Черепнев Михаил Алексеевич.

(1)

Защита информации. 14.02.2018.

1. Физический способ

Нельзя передавать инфо в устной форме, либо знаками (символами)

2. Стеганография

Способ сокрытия факта передачи инфо.

Китай

3. Криптография

Изменение сообщения.
Изменение записи открытого текста.
Преобразование в иной вид.

До греческого алфавитного письма, было символьное письмо.

• Месопотамия 3500 г. до н.э.
• Инд. • Египет • Др. Греция
• Моргуш (на террит. совр. пустыни Каракум)
– здесь возние зороостразы
• миноская книга
> Фдзку 6200 г. до н.э. (Китай)
Записи на черепах. панцирях.
(символьное письмо)

К. Поппер "Философия исторического знания" ! книга.

"Парадигма"
• научная
• ненаучная

1. Легендарная история
2. Документальная история
в 1848 г. - были изданы все летописи
+ Ипатьевская летопись.
затмения = даты.
3. Лингвистическая
4. Антропометрическая

Радиоуглеродный анализ по изуч. Фетанков.
исследования ДНК

5. Артефакты (материалы полученные из земли)

Др. Греция

Квадрат Полибия

? Во 2-ой половине II тысячелетия до н.э. финикийцы изобрели совершенно новую письменность, в кот. каждый знак обозначал отдельный звук, т.е. был буквой.

(2)
21.02.2018.

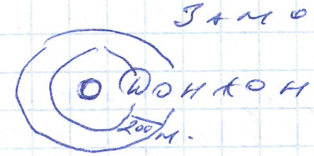
За то, что Новгород не подвергся монг.-тат. разорению он д.б. заплатить 1400 кг. серебра.

Монеты до X в. персидские, потом византийские и ещё позже европейские.

Под Парижем катакомбы 300 км, носят признаки жилья.

Посл. поселение скифов в (гос-во) Крым. Гос-во было разорено готами в III в.

Замок



Замок Копорье. (Ленингр. обл. Тверская обл.) ✓

Стенобитные орудия были тогда эффективнее, чем огнестрельное оружие.

Кирпичников.

Технология огн.-стрелкового оружия исходит с Востока.

Рук-во татаро-монг. и крестоносц. войска одни и те же (римск. папа) (предположение)

Кочевники-караванщики.

Татаро-монг. войско нах. в составе европейского.

(3)

28.02 2018 ① Шифр простой замены

② Шифр многозначной замены.

Спарта в персидско-греческ. войнах применяла шифр перестановки.

Сцитала - палка, обмотанная тканью - текст писали вдоль по граням, потом ткань разматывалась.

Дилижанс - 12 км. в час - шёл днём и ночью.

Шелковый путь через террит. Руси - через Бухару, Самарканд → Волгоград → Болгария Тырново

Волга → Дон

? Петр I закрепостил крестьян

1095 г. - папа римский провозгл. необходимость крестовых походов на Ближний Восток

Книга ! { Эжен Эммануэль

Крепости и осадные орудия

Под крепостью часто делался подкоп

Людовик IX Святой был рук.

Татаро-монг. войска.

Церковь святого Рупрехта в Вене.

Могильник Высокая гора

Террит. от Азова до Богуч[illegible] принадл. папе римскому.

Подвеску рыцаря нашли на террит. Воронежск. обл.

> Куликовская битва

Татаро-монг. войско и подкрепляла генуэзские полки.

Монастырщина (р. Дон) (Воронежская обл.) Богучары?

Дмитрий Донской напал на караван и бился с конвоем.

В Воронежск. обл. местные жители находят по 10-12 предметов каждый год.
Когда в музее Кулик. поля ~~[illegible]~~ содержатся всего ок. 10 предм.

(4)

7.03.2018

III крест. поход 1202 г.

Папа Григорий III → Гонорий III

200 тыс. крестоносцев отправились в Вост. Европу.

