ЛЕКЦИЯ 2

ИСТОРИЯ КРИПТОГРАФИИ. ПОЛЯ ГАЛУА

1. История криптографии

История криптографии насчитывает более 4000 лет, но лишь в 20 веке с помощью работ Шенона она была организована в науку (до этого считалась искусством).

Периодизацию криптографии можно условно разделить на 4 части:

1. **Древний Мир**: криптография использовалась как искусство; не было понятия «ключ шифрования».
2. **Средние Века**: появляются моноалфавитные шифры, полиалфавитные шифры.
3. **Новое Время**: появляются способы вскрытия шифров, причем научными подходами.
4. **XX век**: появление современной криптографии.

1.1. Криптография в Древнем Мире

Древнеиндийский трактат «Камасутра» называют одним из первых пособий, в котором описаны первые способы скрытия информации (по изначальному замыслу Камасутра является пособием по домоводству; обычно с помощью шифра женщины скрывали информацию о месячном календаре).

При строительстве пирамид во времена Древнего Египта использовались шифры в виде головоломок, скрывая информацию о менее важных лицах, чем фараоны (чиновники).

В Библии применялась техника шифрования под названием «Атбаш». Его суть состояла в том, что буквы алфавита заменялись на буквы в обратном порядке (первая буква заменялась на последнюю, вторая — на предпоследнюю, и т. д.). Когда в предсказании из Библии указывалось собственное имя (правителя, города), то это имя шифровалось с помощью Атбаша. Иначе у этой книги возникли бы проблемы со свободным распро-

странением.

В средиземноморских странах появились следующие механизмы:

1. **Скитала** — длинная палка, причем, возможно, с переменным диаметром, на которую наматывалась ленточка; после того, как ленточку намотали, на нее наносили надпись, причем надписи наносили вдоль ленты, после чего ленту разматывали.

2. **Диск Энея** — это диск, в центре которого находилась катушка с нитками, которые специальным образом продевались через отверстия. Этим обеспечивался простой способ уничтожения информации в случае перехвата курьера — катушка ниток могла быть легко выдернута из диска.

3. **Линейка Энея** — это линейка с нанесенными буквами, рядом с которыми находились отверстия; нитка надевалась на линейку, а потом завязывались узелки в нужных местах. По этим узелкам можно было восстановить сообщение.

4. **Книжный шифр Энея** — это шифр, в котором в книге тонкой иглой делаются отверстия рядом с буквами. Страницу можно посмотреть на свет и разглядеть эти отверстия.

5. **Квадрат Полибия** — это таблица, отображающая соответствие между буквами греческого алфавита и количеством факелов, которое необходимо держать в каждой из рук для шифрования соответствующего символа.

6. **Шифр Цезаря** — это моноалфавитный шифр, в котором зашифрованная буква заменялась на букву, идущую через 3 позиции по алфавиту.

Первым криптоаналитиком принято считать **Аристотеля**, который взломал Скиталу. Для этого он брал конус, наматывал на него ленту и ждал момента, пока сообщение не станет читаемым. После этого нужно было взять палку соответствующего радиуса и намотать на нее ленту.

В эпоху арабского возрождения был создан труд **«Китаб Аль Наума»** («Книга тайного языка»). Там было рассказано, что «можно шифровать со сдвигом, как делал Цезарь», а можно просто случайным образом перемешать буквы.

Учёный **Аль Кинди** показал, что этот шифр вскрывается тривиальным образом. Для нужно взять достаточно большой текст и посчитать, сколько раз каждая буква в этом тексте входит. Соответственно, та буква, которая входит больше всего раз, и соответствует самой часто встречаюшейся букве алфавита.

Статистика частоты появления букв была приведена в труде Аль Кинди (он анализировал Коран). Еще ученый пишет о том, что ему удалось расшифровать текст письма к одному из императоров: он предположил, что начало письма имеет вполне конкретный вид («Уважаемый Государь», «Ваше Императорское Величество»), как и конец («С уважением. Подпись»). Предположив это и подставив слова в начало и конец письма, получив соответствие каких-то букв, все остальное письмо расшифровать было довольно просто.

1.2. Криптография в Средние Века

В Средних Веках начинают появляться государственные организации, которые начинают целенаправленно заниматься криптографией, правда, пока не на научной основе (они придумывают техники и занимаются криптографией как искусством). Но они занимаются уже конкретно этим направлением. Они начинают перехватывать письма других организаций, других государств, придумывать шифры, которые потом будут использоваться на государственном уровне, заниматься криптоанализом.

