УДК 735

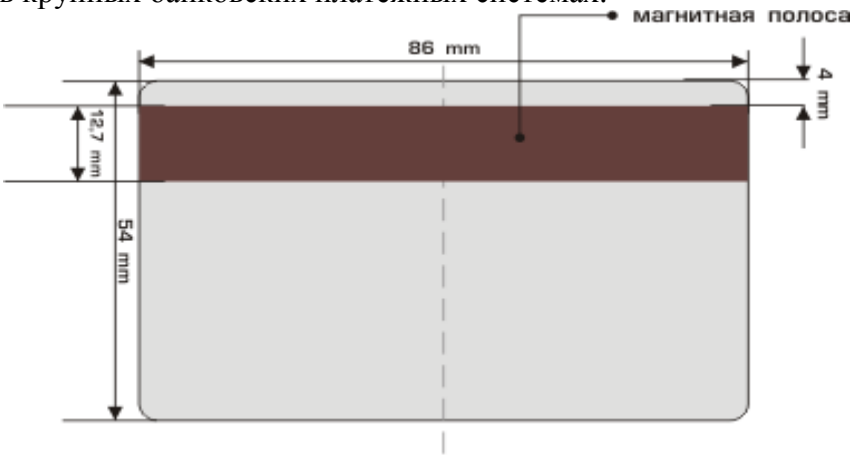
ОПРЕДЕЛЕНИЕ ВЕРОЯТНОСТИ ВЗЛОМА БАНКОВСКОЙ ПЛАСТИКОВОЙ КАРТЫ

Пинчук А.А.
Научный руководитель – к. ф.-м. н., доцент Новосёлов А.А.

Сибирский федеральный университет

Пластиковая карта — пластина стандартных размеров (54x86x0,76мм), изготовленная из специальной, устойчивой к механическим и термическим воздействиям пластмассы. Различаются по своему назначению, функциональным и техническим характеристикам. Один из самых распространенных способов нанесения информации на пластиковые карты - это использование магнитной полосы. Магнитная полоса содержит закодированную запись данных владельца карты. Считывающее устройство мгновенно расшифровывает информацию, содержащуюся на магнитной полосе. Рассмотрим банковскую пластиковую карту, на которой информация о владельце карты хранится в закодированном виде на магнитной полосе.

На магнитной полосе находится три дорожки, на которые можно нанести ту или иную информацию. Все три дорожки магнитной полосы используются, как правило, в крупных банковских платежных системах.



1-дорожка — цифробуквенная информация: до 76 знакомест. QWERTYUIOPASDFGHJKLZXCVBNM1234567890 : ; = + ( ) — ‘ - (клавиша " ‘ Э) ! @ # ^ & * < > / \ Все латинские буквы заглавные. Информация будет окружена служебными символами: " % " в начале строки, " ? " в конце строки. Служебный знак «?» добавляется в конце каждой строки базы данных и означает конец записи на магнитную полосу и при считывании не отображается.

2-дорожка — только цифры: 1234567890 и знак «=», до 37 знакомест пробел отображается на магнитной полосе знаком «=», знак «?» означает конец записи на магнитную полосу и при считывании не отображается. Информация будет окружена служебными символами: " ; " в начале строки, " ? " в конце строки.

3-дорожка — только цифры: 1234567890 и знак «=», до 104 знакомест пробел отображается на магнитной ленте знаком «=», знак «?» означает конец записи на магнитную ленту и при считывании не отображается. Информация будет окружена служебными символами: " _ " в начале строки , " ? " в конце строки.

Итак, первая дорожка содержит 56 знаков с повторениями, и того 76 знакомест. Вторая – 11 знаков с повторениями, и того 37 знакомест. Третья – 11 знаков с повторениями, и того 104 знакоместа.

Проведём опыт, состоящий в нахождении вероятности взлома кодировки магнитной полосы. Опыт считается удачным, если все 3 дорожки будут раскодированы одновременно.

Предположим, что имеется единственная попытка расшифровать код. Какова вероятность того, что считывающее устройство с первой попытки расшифрует закодированную информацию?

Итак, *будем считать, что общее количество различных наборов при выборе k элементов из n с возвращением и с учётом порядка равняется* n^k.

Тогда A_1=*{количество различных наборов на первой дорожке магнитной полосы}*

A_2=*{количество различных наборов на второй дорожке магнитной полосы}*

A_3=*{количество различных наборов на третьей дорожке магнитной полосы}*

Соответственно $A_1={n_1}^{k_1}$, $A_2={n_2}^{k_2}$, $A_3={n_3}^{k_3}$.

Вероятность взлома каждой из трёх дорожек равна : $P_i=1/A_i$, $i=1,2,3$.

Значит вероятность взлома магнитной полосы равна :

$P=P_1*P_2*P_3$

$P=(1/56^{76})*(1/11^{37})*(1/11^{104})=1/(56^{76}*11^{37}*11^{104})=1/(56^{76}*11^{141})\approx 10^{-270}$.

Данный пример показывает, что расшифровать информацию, закодированную на магнитной полосе пластиковой карты, имея единственную попытку, практически не представляется возможным.