В 1204 г. крестоносцы взяли Константинополь.

Книга! "Сокровенное сказание монголов" на уйгурском яз. 1848 г. – переведено.

Борисфен – Днепр (скатный)

Танаис – Дон (тихий)

Итиль – Волга (рядовой)

→ Латинские названия.

Рюриковичи, Гедиминовичи.
Гаплогруппа N1C1.

↳ В России в осн. сосредоточено в Новгородской обл.

Чингисхан, перейдя р. Танаис столкнулся с ханом Бугрда (рус. тюркского племени)

1206 г. – Курултай – Темучин получил имя Чингисхан.

В сер. XIX в. был объявлен грант на ист. исследования татаро-монг. ига – никто не смог.

Деньги были потрачены на изучение летописей.

1215 г. – Взятие монголами г. Пекина.

1212 г. – крестовой поход детей.

Время прав. пап римских совпадает с правлением Чингисхана.

Батый – батл – фр. битва.

В русских летописях татаро-монг. называют татарами, либо огоряне, моавитяне (фр.) (обл. на бл. Востоке)

безбожные, поганые (фр. паганес – язычники)

– это **тамплиеры**

поклонение идолам, солнцу.

Чингисхан захв. Самарканд → Иран → Азербайджан → Судак. (движение Чингисхана к своему родному становищу) – с Востока на Запад.

битва на р. Калке

Слово о полку Игореве

Попытка кн. Игоря установить контроль над степью.

1185 г. – поход Игоря на половцев

Монголам были известны все виды вооружения.

> Романовский район (р. Дон) Ногайский шлях)

Суздальская летопись 1237 г.

1232 г. – папа римская объявил северный крест. поход.

1236 г. – крест. поход против Литвы

Разорена Волжская Булгария.

1237 г. – разорение Рязани.

И т. д. . . .

Заканчивается на границе

Отец Алекс. Невского Ярослав Всеволодович убили в Орде.

Тамплиеры поклонялись козлу идолам, солнцу.
Обвинение в содомии.

Письмо Ал. Невск. от папы Иннокентия IV (1248 г.) на латыни.

Иго – латинское слово. ?

1250 г. поход Ал. Невск. на Москову. ?

Фридрих II отлучен от церкви на Вселенском соборе.
(Людовик Святой IX Фр.)
за убийство папы римского.

1246 г. Курултай – великим ханом избран Гуюк. (Сын Чингисхана)
он стал сопробива. крестоносц.
Пошел походом на Батыя.

1248 г. был отравлен и умер.

1246–1266 гг. монг. войском рук. монголы.

1253 г. – к сыну Батыя Сартаку прибыло посольство Людовика IX.

1257 г. – Сартак был отравлен

1266 г. – в районе Дербента была битва между двумя монг. войсками.

Ясса – закон монголо-татар.
юсон – приказ (латынь)

1251 г. – Курултай – утверд. хана Менке.

1470 "Задонщина"

Дм. Донскому достался караван шёлк.

Битва проходила на шёлковом пути.

Цель - контроль над территориями, где проходил шёлк. путь.

⑤ 14.03.2018

Шифр простой замены

$a_i \to a_{i+3}$

Многозначная замена

$a_i \to \{$ [illegible]

Шифры перестановки
(Сильвестр Медведев - дьяк посольско-приказа конец XVII в.)

Станица Монастырщина Богучарского района Воронежск. обл.
(II том Советск. энцикл.)

В Тульской обл. - с. Монастырщино.

! Задонщина

Схизма с 1373 г - двоевластие периода пап из Рима и во Франции (Авиньон)

Чеканить монету на Руси начали при Дм. Донском.

Православие

1070 г - устав Студита (Константинополь)

- упрощение службы

Осн. молитва до этого? "Господи воззвах" - помощь Господа в трудностях!

После "Отче наш" - отказ от материальных ценностей.

Посольский приказ - 1549 г. до 1612 г.

