ТАЙНОПИСЬ

В начале было Слово…

Потом появилось много слов.
И очень скоро человек понял,
что слова надо прятать.
Так началось зарождение криптографии.
В переводе с древнегреческого
“криптография” означает “тайнопись”.

Зашифрованная переписка

- *Играли ли вы когда-нибудь в разведчиков?*
- *В этой игре разведчик вынужден вести переписку со своими товарищами так, чтобы никто из посторонних не смог прочитать написанного.*
- *Для этого используют шифровки.*
- *Об одном из способов шифровки текста вы сейчас узнаете …*

Способ решетки

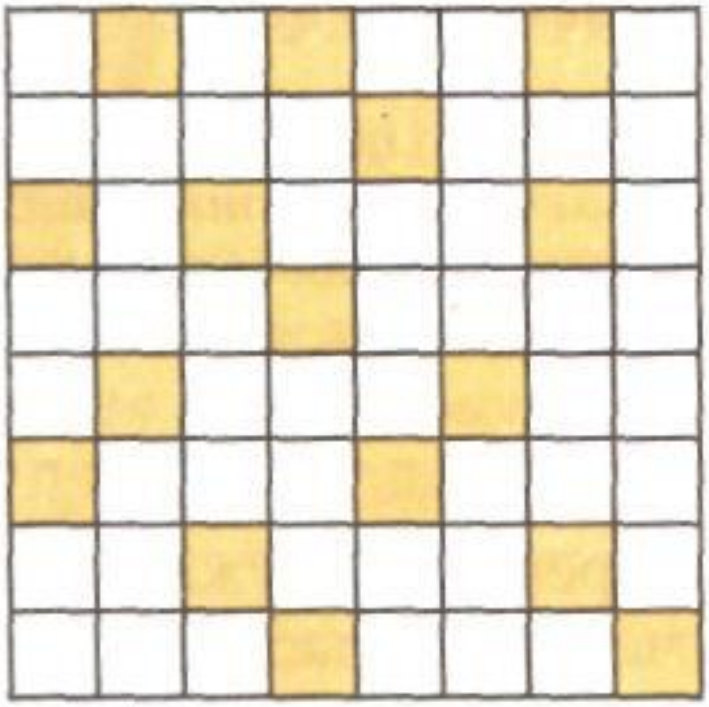


Рис. 133

- *Из плотной бумаги вырежьте квадрат, разделите его на 64 квадратика и прорежьте окошечки (рис. 133).*

Как пользоваться этой решеткой?

Пусть необходимо передать следующее сообщение:
«Наступление планируется 16 сентября пять утра.
Внимание левому флангу. РВС».

- Наложив решетку на листок бумаги, пишут сообщение в окошечках решетки.
- Сначала помещается всего 16 букв: наступление плани...
- Как они расположены, см. на рисунке 134, *а*.

а)

