СЕКРЕТЫ КРИПТОГРАФИИ

Тайны составляют основу науки, техники и политики любой человеческой формации.

- государственная тайна;
- военная тайна;
- коммерческая тайна;
- юридическая тайна;
- врачебная тайна и т.д.

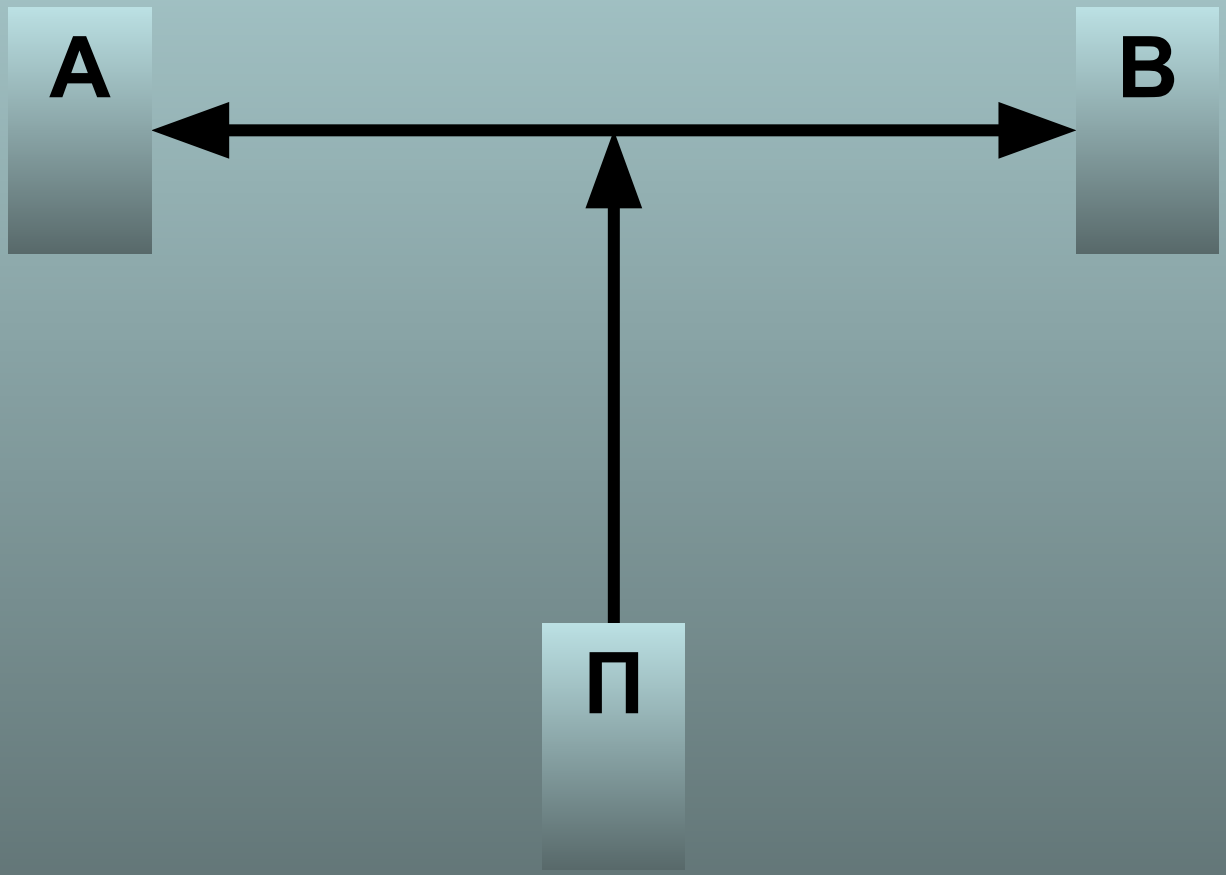
Когда же надо защищать информацию?

В тех случаях, когда есть опасения, что информация станет доступной посторонним, которые могут обратить её во вред законному пользователю.

