Криптография: вчера, сегодня, завтра

Аннотация

Лекция «Криптография: вчера, сегодня, завтра» знакомит слушателей с историей создания методов шифрования, начиная с древности до наших дней, намечая возможные дальнейшие направления развития этой области знаний. Обсуждаются шифр Цезаря, шифры простой замены, основные принципы построения криптосистемы с открытым ключом, математические и вычислительные основы современной криптографии, вопросы расшифровки и надежности шифра, перспективные методы обнаружения перехвата секретной информации. Приведен ряд конкретных примеров шифрования, в том числе при помощи криптосистемы RSA, изложены необходимые теоретико-числовые основы.

Слайд 1.

Криптография как наука о методах обеспечения секретности, целостности и подлинности передаваемой информации является ярким примером сочетания фундаментальных теоретических исследований с решениями актуальных практических задач. Можно сказать, что это одна из старейших наук, история которой насчитывает несколько тысяч лет, что, однако, не мешает систематическому появлению новых результатов (и даже возникновению целых направлений), а также динамичному развитию в соответствии как с внутренними задачами науки, так и с вызовами настоящего времени.

Слайд 2.

В настоящей лекции мы не ставим задачу хоть сколько-нибудь полно описать все направления криптографической науки, цель состоит в начальном ознакомлении слушателей с историей создания методов шифрования, начиная с древности до наших дней, намечая возможные дальнейшие направления развития этой области знаний. Обсуждаются шифр Цезаря, шифры простой замены, основные принципы построения криптосистемы с открытым ключом, математические и вычислительные основы современной криптографии, вопросы расшифровки и надежности шифра, перспективные методы обнаружения перехвата секретной информации. Приведен ряд конкретных примеров шифрования, в том числе при помощи криптосистемы RSA, изложены необходимые теоретико-числовые основы.

Слайд 3.

Широко известен метод шифрования, который применял римский император Гай Юлий Цезарь (102–44 до н. э.) для секретной переписки с генералами своей армии: каждая буква послания заменялась буквой, находящейся в алфавите на 3 позиции правее неё (например, в русском алфавите букву А надо было бы заменить на Г, Б на Д и т. д.).

Слайд 4.

Для удобства использования шифра Цезаря можно применить два диска разного диаметра на одной оси с нарисованными по краям дисков алфавитами. При изготовлении буквы наносятся так, чтобы напротив каждой буквы алфавита внешнего диска находилась та же буква алфавита малого диска. Если теперь повернуть внутренний диск, то мы получим соответствие между символами внешнего диска и внутреннего, которое можно использовать как для шифрования, так и для расшифровки.

Слайд 5.

По-видимому, эффективность шифра Цезаря для защиты военных сообщения была связана с тем, что большинство врагов Цезаря были людьми неграмотными, и многие из них предполагали, что сообщения написаны на неизвестном иностранном языке. В настоящее время шифр Цезаря не имеет практического применения, поскольку, как легко видеть, он легко взламывается. В самом деле, если известно, что шифрование производилось именно сдвигом, то можно, например, под каждой буквой зашифрованного текста написать в столбик весь алфавит, начиная с этой буквы. При использовании заранее подготовленных полосок с алфавитом расшифровка пройдёт очень быстро: если сложить полоски так, чтобы в одной строке образовался текст в зашифрованном виде, то в некоторой другой строке возникнет расшифрованный текст.

Слайд 6.

Вообще же шифр Цезаря, как и все шифры простой замены, взламывается методами частотного анализа, как это проделал Ш. Холмс в рассказе «Пляшущие человечки». Дело в том, что для каждой буквы данного языка можно рассчитать частоту появления в литературных текстах и на основании этих данных сделать

вывод (или, по крайней мере, высказать предположения) о буквах, скрывающихся за символами перехваченного зашифрованного сообщения. Для восстановления таблицы шифровки достаточно сопоставить её с таблицей средних частот букв в зашифрованном тексте.

Слайд 7.

«Пляшущие человечки» – детективный рассказ Артура Конан Дойля, написанный в 1903 г., об очередном расследовании Шерлока Холмса и доктора Ватсона. Перед домом человека, обратившегося к ним за помощью, стали появляться загадочные рисунки. С первого взгляда эти «пляшущие человечки» напоминают детское творчество, однако накопив достаточное количество рисунков, Шерлок Холмс догадался, что это сообщения, зашифрованные шифром простой замены, расшифровал их методом частотного анализа и раскрыл дело. «Флажки» у человечков означали границы слов.

Слайд 8.

