Шифрование информации

ПОДГОТОВИЛ: ШЕРШНЕВ МАТВЕЙ 11"В"

РУКОВОДИТЕЛЬ: ЯНШЕВА ОЛЬГА ВИКТОРОВНА

История шифрования информации.

- Криптография наука о методах обеспечения конфиденциальности, целостности данных аутентификации шифрования.
- История криптографии насчитывает около 4 тысяч лет. В качестве основного критерия периодизации можно использовать технологические характеристики используемых методов шифрования.

История шифрования информации.

- Современный период развития криптографии (с конца 1970-х годов по настоящее время) отличается зарождением и развитием нового направления — криптографии с открытым ключом.
- Практическое применение криптографии стало неотъемлемой частью жизни современного общества её используют в таких отраслях, как электронная коммерция, электронный документооборот, телекоммуникации и других.

История шифрования информации.

- Известны следующие основные способы криптографии:
- 1. Употребление иного алфавита
- 2. Изменение знаков
- 3. Условные знаки или цифр
- 4. Замена одних букв другими по их месту в алфавите
- 5. Запись текста в виде некоторой фигуры, вкраплённой в другой текст
- 6. Написание слов в обратном порядке.

Шифровальные машины.

 Шифрование — обратимое преобразование информации в целях сокрытия от неавторизованных лиц, с предоставлением, в это же время, авторизованным пользователям доступа к ней.
Главным образом, оно служит задачей соблюдения конфиденциальности передаваемой информации.

Шифровальные машины. Энигма.



Виды шифров.

 Шифрование — обратимое преобразование информации в целях сокрытия от неавторизованных лиц, с предоставлением, в это же время, авторизованным пользователям доступа к ней.
Главным образом, оно служит задачей соблюдения конфиденциальности передаваемой информации.

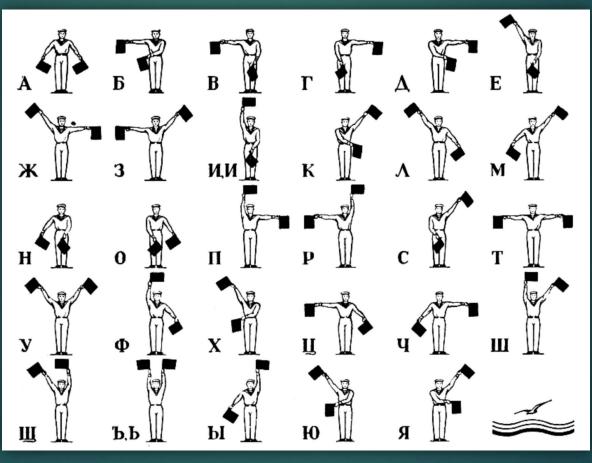
Виды шифров. Шифр Цезаря.

$A \rightarrow E$	$H \rightarrow H$	$P \rightarrow X$	Ш→Э
$P \rightarrow M$	$M \rightarrow O$	С→Ц	Щ→Ю
$B \rightarrow 3$	$K \to \Pi$	$T \rightarrow \Psi$	$R \leftarrow d$
$\Gamma \rightarrow M$	$\Pi \to P$	У → Ш	Ы→А
Д→И	$M \rightarrow C$	Ф→Щ	$P \rightarrow P$
$E \rightarrow K$	$H \rightarrow T$	$X \to P$	$\ni \to B$
$\mathbb{X} \to \mathbb{I}$	$O \rightarrow Y$	Ц→Ы	Ю→Г
$3 \rightarrow M$	$\Pi \to \Phi$	$A \rightarrow P$	Я → Д

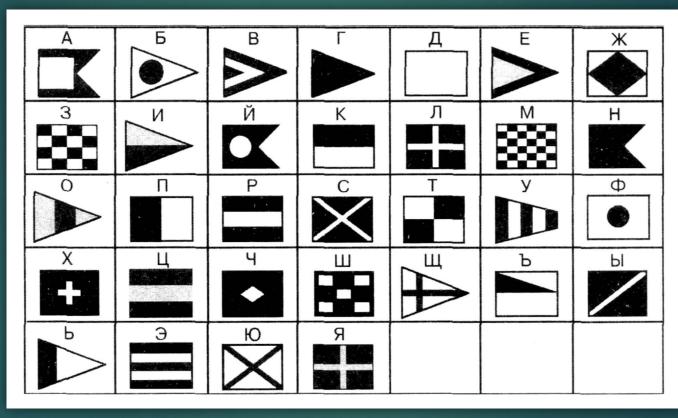
Виды шифров. Азбука Морзе.

A ● —	Л ●−●●	П - • - •
$P - \bullet \bullet \bullet$	M	u •
В •−−	H − •	Ш
$\Gamma ullet$	0	щ•-
д -••	Π • − − •	P • • - •
E ●	P ● - ●	PI - •
Ж ●●● —	C • • •	$P - \bullet \bullet -$
3 • •	T -	Э ● ● − ● ●
И • •	у • • −	Ю • •
й •	$\Phi \bullet \bullet - \bullet$	я • - • -
K - • -	$X \bullet \bullet \bullet \bullet$	

Виды шифров. Семафорная азбука.



Виды шифров. Флажковая азбука.



Виды шифров. Кодировочные таблицы.

A	192	11000000	P	208	11010000
Б	193	11000001	C	209	11010001
В	194	11000010	T	210	11010010
Г	195	11000011	У	211	11010011
Д	196	11000100	Φ	212	11010100
${f E}$	197	11000101	X	213	11010101
Ж	198	11000110	Ц	214	11010110
3	199	11000111	Ч	215	11010111
И	200	11001000	Ш	216	11011000
Й	201	11001001	Щ	217	11011001
К	202	11001010	Ъ	218	11011010
Л	203	11001011	Ы	219	11011011
M	204	11001100	Ь	220	11011100
H	205	11001101	Э	221	11011101
Ο	206	11001110	Ю	222	11011110
П	207	11001111	Я	223	11011111

Практическая часть.



Спасибо 32 BHIMAHIE!!!