Зачем необходима защита информации?

Чтобы предотвратить возможный вред от её разглашения.

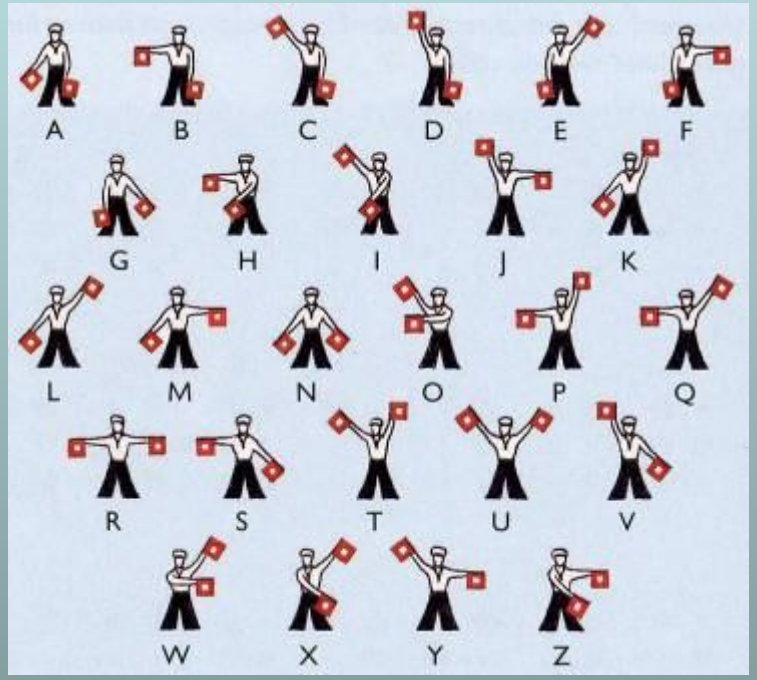
ОСНОВНОЙ ОБЪЕКТ КРИПТОГРАФИИ



Криптография

Стеганография

Шифр


A
B
C
D
E
F
G
H
I
J
K
L
M
N
O
P
Q
R
S
T
U
V
W
X
Y
Z


ПРЕДУПРЕЖДАЮЩИЕ ЗНАКИ
1.1
Железнодорожный переезд со шлагбаумом
1.2
Железнодорожный переезд без шлагбаума
1.3.1
Однопутная железная дорога
1.3.2
Многопутная железная дорога
1.4.1
1.4.2
1.4.3
1.4.4
1.4.5
1.4.6
Приближение к железнодорожному переезду
1.5
Пересечение с трамвайной линией
1.6
Пересечение равнозначных дорог
1.7
Пересечение с круговым движением
1.8
Светофорное регулирование
1.9
Разводной мост
1.10
Выезд на набережную
1.11.1
1.11.2
Опасный поворот
1.12.1
1.12.2
Опасные повороты
1.13
Крутой спуск
12%
1.14
Крутой подъем
12%
1.15
Скользкая дорога
1.16
Неровная дорога
1.17
Выброс гравия
1.18.1
Сужение дороги
1.18.2
1.18.3
Сужение дороги
1.19
Двустороннее движение
1.20
Пешеходный переход
1.21
Дети
1.22
Пересечение с велосипедной дорожкой
1.23
Дорожные работы
1.24
Перегон скота
1.25
Дикие животные
1.26
Падение камней
1.27
Боковой ветер
1.28
Низколетящие самолеты
1.29
Тоннель
1.30
Прочие опасности
1.31.1
1.31.2
1.31.3
Направление поворота

Из истории криптографии

Диск Энея

«Сциталь»

Шифр Цезаря

а	б	в	г	д	е	ж	з	и	й	к	л	м	н	о	п	р	с	т	у	ф	х	ц	ч	ш	щ	ь	ы	ъ	э	ю	я
г	д	е	ж	з	и	й	к	л	м	н	о	п	р	с	т	у	ф	х	ц	ч	ш	щ	ь	ы	ъ	э	ю	я	а	б	в

