Защита информации

Павел Юдаев

МГТУ им. Баумана, Кафедра ИУ-9

Москва, 2014

Раздел 1 - Простые шифры

Информация - это любые данные.

- ~~получение~~ не рассматриваем
- ~~хранение~~ можно представить как передача от “меня сейчас” ко “мне позднее”
- **передача**
- ~~обработка~~ не рассматриваем, хотя есть некоторые тонкости (позже)

Какие сущ. угрозы информационной безопасности, и на каких из этих этапов?

Угрозы и защита:

1) непреднамеренное искажение.

- повреждение данных на носителях, напр. оптических дисках
- повреждение данных при передаче через шумную среду, напр. радиосвязь

Защита:

- checksum (примитивно), коды CRC - только обнаруживают ошибку
- коды, исправляющие ошибки - Error Correcting Codes. Исправляют ошибки типа замены значения бита

Если доля ошибочных битов в каждом блоке данных не более какого-то порога, можно гарантированно восстановить переданную информацию.

Угрозы и защита:

1) непреднамеренное искажение.

Коды, исправляющие ошибки:

- Хэмминга (исправляют 1 ошибку)
- Рида-Маллера
- Рида-Соломона (испр. не менее заданного числа ошибок; компакт-диски)
- коды БЧХ (испр. не менее заданного числа ошибок, большое семейство)

Угрозы и защита:

2) раскрытие самого факта передачи информации

Защита:

- методы стеганографии: подмешивание данных в цифровое изображение, в радиосигнал и т.д.

Угрозы и защита:

3) нежелательный доступ и преднамеренное искажение данных.

- получение третьими лицами доступа к секретным данным
- преднамеренное искажение данных третьими лицами
- отказ от авторства переданного сообщения

Защита:

- физическая: изолированная сеть, только сертифицированное ПО, комната без окон, заземленные стены, режим доступа персонала, отключенные внешние порты компьютеров...
- отказ от авторства возможен без специальных протоколов

Проблемы:

- дорого и не подходит для всеобщего использования

Угрозы и защита:

3) нежелательный доступ и преднамеренное искажение данных.

- получение третьими лицами доступа к секретным данным
- преднамеренное искажение данных третьими лицами
- отказ от авторства переданного сообщения

Защита с помощью криптографии, соответственно:

- шифрование. Какие шифры *достаточно стойкие*?
- криптографические хэш-функции.
- цифровая подпись.

Проблемы: надо строго обосновать степень стойкости этих алгоритмов ко взлому.

Цели курса:

- изучить криптографические примитивы и факты из математики (теории чисел, общей алгебры, ...), которые используются для их построения
- обсудить их стойкость ко взлому
- а также правильное и неправильное (нестойкое ко взлому) использование в протоколах обмена данными

Криптография вокруг нас:

- Данные, переданные по открытым каналам нельзя подслушать, нельзя изменить: HTTPS, WiFi WPA2 ~~и WEP~~, GSM, Bluetooth
- Шифрование файлов на диске: EFS, TrueCrypt
- Защита контента от копирования: (DVD, Blu-ray): CSS, AACS
- Авторизация пользователей в системе: медленные криптографические хэш-функции, случайная соль
- Доступ пользователей к сервисам системы: протоколы Kerberos и др.

А также многое другое, например:

- протоколы голосования без доверенного лица
- доказательства без разглашения информации, напр. авторизация
  (“Я знаю разложение этого числа на множители!” - “Докажи, что знаешь!” - “???”)
- безопасные распределенные вычисления: вычислители не получают информации об исходной задаче.
- bitcoin (digital anonymous cash)

Большинство этих примеров не войдет в курс длиной в один семестр (16 лекций).

Анализ криптографических конструкций:

- точно определим модель злоумышленника: доступные данные и средства, а также цель атаки
- предложим конструкцию
- докажем ее безопасность: если этот злоумышленник взламывает конструкцию (достигает своей цели), то для этого ему необходимо решить некоторую сложную задачу, т.е. широко известную задачу, для которой не найдено полиномиального алгоритма.

Опр.

Принцип Керкгоффса. Безопасность шифра должна обеспечиваться тем, что в секрете держится ключ, но не алгоритм!

Auguste Kerckhoffs (1835 - 1903), современник изобретения телеграфа.

Шеннон: “Враг знает систему”. Claude Shannon (1916 - 2001)

На практике необходимо и достаточно:
Алгоритм шифрования всем известен, многие пытались его взломать, но не смогли. Алгоритм получил сертификат от NSA или ГОСТ.

Варианты использования ключа

- *одноразовый ключ*
- *многоразовый ключ*

Очевидно, во втором случае нужен более сложный алгоритм для обеспечения того же уровня безопасности. Например, чтобы не раскрыть инф-ю, что пара файлов полностью совпадают.

Опр.