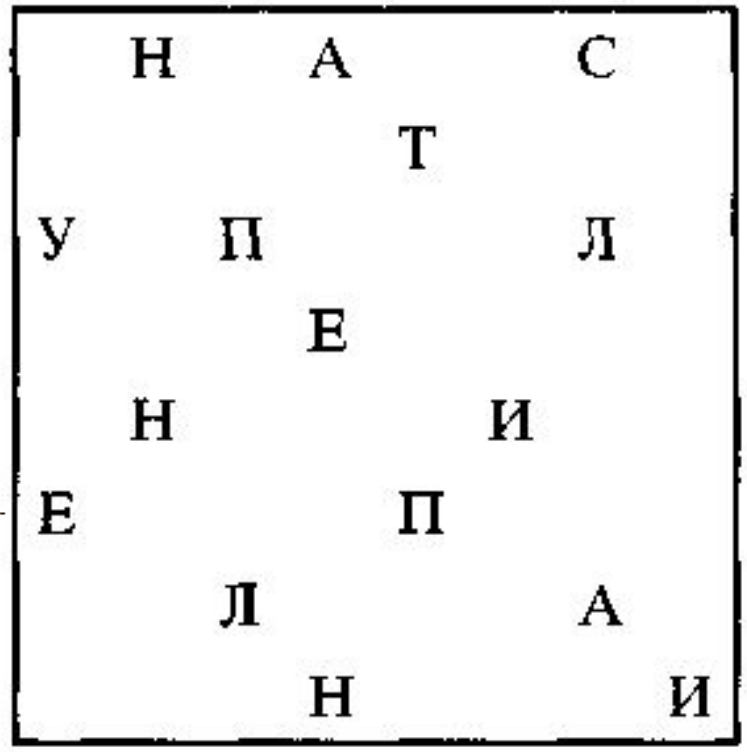


Рис. 134

б)

П	Н	Л	А	Я	Е	С	Р
У	Т	Е	В	Т	Ь	Т	О
У	М	П	У	С	У	Л	Т
Ф	Я	Р	Е	Л	1	А	А
6	Н	Н	С	В	И	Г	Е
Е	Н	Н	У	П	И	Т	М
Я	Р	Л	А	Б	В	А	С
А	Н	Р	Н	И	Я	Е	И

Рис. 134

- **Затем поворачивают решетку против часовой стрелки на 90°.**
- **Все написанные буквы закрыты, в новые окошечки продолжают вписывать текст.**
- **Еще два поворота, и текст вписан.**
- **Если остаются неиспользованные клетки, их заполняют буквами а, б, в... и т. д. (чтобы не было пробелов).**
- **Полностью письмо принимает вид, показанный на рисунке 134, *б*.**

- Его ни за что не прочесть человеку, не имеющему шифровального квадрата.
- А читают так же (накладывая квадрат и поворачивая его против часовой стрелки на 90°).
- После четвертого поворота текст становится ясен адресату…

Из объяснений понятно, что …….

- *Способ шифровки основан на повороте квадрата вокруг его центра.*

- *ПОВОРОТ — геометрическое преобразование фигур, при котором свойства фигур не меняются, может измениться лишь положение фигуры, так как каждая ее точка повернется вокруг некоторой точки на угол поворота.*

- *Квадрат при повороте на 90° вокруг его центра совместится сам с собой.*
- *Каждая же точка внутри квадрата при четырех поворотах на 90° занимает четыре разных положения.*
- *«Окошечки» решетки займут в процессе поворота четыре различных положения.*
- *Чтобы все клеточки 64-клеточного квадрата были заполнены буквами,*

  должно быть 64 : 4 = 16 *окошечек.*

Своя решетка

- Чтобы составить свою решетку, нужно разбить 64-клеточный квадрат на четыре области.
- В первой расставить числа от 1 до 16 в обычном порядке.
- Вторая область получается из первой поворотом по часовой стрелке на 90°.
- Повернув еще на 90°, получим заполнение третьей области, при последнем повороте получается заполнение четвертой области (рис. 135).

1	2	3	4	13	9	5	1
5	6	7	8	14	10	6	2
9	10	11	12	15	11	7	3
13	14	15	16	16	12	8	4
4	8	12	16	16	15	14	13
3	7	11	15	12	11	10	9
2	6	10	14	8	7	6	5
1	5	9	13	4	3	2	1

Рис. 135

- Затем выбирают для окошечек любые 16 клеток, заботясь лишь о том, чтобы в их числе не было клеток с одинаковыми номерами.
- Итак, решетка готова,
можно приступать к шифровке!

На 64-клеточном поле
можно составить
более 4 млрд.
разных секретных решеток!

- Объясним этот факт или,
  как говорят математики, докажем его.

- Клетку № **1** можно взять в качестве окошка в четырех местах.
- В каждом случае можно присоединить клетку № **2**,
  взяв ее также в четырех местах.
- Следовательно, два окошка можно наметить **4x4**,
  т. е. **16** способами.
- Три окошка — **4x4x4 = 64** способами.
- Рассуждая таким образом, устанавливаем,
  что **16** окошек можно набрать **4**x**4**x**4**x...x**4** раз
  (произведение **16** четверок).
- Число это превышает **4** миллиарда.
- Если полагать расчет преувеличенным в несколько раз (так как
  пользоваться решетками с примыкающими друг к другу окошками,
  и эти случаи надо исключить), то все же остается несколько сотен
  миллионов различных решеток.

