

Мат. метод разрещения крип-чесей

1. Снажие разречих
2. Криптография

03.09.
2014
лекция
1

Снажие разречих

преобр-е разречих, с целью удаления из них
дополнит. разречих

Различие от кодир-и:

в кодир-е: с целью иници-а ошибок

но, Снажие не всегда удаляет ошибки

$$\Sigma : A^* \rightarrow A^*$$

снажие

удаляемые слова пр. к.

бено их 2^k штук

этих слов удаляются из всех и хватает.

Кодир-и снажие: $\frac{S_0}{S_1}$ иског. обсле
 $\in (0, \infty)$ регуляторющее обсле

?
кодир-е
это снажие

но не изб. ошибки должны |

хорошее снажие: 0 лег-т

плохое снажие \rightarrow не удаляемые слова | 1 |
записываются в ре-гы

$$\Rightarrow \frac{S_0}{S_0 + 1}$$

Бы. АНР \rightarrow Бы. АНР
ИСТ-Л \rightarrow [кодир] \rightarrow какая-бы-и \rightarrow Лекодир \rightarrow Регулятор

↑
(из-за ошибок)

1
2

Логор - алг-м преобр-я данных *(Архиватор, Уникальн.)

$$\Sigma : A^* \rightarrow B^*$$

$A = \{a_1, \dots, a_k\}$ - входящие элементы

$B = \{b_1, \dots, b_S\}$ - выходной

Лексикер { Установление данных, Решение задач, Установление

алгоритм:

- инициатор без начальных данных { более универсальная)

- с начальными

Мог решать лексикер без нубора данных

Источник

- с избр. вероятностями

- без избр.

Источник данных: $\left(\begin{matrix} a_1, \dots, a_k \\ p_1, \dots, p_k \end{matrix} \right) \Rightarrow \sum_{i=1}^k p_i = 1$

p_i - вероятность появления на выходе

p_i - первое из. или группу \rightarrow Бернштейнский источник

Марковский ист-к порядка t - вероятность появления a_i в t -м избр. от t -го предыдущего. $P(a_i | a_{i-1}, \dots, a_{i-t})$

{ Обычно бывает неизменяющийся для $i > t$ }

Характеристики: считаются:

1. Степень сходимости

2. Скорость сходимости, увлечения

3. Временное значение

4. Рекуррентный, паспортный показатель устойчивости

коэф-т

Строение кодирования $\Sigma : A \rightarrow B^*$

$$a_i \rightarrow b_i, |b_i| = l_i$$

$$b_i \in B^*$$

$$C(\Sigma) = \sum_{i=1}^k p_i l_i$$

"мат. опис. решения ког. сеява"

Применение $C(\Sigma)$

Ког. алг-ы разделенное, если из t постр-я $b_{i_1} \dots b_{i_s} = b_{j_1} \dots b_{j_t} \Rightarrow s = t$ $b_{ik} = b_{jk}$

$\left\{ \begin{array}{l} t \text{ постр-я - однозначно разбить на кодовые} \\ \text{сексы} \end{array} \right\}$

Ког. алг-ы предиксиное, если никакое кодовое слово не является начальном пр. ког. слова

$\left\{ \begin{array}{l} \text{Проф. ког. всегда разделено} \end{array} \right\}$

0,1001,010 - не предиксиное, не разделенное

0,101,100,1101 - предиксиное.

Теорема (Крафта): с длиной k/c l_1, \dots, l_k
для одн. ког. предикси. $\frac{1}{c} \leq \frac{1}{l_i}$ $\forall i$
вопрос \Rightarrow ког. предиксиное \Leftrightarrow код Крафта - минимальный

$$\sum_{i=1}^k \frac{1}{l_i} \leq 1$$

Субоптимальный ког?

A-BO:

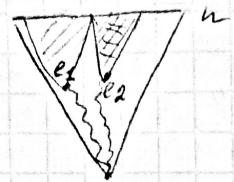
?

ког. чудо
шт-8
кошель
не предик

\Rightarrow Алг. ког. делит на подблоки в гл. переве.
Предикси. ког: слово определяет место в алг-е
и сдвигает её сдвигает

2

Рассмотрим дерево глубиной n
 $N > l_1 + k \in \{1, \dots, k\}$

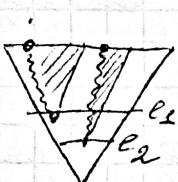


от l_1 отходит чистое дерево
по утверждению
оно отходит на m и
ког. если 2^{n-l_1}
аналогично для l_2

{ не пересек-ся с l_1 . предикс. ког.
 l_1, l_2 не являются на одинаковых }
уровнях

$$\sum_{l=1}^k 2^{n-l_1} \leq 2^n$$

\Leftarrow



Берем l_1 , отмечаем
берем свободную вершину из
чистого верх. висе, выпускаем
по l_1 , от постн. верне.
послед-ем чистое дерево
по листам n .

Рассматриваем l_2 , возвращаем её. Вернем n по
рассуждениям об. верне на конц. или
т.к. возвращ-ся перв-го кр.-тик.

Все эти деревья не пересек-ся, т.к. длина
свобод. вершинов.
Это под-тверждение. \blacksquare

Теорема (Макмиллана)

Число способов размещения k листьев в дереве глубины n с различными кратными
длиной листьев, ирост. возвращ-е перв-го края
Макмиллана.

$\Delta - 60^\circ$

\Leftarrow По пред. теореме
ког. пред. лог. 60° -ы размещаются

\Rightarrow Рассмотрим $(x_1 + x_2 + \dots + x_k)^m =$

$$= \sum_{i_1, \dots, i_m} x_{i_1} \dots x_{i_m}$$

i_1, \dots, i_m
 $\in \{1, \dots, k\}^m$

$$x_i^o = \frac{1}{2^{l_i^o}} \left(\sum_{i=1}^k \frac{1}{2^{l_i^o}} \right)^m = \sum_{i_1, \dots, i_m} 2^{-l_{i_1}^o - \dots - l_{i_m}^o} = \begin{cases} \sum_{i=1}^k 2^{-l_{i+1}^o + \dots + l_m^o} & l_{\max} = \max_i l_i^o \\ 0 & \text{else} \end{cases}$$

$$= \sum_{j=l_{\max} + l_m^o}^{m l_{\max}} \sum_{j=l_{i_1}^o + \dots + l_m^o} 2^{-j} \leq \sum_{j=1}^{m l_{\max}} 2^{-j} \cdot 2^{l_{\max}^o} = m l_{\max}^o$$

{Сумма ряда от j до $m l_{\max}^o$ } $\leq 2^{-j}$

$$\sum_{i=1}^m \frac{1}{2^{l_i^o}} \leq \sqrt[m]{m l_{\max}^o}$$

$$\lim_{m \rightarrow \infty} \sqrt[m]{m l_{\max}^o} = 1.$$

ког. разбивка
 \rightarrow нет дублирования
 исключено
 \rightarrow каждая исключена
 единственный раз

■

Метод Парто.

$$\text{Def - k} \quad S = \begin{pmatrix} a_1 & \dots & a_k \\ p_1 & \dots & p_k \end{pmatrix}$$

$$p_i^o \geq p_j \quad i \leq j$$

a_1	0	1
\dots		
a_j	0	1
\dots		
a_{j+1}	1	0
\dots		
a_k	1	0

Разбивка на 2 части

так, что

$$\sum_{i=1}^j p_i^o \geq \sum_{i=j+1}^k p_i^o$$

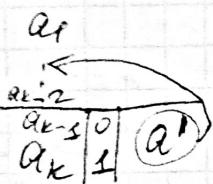
Первое место присвоивается 0
 второе 1.

Далее аналогично \Rightarrow остальные места

В итоге получается префикс. код



алгоритм Капмана



Принцип баланса q'
и k -распределения
 $P'_{k-1} = P_k + P_{k-1}$

q' ставится к оставшимся
в текущем состоянии вероятностям
и если это не засчитано ранее, то заносится
в k -распределение
кап. Капмана

кап. Кап. алгоритм оценки

Кап. алгоритм оптимального, если оценивается
коэффициент этого нода наименее всего для
всех нодов, кодирующихся данным нодом

1-я
над
Самые
нет над

Задача

25,4

1-го, 2-го L.P. и k. Кап

p_i^o симметрический

$$p_i^o > \sum_{j=i+1}^n p_j^o$$

тогда оно поглощает
и нет для него L_P .

10,09
проверка
g

алгоритм Капмана
проверка симметрии



933

$k \bmod q-1$

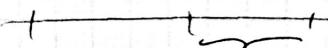
$0 \rightarrow q-1$

$1 \rightarrow \text{однородный } q \text{ на перв. итерации}$

$i \in \{2, \dots, q-2\} \rightarrow i$

Теорема:
ког Хардмана описано.