Пусть M - множество допустимых сообщений, K - множество ключей, C - множество допустимых шифротекстов.
Шифр - это пара алгоритмов (E, D) - шифрование, расшифрование, таких что

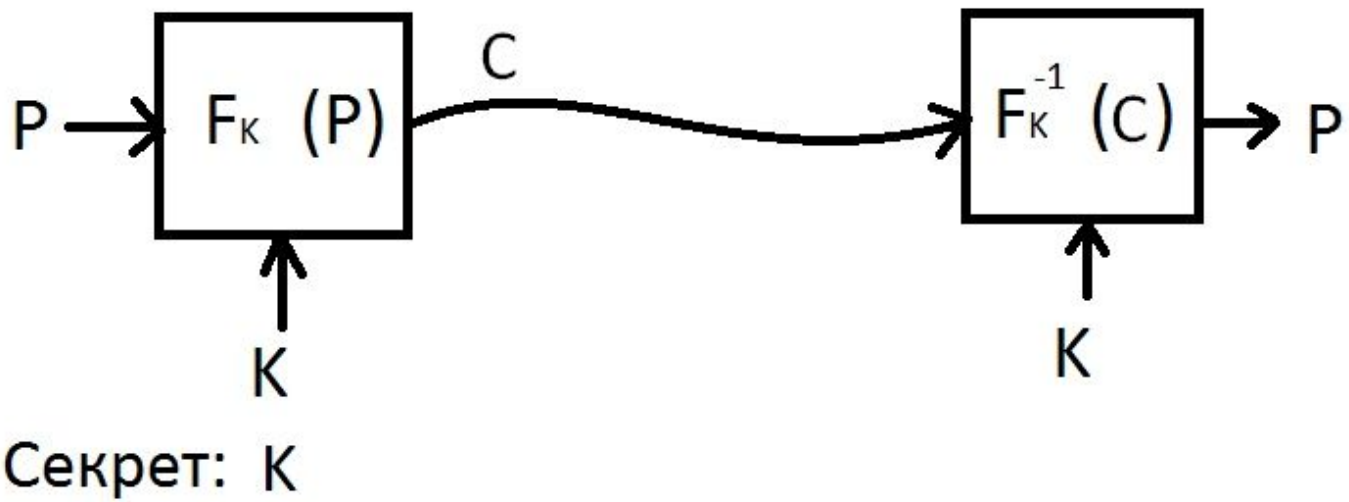
- время работы не более чем полиномиальное от длины входа
- $E : K \times M \to C$
- $D : K \times C \to M$
- $\forall k \in K, m \in M \;\; D(k, E(k, m)) = m$

Последнее равенство определяет *корректность* шифра.

Раздел 1 - Простые шифры

Опр.

Шифр называется *симметричным*, если для шифрования и расшифрования применяется один и тот же секретный ключ.



Опр.

Алфавитные шифры при преобразовании открытого текста в шифротекст заменяют один очередной символ открытого текста на один символ шифротекста по определенному правилу.

Все алфавитные шифры взломаны!

Раздел 1 - Простые шифры

Исторически, первый шифр был:

Опр.

Шифр простой замены, или *моноалфавитный шифр* переводит каждую букву алфавита открытого текста в одну фиксированную букву алфавита шифротекста независимо от ее места в тексте.

Пример

Шифр Цезаря.
Шифрование - это сдвиг алфавита на k букв.
Шифрование: $c = p + k \bmod N$.
Расшифрование:
Докажем корректность шифра:

Основной недостаток шифра: малое количество ключей, всего N. Можно подобрать ключ перебором.

Пример

Произвольный моноалфавитный шифр.
Ключ - произвольная фиксированная перестановка набора $(0, .., N)$. Каждая буква алфавита открытого текста переходит в фиксированную букву алфавита шифротекста.

Задача

Чему равно количество ключей при использовании английского алфавита из 26 букв?

Как взломать шифр простой замены? То есть, как по длинному шифротексту найти ключ и исходный текст?

Т.е. модель:

- злоумышленнику известен только достаточно длинный шифротекст.
- цель - найти ключ шифра

Опр. (Атака с известным шифротекстом)

- если злоум-ку известен только шифротекст.

Known ciphertext attack

Частотный анализ

В любом языке буквы используются с разной частотой.

Рассмотрим английский язык.

Таблицы частоты встречаемости букв (letter frequency):

Буква	Частота
e	0.127
a	0.082
o	0.075
i	0.070
...	...
q	0.010
z	0.007

Также - диграммы, например: *he*, *an*, *in*, *th*, ...

Для взлома достаточно перехватить длинный шифротекст.

UKBYBIPOUZBCUFEEBORUKBYBHOBBRFESPVKBWFOFERVNBCVBZPRUBOFERVNBCVBPCYYFVUFO
FEIKNWFRFIKJNUPWRFIPOUNVNIPUBRNCUKBEFWWFDNCHXCYBOHOPYXPUBNCUBOYNRVNIWN
CPOJIOFHOPZRVFZIXUBORJRUBZRBCHNCBBONCHRJZSFWNVRJRUBZRPCYZPUKBZPUNVPWPCYVF
ZIXUPUNFCPWRVNBCVBRPYYNUNFCPWWJUKBYBIPOUZBCUIPOUNVNIPUBRNCHOPYXPUBNCUB
OYNRVNIWNCPOJIOFHOPZRNCRVNBCUNENVVFZIXUNCHPCYVFZIXUPUNFCPWZPUKBZPUNVR

B	36
N	34
U	33
P	32
C	26

➔ E

➔ T

➔ A

NC	11
PU	10
UB	10
UN	9

digrams

➔ IN

➔ AT

UKB	6
RVN	6
FZI	4

trigrams

➔ THE

Раздел 1 - Простые шифры

Шифр Виженера (XVI в.)