О. Кромвель - основатель разведывательной службы Великобр.

1440 г. - Иоанн Гуттенберг изобрел печатный станок.

1499 - [illegible] Тритемия развитие шифра в [illegible]

	А Б В . . . . Я	1 2 3
1б.	А Б В	Я 1 2 3
2б.	А Б	Я 1 2 3 А

1652 г - созд. Немецкой слободы

(6)
21.03
2018

Находясь в крепости Мария Стюарт переписывалась со своими союзниками.

С помощ. бочонков с пивом у кот. было двойное дно.

Парадокс дней рождения

n – число людей

$p(n)$ вероятность того, что найд. 2 челов. с один. днем рожд. $\approx \frac{1}{2}$ $(n \approx 23)$

$\bar{p}(n)$ разные дни рожд. $p(n) = 1 - \bar{p}(n)$

$$\bar{p}(n) = \left(1 - \frac{1}{365}\right)\cdot\left(1 - \frac{2}{365}\right)\cdots\left(1 - \frac{n-1}{365}\right)$$

$$\frac{365!}{365^n (365-n)!} \approx e^{-\frac{n(n-1)}{2\cdot 365}} \approx e^{-\frac{n^2}{2\cdot 365}}$$

Историю можно изучать по языку

26 фонетических единиц

2 фонема – это $\frac{1}{95}$ всех слов

3 $\frac{1}{27}$

4 $\frac{1}{7,6}$

5 $\frac{1}{8,6}$

6 – $\frac{1}{6,8}$

7 – $\frac{1}{6,8}$

8 – $\frac{1}{6,5}$

9 – $\frac{1}{7,9}$

10 – $\frac{1}{14,6}$

11 – $\frac{1}{63}$

Вероятность, что слово совпадет в двух языках.

$= \frac{1}{26^4} = \frac{1}{456,976}$

x x x x р.я

x x x x

$\frac{1}{26}\ \frac{1}{26}\ \frac{1}{26}\ \frac{1}{26}$

Среднее число общих слов из 4-ех фонем $\frac{30000}{456,976} = \frac{1}{15}$

≈ из 3-ех фонем – чуть меньше (2)

≈ из 5-т и др. $= \frac{1}{350}$

kibitka (кибитка)
company (компания)
reserve (резерв)
abrogue (оброк)
stop (стоп)
steak (стог)
crush (краха)
shuttle (шатать)
rockit (ракета)
arrest

symbol
surprise (сюрприз)
trauma (травма)
troglodyte (троглодит)
truce (трус)
brigade (бригада)
boyard (боярин)
boycott
bracelet
chaquete (жакет)
stool
horizontally (горизонтальный)
knight [knait] - князь
blond+ блондинка.
pappa (жидкий хлеб)
too - too
hockys - pockys
throne - трон
trushing - странность
cupel - пробирная чашка

curator
post - почта

Словарь А. В. Старчевского 1848г
староцерковный язык.
Родина - homeland.

d'Altin
d'Allay
Astraken

(7)
28.03.
2018.

Goosy, goosy, gaga
Yeast hot eater
Da - da
Null yet eater
Jerry
Volcal

$p \approx \frac{1}{6^{30}}$

Pot gote row
Ne poors house
nusty mok
Null yet eater
Cac hot eater row las libe beeter gitter

2 др 2500 $\frac{1}{100}$

3 др 10000 $\frac{1}{27}$

4 др } 30000 $\frac{1}{7}$
⋮
8 др

9 др 20000 }

$\geq$ 10 др - мало $\frac{1}{25} \approx 1$

Вероятность того что случайное слово N есть в словаре [4;8]

$\approx \frac{30000}{26^N}$

Вероятность понимания очередного слова в словарь = сумма вероятностей того, что в нем N долей умножить на вер того, что это слово есть в словаре.