Более ког Хардмана вероятность не избранного



стягивается на оси-х стабильных k -меню

разсеяние испытывает в стат. в пределе, разсеяние
стягивается в поб. окне
(перетягивающее дерево)

{ Абдуктивное - много сценариев }

Абдуктивное кодированием :

буква $\mapsto k/c$

Блоковое кодир

блок $\mapsto k/c$

1-го Теорема Ул. Вс.: $S = (p_1, \dots, p_k) ; p_1 \geq \dots \geq p_k$

Лемма 1:

~~если блок - при упорядочении~~

в k бл. ког разброс k/c упорядочен по убыванию:

$l_1 \leq l_2 \leq \dots \leq l_k$

1-го

блок \in ост. кога не $= S$

кажд
бер.и-
артиль
зг.Хар
→кои

$$\begin{aligned}
 & q_1 q_2 \dots q_i \dots q_j \dots q_k \\
 & p_s p_a \dots p_i \dots p_j \dots p_k \\
 & \sum_1 l_1 l_2 \dots l_i \dots l_j \dots l_k - \text{out.} \\
 & \sum_2 l_1 l_2 \dots l_j \dots l_i \dots l_k \quad \text{буквы сдвигаются} \\
 & \text{Например, } p_i > p_j, l_i < l_j. \quad \text{Однако } \Sigma_1 = p_i l_i + p_j l_j \\
 & \Sigma_2 = p_j l_j + p_i l_i
 \end{aligned}$$

$$C(\Sigma_1) = \sum_{i=1}^k p_i l_i$$

$$C(\Sigma_2) = C(\Sigma_1) - \Sigma_1 + \Sigma_2$$

$$0 < \Sigma_2 - \Sigma_1 \text{ т.к. } \Sigma_1 - \text{out.}$$

$$p_i(l_j - l_i) + p_j(l_i - l_j) > 0$$

$$(p_i - p_j)(l_j - l_i) > 0$$

противоречие □

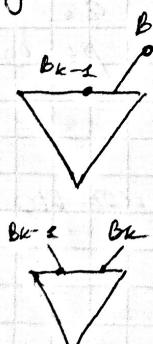
Лемма 2

В конт. переключение кого гнезд b_{k-1} и b_k для $k \leq c$ наименее вероятно для $\alpha_{k-1} \alpha_k$
состоит из сдвигов, не явл. гнездом

$$B_{k-1} = B_0, B_k = B_1$$

также, что

предполагаем, что это гнездо



такое out. когда это сдвигается
т.к. иначе b_k и b_k сдвигались
один сменяя другой
это будет тоже переключение
но со стоящим впереди гнездом
но не из-за такж. сдвигов \Rightarrow

такого тоже быть не может
также иначе другой из них
не сменяется \Rightarrow



$$A = \begin{pmatrix} a_1 & \dots & a_k \\ p_1 & \dots & p_k \end{pmatrix} \quad p_1 \geq \dots \geq p_k$$

$i \in \overline{1-k}$

$$\sum: a_i \rightarrow B_i \quad \text{- некор. кодир-е} \quad B_{k-1} = B_{k-1}' \ 0$$

$$B_k = B_k' \ 1$$

Редукц. нет-к (ориг-е с кор-бов не символов)

$$A' = \begin{pmatrix} a_1 & \dots & a_{k-2} & a_{k-1}' \\ p_1 & \dots & p_{k-2} & p_{k-1}' \end{pmatrix} \quad \text{т.е. } p_{k-1}' = p_{k-1} + p_k$$

$$\sum': a_{k-1}' \rightarrow B_{k-1}'$$

Лемма 3:

Если кодированием \sum' редуцированного алфавита A' однозначно и префиксно, то кодир-е \sum исходного алфавита A однозначно и префиксно.

Д-бо:

Префиксность

Слова отмеч-е только first двух нач. символов

"

Однозначн

$$\begin{aligned} C(\sum) &= \sum_{i=1}^k p_i l_i = \sum_{i=1}^{k-2} p_i l_i + p_{k-1} (l_{k-1}' + 1) + p_k (l_{k-1}' + 1) = \\ &= C(\sum') + \underbrace{p_{k-1} + p_k}_{V_0} \end{aligned}$$

Префиксность \sum -неодн., а \sum' -одн.
т.о. \sum кодир-е нет-к алфавита A

Построим \sum'^1 . аналогичн. однозначн

$$C(\sum^n) = C(\sum'^1) + \underbrace{p_{k-1} + p_k}_{V_0}$$

$$C(\tilde{\Sigma}) < C(\Sigma)$$

$\rightarrow C(\tilde{\Sigma}') < C(\Sigma')$, но Σ' -один из архиворем

1-го Георгиев
по типу (иер-к землемера и пасек)
исследований З. Радиев

Kog Менюма

Принцип:

S:

a_i	p_i	$b_i = \sum_{j=1}^{i-1} p_j$	b_i переборно без отсечки	b_i переборно с отсечкой	kog Men.
Q_1	$1/4 \leq 0,36 < 1/2$	$b_1 = 0$	$0,0...0$	2	00
Q_2	$1/8 \leq 0,18 < 1/4$	$0,36$	$0,0101110$	3	010
Q_3	$0,18$	$0,54$	$0,0101110$	3	100
Q_4	$0,12$	$0,72$	$0,0101110$	4	1011
Q_5	$0,08$	$0,84$	$0,0101110$	4	1101
Q_6	$0,08$	$0,92$	$0,0101110$	4	1110

$$\frac{1}{2e_i} \leq p_i < \frac{1}{2e_{i-1}}$$

$$\begin{array}{r} 0,36 \\ \hline 0,72 \\ \hline 1,44 \\ 0,88 \\ \hline 1,76 \\ 1,52 \\ 1,04 \\ 0,08 \end{array}$$

$$\begin{array}{r} 0,54 \\ \hline 1,08 \\ 0,16 \\ 0,32 \end{array} \quad \begin{array}{r} 0,72 \\ \hline 1,44 \\ 0,88 \\ 1,76 \\ 1,52 \end{array} \quad \begin{array}{r} 0,84 \\ \hline 1,68 \\ 1,36 \\ 0,72 \\ 1,44 \end{array}$$

00
01
100
101
110
111

Kog Men., \neq не одн.

Установка ког. Men. убираем из-за симметрии

Kog Men. префиксальный
0,58

2/3

$$p_i < \frac{1}{2^{l_{i-1}}}$$

$$p_i < 2^{1-l_i}$$

$$l_i < 1 - \log p_i$$

$$A = \begin{pmatrix} a_1 & \dots & a_k \\ p_1 & \dots & p_k \end{pmatrix}$$

$$C(\Sigma_m) = \sum_{i=1}^k p_i l_i < \sum_{i=1}^k p_i (1 - \log p_i) = \sum_{i=1}^k p_i - \sum_{i=1}^k p_i \log p_i = 1 + H(A),$$

згд $H(A) = -\sum_{i=1}^k p_i \log p_i$ - энтропия нес. бэр. A .
 → "мера неоп-ти"

Теорема Шеннона

$$C(\Sigma_m) = 1 + H(A)$$

Если неф-к перескачиває $\rightarrow H=0$
 одн.перескачиває $H=\max (-\log k ?)$

Свойства энтропии нес. Бернулли

1. $H(A) \geq 0$
2. $H(A) \leq \log k$

{Рассмотреть
ненул. шанс не более k }

3. Неп-ко Шеннона

$$\sum_{i=1}^k q_i = 1 \quad -\sum_{i=1}^k p_i \log q_i \geq H(A)$$

Блокир. кодир-е
равноз. вероятн. (в нее не залог)

$$\text{неф-к } B = \begin{pmatrix} b_1 & \dots & b_k \\ q_1 & \dots & q_k \end{pmatrix}$$

$$\text{неф-к } AB = \begin{pmatrix} a_1 b_1 & \dots & a_1 b_k \\ \vdots & \ddots & \vdots \\ a_N b_1 & \dots & a_N b_k \end{pmatrix}; \quad A^N = \begin{pmatrix} (a_{11} a_{12} \dots a_{1N}) \\ \vdots \\ (a_{N1} a_{N2} \dots a_{NN}) \end{pmatrix}$$

$\sum^N: (a_{11} \dots a_{NN}) \rightarrow B$ - блокир.
символы
блохир. блокир-е

Стандартн. такого кодир-я $C^N = NC(\Sigma)$

$$4. \mathcal{H}(A^N) = N \mathcal{H}(A)$$

$\mathcal{Df}_{0,5}$
1-66 Н еб-60
сформулировано для двух « β ».

