

Межрегиональные олимпиады по математике и криптографии

- Проводятся с 1991/92 учебного года
- На базе вузов УМО ИБ
- Приглашаются школьники 8-11 классов
- Очный тур – ежегодно около 2000 школьников
- В 23 городах (XX олимпиада, 2010 год)

Х Х

**Межрегиональная олимпиада школьников
по математике и криптографии**



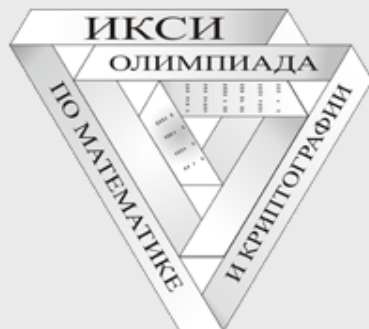
Схема организации

- Заявки вузов на участие
- Ознакомительный тур
- Дистанционный отборочный тур
- Рассылка заданий очного тура
- Очный тур
- Пересылка работ, проверка, критерии
- Размещение результатов, апелляция
- Отчет в РСОШ и заявка на следующий год

Льготы победителям и призерам

- Приказ Минобрауки России «О порядке проведения олимпиад школьников» от 22 октября 2007 года №285
- Ежегодно утверждается Перечень олимпиад школьников
- Льгота 1 уровня: принимаются без вступительных испытаний
- Льгота 2 уровня: приравниваются к набравшим 100 баллов ЕГЭ или дополнительного вступительного испытания





Логин:
Пароль:

[Забыли пароль](#)
[Регистрация](#)

28.02.2011

Критерии определения победителей и призеров XX олимпиады

24.02.2011

Завершается прием апелляций по результатам проверки работ

24.01.2011

Завершена проверка работ всех участников очного тура олимпиады

Олимпиада по математике и криптографии

[Главная](#) [О нас](#) [Задачи](#) [Методика](#) [Новости](#) [История](#) [Файлы](#) [Контакты](#) [Feedback](#)

Новости

26.11.2010

ОБРАЩЕНИЕ вице-президента РАН академика В.В. Козлова к участникам XX Межрегиональной олимпиады школьников по математике и криптографии



Дорогие друзья!

Вы участвуете в юбилейной XX олимпиаде по математике и криптографии.

Криптография - ровесница письменности. Она возникла задолго до Египетских пирамид и к нашему времени, пройдя через этапы «криптография как искусство» и «криптография как ремесло», превратилась в самостоятельную, бурно развивающуюся науку со своими весьма специфическими, но во многом опирающимися на математику методами исследования. Математика и криптография всегда взаимно дополняли и обогащали друг друга. Поэтому не случайно в многовековую историю криптографии вписано много имен видных математиков: Джероламо Кардано, Франсуа Виет, Джон Валлис, Леонард Эйлер. В XX веке становление криптографии как точной математической науки внесли вклад известные ученые К. Шеннон, Р. Винер, А.Н. Колмогоров, В.А. Котельников, А.А. Марков и др.

На протяжении веков руководители государств, политические деятели и высокопоставленные военные активно использовали криптографию. Упомянем в связи с этим греческих полководца Энея и историк Полибия, римского императора Юлия Цезаря, общественного деятеля Цицерона, Френсиса Бэкона, кардинал Ришелье, Оливера Кромвеля, Петра I, Екатерину II, Дж. Вашингтона, Наполеона.

Нередко успехи и неудачи криптографов оказывали серьезное влияние на ход войн, революций, а также определяли внешнюю и внутреннюю политику государств. Характерным примером служит операция «Ультра» в результате которой английские криптографы во время Второй мировой войны смогли дешифровать переписку в сетях связи вооруженных сил Германии. Этот успех в значительной мере переломил ход боевых действий в Атлантическом океане, Средиземноморье и на Западном фронте в пользу антигитлеровской

Публикация материалов олимпиад

Издательский дом «Первое сентября». Учебно-методическая газета.
Выходит с 1992 года

МАТЕМАТИКА

ПОДПИСКА 2011

- Цветная газета с электронными приложениями
- Бумажные и электронные версии
- Скидки для постоянных подписчиков

Оформить подписку

№ 18 – в подарок! Пожалуйста, ознакомьтесь с одним номером газеты.
Вы можете скачать его бесплатно.