КРИПТОГРАФИЯ

НУЛТХСЁУГЧЛВ


Russian, 'FAPS'
Fialka 'Magic Circuit'


Russian
T205
This is all I have of another Russian machi designated T205. To prevent further use it has been crushed
Had this been a military capture, the damage is not enough to prevent information being found by careful examination.
Two rotors are quite badly damaged, two just slightly and two not damaged at all

ШИФРЫ ПЕРЕСТАНОВКИ

Например: масло – смола;

кара - арка

(«Сциталь»)

ШИФРЫ ЗАМЕНЫ

А → 1, Б → 2, В → 3, …, Я → 33

ЗАГАДКА → 9 1 4 1 5 12 1

(Шифр Цезаря)

Составляющие любого шифра :

- общее правило, по которому преобразуется исходный текст (алгоритм шифра);
- конкретная особенность именно этой серии шифрованных сообщений (так называемый ключ).

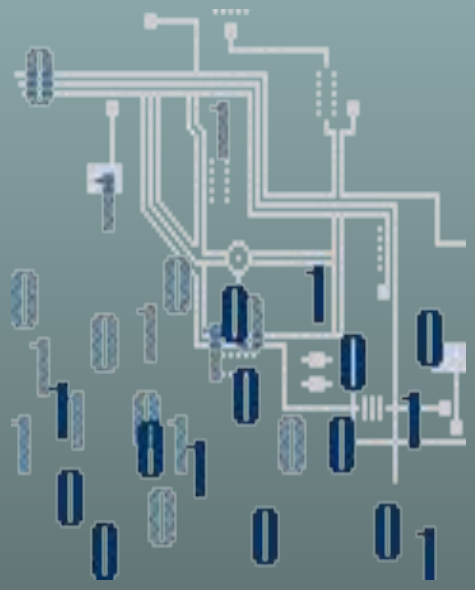
Атака на шифр. Стойкость шифра

Под **атакой на шифр** понимают попытку вскрытия этого шифра.

Под **стойкостью шифра** понимают способность шифра противостоять всевозможным атакам на него.

В криптографии принято работать с универсальным алфавитом, состоящим из двоичных слов некоторой длины.

Телеграфный код - старое техническое применение двоичной системы счисления. Он состоит тоже из 32 символов - двоичных слов длины 5.



__ → 00000, А→ 00001, Б → 00010,

В→ 00011, Г → 00100, Д → 00101, …,

Ю →11110, Я → 11111.

Как выбрать шифр?

- уяснить, что именно противник знает или сможет узнать о шифре,
- какие силы и средства он сможет применить для его вскрытия;

- мысленно встать в положение противника и пытаться с его позиций атаковать шифр.

Вскрытие шифра основано на:

- 1. различные буквы встречаются с разной частотой, а действие подстановки «переносит» эту закономерность на шифрованный текст;
- 2. любой язык обладает так называемой избыточностью, что позволяет с большой вероятностью угадывать смысл сообщения, даже если часть букв в сообщении неизвестна.

Матричный способ

а	б	в	г	д	е	ё	ж	з	и	й	к	л	м	н	о	п
1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17
р	с	т	у	ф	х	ц	ч	ш	щ	ъ	ы	ь	э	ю	я	
18	19	20	21	22	23	24	25	26	27	28	29	30	31	32	33	34

агент б крот

$$\begin{pmatrix} 1 & 4 \\ 6 & 15 \end{pmatrix} \quad \begin{pmatrix} 20 & 34 \\ 2 & 34 \end{pmatrix} \quad \begin{pmatrix} 12 & 18 \\ 16 & 20 \end{pmatrix}$$

Шифр $\begin{pmatrix} 3 & 2 \\ 4 & 3 \end{pmatrix}$

Матрица $\begin{pmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{pmatrix}$