Это полиалфавитный шифр.

Ключ - короткое слово. Шифрование: повторение ключа, так что длина расширенного ключа $k_{ext} = k||k||...$ равна длине текста, и сложение текста и ключа:

$c[i] = (p[i] + k_{ext}[i]) mod N$,

$p[i] = (c[i] - k_{ext}[i]) mod N$

Пример

Пусть k = CRYPTO.

```
K = CRYPTO CRYPTO CRYPT
P = WHATAN ICEDAY TODAY
C = YYYITB KTCSTM VJBPR
```

Задача

Чему равна мощность множества K?

Взлом шифра Виженера

Пусть знаем длину ключа $q = |k|$.
Тогда возьмем каждый q-й символ, получим текст, зашифрованный шифром Цезаря. Шифр Цезаря взломаем с помощью частотного анализа.

Как узнать длину ключа? Рассмотрим два способа.

Метод Касиски (Kasiski, 1863)
(TODO: в 2015 не рассказывать подробно с целью экономии времени, оставить только индекс совпадений)

Основная идея: Если триграмма (три буквы) повторяется в тексте на расстоянии, кратном длине ключевого слова, то она будет зашифрована одинаково.

```
K: ABCDABCDABCDABCDABCDABCDABCD
P: CRYPTOISSHORTFORCRYPTOGRAPHY
C: CSASTPKVSIQUTGQUCSASTPIUAQJB
```

Несколько повторяющихся сегментов позволяют предположить длину ключа:

DYDUXRMHTVDVNQDQNWDYDUXRMHARTJGWNQD

Расстояние между повторяющимися DYDUXRMH равно 18, это позволяет сделать вывод, что длина ключа равна одному из значений: 18,9,6,3 или 2.

Расстояние между повторяющимися NQD равно 20. Из этого следует, что длина ключа равна 20 или 10, или 5, или 4 или 2.

Чаще всего повторяется делитель, равный 2.
Вывод: длина ключа, почти наверняка, равна 2.

Индекс совпадений

Вероятность того, что два случайно (равновероятно) выбранных из алфавита символа совпадают, в английском языке равна $\kappa_a = 1/26 = 0,038$.

Вероятность того, что два случайно выбранных из текста символа совпадают, так наз. *индекс совпадений*, в английском языке равна $\kappa_t = 0.067$.

Задача

Почему $\kappa_t > \kappa_a$?
Указание: для алфавита из N символов представить вероятность появления $i-$ символа в тексте как $1/N + \varepsilon_i$.

Предположим, что длина ключа шифра Виженера равна s.

Разобьем шифротекст на s частей.
В i-ю часть войдут символы в позициях $i + ls$, $l \in \mathbb{Z}_{\geq 0}$

Если мы угадали длину ключа, то κ^i - индекс совпадения для каждой части (по отдельности) будет около κ_t.

Если мы не угадали длину ключа, то κ^i - индекс совпадения для каждой части (по отдельности) будет ниже κ_t. (Почему?)

Значит, $\kappa^i = \kappa^i(s)$.
Предположение: $|k| = \underset{s}{\text{argmax}}(\sum_i \kappa^i(s))$.