Для того чтобы перейти к современным методам шифрования, отметим, что теоретико-числовая модель шифра Цезаря – сложение чисел по модулю n: запись

$$y = x + k \bmod n$$

означает, что значение y полагается равным остатку от деления числа $x + k$ на n. Аналогичным образом, запись

$$y \equiv x \,(\bmod n)$$

означает, что числа x и y дают одинаковые остатки при делении на n. Таким образом, шифрование сдвигом на 3, скажем, сообщения на русском языке, можно описать формулой

$$y = x + 3 \mod 32,$$

а расшифровка этого сообщения задаётся равенством

$$x = y - 3 \mod 32.$$

Мы видим, что обратная операция легко выполняется, если известна величина сдвига. Иными словами, сложности выполнения операций шифрования и расшифровки одинаковы. Вообще, когда речь идёт о шифровании всегда следует понимать, что является секретным для посторонних, а что общедоступным. Например, известен ли способ шифрования, защищен ли канал передачи данных и пр. Кроме того, можно считать, что передаваемая информация есть

натуральное число. Каким образом оно получено для дальнейшего рассмотрения не важно, это может быть сделано любым методом, причем обычно нет необходимости держать его втайне.

Слайд 9.

Для разработки более надёжных способов шифрования используются математические (в частности, теоретико-числовые) методы. Приведём некоторые известные теоретико-числовые факты, которые широко применяются в криптографии. Функция Эйлера $\varphi(n)$ – количество натуральных чисел, меньших n и взаимно простых с n. Например, если p – простое число, то $\varphi(p) = p - 1$. Если $n = pq$, где p, q – простые числа, то $\varphi(n) = (p-1)(q-1)$. Справедлива теорема Эйлера: если числа x и n взаимно просты, то $x^{\varphi(n)} \equiv 1 \pmod{n}$.

Слайд 10.

В 1970-х гг. был разработан принципиально новый метод шифрования, основанный на применении теории чисел и глубоком исследовании современных вычислительных алгоритмов. Он не предполагал ни наличия защищённого канала связи, ни необходимости «скрывать» число n.

В основе метода лежит понятие односторонней функции – такой функции $f(x)$, что по известному x можно достаточно быстро вычислить значение $f(x)$, тогда как нахождение x по заданному значению $f(x)$ невозможно за обозримое время. Односторонняя функция применяется для шифрования сообщения, но расшифровать его с её помощью нельзя. Для расшифровки же используется некоторый секретный ключ y, помогающий вычислить x, зная $f(x)$.

Слайд 11.

Рассмотрим широко применяемую криптосистему с открытым ключом RSA. Ключевую роль в её построении играет то обстоятельство, что возможность человечества находить большие простые числа (т. е. доказывать простоту конкретных больших чисел) значительно опережает возможности в области разложения на множители. Текущий рекорд разложения на множители произвольных чисел – менее 200 знаков, а проверить на простоту можно любое число вплоть до 10^{15000}. Вообще же, наибольшим из известных на сегодня простых чисел является $2^{43112609} - 1$, состоящее из 12 978 189 цифр (это простое

число Мерсенна найдено 23.08.2008 на математическом факультете университета UCLA в рамках проекта по распределённому поиску простых чисел Мерсенна GIMPS).

Слайд 12.

Опишем принцип действия криптосистемы RSA.

- Выбираются два больших простых числа p, q (на сегодняшний день обычно выбирают числа, содержащие от 200 до 400 знаков) и вычисляется их произведение n, которое не может быть разложено на множители за разумное время (даже с использованием компьютеров ближайшего будущего).
- Вычисляется значение функции Эйлера $\varphi(n) = (p - 1)(q - 1)$.
- Выбирается целое число e ($1 < e < \varphi(n)$), взаимно простое со значением функции $\varphi(n)$. Обычно в качестве e берут простые числа, содержащие небольшое количество единичных битов в двоичной записи, например, простые числа Ферма 17, 257 или 65537. Число e называется открытой экспонентой.

Слайд 13.

- Вычисляется число d, обратное по умножению к числу e по модулю $\varphi(n)$, то есть число, удовлетворяющее условию $de \equiv 1 \pmod{\varphi(n)}$, т. е. $de = 1 + k\varphi(n)$, где k – некоторое целое число. Число d называется секретной экспонентой.
- Пара $P = (e,n)$ публикуется в качестве открытого ключа системы RSA.
- Пара $S = (d,n)$ называется секретным ключом RSA и держится втайне.
- Шифрование и расшифровка происходят по стрелкам на схеме:

$$M \to C = M^e \bmod n \to S = C^d \bmod n = M.$$

Корректность расшифровки обеспечивается теоремой Эйлера: если числа x и y взаимно просты, то

$$x^{\varphi(n)} \equiv 1 \pmod{n},$$

поэтому

$$S = C^d \bmod n = M^{de} \bmod n = M^{1+k\varphi(n)} \bmod n = M \cdot \left(M^{\varphi(n)}\right)^k \bmod n = M.$$

Слайд 14.

В рассматриваемой криптосистеме односторонней функцией является

$$f(x) = x^e \bmod n.$$

Оказывается, что при перехвате зашифрованного сообщения $C = M^e \bmod n$ восстановить значение M, не зная секретного ключа, практически невозможно: быстрый способ решения этой задачи неизвестен, а при умело выбранных больших числах любой перебор значений займёт слишком большое время. Отметим также, что знание секретного ключа позволяет провести расшифровку, применяя ту же операцию возведения в степень, что и при шифровании, но с другим показателем, а существующий алгоритм возведения в степень позволяет относительно быстро вычислять эти значения. Взломать криптосистему можно, узнав значение функции $\varphi(n)$ или разложив число n на множители, но уже для 400-значных чисел это сегодня неподъёмные задачи.