Теорема (Шеннона)

Гарноть кодир-я $C(\Sigma)$ не меньше энтропии исходной $\mathcal{H}(A)$ и \exists шенноновское кодирование, способность которого $C(\Sigma) = \mathcal{H}(A) + \epsilon_N$, где $\epsilon_N \rightarrow 0$ при $N \rightarrow \infty$

примеч

$$(C(\Sigma) \approx \mathcal{H}(A))$$

1-60:

$$C(\Sigma) = \sum_{i=1}^k p_i l_i \quad \textcircled{3}$$

$$l_i = -\log \frac{1}{2^{q_i}} \quad \text{делаем замену } q_i = \frac{l}{2^i}$$

$$\textcircled{3} - \sum_{i=1}^k p_i \log q_i \quad \textcircled{3}$$

$$\sum_{i=1}^k \frac{1}{2^i} p_i \leq 1 \quad (\text{если первое})$$

тогда $q_0 = 1 - \sum_{i=1}^k q_i$

Добавим в Σ единичную вероятность p_0

$$\textcircled{3} - \sum_{i=0}^k p_i \log q_i \geq \mathcal{H}(A)$$

$$C(\Sigma) \geq \mathcal{H}(A)$$

$$C(\Sigma) = \mathcal{H}(A) + 1$$

$$C(\Sigma^N) = NC(\Sigma)$$

$$C(\Sigma^N) = \mathcal{H}(A^N) + 1$$

$$\rightarrow NC(\Sigma) = N\mathcal{H}(A) + 1$$

$$C(\Sigma) = \mathcal{H}(A) + \frac{1}{N}$$

по итогам Теореме
использовались кодом Шеннона
и Болгарии из подтверждения

ср. мн. код. симв. не лучше алг-ра
 $C^N = \begin{cases} C(\Sigma), & \text{если кодир-е } A \\ \frac{1}{N} C(\Sigma^N), & \text{если кодир. } A^N \end{cases}$
В Г. лучше исп. C^N вместо C

□

Критерий разделимости кодированных последовательностей

Рассмотрим $A = \begin{pmatrix} a_1 & \dots & a_r \\ p_1 & \dots & p_r \end{pmatrix}$; $\Sigma: Q_j \rightarrow B_j$
 $B_i \in B^*$, $B = B_1, \dots, B_r$.

Слова B_i будем называть лексематическим кодом

$B_j = B' B_{j1} \dots B_{ji} B''$. - критерий разделимости не
 при выполнении условия: $\left\{ \begin{array}{l} B' - \text{некоторый префикс} \\ B'' - \text{ее суффикс} \end{array} \right.$
 1. B_j -эл. кодом и $B_{i1} \neq B_j$

2. B' -эл. суффиксом в некот. других критер. разделим.
 на эл. кодов

3. B'' -эл. префиксом в некот. др. критер.
 разделим. на эл. коды (B' и B'' не являются префиксами)

4. $B' \cap B''$, где "1"-первая часть
 допускается такое пересечение

Пример

$$\begin{aligned} a_1 &\rightarrow b_1 = \overbrace{b_1 b_2}^{1} \\ a_2 &\rightarrow b_2 = \overbrace{b_1 b_3}^{2} \overbrace{b_2}^{1} \\ a_3 &\rightarrow b_3 = \overbrace{b_2 b_3}^{1} \\ a_4 &\rightarrow b_4 = \overbrace{b_2 b_1}^{1} \overbrace{b_2 b_2}^{2} \overbrace{b_3}^{1} \\ a_5 &\rightarrow b_5 = \overbrace{b_2 b_2}^{1} \overbrace{b_1 b_2}^{2} \overbrace{b_3}^{1} \end{aligned}$$

$$|B_i| = l_i; \quad L = \sum_{i=1}^r l_i; \quad w = \max$$

Теорема (Маркова А.А.)

Чтобы проверить разделимость кодированных достаточно рассмотреть последовательность во входном алфавите символов не более $N(\Sigma) \leq \frac{(w+1)(L-w)}{2}$

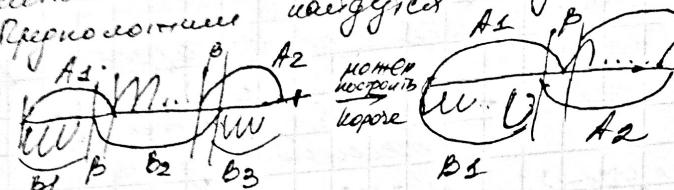
Л-бо:

T_1

T_2

B_5

если в одну строку наше правило не
использует все первые. Использовать правило в
строке в то же самое время с тем
которое не используется в одинаковой прописке,
символах



Если первое правило, то оно сам. прописке, это же
все р. правила.

Однако как это-то один egg/прописка.

$$|B_j| = l_j \text{ кон-бо в строке слова } l_j - 1$$

$$\sum_{j=1}^k (l_j - 1) = L - k - \text{число строк сверху из числа}$$

число верхних правил.

Удобно. Тогда получим для egg/прописки первых

$$\# L - k - \frac{d}{2} + \frac{k}{2} = \frac{L - k + d}{2} - \text{число}$$

длинных строк

Чтобы
в конце
столбца

иметь количество строк w

$$\frac{L - k + d}{2} (w + 1) \geq N(\Sigma)$$

длина постро-
в бинарной
арифм.

Теорема 2 (Маркова)
 Кодирование Σ не для разделяемое \Leftrightarrow в чарте
 Маркова существует преобразование π из нуля в
 единицу.

1-60
 Пример Маркова:

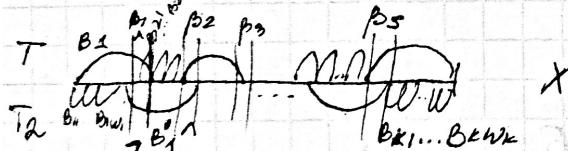
$$G = (V, E), V = (S \cap P) \cup \{"1"\}$$

S -мн-во сурсов, P -мн-во целевых.
 в началь. расп. в $S \cap P$.

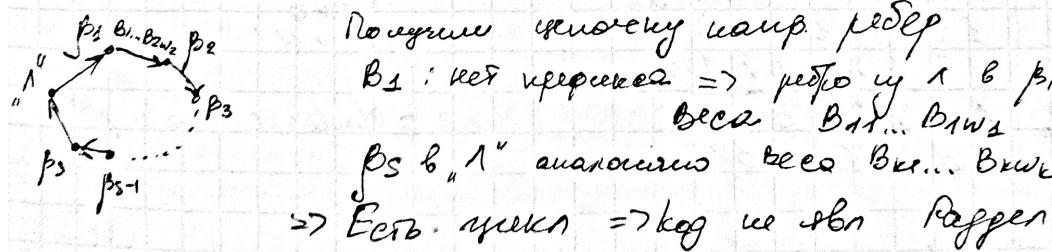
Ребро с весом $B_{i_1} \dots B_{i_k}, E, \text{если } f\beta' B_{i_1} \dots B_{i_k} \beta'' = B_j$
 Ребро содержит $\beta' \in \beta''$
 Оно направлено из β' в β''

нечт.
 бесц.
 - конеч.
 или
 "1"

Пример код. переход
 из состояния B_1 в конф. альфа
 Задача разбивка на код. сист. 24.09.
 Лекция 4.



Конечно, это впр. М. неавтомат генер., эф. нач. состоян.
 м-трансформация кодов
 Все β_1, β_3 - это есть как генер. и целевые. - это же вероят. в пр. М.



Повторение цепочки нач. ребр

B_1 : код целевое \Rightarrow ребро из 1 в β_1
 веса $B_{1w1} \dots B_{1w3}$

β_3 в "1" аналогично веса $B_{3w1} \dots B_{3w3}$
 \Rightarrow Ест. генер. \Rightarrow код не для Rabin.

Обратно: аналогично, только в обр. стороны \square

Пример:

$$\Sigma: a_1 \rightarrow B_1 = CC$$

$$a_2 \rightarrow B_2 = \overbrace{CC}^1 a$$

$$a_3 \rightarrow B_3 = \overbrace{CCC}^1 a$$

$$a_4 \rightarrow B_4 = \overbrace{AA}^1 a$$

$$a_5 \rightarrow B_5 = \overbrace{AB}^1 a$$

$$V = \overbrace{A}^1, \overbrace{A}^1, \overbrace{A}^1, \overbrace{B}^1, \overbrace{A}^1$$



Решка нее не
пересекают

aaa... многое добавить, некоторые места, места
не погружаются в
шаблон: $\overbrace{A}^1 \overbrace{CC}^1 a \overbrace{B}^1 \overbrace{CC}^1 a \overbrace{A}^1$

Аддукционное методом синтакс

Аддук. ког. Харес.
-ие слн. опт.