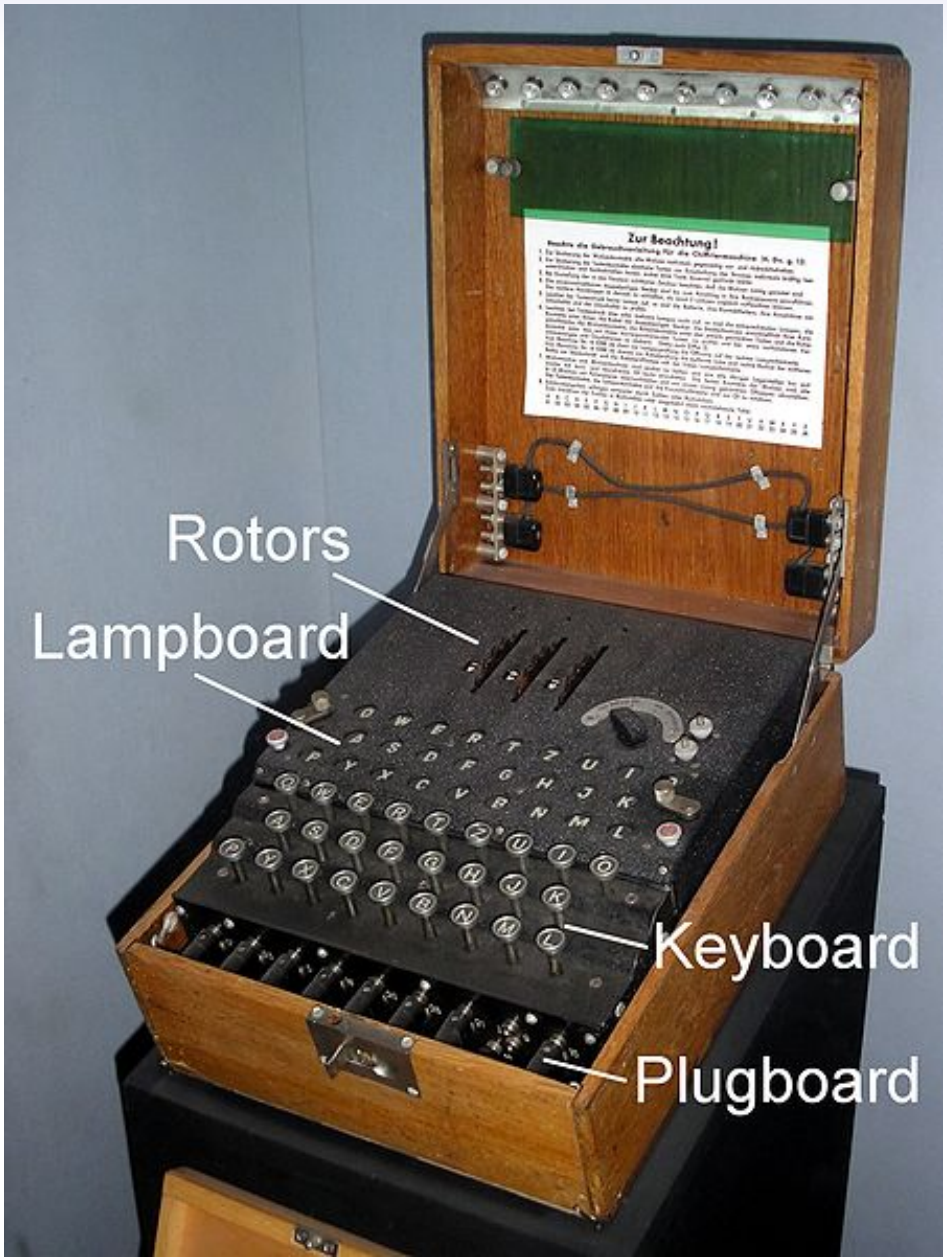
Раздел 1 - Простые шифры

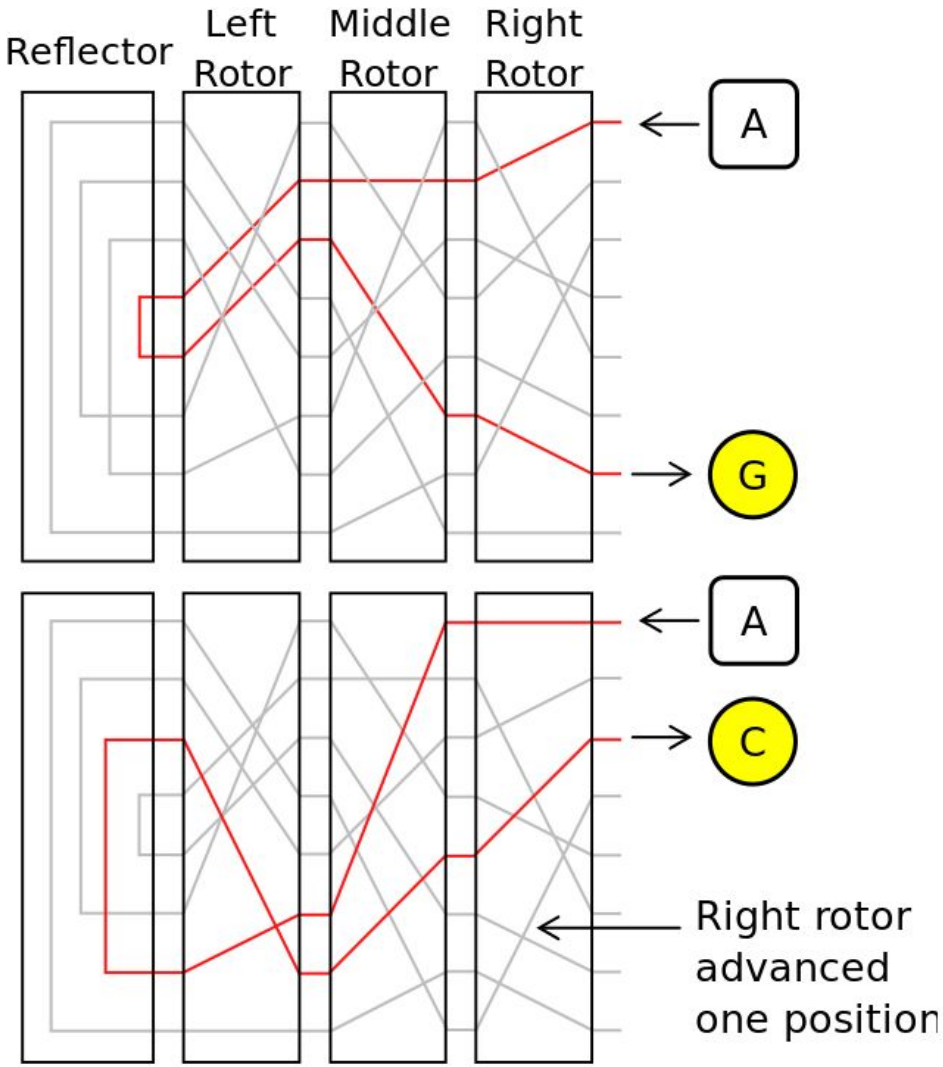
Начало исторической справки. Не для экзамена.