РУБРИКИ	№08 (694), 16-30.04.2010	ССЫЛКИ
	Хотите получать свежий номер в день выхода? Оформите электронную подписку! Номера в формате PDF 1-го и 16-го числа каждого месяца. Стоимость подписки на месяц всего 130 рублей.	ГЛАВНАЯ СТРАНИЦА издательского дома "ПЕРВОЕ СЕНТЯБРЯ"
Электронная «Математика» информационный спутник газеты	На финишной прямой Заканчивается апрель, и вместе с последним снегом тает и время, оставшееся до экзамена. Остался месяц, и подготовка к экзамену переходит в завершающую стадию. Прошли всевозможные	ПОДПИСКА РЕКЛАМОДАТЕЛЮ
Колонка редактора		НАШИ КООРДИНАТЫ
Официальные		РЕДКОЛЛЕГИЯ

Публикация материалов олимпиад

ЕДИНАЯ КОЛЛЕКЦИЯ
ЦИФРОВЫХ
ОБРАЗОВАТЕЛЬНЫХ РЕСУРСОВ
Лауреат Премии Правительства РФ в области образования

КАТАЛОГ КОЛЛЕКЦИИ ИНСТРУМЕНТЫ ЭЛЕКТРОННЫЕ ИЗДАНИЯ РЕГИОНАЛЬНЫЕ КОЛЛЕКЦИИ НОВОСТИ КОНТАКТЫ

Введите поисковый запрос, например: [теорема Пифагора](#)
криптография [Расширенный поиск](#) технология ™

→ → [ПОИСК](#)

Найдено документов - 17

	формат
<p>1. Зубов А.Ю. и др. - Олимпиады по криптографии и математике</p> <p>В сборник включены условия, ответы и решения пятнадцати олимпиад по криптографии и математике, проведенных в Москве с 1991 по 2005 гг. Условия задач предварены элементарным введением в криптографию, использующим сюжеты из известных литературных произведений. Для учащихся старших классов, учителей математики и информатики, а также студентов младших курсов, интересующихся вопросами информационной безопасности. [Карточка ресурса]</p>	 pdf 1.03 мб
<p>2. Иван Валерьевич Яценко - "Некоторые математические понятия криптографии"</p> <p>Иван Валерьевич Яценко III Летняя школа "СОВРЕМЕННАЯ МАТЕМАТИКА" (Дубна, 21 июля 2003 года)</p> <p>Будут рассмотрены примеры классических шифров, начиная от древних и до современных. Будет обсужден вопрос как вскрывают шифры замены и перестановки и бывает ли что-то еще и в каком смысле. [Карточка ресурса]</p>	 avi 703.21 мб
<p>3. Иван Валерьевич Яценко - "Основные математические понятия криптографии, занятие второе"</p> <p>Иван Валерьевич Яценко III Летняя школа "СОВРЕМЕННАЯ МАТЕМАТИКА" (Дубна, 27 июля 2003 года)</p> <p>Это занятие будет более теоретическим --- мы обсудим вопрос о построении абсолютно стойкого шифра, как его строить, и почему он не очень удобен на практике. [Карточка ресурса]</p>	 avi 704.28 мб

Примеры задач

XVI Олимпиада

***Гьюь Фюббшн эй яюэовл,
Пфзшэюь юришь эй шчъйфшвл:
Г эйщ юбюрйээпо бвпвл —
С Фюббшн ьюцэю вюылью сйфшвл.***

XV Олимпиада

Задача №3

При зашифровании текста на русском языке (в текстах строчные и заглавные буквы не различались, а пробелы и знаки препинания опускались) каждую букву заменяли парой цифр. При этом, разные буквы текста заменялись разными парами, а одинаковые – одинаковыми. Найдите все возможные места расположения слова **ПОДЪЕЗД** в исходном тексте по зашифрованному тексту:

92 97 36 72 97 92 70 73 97 90 97 72 38 39 74 76 97 34
79 78 97 70 76 74 72 74 73 74 76 70 70 97 76 74 96 74
37 39 75 97 70 39 74 79 39 37 71 74 98 35 94 90 98 97
94 96 74 98 74 76 97

Диск Альберти

Каждое положение диска, получающееся из исходного поворотом на угол, кратный величине сектора, задает соответствие между буквами на диске и на основании. При зашифровании очередной буквы текста, ее заменяли соответствующей ей буквой при текущем положении диска, после чего диск поворачивался на один сектор по часовой стрелке.

