Государственное бюджетное общеобразовательное учреждение
гимназия № 73 «Ломоносовская гимназия» Выборгского района
Санкт-Петербурга

Возможности криптографии в древнем мире

Работу выполнил: Боревич Андрей Алексеевич, 4.3 класс;

Руководитель: Боревич Ирина Сергеевна

Цель и задачи работы

Рассмотреть возможности некоторых, самых известных и интересных шифров древности

- **познакомиться с историей криптографии,**
- **создать модели некоторых шифров древности,**
- **проверить на практике механизм их использования для передачи сообщений, а также возможность взлома.**

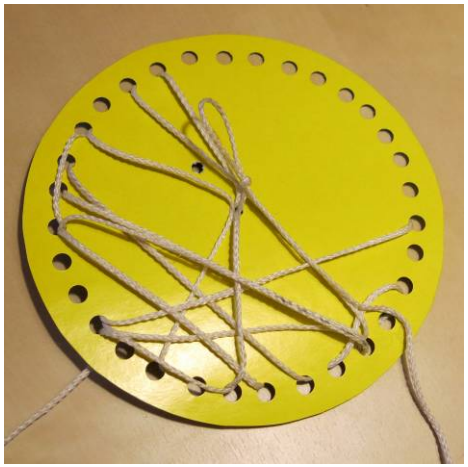
Методы

Чтобы оценить возможности шифров, мы создадим их действующие модели из подручных средств (картон, шнур, деревянные цилиндры) и на практике оценим сложность процесса зашифровки, дешифровки и взлома шифров.

Криптография

(от др.-греч. κρυπτός — скрытый и γράφω — пишу) – это методы сокрытия содержания сообщения с помощью кодов или шифров.

Шифры древности



Диск Энея (Греция, 4 в.д.н.э.)

Квадрат Полибия (Греция, 2 в.д.н.э.)

Скитала (Греция, 7 в.д.н.э.)

Шифр Цезаря (Рим, 1 в.д.н.э.)

Скитала

Тип: шифр перестановки

Период: VII в.до н.э.

криптография в древнем мире

КТАВВМРОФДНИИ ГИРЕПРПЯЕМЕ

Шифр Цезаря

Тип: шифр замены

Период: I в.до н.э.

криптография в древнем мире

НУЛТХСЖУГЧЛВЕ ЗУИЕРИП ПЛУИ

0 НУЛТХСЖУГЧЛВ

1 мткcфретвцкб

2 лсйрупдсбхйа

3 криптография

4 йпзоснвпяузю

…..

Приложение 2. Сравнительная таблица шифров древности

	Тип шифра	Время возникновения	Место возникновения	Сложность зашифровки		Сложность расшифровки		Сложность взлома	Примечания
				время	место	время	место	место	
Скитала	Шифр перестановки	VII в.до н.э.	Спарта (Греция)		4		3	2	Непросто пользоваться для зашифровки и расшифровки сообщений, при этом взломать ее просто, т.к. буквы не заменяются, нужно просто найти правильный порядок
Диск Энея	Стеганография	IV в.до н.э.	Стимфал (Греция)		3		4	1	Шифровать и расшифровывать несложно, но манипуляции с нитью отнимают много времени. Если диск поврежден, дешифровка невозможна
Квадрат Полибия	Шифр замены	II в. до н.э.	Аркадия (Греция)		1		1	4	Просто шифровать и дешифровать, взлом, если буквы расположены в хаотичном порядке – только с применением частотного анализа.
Шифр Цезаря	Шифр замены	I в.до н.э.	Древний Рим		2		2	3	Просто шифровать и дешифровать, взломать можно методом грубой силы (техника «завершение простого компонента»)

Заключение: выводы

- Шифры древности достаточно просты в применении.
- Шифры древности достаточно просто взламываются.
- Изучая шифры древности, мы видим некоторые приёмы, которые присущи сразу нескольким шифрам.

Возможности криптографии Древнего Мира были существенно ограничены, в связи со слабым развитием письменности и математики.

Спасибо за внимание

Еинаминв аз обисапс

Омюожяс ею акжйюкг