Слайд 15.

В заключение обсуждения криптосистемы RSA рассмотрим пример. Числа p, q для наглядности выбраны трёхзначными.

Этап	Описание операции	Результат операции
Генерация ключей	Выбор двух простых чисел	$p = 139,\ q = 157$
	Вычисление модуля	$n = pq = 139 \cdot 157 = 21823$
	Вычисление функции Эйлера	$\varphi(n) = (p-1)(q-1) = 21528$
	Выбор открытой экспоненты	$e = 7$
	Вычисление секретной экспоненты	$d = 6151 \quad (k = 2)$
	Публикация *открытого ключа*	$(e, n) = (7, 21823)$
	Сохранение *секретного ключа*	$(d, n) = (6151, 21823)$
Шифрование	Выбор текста для шифрования	$M = 2011$
	Вычисление шифротекст	$P(M) = M^e \bmod n = 2011^7 \bmod 21823 = 11295.$
Расшифровка	Вычисление исходного сообщения	$S(C) = C^d \bmod n = 11295^{6151} \bmod 21823 = 2011.$

Слайд 16.

Как было сказано выше, современная криптография опирается на фундаментальные математические исследования, а также технологический и алгоритмический прогресс. Но этим перечень научных дисциплин, связанных с защитой информации, не исчерпывается. В качестве примера кратко коснемся квантовой криптографии, в основу которой заложены принципы квантовой физики. Для передачи информации используются объекты квантовой механики; процесс отправки и приёма информации выполняется физическими средствами, например, при помощи электронов в электрическом токе или фотонов в линиях волоконно-оптической связи. Факт перехвата данных может рассматриваться как изменение некоторых параметров физических объектов – переносчиков информации. Технология квантовой криптографии опирается на принципиальную неопределённость поведения квантовой системы: невозможно одновременно измерить один параметр частицы, не исказив другой. Это фундаментальное физическое свойство природы известно как принцип неопределенности, сформулированный В. Гейзенбергом в 1927 г. Используя квантовые явления, можно спроектировать и создать такую систему связи, которая всегда может обнаруживать подслушивание (перехват). Это обеспечивается тем, что попытка измерения взаимосвязанных параметров в квантовой системе вносит в неё нарушения, разрушая исходные сигналы, а значит, по уровню шума в канале законные пользователи могут распознать степень активности перехватчика.

Сегодня квантовая криптография только приближается к практическому уровню использования. Считается, что это очень перспективное направление криптографии, поскольку применяемые в нем технологии позволяют вывести безопасность информации на высочайший уровень. Возможно, нам осталось лишь немного подождать, и уже очень скоро квантовая криптография будет также на слуху у всех, как криптосистемы с открытым ключом в наши дни.

Вопросы

a) Предварительные вопросы. Вопросы до лекции, позволяющие определить степень осведомленности о тематике лекции и наличие знаний, необходимых понимания лекции (если они необходимы).

1. Кто-нибудь слышал слово «криптография»? Что оно означает?

2. Читали ли вы рассказ о Шерлоке Холмсе «Пляшущие человечки»?

3. Как бы вы зашифровали информацию, которую нужно кому-то передать, сохранив в тайне для всех остальных (в том числе, и для передающего)?

b) Промежуточные вопросы. Вопросы, которые можно задать во время лекции, позволяющие определить степень освоения материала, необходимого для продолжения лекции.

1. Кусок перехваченного текста выглядит так: «ЯЭОЪ». Известно, что был применен шифр Цезаря. Расшифруйте текст.

2. Известно, что в перехваченном тексте, состоящем из 835 знаков, применен шифр простой замены, и буквы русского алфавита заменены на различные символы. Подсчет показал, что символы «%», «#» и «&» встречаются, соответственно, 75, 32 и 1 раз. Используя частотный анализ, выскажите гипотезу о том, какие буквы русского алфавита скрываются за этими символами.

3. Докажите, что $2011^7 \bmod 21823 = 11295.$

c) Итоговые вопросы. Вопросы, позволяющие определить уровень освоения материалов лекции. Ответы на вопросы.

1. С какими основными методами шифрования вы познакомились?

Ответ: шифр Цезаря, шифр простой замены, криптосистема RSA, квантовая криптография.

2. Какие области высшей математики имеют своё приложение при построении криптосистемы RSA?

Ответ: теория чисел, вычислительная математика, теория алгоритмов.

3. В чем заключаются преимущества криптографии будущего – квантовой криптографии?

Ответ: В такой системе невозможно захватить информацию, переданную через сеть, не нарушая при этом ее работы, поэтому легко обнаружить попытку прослушки информации и принять меры по её защите.

Список тем, которые можно изучать в качестве продолжения лекции или которые связаны с тематикой лекции.

1. Теория делимости целых чисел.
2. Системы счисления. Представление числа в различных системах счисления.
3. Быстрые алгоритмы распознавания простоты числа и возведения в степень по модулю.