Ког "Сонка куэр" Б.Я. Рыбко.

$$W = d2 131d 233$$

1	d	d	1	3	1	2	2	3	3
2	1	1	2	1	3	1	1	2	2
3	3	3	3	2	2	3	3	1	1
	<u>1</u>	<u>1</u>	<u>2</u>	<u>3</u>	<u>1</u>	<u>2</u>	<u>3</u>	<u>1</u>	<u>3</u>
нумерация слогов	2	1	2	3	2	3	1	3	1

$$\begin{matrix} 2 \rightarrow 10 \\ 1 \rightarrow 0 \\ 3 \rightarrow 11 \end{matrix}$$

В арифе: сонка 95

Lempel, Ziv

Методы: LZ 44, LZ 48

метод
сжатия
окна

метод
сжатия
словаря

LZ 77

$w = abba-bbaab$... находит $\exists p$ такое
что p имеет $\exists t$. оконч. окн. = 8.
и в архиве. которое берет в окне

(1, 4, 3)

найден номер t ищется
 $t-8$ подстр. ищется
 $t+20$
ищется

окн. пропись

окно C;

(0, "C")

в борде t передает
найдено $t+20$ ищется

aab:

(-1, 5, 3)

забывает гаджет

подстрок.

затем проверяется

окно на предмет проп.

и т.д.

Помимо прописи проверяется
на подстр., которую для чистки
 $(1, 4, 3) \rightarrow (4, 3)$

В архиве: под строка
и подстроки окно, с $t-20$
ищются

Как декодировать?
из подстр. возвращается блоки

LZ 78

$w = \overbrace{aaa}^a \overbrace{bba}^b \overbrace{baab}^a \overbrace{aa}^b \dots$

a	aa	b	ba	baa	baaa	bab	"
1	2	3	4	5	6	7	
$(0, "a")$	$(1, "a")$	$(0, b)$	$(3, a)$	$(4, a)$	$(5, a)$	$(4, b)$	

если ищется подстроку
ищется подстроку
в строке ищется
к ищется
ищется

Помимо

строки

т.д. не передан

в строке, ищется

В архиве: ищется

декодир-е;

борт-е ищется

Арифметический ког

Кодирующее блоками, группами k -битов вспомогательное языковое

$$A = \{a_1, \dots, a_L\}, |A| = k$$

кодируется
но $i=1, k$

послед-в в (в арг. A)

W разбивается на блоки gr: L

$$w = \underbrace{\overbrace{|}^e \overbrace{|}^e \dots \overbrace{|}^e}_{L} \underbrace{|}_{L}$$

это же подразумевается в языке.

"арифметическое сопр-вие"

на языке L оп-ции генер

Берет-ся единица

Однодорожечка из 0 и 1

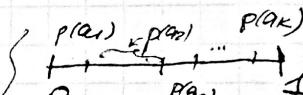
$D(a_i)$ -часть языка a_i на языке L

$$\# p(a_i) \neq \frac{D(a_i)}{L}$$

тогда
запись
из блоков

$$Q \text{ равна} : p(a_i) = \frac{D(a_i) + d}{(L) + k}$$

$$\text{Тогда } \sum_{i=1}^k p(a_i) = 1$$



L разбивается на блоки
gr L

раскладывается в эти
периоды

$(a_1, \dots, a_L) \leftarrow$ кодируется как блок
кодируется по $j \in \mathbb{Z}_L$

$$\text{коэффициенты} : b_i = \sum_{t=1}^{L-1} p_{it}, \quad \bar{b}_1 = 0$$

$$a_1, a_2, a_3, \dots, a_k$$

$$b_1 = 0, b_2 = 1, b_3 = 1 \text{ ... начиная с j}$$

Упр-ва с кот. работают
чт-го обозначает b_i , т.
 $b_i = 0, 1, \dots, k-1$

$$b'_j = b'_{j-1} + b_j \cdot \delta_{j-1}$$

$$b'_j = b'_{j-1} + b_{j+1} \cdot \delta_{j-1}; \quad \delta_j = b'_j - b'_j$$

Без-значка языка языка

|D-язык. языка отсутствует|

Диаграмма предиката.

θ_2

г1. $F = \log \delta E T + C$ излучение

1-тв:

Арифм. код - предикативный

0,55

df

Сравнение различных методов

01.10
Лекция 5.

Арифм. код	L2-47	L2-48	Типич. харак.	Сопка ким?	
?	2-4	2-3	>8	?	Степень снижения
2. Нижняя	Всесоцки	Всесоцки	пропорц. К	очень быстро	2. Скорость изменения
3. Сущ-е Всесоц от увелеч. дл. дока	10:1	3:2	?	?	3. Скорость изменения
4. \rightarrow II-	много изменяется всеобщее значение + малые значения разных	Хуже L2-47 по 1 и 2	Громоздкий алгоритм	?	4. Время, "
5. * Нужно арх. хар на 1-10% (но сдвиги) * не требует коррекции на вероятностях * В2-3 раза быстрее стационар. метода + в ким. случае не увеличение ошибок	<ul style="list-style-type: none"> зр-ен на разные виды данных различные алгоритмы длительность 	<ul style="list-style-type: none"> текстовое различие значениях 	Используется во всех алгоритмах	Используется для выделения разных в ОЗУ	5. " + " ПК

Мет-к А.

3. Изменение вероятности ошибок при изменении шага

$$A = \begin{pmatrix} a_1 & \dots & a_k \\ p_1 & \dots & p_k \end{pmatrix}, p_i - \text{шаги}.$$

Будем рассмотреть блоковое коды

Кодир-е $\Sigma^N : A^N \rightarrow B^*$.

$a \in A^N$

Вероятность появления блока a при N = произвр-е вероят.

(k^N -блоков, образуемых блоки)

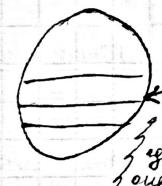
Определение:

m_i - частота появления символа a_i в блоке $\text{gr}_i N$

$$\sum_{i=1}^k m_i = N$$

$$\text{Вероятность появления } a \text{ в блоке } \text{gr}_i N = \frac{m_i}{N}$$

Мн-во N -блоков - разделено на "рабочие" и "искусственные"



$T(m_1, \dots, m_k)$ - мн-во блоков с заданными рабочими частотами в первом блоке. Тогда мы будем брать блоки из gr_i . Рабочий блок - блок с рабочими частотами в первом блоке. Искусственный блок - блок с рабочими частотами в первом блоке.

Оценка $|T(m_1, \dots, m_k)| = \frac{N!}{m_1! \dots m_k!}$ - статистика максимумов

как-то $\leq (N+1)^k$

или $\leq \min(m_i) \text{ or } 0 \text{ if } m_i = 0$

Теорема (Рыжихова)

$\forall \epsilon > 0 \exists N_0$ такое, что при $N > N_0$ выполняется. Блоковой код со средней ошибкой $\log(N)$ символов, превосходит среднюю ошибку, определяемую $C^* \leq H(A) + \epsilon N$, где $\epsilon \rightarrow 0$ при $N \rightarrow \infty$

1-60

Блоковое слово

$$\overbrace{\log(N+1)}^{k \log(N+1)} + \overbrace{\log|T(m_1, \dots, m_k)|}^{\text{число}}$$

$$C(\Sigma^N) = \sum_{i=1}^N p(a_i) \cdot l_i \leq \sum_{i=1}^N p(a_i) (k \log(N+1) + \log|T(m_1, \dots, m_k)|)$$

$$\mathbb{D}/\mathcal{F} |T(m_1, \dots, m_k)| = \frac{N!}{m_1! \dots m_k!} \leq 2^{N H(\frac{m_1}{N}, \dots, \frac{m_k}{N})}$$

③

$$\text{def } H\left(\frac{m_1}{N}, \dots, \frac{m_k}{N}\right) = -\sum_{i=1}^k \frac{m_i}{N} \log \frac{m_i}{N}$$

$$\textcircled{2} \quad \sum_{i=1}^k p(u_i) \left(k \log(N+1) + 2 + N H\left(\frac{m_1}{N}, \dots, \frac{m_k}{N}\right) \right) \leq$$

$$\textcircled{3} \quad -N \sum_{j=1}^k \frac{m_j}{N} \log \frac{m_j}{N} \stackrel{\substack{\text{неп. бд} \\ \text{иначе}}}{\leq} -\sum_{j=1}^k m_j \log p_j =$$

$$= -\sum \log p_j^{m_j} = -\log p(u_i)$$

$\begin{cases} p(u_i) = \prod p_j \\ \log p(u_i) = \sum \log p_j \end{cases}$

$$\textcircled{4} \quad -\sum_{i=1}^k p(u_i) \log p(u_i) + \sum_{i=1}^k p(u_i) / k \log(N+1) + 2 =$$

$$= H(A^n) + k \log(N+1) + 2$$

$$C^n = \frac{c(\Sigma^n)}{n}$$

$$c(\Sigma^n) \leq H(A^n) + k \log(N+1) + 2$$

$$NC^n \leq NH(A) + k \log(N+1) + 2$$

$$C^n \leq H(A) + \underbrace{\frac{k \log(N+1) + 2}{n}}_{n \rightarrow \infty \rightarrow 0} \quad \blacksquare$$

Keg Абеннигена 1968

Всегда $n \geq 3$
Задано $n \in \mathbb{N}$
Начальные условия: $n_0 = 0$, $n_1 = 2^{n-2}$