Развитие шифра Виженера - роторные машины, в т.ч. Энигма (Германия, 1940-е годы, 3-5 роторов, до 2^{36} ключей).

Шифр Энигмы взломан союзниками во время II мировой войны.

Обзоры:
Сингх, “Книга шифров”.
Википедия: Криптоанализ “Энигмы”.


Rotors
Lampboard
Keyboard
Plugboard


Reflector
Left Rotor
Middle Rotor
Right Rotor
A
G
A
C
Right rotor advanced one position

Для взлома шифра Виженера было достаточно перехватить шифротекст небольшого объема.

В случае Энигмы взлом был осуществлен после того, как проводящие атаку на шифр выкрали шифровальную машину и смогли получать шифротексты для произвольных открытых текстов.

Это разные атаки.

Опр. (Атака с выбором открытого текста)

Если злоумышленник может выбирать открытые тексты один за другим, получать их шифротексты, и выбирает следующий открытый текст m, зная все предыдущие пары (c, m), то он осуществляет *атаку с адаптивным выбором открытого текста*.

Adaptive chosen plaintext attack

Жаргон / новояз, частично скрывающий информацию

- Где бревно?
- Кто его знает, говорят, на спутнике макаку чешет.

Перевод:
- Где капитан Деревянко?
- Не знаю, но, говорят, что работает по закрытому каналу связи и отслеживает американские испытания прототипа торпеды Mk-48

Конец исторической справки.

Раздел 1 - Простые шифры

Эту секцию следует вспомнить (или изучить) самостоятельно.

Пусть U - конечное множество.

Опр.

Распределение вероятности P над множеством U - это функция $P: U \to [0,1]$, такая что $\sum_{u \in U} P(u) = 1$

Равномерное распределение: $\forall u \in U\ P(u) = 1/|U|$

Точечное распределение: $P(u_0) = 1, \forall u \neq u_0\ P(u) = 0$

Опр.

Любое подмножество $A \subseteq U$ наз. *событием*. Вероятность события $A \subseteq U$ $P(A) = \sum_{u \in A} P(u)$,

$P(U) = 1$, $P(\emptyset) = 0$.

Пример

$U = \{0,1\}^8$, $A = \{u \mid u[1]u[2] = 11\}$

Если на U равномерное распределение, то $P(A) = 1/4$.

Опр.

Случайная величина (с.в.) - это функция $X: U \to V$

Пример

$y \in U = \{0,1\}^n$, с.в. X: $X: U \to \{0,1\}$, $X(y) = y[1] \in \{0,1\}$

Опр.

С.в. имеет распределение на V:
$P(X = v) \equiv P(X^{-1}(v))$,
где $X^{-1}(v) \subseteq U$

Опр.

Пусть на множестве U - равномерное распределение вероятности. *Равномерно распределенная (р.р.) с.в.* на множестве U - это тождественная функция X:
$\forall u \in U\, X(u) = u$.

Опр.

События A, B *независимы*, если $P(A\&B) = P(B) \cdot P(B)$

Опр.

С.в. X, Y, принимающие значения из V, *независимы*, если $\forall a, b \in V \; P(X = a \;\&\; Y = b) = P(X = a) \cdot P(Y = b)$

Пример

Пусть строка x - р.р. с.в. из $\{0,1\}^n$. Тогда с.в. $Y = x[1]$ и с.в. $Z = x[n]$ - независимы, обе $\{0,1\}^n \to \{0,1\}$.

Пример

Пусть X, Y - независимые, равномерно распределенные с.в. на $\{0,1\}$. Пусть $Z = X + Y$. Тогда $P(Z = 2) = P(X = 1 \& Y = 1)$ $= P(X = 1)P(Y = 1) = 1/2 \cdot 1/2 = 1/4$.

Пример

Пусть X, Y - равномерно распределенные с.в. на $\{0,1\}$. Пусть $Y = X$ с вероятностью 0.9, $Y = 1 - X$ с вероятностью 0.1.
Пусть $Z = X + Y$.
Тогда $P(Z = 2) = P(X = 1 \& Y = 1) = 1/2 \cdot 9/10$
$\neq P(X = 1)P(Y = 1) = 1/2 \cdot 1/2$.

Опр.

Пусть X - дискретная с.в., принимающая значения a_i и с вероятностью p_i. Тогда *математическое ожидание* $E(X) = \sum_i a_i p_i$.