Итого $\frac{1}{100} \cdot \frac{2500}{26^2}$ (×1) $+ \frac{1}{27} \cdot \frac{10000}{26^3} +$

$+ \frac{1}{7} \cdot 30000 \left(\frac{1}{26^4} + \dots \frac{1}{26^9}\right) + \left(\frac{1}{25} + \frac{1}{15}\right)$

$- \frac{25000}{26^{10}} \approx \frac{1}{10} + \frac{30000}{26^4} \approx \frac{1}{6}$

Формула полной вероятности

1. имеем массив из различных эл-ов

Выбираем с повторением два массива размера $M(N)$ так чтобы с вер $= \frac{1}{2}$ эти два массива пересекались

Тогда $M(N) = C\sqrt{N}$

$N = 365$ $M(N) \approx 16$, } $\Rightarrow C \approx 1$

Общее число наборов долей из 4х долей: 26^4

Тогда множества, которые пересекаются с вер $\geq \frac{1}{2}$ имеют объём $\approx \sqrt{26^4} \approx 700$

$\frac{30000}{700}$ слов 4.

≈ 40

...

40

Всего совпадений $40 \times 20 = 800$

P (слов по долям и по смыслу

$\frac{800}{10000} = \frac{1}{10}$

$N = 5$ $\frac{30000}{26^2 \times 5} = 10 \Rightarrow 50$ — число совпадений двоичного ряда.

$\frac{50}{10000} = \frac{1}{200}$

$N = 6$ $\frac{1}{5200}$

Елена Глинская — (королевская / литовская)

Иван Грозный выдал Англии беспошлинное право торговли на Руси.

Английская книга посланника (купца) Джером Горсей.

В Вологде Иван Грозный строил флот

√ Иван Грозный получил от Елизаветы англ. право на политич. убежище.

Исслед. костей Ив. Гр. показало большое содержание ртути.

1575–1576 г. — царем был Семен Бекбулатович.

"Спецслужбы России 2016 г."

Ив. Грозный "был **удушен**

Алексей Мих. вел переговоры с Рудольфом II Австрийским о совместной борьбе с Польшей. Применялась шифровальная азбука **Воркача**.

Рудольф вел переговоры также с поляками.

Династия Юаней ввела бумажные деньги.

— Бит конный.

Петр I

Оборонительные линии.

Первые в Сев. Казахстане по Ишиму
в Центр. Каз. по верховью Оби!

При Петре I в Петербурге было построено 59 крупных и более двухсот мелких судов. ?

8

4.04 2016

Договоры Игоря с Византией

Вольфаст, Кари, Руалд, Актеву, Труан, Рудуг, Рулеф, Роар, Веремуд — представители Руси кот. упом. в дог. кн. Игоря с Виз. (пристанями)

Рядом с Портами были кладбища транспортировки рабов.

Париж — "кладбище невинных" — массовое захоронение рабов

Сельв. Медведев - дьяк посольск. приказ. заним. шифровками.

1549 г. - созд. посольск. приказ - спец. служба.

Применял шифр сцитала.

До него шифров. - азбука Ворчача, вязь.

У Петра цифирная азбука

Оборонит. линия Псков-Смоленск-Брянск постр. ≈ 1707 г. в период Сев. войны.

Карл XII умер в 1718 г., а Петр присоед. к России Кольский п-ов...

Петр отправлял боярских детей за границу без гос. обеспеч. и насильно.

Русская правда

Петр I и креп. право. (?)

Персидский поход 1723 г. попал в плен Петр I

Екатерина II применяла шифр Виженера.

$a_i \to a_i + g(i)$

номер в алфавите; номер в тексте

I Екатерина II вместе с Гильбертом устроила 100 математич. школ в [crossed out] С-Петербурге.

с VII по XIX в - Россия - торговля с Фараоновск. канала до суэцкого канала.