08.10.
Лекция
6

Она очень быстро растет

$$n_2 = 2^0 = 1$$

$$n_3 = 2^1 = 2$$

$$n_4 = 2^2 = 4$$

$$n_5 = 2^4 = 16$$

$$n_6 = 2^{16} = 65536$$

$$n_7 = 2^{65536}$$

Некоторое обобщение
 $\log^i x = \underbrace{\log \log \dots \log}_{i \text{ раз}} x$

$\text{Bin}_i x$ — общая непрерыв. величина
 $\text{Bin}'_i x$ — $\text{Bin}_i x$ для первого единичного

$$\log^* x = i \Leftrightarrow n_i \leq x < n_{i+1}$$

$$\log^* x = \underbrace{\log L \log L \dots L \log x - 1}_{i-1} - 1 = 1$$

Пример:

$$\log^* 37 = 4 \quad \text{т.к. } n_4 \leq 37 < n_5$$

$$\lfloor \log 37 \rfloor = 5, \lfloor \log 5 \rfloor = 2, \lfloor \log 2 \rfloor = 1$$

Лог. нечетности

$$\text{Lev } x = \underbrace{1 \dots 1}_{\log^* x}, 0, \underbrace{\text{Bin}'_1 \lfloor \log^i x \rfloor, \text{Bin}'_2 \lfloor \log^{i-1} x \rfloor, \dots, \text{Bin}'_k x}$$

Пример
 $x = 37$

$$\text{Bin}' 37 = 00101$$

$$1 \lfloor \log 37 \rfloor = 5, \text{Bin}' 5 = 01$$

$$2 \lfloor \log 5 \rfloor = 2, \text{Bin}' 2 = 0$$

$$3 \lfloor \log 2 \rfloor = 1$$

$$\text{Lev } 37 = 1110 \xrightarrow{\text{последний}} 01, \underline{00101}$$

Прич

последний

Вопрос: какое значение имеет $\text{Lev } x$?

$\log^* x$ — общая величина, где больше всего единичных нулей

$$\text{Число единичных единиц} |\text{Lev } x| = \log x + \log(\log(1+o(1)))$$

\Rightarrow лог. нечетн. — непрерывность

1. Рекафарь, 1980 ког. НСБ - предложил метод
 2. Рекафарь, определил изложение чу к. НСБ
 (референс)

DFF

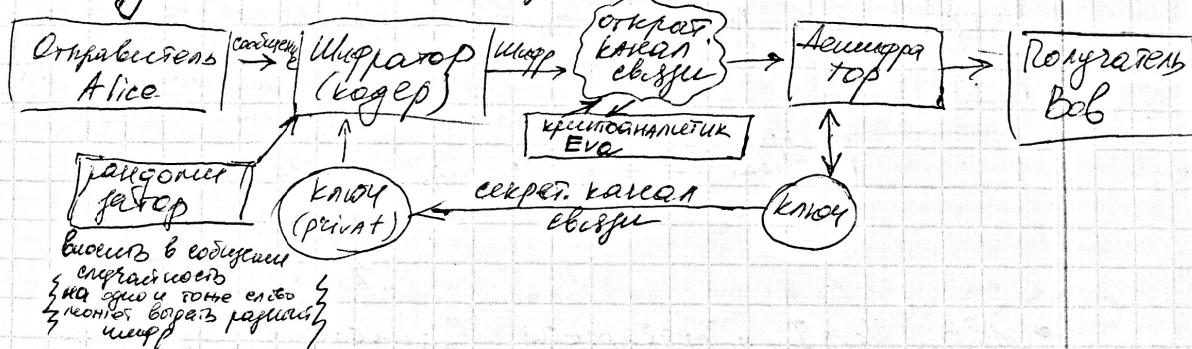
Криптография

Криптология

Криптография
 широкое изучение
 изучение гравиции в

Криптотехнология
 наука-искусство (наука "загадочности")
 изучение и изучение

Модель канала связи



- 5-4 BB go H.3 Шифр "Скита" (Скита)
 Барбакан, насыщенный памятью. На светах напоминает саблезубого.
 Потом зеркало передается
 Секрет. код - разделяет временные



Заслоняющее - к заслоне по радиусу
 заслоняет проникать

- 1 фн. 3 Шифр Чифре
 Существует пары байт на 3 единиц. Чифре
 (Запись)

$$z = x + y, \quad x - \text{текст}, \quad y - \text{ключ}, \quad z - \text{шифрованный текст}$$

- Иоганн Венцеслау 1586г

"Лучшее значение"
лучшее, превосходящее чисто общего не очень проще

Уг - зекко б аяп

42 - Bank

$$y_2 = c \sin y_1$$

- 28 ж.д. Кагар Томид

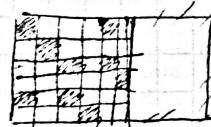
5
B C D E
F G H I K
L M

keep - to everybody
mention → napa

~~keep in the same~~
elevation → width

Деяние на алгоритм \rightarrow набор знаний

- 1500 Речетка Иеронимо тогда



III - o keep eras
Pococeroy →

в отверстие рамки. но синеву
которая висела на 90° и
протяжала рукоятка и га.
= 14-я с перекосом. синевы нет

Преподаватель: БАВОЧКА
МЧУНОТС
МЫИЧРО
БУХСОО
МЛООСТС
ДАСНГІ

- КВБ, Реп I «Торадарский Гранит»

Б В Р А Н З К Л М Ч
Щ Ш Ч Г Х Ф Т С Р П

дуктор несет. на верх. гаечные
и насадки

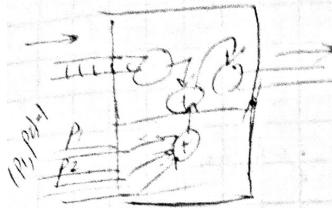
и макаров.

уровень энзимов. Углекл., а также
уровень патогенеза болезни

"МЫЛУАЛ ЧОСОЛУ БІЧПИЕК"

- 1926 Ширр Вернера (Лист однократно засебив)

deurst
kunstenaar



На вход машины f_5, f_0
поступает изображение лекции
На выходе этого изображения
в виде отображения

Более этого изображение идёт в клоуном

написано \rightarrow результатом

Результатом будет изображение клоуна
изображение которого идёт в клоуна
и на выход

один

клоун получает
результат

Например $A = \{a_1, \dots, a_L\}$, $|A| = L$

X - это - то исходное сообщение. $|X| = L^2$

Y - это - то изображение $|Y| = L^2$

K - это - то изображение

$x \in X, y \in Y, k \in K$, $y = F_k(x)$ - изображение
(из исход. x , с помощью k , получается y).

$x = F_k^{-1}(y)$ Задача

Например, изображение сообщения содержит букву, если

буква есть в сообщении;

1) $P(x|y) = P_x(x) > 0$ вероятность появления x , при условии что y ,

2) $P_y(y) = 1/M$ вероятность появления y в клоуне равна вероятности

Теорема (Шеннон, 1949)

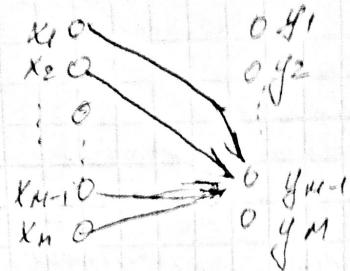
Пусть $|X| = |Y| = |K|$. Изображение является совершенным
сигнальным \Leftrightarrow выполнено следующее условие

1. $\forall x \in X \forall y \in Y \exists k \in K$, т.е. $y = F_k(x)$

2. $P_k(k) > 1/M$ (каждое правило работы вероятно)

1 - 80

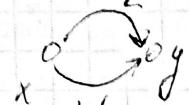
2) $P(x|y) = P_x(x) > 0, P_y(y) = 1/M$



Чтобы сформировать для этого набора
условия для генерации
некой величины

\Rightarrow Равн. глуб. характеристики
беседа = некая

Предн. начиная с пары (x, y) т.к. $\exists k$ предикт. величина
 $f_k \neq k'$, $k, k' \in K$
 $\& \exists F_k(x) = F_{k'}(x) = y$



Но принципиально интереснее исследовать
 k -юю не избранный подсчет из какого-либо x
Предикторное значение устанавливается

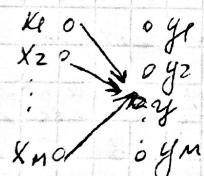
$\exists y' \text{ т.е. } P_3(y') = 0$

$$P(x_i | y) = \frac{P(y|x_i) P_x(x_i)}{P(y)}$$

$$\underset{\text{"и так далее" }}{P_x(x_i)} \Rightarrow P_y(y) = P(y|x_i)$$

\hookrightarrow нулевое значение в L

2. Задачка. y



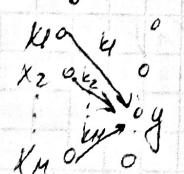
$$F_{k_i}(x_i) = y$$

Всемирно-известный ф. Гарднер

$$P(y|x_i) = P_k(k_i)$$

$$P_x(x) = \frac{P_k(k_i) \cdot P_x(x_i)}{P_x(y)} \Rightarrow P_k(k_i) = \frac{1}{M}$$

