Криптографические атаки
Сафонова Анна

Задание № 1.
Докажите, что при неравномерном распределении вероятностей на множестве ключей криптосистемы минимум средней трудоёмкости метода полного перебора достигается при опробовании ключей в порядке убывания их вероятностей.

Решение

Пусть есть систему шифрования:
K – множество ключей и
p_k – вероятность ключа $k \in K$

Средняя трудоёмкость T для метода полного перебора есть среднее количество попыток до взлома с использованием ключей k.

Вероятность наступления успеха (шифр взломан) на выбранном ключе k_t :
P(k= k_t) = $(1-p_1)\cdot(1-p_i)\ldots p_t$
где p_i -вероятность ключа k_i
Средняя трудоемкость T тем меньше чем меньше попыток нужно сделать, соответственно вероятность взлома на каждом новом ключе нужно максимизировать.

1. Вероятность что шифр взломан на первом же выбранном ключе:
P(k= k_1) = $p[k_1]$
Понятно, что, чтобы максимизировать эту вероятность нужно выбрать ключ с максимальной вероятностью
argmax(P(k= k_1)) = argmax($p[k_1]$) = k[$p=max(p_i)$]
Соответственно целесообразно выбрать ключ с max вероятностью

2. Считаем, что утверждение верно для (и мы так и выбирали) до какого-то ключа $k_{(t-1)}$
Проверим будет ли справедливо это для следующего ключа k_t

Вероятность в этом случае будет равна
P(k= k_t) = $(1-p_1)\cdot(1-p_i)\ldots p_t$ (множители до p_i и к моменту выбора ключа k_t уже константа)

argmax(P(k= k_t)) = argmax($p[k_t]$) = k[$p=max(p_i)$] (p_i это вероятности оставшихся ключей)

То есть на любом шаге разумно выбирать ключ с максимальной вероятностью среди оставшихся.

Задание № 2
Временная сложность дешифрования криптосистемы на момент разработки в 2023 году оценена: а) в 100 лет, б) в 1000 лет.
Определить, сколько лет в соответствии с законом Мура время дешифрования криптосистемы не превысит года.

Решение

Согласно эмпирическому закону Мура, вычислительные мощности криптоаналитика удваиваются через каждые 24 месяца(в курсе указано 18 месяцев)

Формула отражающая уменьшение сложности дешифрования системы:

start_time_estimation -первоначальная оценка сложности
end_time_estimation = start_time_estimation/ 2^n (n – количество сокращений)
n= log2(start_time_estimation/end_time_estimation)
end_time_estimation <=1 год

1. start_time_estimation = 100 лет
=> n >= 6,644

18месяцев*6,644 = 119,592 месяцев = 9,966 лет
То есть при соблюдении закона Мура и удвоении вычислительной мощности компьютерных систем раз в 18 месяцев, потребуется около 9,966 лет для сокращения дешифрования криптосистемы при сокращении до 1 года.

24месяца*6,644 = 159,456 месяцев = 13,288 лет
То есть при соблюдении закона Мура и удвоении вычислительной мощности компьютерных систем раз в 24 месяца, потребуется около 13,288 лет для сокращения дешифрования криптосистемы при сокращении до 1 года.

2. start_time_estimation = 1000 лет
=> n >= 9,966

18месяцев*9,966 = 179,388 месяцев = 14,949 лет
То есть при соблюдении закона Мура и удвоении вычислительной мощности компьютерных систем раз в 18 месяцев, потребуется около 14,949 лет для сокращения дешифрования криптосистемы при сокращении до 1 года.

24месяца*9,966 = 239,184 месяцев = 19,932 лет
То есть при соблюдении закона Мура и удвоении вычислительной мощности компьютерных систем раз в 24 месяцев, потребуется около 19,932 лет для сокращения дешифрования криптосистемы при сокращении до 1 года.