ЗАНИЕ №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 у нас есть множество ключей K для некоторой криптосистемы, и пусть $P(k)$ обозначает вероятность того, что ключ k является искомым ключом. При этом, мы предполагаем, что вероятности ключей распределены неравномерно.

Допустим, ключи упорядочены таким образом, что $P(k_1) \geq P(k_2) \geq \ldots \geq P(k_n)$, где n – количество ключей в множестве K.

Теперь рассмотрим среднюю трудоемкость метода полного перебора. Если искомый ключ будет первым проверенным ключом, нам понадобится 1 попытка для его нахождения, если он будет вторым — 2 попытки, и так далее.

Таким образом, средняя трудоемкость T может быть вычислена следующим образом:

$$T = \sum_{i=1}^{n} i \times P(k_i)$$

Если ключи упорядочены в порядке убывания их вероятностей, то каждый ключ будет проверяться как можно раньше, и в результате средняя трудоемкость будет минимальной.

Для доказательства рассмотрим два соседних ключа в последовательности: k_i и k_{i+1} таких, что $P(k_i) < P(k_{i+1})$. Если мы поменяем местами эти два ключа, средняя трудоемкость уменьшится, так как более вероятный ключ будет проверяться раньше.

Это доказывает, что наилучший порядок проверки ключей для минимизации средней трудоемкости — это порядок убывания их вероятностей.

Вывод:

При неравномерном распределении вероятностей ключей криптосистемы оптимальный способ минимизации средней трудоемкости метода полного перебора — это проверка ключей в порядке убывания их вероятностей.

ЗАНИЕ №2

Временная сложность дешифрования криптосистемы на момент разработки в 2023 году

оценена:

a) в 100 лет;

b) в 1000 лет.

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

Решение:

Закон Мура – это эмпирическое наблюдение, впервые сформулированное Гордоном Муром, сооснователем Intel, в 1965 году. Закон Мура гласит, что количество транзисторов на интегральной микросхеме (что является мерой производительности компьютера) удваивается примерно каждые два года.

На практике это означает, что производительность компьютеров, их вычислительная мощность и память, также удваиваются каждые два года, при этом стоимость производства на единицу производительности уменьшается.

Если мы рассматриваем временную сложность дешифрования как некоторую задачу, требующую определенной вычислительной мощности для ее решения, то увеличение производительности компьютеров в два раза каждые два года приведет к уменьшению времени, необходимого для дешифрования, в два раза за тот же период времени.

Давайте рассмотрим каждый из двух случаев:

<u>Временная сложность дешифрования 100 лет:</u>

Если на момент разработки в 2023 году временная сложность дешифрования составляет 100 лет, то через два года, в 2025 году, она уменьшится вдвое и составит 50 лет. Через еще два года, в 2027 году, она уменьшится до 25 лет и так далее.

Проанализируем это:

Год	Сложность дешифрования
2023	100 лет
2025	50 лет
2027	25 лет
2029	12 лет и 6 месяцев
2031	6 лет и 3 месяца
2033	3 года, 1 месяц и 15 дней
2035	1 год, 6 месяцев и 22 дня
2037	9 месяцев, 1 неделя и 4 дня

Таким образом, к 2037 году временная сложность дешифрования уменьшится до менее чем года.

Временная сложность дешифрования 1000 лет:

Используя аналогичную логику:

Год	Сложность дешифрования
2023	1000 лет
2025	500 лет
2027	250 лет
2029	125 лет
2031	62 года и 6 месяцев
2033	31 год и 3 месяца
2035	15 лет, 7 месяцев и 2 недели
2037	7 лет, 9 месяцев и 3 недели
2039	3 года, 11 месяцев и 14 дней
2041	1 год, 11 месяцев и 21 день
2043	11 месяцев, 2 недели и 6 дней

Таким образом, к 2043 году временная сложность дешифрования уменьшится до менее чем года.

Вывод:

В соответствии с законом Мура, если временная сложность дешифрования криптосистемы на момент разработки в 2023 году составляет 100 лет, то к 2037 году она уменьшится до менее чем года. Если сложность составляет 1000 лет, то уменьшение до менее чем года произойдет к 2043 году.

Однако, следует понимать, что закон Мура не является физическим законом, и есть пределы, до которых можно увеличивать плотность транзисторов на чипе. Тем не менее, на протяжении многих десятилетий этот закон остаётся актуальным, хотя многие эксперты и инженеры в области полупроводников предполагают, что темпы удвоения плотности транзисторов могут замедлиться в ближайшие годы из-за физических и технологических ограничений.

ЗАНИЕ №3

Оцените трудоёмкость реализации оперативного метода Хеллмана для симметричного блочного шифра с ключевым множеством порядка 2^{64}, если размер блоков данных равен 64 бита.

Решение:

Для начала рассмотрим, что такое оперативный метод Хеллмана.

Оперативный метод Хеллмана применяется для симметричных блочных шифров и позволяет снизить стоимость атаки методом полного перебора вдвое при условии, что у нас есть возможность сделать два выбора начальных данных.

Таким образом, если криптоаналитик может выбрать два разных открытых текста и получить их шифртексты, он может применить метод Хеллмана.

По методу Хеллмана трудоёмкость атаки составляет примерно квадратный корень из общего числа ключей.

1. **Оценка трудоёмкости:**

   Пусть *N* — общее число ключей. В нашем случае $N=2^{64}$

   Тогда трудоёмкость атаки по методу Хеллмана составит $\sqrt{N}$

   Таким образом, трудоёмкость атаки: 2^{32}

2. **Решение:**

   Для симметричного блочного шифра с ключевым множеством порядка 2^{64} и при размере блоков данных в 64 бита, трудоёмкость реализации оперативного метода Хеллмана составляет порядка 2^{32} попыток.

Вывод:

Применение оперативного метода Хеллмана позволяет существенно сократить количество попыток при атаке на симметричный блочный шифр методом полного перебора. В данном случае, для шифра с ключевым множеством порядка 2^{64}, количество попыток сокращается до 2^{32} .