Известные шифры того времени:

1. **Решетка Кардано** представляет собой решетку с отверстиями в рамках этой решетки. Решетка накладывалась на пустой лист бумаги, и потом внутри нее писались те буквы или части слов, которые нужно было передать. После этого решетка снималась, и пустоты заполнялись осмысленным текстом. Строго говоря, это не шифрование, а стеганография — искусство скрытия текста.

2. **Шифр Бэкона**: Френсис Бэкон предложил первый в мире двоичный код. Он писал какие-то буквы заглавными, а другие — строчными.

   Конечно, более корректно это называть **кодом** Бэкона, поскольку здесь нет ключа, в отличие от, например, шифра Цезаря.

3. **Шифр Виженера**: здесь для каждой буквы ключа указывается позиция алфавите, после ключ, повторяясь, пишется над текстом, который нужно зашифровать, и затем каждая буква сдвигается на столько позиций, какая позиция у соответствующей буквы ключа.

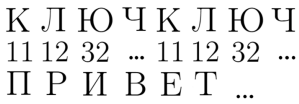

Рис. 2.1

Этот шифр является полиалфавитным, потому что используется не один вспомогательный алфавит, а несколько. Если в качестве ключа шифрования взять какую-нибудь книгу или другой текст, то этот шифр будет практически невскрываемым. Ключом здесь будет являться указание книги.

Шифр Виженера можно модифицировать: уже зашифрованный текст можно использовать в качестве ключа и зашифровывать им необходимые данные.

В 17 веке начинают появляться организации, которые занимаются созданием шифров и дешифровкой на государственном уровне.

1.3. Криптография в XX веке

К XX веку получили свое развитие теория вероятностей, зачатки теории чисел.

Кроме того, в конце XIX века появились некоторые труды по криптографии. Например, «Военная Криптография» **Огюста Керкгоффса**, в котором он сформулировал 6 принципов криптографии. Например: аппарат для шифрования должен быть относительно прост в использовании; шифрованный текст должен без проблем передаваться по телеграфу. В том числе, он сформулировал важный принцип: система не должна требовать секретности на случай, если она попала в руки врага. Имеется в виду, что если у нас есть шифровальное устройство, то мы должны допускать, что враг знает, как оно устроено. Должен быть только некий секретный материал, называемый ключом, не зная который, враг не может дешифровать текст.

Принцип Керкгоффса обязан использоваться в разработке любых, в том числе и современных систем. Он говорит о том, что стойкость алгоритма шифрования не должна быть основана на его скрытости.

Страны готовятся к войне, поэтому снова появляются организации, которые на государственном уровне занимаются криптоанализом и разработкой шифров: «Комната 40», MI-8 (США); «Бюро Шифров» в Польше. Впервые в Польше к разработке шифров, к дешифрованию привлекли математиков. До этого криптоанализом занимались, в основном, лингвисты и полиглоты. Никакого математического образования у них не было.

Появляется множество работ по криптографии (например, **Индекс Совпадений** — метод криптоанализа полиалфавитных шифров. Разработан Уильямом Фридманом в 1918 году). Начинает разделяться вонная и гражданская криптография.

Во время Первой Мировой войны произошла цепь событий, ключевую рольв в которой сыграла **телеграмма Циммермана**. Из-за того, что английские солдаты обрезали все кабели вдоль побережья Атлинтики, немцы отправили в Мексику (своеим возможным союзникам) телеграмму, которую без труда перехватили англичане. Расшифровав её, они выяснили, что Мексике было предложено вступить в Первую Мировую войну в обмен на несколько южных штатов. В американском посольстве произошла утечка информации, и о предложении Германии узнала общественность. После этого Америка

вступила в войну.

Еще до Второй Мировой войны появляются роторные машины. Самая известная из них была **«Энигма»**, которая в количестве десятков тысяч штук использовалась в Германии. Для того чтобы ее вскрыть, и были придуманы первые компьютеры.

Сам факт вскрытия германских шифров держался в секрете для того, чтобы Германия не могла поменять алгоритмы шифрования. И это иногда было тяжелым решением. В качестве примера можно взять бомбардировку Ковентри (этот город практически полностью был разрушен).