Опр.

Пусть X - с.в. и $E(X)$ конечно. Тогда *дисперсия* $D(X) = E[(X - E(X))^2]$. (Дисперсия - второй центральный момент этой с.в.)

Теорема 1 (Неравенство Маркова)

Пусть X - неотрицательная с.в., $E(X)$ конечно, число $a > 0$. Тогда $P(X \geq a) \leq \frac{E(X)}{a}$

Теорема 2 (Неравенство Чебышева)

Пусть X - с.в., $E(X)$ и $D(X)$ конечны, число $a > 0$. Тогда $P(|X - E(X)| \geq a) \leq \frac{D(X)}{a^2}$

Раздел 1 - Простые шифры

Опр.

Операция XOR, $\oplus$ - это сложение по модулю 2.
XOR двух строк a, b равной длины - это строка
$c: \ c[i] = a[i] \oplus b[i]$

Теорема 3 (О сумме случайных величин)

Пусть X - произвольная с.в., принимающая значения из $\{0,1\}^n$,
Y - равномерно распределенная с.в. на $\{0,1\}^n$,
X, Y независимы.
Тогда $Z = X \oplus Y$ - равномерно распределенная с.в. на $\{0,1\}^n$.

Док-во

Операция $\oplus$ почленная, поэтому достаточно док. для $n = 1$.
Пусть $X : P(X = 0) = p_0,\ P(X = 1) = p_1 = 1 - p_0$

Заметим, что $P\big[(X, Y) = (0, 0)\big] = P(X = 0) \cdot P(Y = 0) = p_0/2$

$P(Z = 0) = P\big[(X, Y) = (0, 0)$ или $(X, Y) = (1, 1)\big] =$

$P\big[(X, Y) = (0, 0)\big] + P\big[(X, Y) = (1, 1)\big] = p_0/2 + p_1/2 = 1/2$

Итак, $P(Z = 0) = 1/2$, значит $P(Z = 1) = 1/2$,
Z - р.р. с.в. на $\{0,1\}$, ч.т.д.

Задача

Возможно ли обобщить для сложения (и вычитания) по модулю n? Доказать это.

Задача

А для суммы $Y \oplus X_1 \oplus ... \oplus X_n$, где все с.в. попарно независимы?

Теорема 4 (Парадокс дня рождения)

Пусть $X_1, ...X_n \in U$ - независимые одинаково распределенные с.в. Пусть $|U| \geq 500$, $c = 1.2$ и $n = c \cdot |U|^{1/2}$.

Тогда $P(\exists i \neq j : X_i = X_j) \geq 1/2$

Док-во

Докажем для равномерно распределенной с.в.
(Для неравномерного распределения вероятность совпадения будет выше - почему?)
Обозначим $N = |U|$. Пусть случайная величина X_1 приняла значение a_1. Пусть $X_2 = a_2$. Вероятность, что они не совпадут, равна $1 - \frac{1}{N}$.

Добавим к набору (a_1, a_2), $a_1 \neq a_2$ третью случайную величину, принявшую значение $X_3 = a_3$. Вероятность того, что при этом снова нет совпадений, равна $1 - \frac{2}{N}$. И так далее, вплоть до значения последней случайной величины, для которого вероятность несовпадения с предыдущими значениями будет $1 - \frac{n-1}{N}$.

Поэтому вероятность того, что значения всех случайных величин будут различными, равна
$p(n) = 1 \cdot (1 - \frac{1}{N}) \cdot (1 - \frac{2}{N}) \cdot ... \cdot (1 - \frac{n-1}{N})$.

Воспользуемся тем, что $e^{-x} \geq 1 - x \; \forall x \in R$.

$$p(n) \leq \prod_{i=1}^{n-1} e^{-x/N} = e^{-\frac{1}{N}\sum_{i=1}^{n-1} i} = e^{-\frac{n(n-1)}{2N}}$$

