Раздел: Анализ Защищенности ПО (на веб)
Практическое задание: Модуль 3. Криптографические атаки
Выполнил: Александр Ганицев

Задание.

Задание № 1
Что нужно сделать

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.

Формат сдачи

Напишите ответ в свободной форме. Он должен содержать математически строгое доказательство необходимых утверждений.

Задание № 2
Условие задачи

Временная сложность дешифрования криптосистемы на момент разработки в 2023 году оценена: а) в 100 лет, б) в 1000 лет.

Что нужно сделать

Определить, сколько лет в соответствии с законом Мура время дешифрования криптосистемы не превысит года.

Формат сдачи

Напишите ответ в свободной форме. Он должен содержать полученные оценки и решение, описывающее, каким образом получен ответ.

Задание № 3
Что нужно сделать

Оцените трудоёмкость реализации оперативного метода Хеллмана для симметричного блочного шифра с ключевым множеством порядка 264, если размер блоков данных равен 64 бита.

Формат сдачи

Напишите ответ в свободной форме. Он должен содержать полученную оценку и решение, описывающее, каким образом получен ответ.

З**адание № 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.

Возьмём систему шифрования со множеством ключей K и вероятностями P(k), где k будет принимать значения из множества ключей K. Средняя трудоёмкость T для метода полного перебора в данной криптосистеме определяется как сумма произведений вероятностей P(k) на количество попыток, которые необходимы для взлома при использовании ключа k, для всего набора ключей k:

T = Σ(P(k) * k), где k есть количество попыток для взлома с использованием ключа K.

Согласно заданию, начнём перебор ключей в порядке убывания их вероятностей. Начиная с ключа k1 имеющего наибольшую вероятность P(k1) перейдем к ключу k2 со следующей по величине вероятностью P(k2), и так далее, до тех пор, пока не переберём все ключи. В случае с первым ключом вероятность будет высокой, что означает низкую трудоемкость. Вероятность успеха для ключа k2 будет ниже, что означает более высокую трудоёмкость по отношению к ключу k1. И так в процессе продвижения ко ключам с меньшими вероятностями будет расти трудоёмкость взлома криптосистемы.

Прохождение взлома системы с использованием данного подхода минимизирует среднюю трудоёмкость T, и отсюда следует, что при неравномерном распределении вероятностей на множестве ключей криптосистемы минимум средней трудоёмкости метода полного перебора достигается при опробовании ключей в порядке убывания их вероятностей.

Задание № 2

Временная сложность дешифрования криптосистемы на момент разработки в 2023 году оценена: а) в 100 лет, б) в 1000 лет.
Что нужно сделать: Определить, сколько лет в соответствии с законом Мура время дешифрования криптосистемы не превысит года.

Согласно современным воззрениям на эмпирический закон Мура (https://habr.com/ru/articles/740958/), и несмотря на то, что он перестаёт действовать, уступая закону Хуанга, рассмотрим период 24 месяца (2 года), в течении которого удваивается число транзисторов на плате микросхемы.

t_start = 100 лет

Вычислим количество удвоений максимальной производительности:

N_doubling = log2(36,500 / 365) / log2(2) = 6.6

Для нахождения количества лет, которое потребуется для сокращения времени дешифровки криптосистем до 1 года:

t_year = t_start / 6.6 = 15.15 лет

Вывод, при соблюдении закона Мура и удвоении вычислительной мощности компьютерных систем раз в 24 месяца, потребуется около 15.15 лет для сокращения дешифрования криптосистемы при сокращении до 1 года.

Задание № 3.

Оцените трудоёмкость реализации оперативного метода Хеллмана для симметричного блочного шифра с ключевым множеством порядка 264, если размер блоков данных равен 64 бита.

Оперативный метод Хеллмана - это атака, которая пытается найти общий секретный ключ, путем перебора всех возможных ключей и сравнения результатов шифрования или дешифрования с зашифрованным текстом.

При оценке трудоёмкости T данного метода мы будем учитывать следующие факторы:

1. Размер ключевого множества (K): У нас есть 264 возможных ключа.

2. Размер блока данных (N): У нас блок данных размером 64 бита.

3. Время на проверку каждого ключа: это время, которое занимает проверка одного ключа с использованием блочного шифра и сравнение полученного зашифрованного текста с известным.

T = (K * N) / (2 * t), где:

K - размер ключевого множества (264 в данном случае).
N - размер блока данных (64 бита).
t - время на проверку каждого ключа (в зависимости от вычислительной мощности).
Как и в предыдущем задании условимся, что t - это время, которое занимает проверка одного ключа, и давайте предположим, что это занимает одну миллисекунду (0,001 секунды). Тогда трудоемкость можно оценить как:

Трудоемкость = (264 * 64) / (2 * 0.001) = 8448000 бит/с

Это очень большое количество операций в секунду, и означает, что перебор 264 ключей с использованием оперативного метода Хеллмана на обычном компьютере не является выполнимой при разумных условиях.