Единичная матрица $\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$

Умножение матриц

$$\begin{pmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{pmatrix} \cdot \begin{pmatrix} b_{11} & b_{12} \\ b_{21} & b_{22} \end{pmatrix} = \begin{pmatrix} a_{11}b_{11}+a_{12}b_{21} & a_{11}b_{12}+a_{12}b_{22} \\ a_{21}b_{11}+a_{22}b_{21} & a_{21}b_{12}+a_{22}b_{22} \end{pmatrix}$$

$$\begin{pmatrix} 3 & 2 \\ 4 & 3 \end{pmatrix} \cdot \begin{pmatrix} b_{11} & b_{12} \\ b_{21} & b_{22} \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$$

$$\begin{pmatrix} 3b_{11}+2b_{21} & 3b_{12}+2b_{22} \\ 4b_{11}+3b_{21} & 4b_{12}+3b_{22} \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$$

$$\begin{cases} 3b_{11}+2b_{21} = 1; \\ 4b_{11}+3b_{21} = 0; \end{cases} \qquad \begin{cases} 3b_{12}+2b_{22}=0; \\ 4b_{12}+3b_{22}=1. \end{cases}$$

$b_{11}=3,\ b_{12}=-2,\ b_{21}=-4,\ b_{22}=3.$

Ключ

$$\begin{pmatrix} 3 & -2 \\ -4 & 3 \end{pmatrix}$$

$$\begin{pmatrix} 1 & 4 \\ 6 & 15 \end{pmatrix} \cdot \begin{pmatrix} 3 & 2 \\ 4 & 3 \end{pmatrix} = \begin{pmatrix} 19 & 14 \\ 78 & 57 \end{pmatrix}$$

$$\begin{pmatrix} 20 & 34 \\ 2 & 34 \end{pmatrix} \cdot \begin{pmatrix} 3 & 2 \\ 4 & 3 \end{pmatrix} = \begin{pmatrix} 196 & 142 \\ 142 & 106 \end{pmatrix}$$

$$\begin{pmatrix} 12 & 18 \\ 16 & 20 \end{pmatrix} \cdot \begin{pmatrix} 3 & 2 \\ 4 & 3 \end{pmatrix} = \begin{pmatrix} 108 & 78 \\ 128 & 92 \end{pmatrix}$$

19 15 78 57 196 142 142 106 108 78 128 92

агент б крот

Шифр Кардано

Лёд тронулся. Командовать парадом буду я. Грузите апельсины бочках.

				1			
2							
							4
				3			

	л		ё			д	
				т			
р		о				н	
			у				
	л				с		
я				к			
		о				м	
			а				н

	л	д	ё		о	д	
			в	т			а
р	т	о			ь	н	
п			у	а			р
	л	а			с	д	
я			о	к			
	м	о			б	м	у
д			а				н

у	л	д	ё	я	о	д	н
ы	г	б	в	т	р	о	а
р	т	о	у	ч	ь	н	з
п	к	и	у	а	а	т	р
х	л	а	а	е	с	д	б
я	а	в	о	к	п	г	е
д	м	о	л	е	б	м	у
д	ь	ж	а	с	з	и	н

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

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

1 – в 4 местах; 2 – в 4 местах,

2 окошка – 4x4 = 16 способов,

3 окошка – 4x4x4 = 64 способа,

16 окошек - 4^{16} способов – более 4000 млн. способов

Как скрыть решетку от противника?

Обозначим окошки цифрой 1, а остальные клетки цифрой 0.

Первый ряд: 01010010,

или, отбросив передний нуль, - 1010010.

Остальные ряды: 1000

10100010

10000

1000100

10001000

100010

10001

$1010010_2 = 64+16+2=82_{10}$

$1000_2 = 8_{10}$

$10100010_2 = 128+32+2 = 162_{10}$

$10000_2 = 16_{10}$

$1000100_2 = 64+4 = 68_{10}$

$10001000_2 = 128+8 = 136_{10}$

$100010_2 = 32 + 2 = 34_{10}$

$10001_2 = 16 + 1 = 17_{10}$