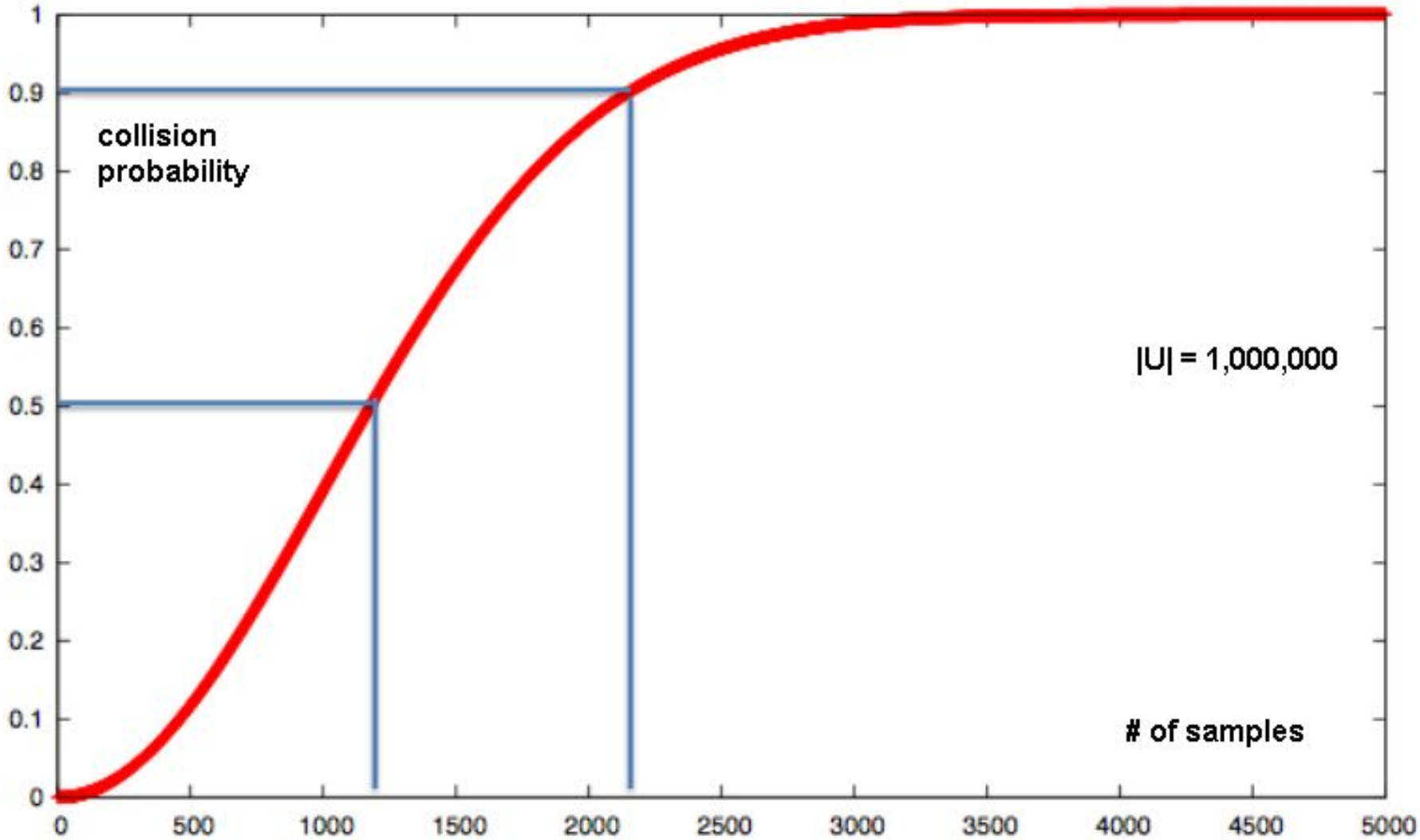
Т.к. $n = 1.2 \cdot \sqrt{N}$, то $-\frac{n(n-1)}{2N} = -0.72 + \frac{0.6}{\sqrt{N}}$.

Тогда $p(n) \leq e^{-0.72+\frac{0.6}{\sqrt{N}}}$.

Чтобы доказать теорему, нужно $p(n) < 0.5$.

Решая неравенство $e^{-0.72+\frac{0.6}{\sqrt{N}}} < 0.5$, находим, что $N > 499.3$.
Поэтому при $N \geq 500$ $p(n) < 0.5$.

Вероятность, что в наборе $(a_1, ..., a_n)$ найдется два равных значения, равна $1 - p(n) > 0.5$. Ч.т.д.


collision
probability
|U| = 1,000,000
# of samples
1
0.9
0.8
0.7
0.6
0.5
0.4
0.3
0.2
0.1
0
0
500
1000
1500
2000
2500
3000
3500
4000
4500
5000

Пример

- $U = \{0,1\}^{128}$
- приняли $1.2 \cdot 2^{64}$ случайных сообщений из U
- с вероятностью более 0.5 среди них найдутся два равных сообщения

Замечание (*)

Очевидно, что при $p(n) < 0.5$ и $|U| \nearrow$ будет $c \searrow$.
Но $c \geq \sqrt{2ln(2)} \approx 1.177$.

Шифр одноразовый блокнот,
он же шифр Вернама (1917), One Time Pad.

Опр. (Одноразовый блокнот)

$M = C = K = \{0,1\}^n$.
Ключ - случайная строка. Каждый ключ используется только один раз.
$c = E(k, m) = k \oplus m$
$D(k, c) = k \oplus c$

$D(k, E(k, m)) = k \oplus k \oplus m = m$ - верно.

Является ли одноразовый блокнот стойким шифром (secure cipher)?
Что такое “стойкий шифр”?
Какими возможностями обладает злоумышленник?

Так как ключ используется только один раз, реалистичной моделью атаки является следующая:

Злоумышленник знает только шифротекст.
Атака с известным шифротекстом (known ciphertext attack).

Варианты определения цели злоум-ка:

- злоум-к не может узнать ключ (?!)
- злоум-к не может узнать все сообщение целиком (?!)
- идея Шеннона: злоум-к не может узнать никакой информации о сообщении по шифротексту.

Стойкость с информационно-теоретической точки зрения, по Шеннону (Shannon, 1949)

Опр.