Диск Альберти

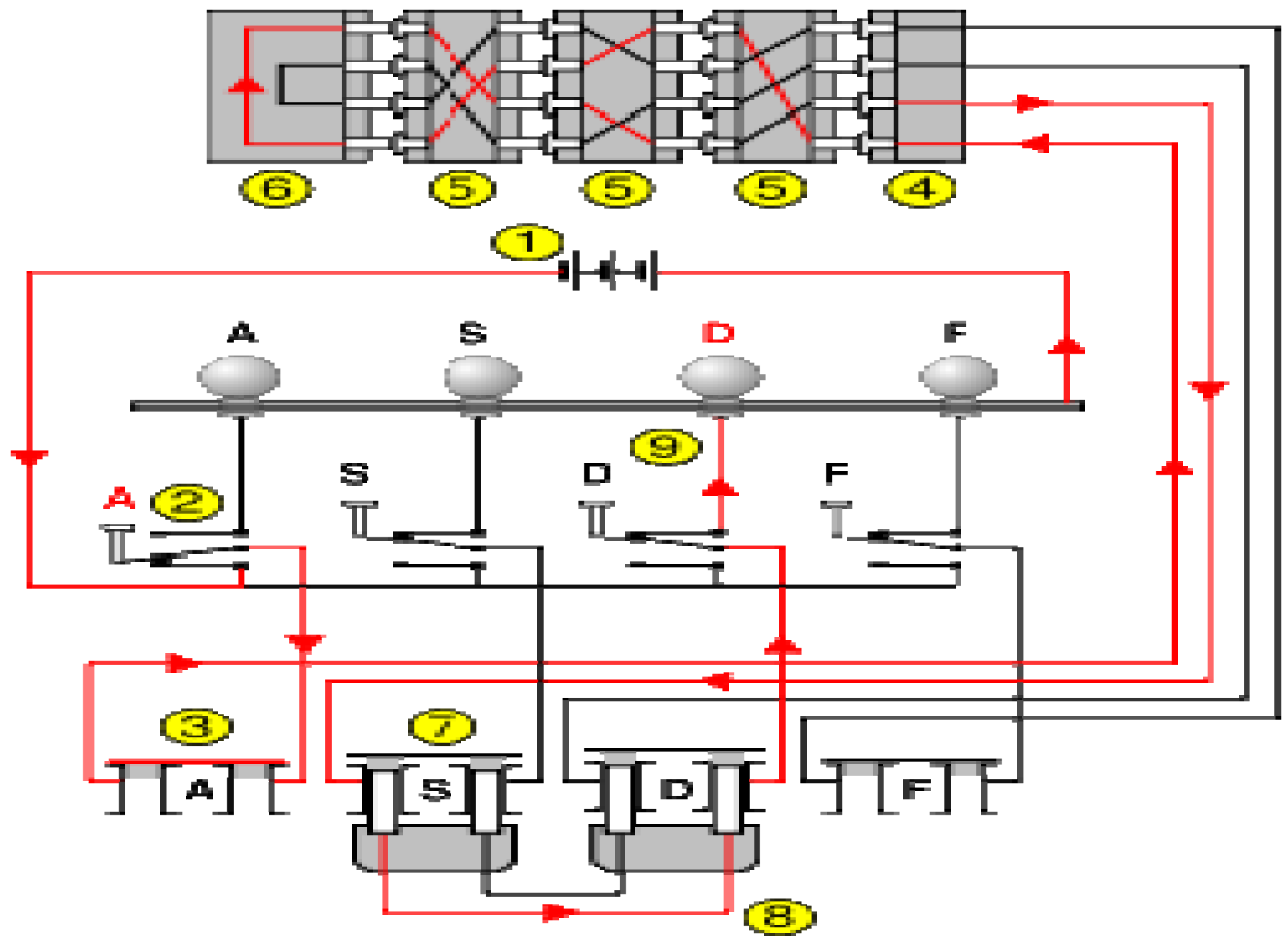
Докажите, что если в результате зашифрования получился текст

*РЖВЦЦФШУФЁУМЙУЩЦЯЦЛМВЧЬБЯ
ВЭЪХПЬМЕДБЙЧМПЬИМЕЕРЧСЩГШ
ТЦЭ*

то в исходном тексте не было слова
КРИПТОГРАФИЯ.

Интернет-олимпиада

Найдите результат зашифрования текста SAFFSDAAS, если известно, что правый ротор сдвигался на один шаг при каждом нажатии клавиши, а остальные роторы - на один шаг после полного оборота соседнего справа ротора. При этом контакты на роторах расположены так, что при сдвиге ротора на один шаг нижний по схеме контакт переходит наверх, а остальные сдвигаются на шаг вниз.