Закреп. крестьян

1497 - Судебник
Единый срок для переходов крестьян - Юрьев день (неделя до и нед. после 26 ноября)

1581 - Иван Гр. издал указ о заповедных летах (в эти годы запрещ. переход кр-ян от одного хоз. к др. в Юрьев день)

1597 г - Указ об урочных летах - уст-н 5-й срок сыска беглых кр-ян

1607 - 15-й срок сыска беглых кр-ян

1649 - Соборное уложение
Закрепощение крестьян (кр-не прикр. к земле, а принадл. к тому или иному пом. передав. по наследству)
(Алексей Михайлович)

9
11.04

Белгородская черта 1636-1640

Симбирская черта 1648-1654

Старая Закамская линия 1652-1656

Псков - Смоленск - Брянск 1706-1708

Царицынская линия 1718-1723 (Волгоград по Дону - Нижн.-Тел.)

По Яику, Оренбург 1731-1735-1739

Новая Закамская линия 1731-1736

Новая Симбирская линия 1847-1854

Сырдарьинская линия 1853-1864

Кокандская линия 1864 (Иссык-Куль, Балхаш)

Постройка Суэцкого канала 1859-69 г. (финансир-сь Францией прокоп. по террит. Египта)

С VII по XIX в. Россия представляла интерес для мировой торговли европейцев

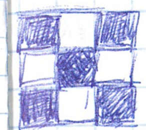
1482 г. - изгнание генуэзцев из Крыма

Революция 1917 г.

Большевики перехватили немцев. (Пулемет Максим, печатн. станок немецк.)

Белые перехв. англ. и др.

1937 г. Котельников криптограф СГ - и о возможностях эфира проводов



По проводам передавалось шифрован. сообщ. (точечный шифр) Поточный

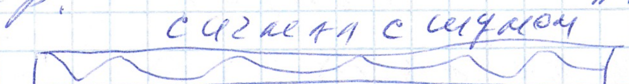
Шифровальная машина Энигма

Советские не расшифр.

Англичане расшифр.

БЭЛЛ

Откр. Получ.



1970 г.

(10) 18.04 Гаммирование — способ шифрования

$c_1 = \gamma \oplus m_1$ γ — сл. посл. 0, 1

$c_2 = \gamma \oplus m_2$

$m_1 \oplus m_2$

> Воспоминания Берли.

1976 г.

Diffie Hellman $\mathbb{Z}_p^* \supseteq \{ g^{x} (\bmod p) \mid x \in \mathbb{N} \}$ (остаток)

$\langle g \rangle_n \{ g^n \equiv 1 (\bmod p),\ n - \text{мин} \}$

A   B

$|a| = s$, $a \in_R \mathbb{N}$ $b \in_R \mathbb{N}$

g^a g^b

DH: g^b, g^a → g^{ab};   DLOG → a

$(g^b)^a = (g^a)^b$

$g^i \overset{?}{=} g^a$ за 2^s ⇒ $i = a$

$s \ll 2^s$ $n = 2^{512}$

$a = \sum_i a_i 2^i$ $a_i \in \{0, 1\}$

g^{2^i} — $i = 0, \ldots, s$ $\prod_{i: a_i = 1} g^{2^i} = g^a$ за 2s умнож.

Аутентификация

$a, b \to (a, b) = r_{i+2}$ $r_{i+2} | a$, $r_{i+2} | b$

$a = b q_1 + r_1$; $0 \le r_1 < b$

$b = r_1 q_2 + r_2$; $0 \le r_2 < r_1$

$r_1 = r_2 q_3 + r_3$; $0 \le r_3 < r_2$

ОТА

$(\prod p_i^{a_i}, \prod p_i^{b_i})$

$r_i = r_{i+1} q_{i+2} + r_{i+2}$; $0 \le r_{i+2} < r_{i+1}$

$r_{i+1} = r_{i+2} q_{i+3}$

РАЕ (расширенный алгоритм Евклида)