Черчиллю было известно о предстоящей бомбардировке, но он ничего не мог сделать, потому что, если бы он начал эвакуацию города еще до того, как бомбардировщики поднялись в воздух, стало бы очевидно, что Англия читает переписку Германии. Максимум, что он мог сделать — это подвезти к городу побольше пожарных и скорых машин.

Рузвельт потом в своих письмах напишет Черчиллю: «Война все чаще заставляет нас играть в богов. Я не знаю, что я сделал бы на Вашем месте».

Во время Второй Мировой войны в войсках США работает Клод Шеннон. После Второй Мировой он опубликовал несколько работ. И именно эти работы явили собой начало тематической криптографии. Они представили статистический взгляд на криптоанализ и на шифрование текстов. Именно с этого момента начали считать криптографию полноценной наукой о шифровании текста, о вскрытии информации.

2. Поля Галуа

Определение 1: Кольцо *— это множество с двумя бинарными операциями: сложением и умножением.* ♣

Определение 2: Поле *— это коммутативное аддитивное кольцо с единицей.* ♣

Определение 3: Конечное поле *или* ***поле Галуа*** *— это поле с конечным числом элементов.* ♣

Операция сложения:

$$F; \quad a, b \in F;$$

$$" + " : a + b = c \in F;$$

$$\exists "0" : \forall a \in F : \ a + 0 = a \qquad \text{— нейтральный элемент.}$$

$$\exists "-a" : \forall a \in F : \ a + (-a) = 0 \qquad \text{— обратный элемент.}$$

То же самое с операцией умножения, только мы не требуем наличия обратного элемента для нуля.

Примерами бесконечных полей могут служить множества рациональных чисел, комплексных чисел и кватернионов.

В качестве примера конечного поля можно привести группу вычетов любого числа. Рассмотрим на примере числа 7:

$$\{0, 1, 2, 3, 4, 5, 6\}.$$

Операции сложения и умножения определим следующим образом, делая всё по модулю 7:

$$\mod 7\ \{x, 1, 4, 5, 2, 3, 6\} \qquad \text{— для умножения.}$$

Рассмотрим теперь другую группу вычетов:

$$\{0, 1, 2, 3, 4, 5\}.$$

В этом случае аксиома о существовании обратного элемента не выполняется, потому что в группе присутствуют делители нуля. Например, числа 2 и 3 являются делителями числа 6, или нуля по модулю 6. Для них нельзя найти обратные элементы. Значит, эта группа не является полем.

Наименьшим конечным полем является группа вычетов по модулю 2:

$$\{0, 1\}.$$

Можно перееопределить элементы, поменяв их ролями:

$$\text{"0"} = 1, \quad \text{"1"} = 0.$$

Нужно ввести операции таким образом, чтобы:

$$1 + 1 = 1\ (\text{AND}), \quad 0 \times 0 = 0, \quad 0 \times 1 = 1\ (\text{XOR}).$$

Поля Галуа бывают двух типов.

1. z_{p} — поле, содержащее простое число элементов.
2. $GF(p^{\text{n}})$ — здесь число элементов является равным простому числу в некоторой степени. Элементы этого поля можно прелставить в виде многочленов таким образом, что коэффициенты этмх многочленов будут принадлежать полю z_{p}.

   Операция сложения определяется сложением соответствующих степеней, причём аргументы берутся по модулю числа p.

   Операция умножения определяется как обычное умножение многочленов, но при этом добавляется аргумент «модуль» — некий неприводимый многочлен.

Пример 2 Рассмотрим $GF(9)$:

$$0,\ 1,\ 2,\ x+0,\ x+1,\ x+2,\ 2x+0,\ 2x+1,\ 2x+2;$$

$$/x^2+1 \qquad \text{— модуль.}$$

В операции сложения берём результат по модулю 3.

В операции умножения мы можем получить многочлен большей степени, чем помещается в поле, так что его приходится брать по модулю неприводимого многолчена (без него операция умножения неопределена). $*$

Пример 3 $GF(2^3)$ — в этом случае коэффициенты могут быть 0 или 1 (они принадлежат полю z_2).

$$0,\ 1,\ x,\ x+1,\ x^2,\ x^2+1,\ x^2+x,\ x^2+x+1;$$

$$(x+1)+(x^2+1) = x^2+x.$$

Также элементы поля можно представить в двоичном виде:

$$0, 1, 10, 11, 100, 101, 110, 111.$$

$$11 + 101 = 110\,\text{XOR}.$$