Шифр (E,D) над (K,M,C) является *абсолютно стойким*, если
$\forall m_0,\ m_1 :\ len(m_0) = len(m_1)$ и $\forall c \in C$
$P[c = E(k, m_0)] = P[c = E(k, m_1)]$
где ключ k - это значение равномерно распределенной случайной величины на множестве ключей K.
$k \xleftarrow{R} K$

Теорема 5

Одноразовый блокнот абсолютно стойкий.

Док-во

$\forall$ фикс. m $P(E(k,m)=c) = \left|\{k \in K:\ E(k,m)=c\}\right|/|K|$.
Значит, если $\forall m, c\ |\{k \in K : E(k,m)=c\}| = const$, то шифр абсолютно стойкий.
Пусть $m \in M$ и $c \in C$. Сколько ключей отображают m в c?
$\forall m, c\ k = m \oplus c$, следовательно $|\{k \in K:\ E(k,m)=c\}| = 1$.
Следовательно, одноразовый блокнот - абсолютно стойкий шифр. Ч.т.д.

Утверждение

Если шифр абсолютно стойкий, то $|K| \geq |M|$.

Док-во (От противного)

Пусть $|K| < |M|$. Пусть $E(k_0, m_0) = c_0$.
$S := \{m | \exists k \in K : D(k, c_0) = m\}$, $|S| \leq |K| < |M|$

$\Rightarrow \forall m_1 \in M \setminus S : \; P[c = E(k, m_1)] = 0$
$P[c = E(k, m_0)] > 0$.
Ч.т.д.

Т.е. у абсолютно стойкого шифра длина ключа не меньше длины сообщения. Не очень практично!

Пример

Двухразовый блокнот - не стойкая криптосистема.
$c_1 = m_1 \oplus k$,
$c_2 = m_2 \oplus k$,
злоум-к вычисляет $c_1 \oplus c_2 = m_1 \oplus m_2$
и язык (или протокол обмена данными) имеет достаточно избыточности, чтобы по значению $m_1 \oplus m_2$ узнать значения m_1 и m_2.

Еще проще взломать многоразовый блокнот.

Пример такой атаки: Project Venona.

Семинар 1:

Задача

пусть T - с.в., сумма N независимых с.в. X_i с распределением Бернулли
$P(X_i = 0) = \frac{1}{2} + \gamma$,
$P(X_i = 1) = \frac{1}{2} - \gamma$.
Вывести
$E(X_i) = \frac{1}{2} - \gamma, \quad D(X_i) = \frac{1}{4} - \gamma^2$
$E(T) = N(\frac{1}{2} - \gamma)$,
$D(T) = N(\frac{1}{4} - \gamma^2)$

Использовать:
$D(X) = E((X - EX)^2)$,
$cov(X, Y) = E((X - EX)(Y - EY))$,
$D(X + Y) = D(X) + D(Y) - 2cov(X, Y)$

Некоторые итоги:

A. Стойкость шифров с одноразовым ключом:
A.1. Абсолютная стойкость к атаке с известным шифротекстом.

B. -

C. Шифры:
C.1. Алфавитные.
C.2. Одноразовый блокнот.

Раздел 1 - Простые шифры

Основная литература по курсу:

- Joshua, Katz, *Introduction to Modern Cryptography*
- Рябко, Фионов, *Криптографические методы защиты информации*, Москва, 2005
- A. Menezes, P. Van Oorschot, S. Vanstone, *Handbook of Applied Cryptography*, http://cacr.uwaterloo.ca/hac/
- Курс лекций *Cryptography I*, http://coursera.org/

Литература к лекции 1:

- Краткий курс по теории вероятности для дискретных переменных,

  http://en.wikibooks.org/High_School_Mathematics_Extensions/Discrete_Probability

Дополнительная литература по курсу:

- Шнайер, *Прикладная криптография* (Schneier, *Applied Cryptography*) - скорее энциклопедия, чем учебник.
- Шнайер, *Практическая криптография* (Schneier, *Practical cryptography*) - скорее энциклопедия, чем учебник.
- Tom Olzak, *Enterprise Security. A practitioner's guide* - прекрасный обзорный материал.

  `http://resources.infosecinstitute.com/enterprise-security-book-chapter-1/`
- Смарт, *Криптография* (Smart, *Cryptography: An introduction*)
- Ященко, *Введение в Криптографию* - книга короткая и понятная, легко читается.
- Грушо, *Анализ и синтез криптоалгоритмов*
- Курс лекций Udacity CS387: Applied Cryptography. Lecture notes: `http://goo.gl/dDkhq`, class: `https://www.udacity.com/wiki/cs387`

- Саймон Сингх, *Книга Шифров* (Simon Singh, *The Code Book*), 1999 - о криптографии и ее истории
- Дэвид Кан, *Взломщики кодов* (David Kahn, *The code breakers*), 1967 - об истории создания и развития шифров
- Хорошко, *Методы и средства защиты информации* - материал ортогонален этому курсу: физические и организационные приемы
- список книг: `http://habrahabr.ru/qa/3994/`