символы «а», «з», «р». (параметры *n2 ,* *t1,* *t2* см. в приложении у преподавателя, в соответствии с номером своего варианта).  
7**.** Опишите и поясните основные шаги обобщенного алгоритма подбора паролей.