$d = r_{i+2} = ua + vb$, $u, v \in \mathbb{Z}$

$(a, p) = 1 \Rightarrow \exists u, v: au + pv = 1 \Rightarrow$

$\Rightarrow u = a^{-1} (\bmod p)$

$\{ \bar{a} \mid (a, p) = 1 \} = \mathbb{Z}_p^*$

$\varphi(p) = \# \mathbb{Z}_p^*$

p - простое ⇒ $\varphi(p) = p - 1 \Rightarrow a^{p-1} \equiv 1 (\bmod p)$, $(a, p) = 1$

p = n - составное ⇒ $a^{\varphi(n)} \equiv 1 (\bmod n) \Rightarrow$ $\varphi(n) < n - 1$

p — псевдопростое число Кармайкла.

$2^k+1=(2^{k_1})^t+1^t=(2^{k_1}+1)\times$
$\times((2^{k_1})^{t-1}-(2^{k_1})^{t-2}+\ldots 1)$

$k=k_1 t$

$2^{2^s}+1$ — простые Ферма

$s=0,1,2,3,4$ — простое

$s=5$ — составное

$2^k-1=(2^{k_1})^{k_2}-1^{k_2}=(2^{k_1}-1)\times$
$\times(2^{k_1(k_2-1)}+\ldots+1)$

$k=k_1\cdot k_2$

Простое ⇒ k простое

2^p-1 — числа Мерсенна
пр.

$p=561 \mid 3$

$(a,3)=(a,17)=(a,11)=1$

$a^2=1 \pmod 3$ $\quad a^{10}=1 \pmod{11}$

$a^{16}=1 \pmod{17}$

$a^{560}=1(561)$

91 наим. псевдо простое по осн. 3 $\quad 3^{90}\equiv 1 \pmod{91}$

$\gamma \oplus m=c$

$k=k_1 \mid k_2$

$x_0=0$

M — большое

$x_i=k_1x_{i-1}+k_2 \pmod M$

$x=x_0|x_1|x_2|\ldots$ псевдослучайные последова-ти

$x_i=x_j$

$x_{i+k}=x_{j+k}\quad \forall k\in\mathbb{N}$

$x_{i+1}=ax_i+bx_{i-1}$

x_0,x_1

$y^2=ay+b$

y_1, y_2

$x_i=y_1^i, y_2^i$; $\quad x_i=c_1y_1^i+c_2y_2^i$ — решение

$y_1^{i+1}\overset{?}{=}ay_1^i+by^{i-1}$ $\quad x_0=c_1+c_2$

$x_1=c_1y_1+c_2y_2$

$y_1\neq y_2 \quad x\to c_1;c_2$

Эл. цифровая подпись

Веноне

США 1943-1950 гг.

Авизо

1994 эл.ц. подп. ЦБ
$\mod p \quad p \approx 2^{512}$

ГОСТ Р34-10, 2001

ГОСТ Р34-10, 2012

RSA $n = p \cdot q$, $(p) = (q)$ $p \neq q$ - пр

$\varphi(n) = (p-1)(q-1)$

$(e, \varphi(n)) = 1 \quad d = e^{-1} (\mod \varphi(n))$

I этап A --- e, n ---> B

II эт m - сообщение

$m^d (\mod n), m)$

$m \overset{?}{=} (m^d)^e (\mod n)$

$m^{e \cdot d} = m^{1+\varphi(n) \cdot k} =$

$= m \cdot (m^{\varphi(n)})^k = m (\mod n)$ ⟹

$m \overset{?}{=} (m^d)^e (\mod n)$

$\Pi(a\,b) = \Pi \cdot b$

$b \in G \quad b \in G$

$ab_1 \neq ab_2$

$ab_1 \neq ab_2$

$a^{|G|} \; \Pi b = \Pi b$

$b \in G \quad b \in G$

$a^{|G|} = 1$

$f_K(x) = x^e (\mod n) \quad \log n = 2^{\frac{|n|}{\sqrt{n}}} = 2^{\log n}$

$f_K^{-1}(x^e) = x (\mod n)$ выч. игра известном к

$K = (p, q)$

Аутентификация

$C_x^x \; d \; (x^d)^e = x (\mod n) \quad (y, y^e)$

Шифрование RSA Ассиметричн. сист!