\Leftarrow заданна y , требуется найти
беседа пары (x_i, k_i)



т.е. $F_{k_i}(x_i) = y$

$$P_y(y) = \sum_{(x_i, k_i)} P_x(x_i) \cdot P_k(k_i) = \frac{1}{M} \sum_{i=1}^M P_x(x_i) = \frac{1}{M}$$

$$P(x_i|y) = \frac{P(y|x_i)P_x(x_i)}{P_y(y)}$$

Теорема (Монтецци)
Ингр. Вероятность слч. события. скретчинга

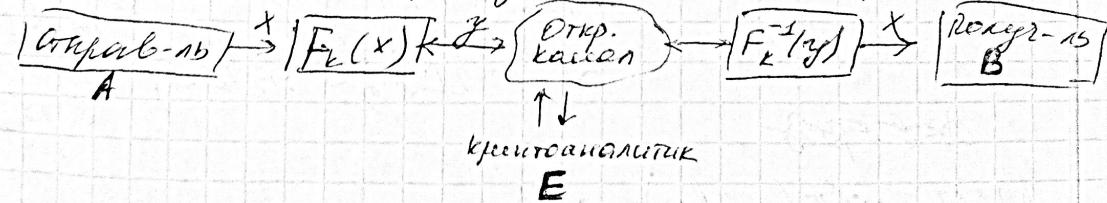
1. Решение Рассматривается
(скретчинг открытое)

2. Решение скретчинга
(скретчинг заблокирован)

1. Ищется число y , которое входит в поле. Время
2. Это Φ -число соответствует к ищему не открытому полю. Время
3. При записи дол. инфр.-чисел (наибол.) обратное к ищему будет фиксироваться Φ/δ развертывание я полей. Время.

Ингр. Φ . угад. 1-2 \rightarrow одностр. Φ -число
1-3 разл \rightarrow одностр. Φ с наиб. числом.

Модель хакера общий вид с отп. ключом



$$x^k \equiv y \pmod p$$

где x, k неизвестны и нужно найти спрашиваем
Ответ: число y, x возвращаются x
 $x = \log_k y \pmod p$ решается, но требуется
(одностр. Φ)
Следовательно находит - хакер

$$ax \equiv b \pmod{p}$$

22. Elek.
T. Dörges

Теорема (Діріхле)

Якщо $(a, m) = 1$, тоді $a^{\varphi(m)} \equiv 1 \pmod{m}$.
 $\varphi(m) - \phi$. Для всіх $x < m$ виконується $a^x \pmod{m}$.

$$m = p_1^{e_1} p_2^{e_2} \dots p_k^{e_k} \rightarrow \varphi(m) = m \left(1 - \frac{1}{p_1}\right) \dots \left(1 - \frac{1}{p_k}\right)$$

$$ax \cdot a^{p-1} \equiv b \cdot a^{p-1} \pmod{p}$$

$$x \equiv b \cdot a^{p-1} \pmod{p}$$

Протокол

A: \mathcal{A} та \mathcal{B} зустрілися

$$(x_A, y_A) \in \mathbb{Z} \quad x_A \cdot y_A \equiv 1 \pmod{p-1} \quad A \xrightarrow{m} B$$

$$B: (x_B, y_B) \in \mathbb{Z} \quad x_B \cdot y_B \equiv 1 \pmod{p-1}$$

Функція m -го квадрату $K_A^{p-1} = h(x_A, y_A)^T$

$$K_B^{p-1} = h(x_B, y_B)^T$$

$$K_{AB}^{p-1} = h(x_A, y_A)^T, h(x_B, y_B)^T \xrightarrow{m \text{ біт}} \mathbb{F}_p$$

Шифр

$$A) x_1 \equiv m^{x_A} \pmod{p} \rightarrow B.$$

$$B) x_2 \equiv x_1^{y_B} \pmod{p} \rightarrow A$$

$$A) x_3 \equiv x_2^{y_A} \pmod{p} \rightarrow B$$

$$B) x_4 \equiv x_3^{y_B} \pmod{p} = m^{x_A y_A + x_B y_B} \pmod{p} = (m^{x_A y_A + x_B y_B}) \pmod{p}$$

Задача: исследовать протокол Форберг-Негара и найти критич. недостатки.

Договор: А и Б хотят обменяться секретами.

неко.

Решение: неко. неко. неко. неко.

и т.д.

лев в прав-ко

15.7

Учтыв: есть общ. ключ и общий секрет.

(передача в Генератор)

Решение Р
Будущее.

Криптосистема Шамшура

$$K_{priv} = g^{x_A} \mod p$$

общий общ. засекр.

Лс.10
Печенье
Н.Ф.

A: берет $x_A, y_A \equiv 1 \pmod{p-1}$, $1 < x_A, y_A < p-1$

B: $x_B, y_B \equiv 1 \pmod{p-1}$, $1 < x_B, y_B < p-1$

$$A \xrightarrow{m?} B \quad K_{priv}^A = g^{x_A, y_A} \mod p, \quad K_{priv}^B = g^{x_B, y_B} \mod p$$

A: $\alpha_1 = m^{x_A} \pmod{p} \rightarrow B$

B1: $\alpha_2 = \alpha_1^{x_B} \pmod{p} \rightarrow A$

A: $\alpha_3 = \alpha_2^{y_A} \pmod{p} \rightarrow B$

B: $\alpha_4 = \alpha_3^{y_B} \pmod{p} = m^{(x_A x_B y_A y_B)} \pmod{p} \equiv$

$m \cdot (m^{p-1})^t \pmod{p}$

$\equiv 1 \pmod{p}$ но т. Генератор

Генер.

1. Решение - е критич.

2. А не-к. передает

3. Понимание имеет неизвестные соедин.

Кардинальная ошибка, т.к. факт использования лежит в основе крипто-
системы. Т.е. нарушено конфиденциальность.

Криптосистема Шнорр-Лиггс, Картри
 (Shamir) 1982
 (Мирка)
 Хемминг

$$k_{\text{pub}} = b^p - x \cdot c \text{ mod } p, g \in GF(p)^F$$

$$\begin{array}{ll} A: 1 < x_A < p-1 & k_{\text{priv}}^A = b^{x_A} g \\ B: 1 < x_B < p-1 & k_{\text{priv}}^B = b^{x_B} g \end{array}$$

$$A: y_A \equiv g^{x_A} (\text{mod } p) \rightarrow B$$

$$B: y_B \equiv g^{x_B} (\text{mod } p) \rightarrow A$$

$$A: z_A \equiv y_B^{x_A} (\text{mod } p) = g^{x_B x_A} (\text{mod } p)$$

$$B: z_A = y_A^{x_B} (\text{mod } p) = g^{x_A x_B} (\text{mod } p) = z_A$$

E: знает y_A, y_B, p, g , надо: x_A, x_B - секретные

Процесс формир-ет обеим скрыт клюра

Криптосистема Эль-Гамал (ElGamal) 1984

одинакова для обеих

$$A: x_A \quad k_{\text{priv}}^A = b^{x_A} g$$

$$B: x_B \quad k_{\text{priv}}^B = b^{x_B} g$$

$$B: y \equiv g^{x_B} (\text{mod } p) \rightarrow A$$

A: не знает координат

$$y_A \equiv g^{x_A} (\text{mod } p), A \xrightarrow{m?} B, z \equiv \text{inv } y_B^{x_A} (\text{mod } p)$$

$$(y_A, z) \rightarrow B$$

$$B: z \cdot \underbrace{(y_A^{x_B})^{-1}}_{g^{x_A}} (\text{mod } p) \equiv m (\text{mod } p)$$

E: можно решить алг-го

Криптосистема RSA
 (Ronald Rivest, Adi Shamir, Leonard Adleman)

Установите, что криптосистема форсирована
и атакуема.

Решение A. Форсирована атака

A: $k_{\text{pub}} = h^n = p, q, \ell \not\mid$
 $k_{\text{priv}} = h^p, q - \text{простые}, d \not\mid$

$1 < e < \varphi(n)$, $e \cdot d \equiv 1 \pmod{\varphi(n)}$, $\varphi(pq) = (p-1)(q-1)$

B: $\xrightarrow{m?} A$

$(e, \varphi(n)) = 1?$

необходимо

B: $x \equiv m^e \pmod{n} \rightarrow A$
A: $m^d \equiv x^d \pmod{n} \equiv m^{ed} \pmod{n} \equiv m \left(m^{\varphi(n)} \right)^t \pmod{n} \quad | t \in \mathbb{Z}$
 $\equiv m \pmod{n}$

E: находит d, $\varphi(n)$ -найден.