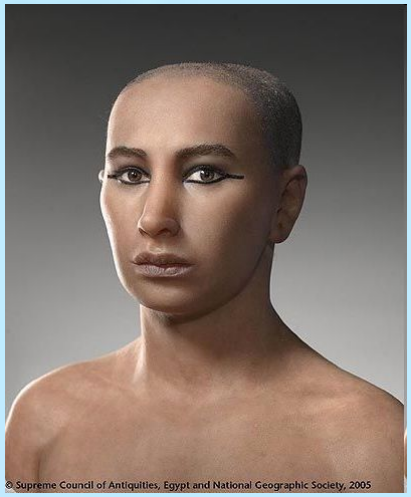
- Попробуй-ка отыскать ту, которая требуется!

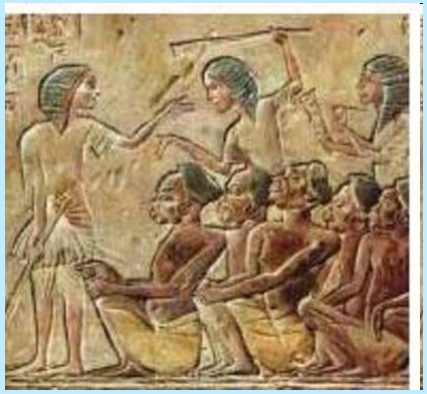
История тайнописи

- Еще до введения в обиход понятия «криптография» человек пользовался сокрытием информации с помощью доступных для своего времени способов.

У египетских фараонов …

- Во времена правления династии египетских фараонов применялся довольно своеобразный метод передачи тайного письма.
- В качестве носителя информации выбирался раб, точнее, его голова.
- Голову брили наголо и водостойкой растительной краской наносили текст сообщения.
- Когда волосы отрастали, его отправляли к адресату.
- После того, как раб-носитель информации добирался по назначению, волосы снова сбривали и читали нанесенный текст.
- Для удобства обработки голову предварительно снимали с плеч.
- Главными недостатками данного метода являлись слабая оперативность передачи сообщений и большая ненадежность.
- Ведь в процессе путешествия носителя сообщения тот мог быть убит, мог заболеть, наконец, просто сбежать.





- **Вообще-то, древнеегипетские фараоны и жрецы были довольно изобретательными криптографами, о чем свидетельствуют сохранившиеся папирусы.**
- **Именно тогда на практике было применено такое понятие, как “криптографический ключ”.**
- **В качестве носителя сообщения применялась узкая и длинная лента папируса, а ключом служила палка строго определенного диаметра.**
- **Папирус наматывался на палку в виде спирали и на него вдоль палки наносился текст передаваемого секретного сообщения.**
- **После этого лента сматывалась и отсылалась адресату.**
- **Тот, в свою очередь, наматывал этот папирус на свою палку точно такого же диаметра и читал это послание. В данной схеме скрытой связи именно диаметр палки являлся ключом.**

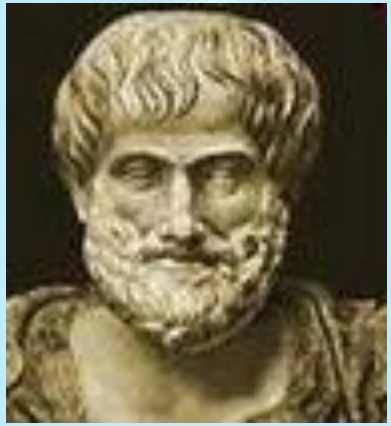
- **Надо сказать, что данный метод сокрытия передаваемых сообщений был довольно широко распространен, вплоть до времен Юлия Цезаря.**

Гай Юлий Цезарь

- **Тот, в свою очередь, значительно усовершенствовал его, усложнив ключ посредством применения переменного диаметра стержня.**

Нерон

- **Кстати, Юлий Цезарь был достаточно одаренным криптографом своей эпохи.**



Аристотель

- **Большой вклад в развитие тайнописи внесли в свое время Аристотель, Пифагор, Нерон.**

Пифагор

Но…

- Большой урон дальнейшему развитию криптографии был нанесен во времена средневековой инквизиции.
- Людей, владеющих основами тайного письма, считали колдунами и безжалостно сжигали на кострах.