XV Олимпиада по математике и криптографии для 9-11 классов

Задача №1

Докажите, что десятичная запись квадрата натурального числа не может состоять из одинаковых цифр.

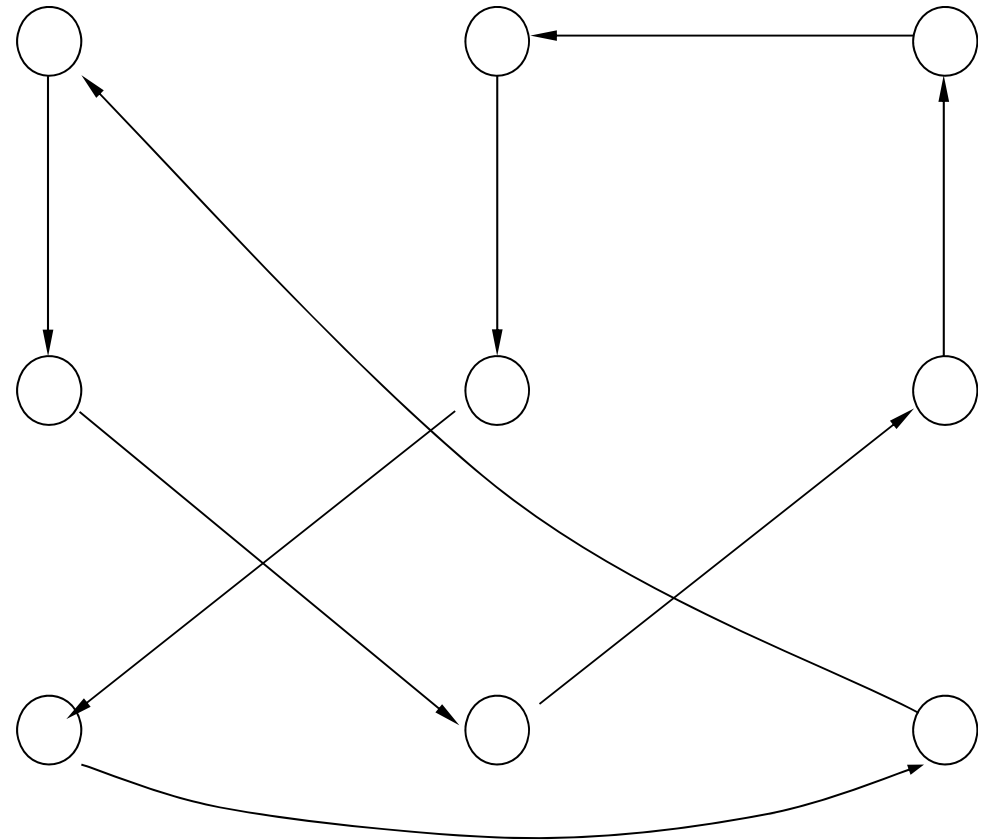
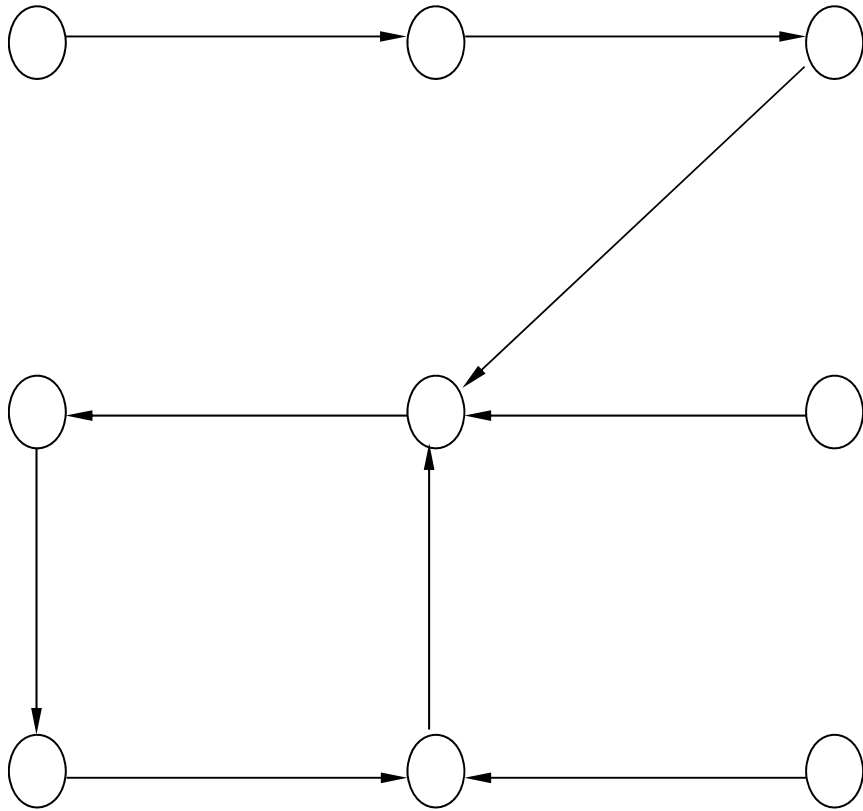
Аладдин в пещере