когда решается задача факторизация; разложение n на два простых числовых множин

3-я атака - подбором - сопоставление потенциальных ответов
проверка - итеративный (указание на вероятность)
авторизация - проверка правильности

Изотомия кодов

Проверка неравенства

3-я атака - подбором - авторизацией.

Есть некот. изоморфные коды с одинак. $y = F_k(x)$
A: k_{priv} , k_{pub} B: k_{priv}^B , k_{pub}^B

Если B: $F_{k_{\text{pub}}^B}(x) = y \rightarrow A: F_{k_{\text{priv}}^B}^{-1}(y) = x$ - первая
рекурсия RSA

Вторая

$F_{k_{\text{priv}}^B}^{-1}(x) = y$; $(x, y) \rightarrow A: F_{k_{\text{pub}}^B}^{-1}(y) = x$

Секр. + Частн. key:

B: $F_{k_{pub}}^A(x) = y$, $F_{k_{priv}}^B(y) = z$, $(yzx) \rightarrow t$.

A: $F_{k_{pub}}^{-1}(z) = y$. Против. ч и полз. y.
Если склад., то не симметрическ.
 $F_{k_{priv}}^{-1}(y) = x$.

8/7 18,6

Не кван. криптосистема. Использование физ. Частн. избыточн.

~~29, 20.
Лекция
№ 9.~~

05.11.
Лекция
№ 9.

Криптосистема. Меркель - Хеджмана 1978.

Рабоф Картин

(построена на основе оранже)

$A = \{a_1, \dots, a_k\}$ - набор векторов

$$S = \sum_{j=1}^k a_{ij} > e < t$$

сумма некоторой из оранжей есть
канонич. чисел - e:

$$a_i > \sum_{j=1}^k a_j \Rightarrow \text{б-р } A \text{ - супервектор. вектор}$$

3. оранже с супервектор. в-ром называется леж.

Возможна $M > \sum_{i=1}^k a_i$, $(w, M) = 1$

$A' = (a'_1, \dots, a'_k)$, где $a'_i = a_i \cdot w \pmod{M}$

$\{A'\}$ не содержит об-воск супервекторов

A. формирует криптосистему

A: Крип = $hA, w, M\}$, Крип = $hA'g$

B $\xrightarrow{m?} A$, $m \in E^k$ $\left\{ \text{отличие или нет пересеч} \right\}$

B: $S' = \sum_{i=1}^k m_i a_i \rightarrow A$

A: $S' \cdot w^{-1} \pmod{M} = S$

Также решетка f означает S использует A .
(это легко проверить).

Пример:

$A = (2, 3, 7, 15, 31)$; $M = 61 > 58$; $w = 17$

(Упр.)

Криптосистема Мак - Эллис 1978г.

(Mc Eliece)

стр. рас. $d \geq 2t + 1$

G - портн. матр. лин. функ. кода q_1, n_1 размера $n \times k$
(портн. лин. кода с эффектом ошибки t декод.) I

S - неворонн. матрица размера $k \times k$

P - нестационарная матр. размера $n \times n$
(в матр. строке, строке не более 1)

II $C \in A$, A -ансамбль кодов с генераторами

III C исправляет не менее t ошибок

$$G' = SGP, G' \in A$$

A: G' , Крип = $hG, S, P\}$, Крип = $hG', t\}$.

B $\xrightarrow{m?} A$, $m \in E^k$

B: $mG' + e = y$, где $e \in E^m$, $w(e) \leq t$, $y \in E^n$; $y \rightarrow A$

A: $yP \stackrel{?}{=} MSGPP^{-1} + EP^{-1} = MSG + EP^{-1}$

как будто
использование
 EP^{-1}
не как уе

Исп. блок MS, G кода эффициентный \Rightarrow меньше декоду 17

робота и консервация MS,

$$MS \cdot S^{-1} = M.$$

E: где ρ - плотность; μ - масса G ; радионуклид синтезирован на стартовой проверке.
(масса G' та же что и G)

или изотопия?

Пример:

$$\begin{matrix} n & |C| & t \\ (1024, & 644, & 38) \end{matrix}$$

$$(6624, 5129, 115) \rightarrow \text{исходная эффективность изотопа}$$

$$|A| \geq 10^{149}$$

Капитализм Мак-Грея
имеет генеральное колоссальное значение
для всего общества

Информация о нем распределяется по сп-ю с тем
же темпом, что и капитал

Модернизация промышленности. Мак-Грея \rightarrow можно подразумевать
(Последует промышленность в гармонии)
на промышленность. Мак-Грея

21.8

21.8

Когда Романов рекомендует мне не писать о нем. Мак-Грея

Криптостойкость Ницерайтера 1978

Н-стр. матр. $m \times n$. С ул. и с квадрат. $d > 2t + t$
 над полем $\mathbb{F}(q)$, размер $m \times m$, где
~~некоэффициенты~~ н-коэффициенты проверок

S-матрица (матр. $m \times m$)

D-диагональная ($n \times n$) (матр. эл. поле нечетн.)

P-перестановка ($n \times n$)

(6 строк, столбцы по 1 единичной)

$$f': H' = SHDP \quad K_{\text{priv}} = \{H, D, S, P\}, \quad K_{\text{pub}} = \{H', t\}$$

$$B^m \rightarrow A \quad m \in B^t(\bar{o}) \subseteq F_q^n$$

$$\{ B'_x \in F_q^n, \quad H'x = B'_x \rightarrow A \\ \exists x \text{ такое что } B'_x = B_x + e, \text{ число } e \text{ под. в-р когда } x \in H \cdot H' \}$$

$B_x = 0, \text{ если } x \in$
 $\text{тогда } e \text{ неизв. и.б.}$

$$A: S^{-1} B'_x = S^{-1} S H D P x^T = H \underbrace{D P x^T}_{x' \rightarrow \text{чт. что ищем } x}$$

$\{$ т.е в качестве цифры передается в-р ошибок $\}$

E: криптотека генерирует квад. когда из имеющихся

Криптостойкость на эллиптических
 криптокомпьютерах
 (Эллиптическая криптография)

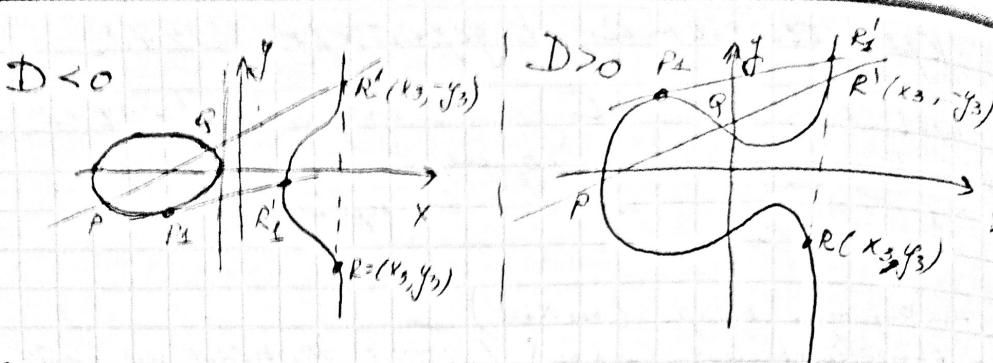
Л. Н.
 Красовский
 1980.

$$y^2 = x^3 + ax + b$$

исследование 31. крипто:

$$D = \left(\frac{a}{3}\right)^3 + \left(\frac{b}{2}\right)^2 \neq 0$$

или не существует
 квадратных корней



Рассмотрим пересечение 2н. кривых
в некот. приближении. Точки пересечения P, Q, R'
Сумматор, иди:

- 1) $P + Q = R$
- 2) $-R' = R$

Если пересеч. в линиях совпадают \Rightarrow касательные
 $P + Q = R$ (т.е. $P + Q$ как и R симметричны относительно линии пересечения)

" $\angle 2JP$ (уголом между точками P)

Пересечение - вертикальная
Декомпозиция удаляемая точка: „-“ 0

- 2) $0 + P = P + 0 = P$
- 3) $P + Q = Q + P$
- 4) $(P + Q) + T = P + (Q + T)$

$P(x_1, y_1), Q(x_2, y_2)$, и иск.-ся координаты $R = (x_3, y_3)$

$$k = \frac{y_2 - y_1}{x_2 - x_1}$$

Равенство означает: пересеч. кривой с
уравнением $y = kx + b$ для P, Q

Если $P \neq Q$:

$$x_3 = k^2 x_2 - k x_1, y_3 = k(x_2 - x_1) - y_1$$

Если $P = Q$:

$$k = \frac{3x^2 + a}{2y}$$

Экспоненциальная кривая над $\mathbb{F}(p)$

$$E_p(a, b) = \{(x, y) \mid y^2 \equiv x^3 + ax + b \pmod{p}\} \cup \{\infty\}$$
$$0 \leq x, y \leq p-1$$