И тем не менее …

- Наибольшего расцвета криптография достигла в период Эпохи Возрождения.

Леонардо да Винчи

- Творческие периоды жизни таких великих людей, как Леонардо да Винчи, кардинала Ришелье, Людовиков XII-XIV и других дали толчок к зарождению научного подхода к проблемам тайнописи.

Людовик XII

Кардинал Ришелье

- Именно в эти годы возникло понятие “кодирование сообщений”, т.е. замены букв и цифр открытого текста на буквы, цифры, знаки, согласно заранее обусловленного правила, закона.

Людовик XIII

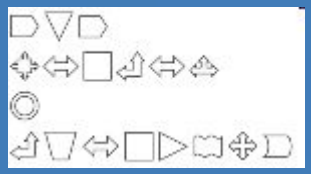
Людовик XIV

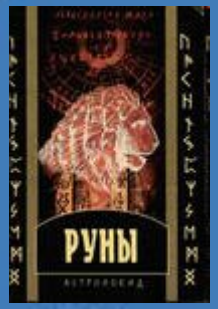
- И именно в это же время было положено начало развитию службы дешифрования и декодирования скрытой информации.

Наконец…

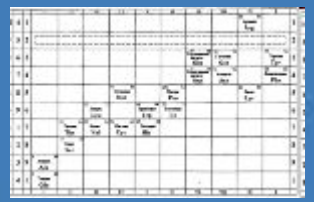
- Окончательное становление криптографии на математическую основу произошло в сороковые-пятидесятые годы XIX-го века.
- Именно в это время были разработаны основы математического шифрования и кодирования, открыты основные полиномы, имеющие самое непосредственное значение для вопросов криптоанализа.

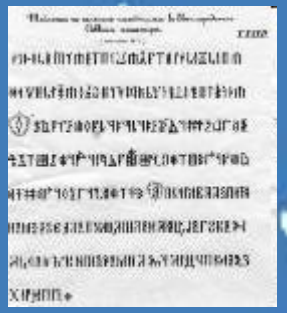
Тайнопись в картинках

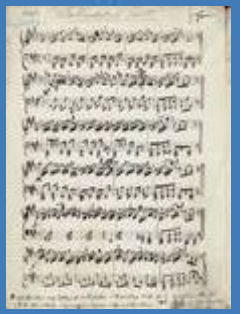




Глаголица	XI – XVI
Литорея	XIII – XVIII
Измененные знаки	XIV
Пермская азбука	XV
Полусловица	XVII
Цифровой разряд	
Вязь	XIX
Греческая азбука	
Цифр. разряд с арабск. цифр.	
Условный порядок букв в слове	
Значковый разряд	
Латинская азбука	
Обратное направление письма	
Нарочито придуманные азбуки	
Тайнопись “в квадратах”	
Описательный разряд	
Акростих	







13 ноября – день шифровальщика

- С древнейших времён люди имели свои секреты и предпринимали все возможные меры к их сохранению.
- Наиболее слабым местом процесса защиты таких сведений всегда была их передача.
- Поэтому тайнопись, кодирование информации возникли ещё на заре цивилизации.
- С появлением государств, а в особенности их специальных служб, работа по зашифровке своих охраняемых сведений и, напротив, расшифровка секретов противника постепенно становились всё более значимыми.
- **Квалификация - специалист по защите информации**
- Специальность - комплексная защита объектов информатизации
- Под грифом особой важности
- Люди этой профессии – шифровальщики, при жизни окружены тайной, а после смерти, оказывается, мало кто знал, что за подвиги они совершили…

Спасибо за внимание!

Волошина Н.Н.
Алматы РК