I эт A --- e, n --- B

m - сообщ.

$c = m^e (\mod n)$

$c^d \equiv m^{ed} \equiv m (\mod n \quad c = m^e (\mod n)$

1976

1962 А.О. Гельфонд

$= a^x, a, p \longrightarrow x \qquad p$ - простое

$x \pmod{p-1} = x_1 + [\sqrt{p-1}]\, x_2$

$x_1 \in \{0, 1, \dots, [\sqrt{p-1}] - 1\}$

$x_2 \in \{0, 1, \dots, [\sqrt{p-1}] + 2\}$

$p-1 < p-1+3[\cdot] - 2\sqrt{p-1}$

$3 \cdot [\cdot] - 1 + (\sqrt{p-1} - 1)^2$

$[\cdot] - 1 + [\cdot]([\cdot] + 2)$

$a^{-1}, a^{-2}, \dots, a^{-[\sqrt{p-1}]}$

mod p [i]

$a^{-i} \pmod{p}$ — $2[\sqrt{p-1}]$ умнож.

$[\sqrt{p-1}]$ память

generic algorithm

$(a^{[\sqrt{p-1}]})^i \pmod{p}$, $i = 1, \dots, [\sqrt{p-1}] + 2$

i, j: $a^{([\sqrt{p-1}] j)} = a^x a^{-i} \pmod{p}$

$a^{i + j[\sqrt{p-1}]} \equiv a^x \pmod{p}$

$i + j[\sqrt{p-1}] \equiv x \pmod{\mathrm{ord}_p a}$

Задача Диффихеллмана

$a^x, a^y, a, p \to a^{xy}$ DH

Кодирование

$1 \to 1101$

$0 \to 0000$

1950

Хэмминг

Расстояние Хэмминга — число позиций, где биты не совпадают

$(0\,1 \dots 1)_4$

$(1\,0\,0 \dots 0)_4$

Упорядоченный код: Пусть это линейное простр. $A(\bar{m}) = \bar{c}$

$(\underbrace{m_1, \dots, m_k}_{\text{инф. биты}}\ \underbrace{c_1 \dots c_r}_{\text{проверочные}})$ — кодовое слово

$A(\bar{m}_1) = \bar{c}_1$

$A(\bar{m}_2) = \bar{c}_2$

$A(\bar{m}_1 + \bar{m}_2) = \bar{c}_1 + \bar{c}_2$

$A(\underbrace{0 \dots 0\overset{i}{1}0 \dots 0}_{k}) = \tilde{c}_i = (\tilde{c}_1 \dots \tilde{c}_k)$

$G \; (\tilde{\varphi}_1, \ldots, \tilde{\varphi}_k) \begin{pmatrix} 0 \\ \vdots \\ 0 \\ 1 \\ 0 \\ \vdots \\ 0 \end{pmatrix} = \tilde{c}_i$, i

$$\begin{pmatrix} 10\ldots0, & \tilde{c}_1 \\ 010\ldots0, & \tilde{c}_2 \\ 00\ldots01, & \tilde{c}_k \end{pmatrix} \qquad 2^r - 1 = n, \quad k = 2^r - 1 - r$$

$m \cdot (E, A^T)$ – порождающая матрица $= (m, mA^T) = (m, (Am^T)^T) = (\bar{m}; \bar{c})$

$$\left(\underset{n}{A, E_r}\right)\begin{pmatrix} m^T \\ c^T \end{pmatrix} = Am^T + c^T = 0 \Rightarrow$$

$\Rightarrow \bar{c} = c \Leftrightarrow$ код. слово

$d = 3$ ⇓ испр. ошибку

мин. число = пров. инфор. сост. из разн. столбцов