Пример:

$$E_7(2, 6) \quad y^2 \equiv x^3 + 2x + 6 \pmod{7}$$

y	y^2	x	$x^3 + 2x + 6$
0	0	0	6
1	1	1	2
2	4	2	4
3	2	3	4
4	2	4	1
5	4	5	1
6	1	6	3

$$(4, 1); (5, 1); (4, 6); (5, 6); (1, 3); (1, 4); (2, 2); (2, 5); (3, 2); (3, 5); (0, 0)$$

Теорема (Кассе) 1938г

Кол-во точек эл. кривой $E_p(a, b)$ уменьш. не ≥ 1

$$\#E_p(a, b) \leq p + 1 + 2\sqrt{p}; \quad \#E_p(a, b) \geq p + 1 - 2\sqrt{p}$$

$$4 \leq \#E_7(2, 6) \leq 12$$

$$[m]P = \underbrace{P + P + \dots + P}_{m \text{ раз}}$$

множество
точек

Упрощение:

$$\text{для } P = (5, 1)$$

[2]P

$$k = \frac{3x^2 + a}{2y} = 0$$

$$x_3 = k^2 - 2x = -10 = 4 \quad (4, 6)$$

$$y_3 = k(x_4 - x_3) - y_1 = -1 = 6$$

"т.ч. сокращение P факт все точки эл. кривой
яв-ся генератором"

Знайдіть P та $CMP = R$
користуючись у - f -ра та G

Криптосистема Эл-Раманна на эліптических кривих

$E_p(a; b)$ (1) G - генератор

$$k_{pub} = f(E_p(a, G); (1)b, D_A f), k_{priv} = f(C_A f)$$

A: $0 < C_A \leq p-1$; $D_A = [C_A]G$

B: $0 < C_B \leq p-1$, $D_B = [C_B]G$ $k_{priv}^B = f(C_B f)$

B': $0 < m \leq p-1$, $m \xrightarrow{?} A$

B: $R = [C_B]D_A = (x, y)$; $m' \equiv x \cdot m \pmod{p}$
 $(m', D_B) \rightarrow A$

A: $[C_A]D_B = [C_A] \cdot [C_B]G = [C_B][C_A]G = [C_B]D_A = R$
 $m \cdot x^{-1} \equiv m \pmod{p}$

E: D_A, D_B, G

найти $C_A, C_B \rightarrow$ та f - генератора
(секретне число підтверджувача)

Задача
 $\mathbb{F}(2^4)$ $f(x) = x^4 + x + 1$

$$y^2 + xy = x^3 + ax^2 + b$$

$a = g^4$; $b = g^0 = 1$, f - генератор, $2n-1$ корін

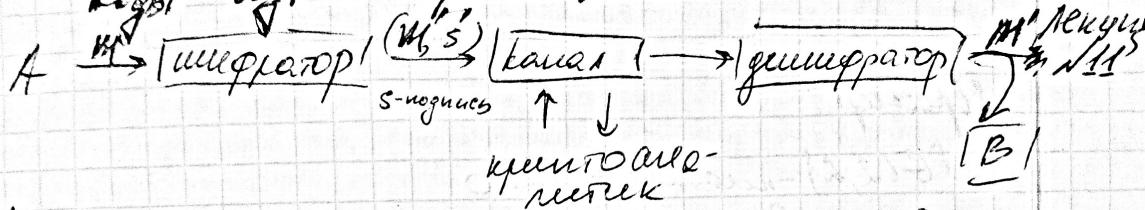
1. Найти 1001 -бо корін f відповідно (затягнувся)
2. $k_{pub} = f(\mathbb{F}(2^4)) \rightarrow y^2 + xy = x^3 + g^{128}x + 1$, $G = (g^5, g^3)$

$K_{priv} = \{ C_A = 3f \}$, C_B включается единицей

Итак $B; M = (10\ 11) \rightarrow A$.

Шифрование, дешифрование

Коды аутентификации



K -общий секрет. имена
 m - ини-бо сообщение
 M - ини-бо сообщ.
 $s \in S$ - ини-бо подпись.

Оп.: Коды аутентификации наз. набор (M, K, S)

таких, что $\forall m, m' \in M \quad \forall k \in K$ верно

$$F(m, k) = F(m', k) \Rightarrow m = m'$$

$$F: M \times K \rightarrow S$$

Проективная геометрия $PG(2, q)$ наз

послес $GF(q)$

- это ини-бо точки в кол-ве $q^2 + q + 1$ и
такого же кол-ва прямых (иных ини-бо точек),
составленных из $q+1$ точек. При этом
точкам, прям.,

1. \forall 2 точки проходит 1 прямая

2. Помимо 2 прямого пересек - аз по 1 точке

$d = (V, E, \lambda)$ -схема

- ини-бо наборов из k , состоящих из V вершинов,
(V -это-точ.,
какие, это
точки именем t)

и пара будет возвращаться. С d есть наборах

потом

$PGL(2, q)$ - группа (группа автоморфизмов)

Было бы $3^2 = 9$, но в ней есть изоморфия
3-го порядка.

Надо доказать что:

$$\frac{C_6}{C_2} = \frac{C_{q^2+q+1}}{\frac{C_2^2}{q+1}} = \frac{(q^2+q+1)(q^2+q)}{(q+1)^2 q} = q^2 + q + 1$$

Пример:

$PGL(2, 2)$ - неиссякаемое поле

Примеры:

012

034

065

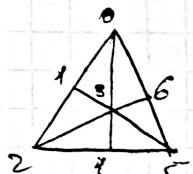
135

236

245

146

- правильные



когда $\chi_{\text{для } f}$?

$$H = \begin{pmatrix} 0 & 0 & 1 & 1 & 1 & 1 \\ 0 & 1 & 0 & 0 & 0 & 0 \\ 1 & 0 & 1 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 \end{pmatrix}$$

Правильные \rightarrow неиссякаемое

\rightarrow бесконечное количество слов для

каждой комбинации

Рассмотрим $PGL(2, q)$



α -изоморфизм, $|\alpha| = q+1$

$$M = \alpha, |M| = q+1$$

$$K = PGL(2, q) \setminus \alpha, |\alpha| = q^2$$

(S -изоморфизм если $k \in m, m \in L$)

$F(m, k) = S$ -изоморфизм, при этом если $m \in L$
 $m \in M, k \in K, s \in S$

$A: S = \text{Fl}(n, k) \quad (m, s) \rightarrow B$

$E:$ есть ли в \mathbb{F}_q , корень ненулевого ви

Вероятность умножения ненулевого?

если умножить так, что b не делится на a

это вероятность проходит $p+1$ промежутка, одна из них должна

\Rightarrow вероятность проходит φ промежуток

Вероятность ненулевого: $P_n = \frac{1}{q}$

$$|M| = q^{t-1}$$

$$|K| = p^2; |S| = p^2 + q$$

Mark Buhler, Еврон + Рильдерг 1974г

Гордансон, Синг, Гадаевский 1994г

Пусть для p -квар. корня L_n, k, d, I_q
выбраны $I^n \in C, I^n = (\underbrace{1, \dots, 1}_n)$

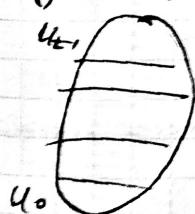
$$\langle I^n \rangle \subset C$$

или обозначим

$$P = C / \langle I^n \rangle$$

размером n
некоторый размер m

Чтобы найти ненулевого конфиденциальную вероятность



$$M = \{0, \dots, M_{t-1}\}$$

$A: u_i \xrightarrow{?} B$

$$u_i \rightarrow u_i = \begin{pmatrix} u_i + d_0 I^n \\ u_i + d_1 I^n \\ \vdots \\ u_i + d_{t-1} I^n \end{pmatrix} \quad d_j \in GF(q)$$

$K = \{s_1, \dots, s_j\} \times \{t_0, \dots, t_{j-1}\}$

m -коэф.; (x, y) -код; g_{xy} -норма

$$|M| = t = q^{k-1}; |k| = nq; |S| = q$$

Def

Задача

Нап-р в бирюк-теч. числе. норма
состав-е преобр. ного.
(нап-р x, y японск. кодами A и B ,
 E ее не знает.)

Схемы распределения секретов (пороговое схемы)

U_1, \dots, U_n - полупаралл.

S - секрет

U_i - определяет значение S_i секрета S

$F(S_1, \dots, S_k) = S$ при условии, что определенное
имеет $j > k$, $j \leq k$ - каскад восстановления
секрета. Т.е. то значение, которое
восстанавливается секрет

Система Шамара 1979

Ряд $S = a_0$

$$U_i \text{ определяет } f_{i1}, f_{i2}(x) = a_0 + a_1 x + \dots + a_k x^k$$

Всего в схеме $\leq k$ ну-е \rightarrow не склонны к ошибкам