Интуитивная криптография (до начала XVI века)

Базовая модель классической криптосистемы



Угрозы в фокусе темы



Шифр Атбаш (Atbash), моноалфавитная замена (substitution) (1 век н.э.)

Открытый текст:

ПРИМЕРШИФРААТБАШ

Α	Б	В	Г	Д	E	Ж	3	И	K	٦	Ź	#	9	5	Р	С	Т	У	Ф	X	Ц	Ч	Ш	Щ	Ъ	Ы	Ь	Э	Ю	Я
Я	Ю	\in	Ь	Ы	Ъ	Щ	Е	Д	Ц	X	Ф	У	Т	U	Р	⊐	0	I	Μ	Л	К	Ν	3	Ж	Е	Д	٦	В	Б	Α

Жифротекст:

СРЧФЪРЗЧМРЯЯОЮЯЗ

Древнерусская тайнопись

Пермская азбука - шифр



VZZJITTATHYITLICVETHIZL 4ETECHISTEISETECICETHYIST TIJUTALIAIKYJ Y Y CYJ Y Y Y K CYJ ITTSACTOR ILLERACTOR SALVERT TH3TAP *** CTTITLULAT JANA TALA LYTINET LYTINET TENTER THAT LCAP 12. 2. 2. LL JELL STULLI HCTVELYSTEGETTEIZEBTY LC+1+CT kTk171k2Tk[TL3Tk JEIRTTYTL, 4KTECHI3TKITIET FCIETTAL SIE LE L'ALVIET L'ALVERTE PA CYETEITICLE IS BELLINISTERY TLZYCVITLILATICATOLITIC 上る。377たブイフムハンしはたい上のたとした YITTHCYTIITULYY, 3YHIJ147426 LTTTLLLITECTICHTLLTLLTLLT 2,717k7k27&**F**11441**V**1**Y**37**L**7,4 SFAFA F LICHSAT TAILTUATAFIRD

Шифр изгороди (rail fence)

Открытый текст:

ПРИМЕРШИФРАИЗГОРОДИ



Шифротекст:

ПИЕШФАЗООИРМРИРИГРД



Простая литорея (ХVІІ век)

Открытый текст:

ШИФРОВКА

Α	Б	В	Γ	Д	Ε	Ж	3	И	К	Л	М	Н	0	П	Р	С	Τ	У	Ф	Х	Ц	Ч	1	Е	Ъ	Ы	Ь	Э	Ю	Я
Α	Щ	Ш	Т	Ц	E	Х	Ф	И	Т	С	Р	П	0	Н	М	Л	К	У	3	Ж	Д		4	Б	Ъ	Ы	Ь	m	Ю	Я

> Шифротекст:

ВИЗМОШТА

бвгджзклмн щшчцхфтсрп

Криптоанализ

- Древнерусская тайнопись, шифры «Атбаш», «Изгородь» «Литорея» основаны ТОЛЬКО на знании алгоритма и статических данных (таблиц замен)
- Это примеры бесключевых шифров
- Взлом подобных шифров НЕ являются предметом криптоанализа

Шифр «Сцитала» (Scytale) (Спарта V век до н.э.)

> Открытый текст:

ПРИМЕРШИФРАСЦИТАЛА

Шифротекст:

ПШЦРИИИФТМРАЕАЛРСА

П	P	И	M	E	P
Э	И	Ф	P	Α	С
ц	И	Т	Α	Л	A

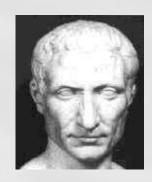


Пример атаки

- ullet Ключом шифра является диаметр цилиндра, который предположительно не может превосходить 10 сантиметров. При высоте строки в 1 сантиметр на одном витке такого жезла уместится не более 32 букв $10\pi < 32$. Таким образом, число перебираемых вариантов вряд ли превосходит 32.
- Методика взлома (Аристотель): на длинный конус наматывалась лента, а затем эту ленту начинали сдвигать по конусу. Там, где буквы текста формировали слова или слоги, диаметр конуса совпадал с диаметром цилиндра.
- Это пример атаки методом «грубой силы» (brute force) полный перебор ключей (секретов) шифра при известном алгоритме зашифровки. Чтобы предотвратить этот тип атаки, число возможных ключей должно быть очень большим

Шифр Цезаря (1 векдо н.э.)

Открытый текст:



ПРИМЕРШИФРАЦЕЗАРЯ

Α	Б	В	Γ	Д	Е	Ж	3	И	К	Л	М	Н	0	Π	Р	С	Т	У	Ф	К	Д	Ъ	Ш	Щ	Ъ	Ы	Ь	Э	Ю	Я
Г	Д	Ε	Ж	3	И	К	Л	М	H	0		Р	n	Н	У	Ф	К	Г	Д	Е	E	Д	Ы	Р	Э	Ю	Я	Α	Б	В

Шифротекст:

ROT13

Еще совсем недавно (в 1980-х годах) применялся метод шифрования ROT13, в котором использовался сдвиг алфавита на 13 букв вместо трех. Этот шифр использовался в различных онлайновых форумах для публикации запрещенной информации, для ее распространения среди пользователей.

Примеры атак

- Атакой грубой силой за n-1 шагов
- Применим метод частотного криптоанализа:
 - Строим гистограмму частот встречаемости символов в шифровке
 - Строим гистограмму частот встречаемости символов в эталонном файле
 - По схожести фрагментов гистограмм принимаем решение о значении смещения (ключа)