Аладдин находится в подземелье, состоящем из девяти одинаковых залов, причем он не знает в каком именно. Если он потрет волшебную лампу, Большой Джинн перенесет его в другой зал в соответствии со схемой на левом рисунке. Если Аладдин потрет волшебное кольцо, Маленький Джинн перенесет его в соответствии со схемой на правом рисунке.

Какую последовательность действий с лампой и кольцом надо проделать Аладдину, чтобы он мог утверждать, что находится в центральном зале? Выполнять какие либо другие действия, например, ставить отметки в залах не разрешается. Схемы перемещения Аладдину известны.

-

Аладдин в пещере



Кто больше знает?

Кодовая комбинация замка в хранилище банка состоит из десяти цифр. Один из сотрудников банка случайно узнал, что в этой комбинации не использовалась цифра 0, а другой – что нет одинаковых цифр на соседних местах. Кто из этих сотрудников обладает большей информацией и почему?

XV Олимпиада по математике и криптографии для 9-11 классов

Задача №4 (начало)

Центральный замок автомобиля открывается и закрывается с помощью брелка. При получении сигнала брелка замок открывается (если был закрыт) или закрывается (если был открыт). В брелке и замке имеются счетчики (назовем их СБ и СЗ), на которых изначально было выставлено одно и тоже число.

XV Олимпиада по математике и криптографии для 9-11 классов

Задача №4 (продолжение)

Пусть N – текущее значение СБ. При нажатии на кнопку брелка, СБ меняет значение на $N+1$, старое же значение N в зашифрованном виде передается замку. Микрокомпьютер замка расшифровывает полученный сигнал и находит число, переданное брелком. Если это число равно или превосходит значение СЗ, то замок срабатывает, а значение СЗ становится $N+1$. Если это число оказывается меньше или при расшифровании обнаруживается ошибка, то замок остается в прежнем состоянии

XV Олимпиада по математике и криптографии для 9-11 классов

Задача №4 (окончание)

Злоумышленник способен:

- а) запоминать сигналы брелка,
- б) поставив помеху, исказить сигналы брелка (при этом сам злоумышленник получает сигнал без искажений),
- в) посылать замку ранее запомненные сигналы.

Как злоумышленнику открыть замок? Алгоритмы шифрования и расшифрования ему неизвестны.

Подарок с задержкой

Клара решила подарить Карлу на Новый год один коралл. Сама Клара праздник будет встречать в другом городе, а ей очень хочется, чтобы Карл раньше времени не вытащил подарок из коробки. Поэтому Клара решила положить коробку с подарком в сейф, запирающийся на кодовый замок.

Подарок с задержкой

Комбинацию из цифр $x_1x_2\dots x_{100}$, отпирающую замок, она выбрала так, что на месте с номером i находится последняя цифра $(N+i-100)$ -го числа Фибоначчи. Для подбора подходящего числа N Клара написала программу для компьютера, вычисляющую последовательно числа Фибоначчи, и выяснила, что за одну секунду на компьютере Карла удастся вычислить 500 новых чисел.

Подарок с задержкой

Ровно за 5 суток до Нового года Клара передала Карлу эту программу, сообщила правило построения кодовой комбинации и значение $N=216000000$. Может ли Карл, вообще не используя компьютер, открыть сейф до наступления Нового года? (Примечание: последовательность Фибоначчи определяется так: первые два ее элемента равны 1, а каждый последующий равен сумме двух предыдущих.)

www.cryptolymp.ru