ЗАДАЧА

Мне нужно передать молодому человеку записку

«ЗАВТРА В СЕМЬ НА ТОМ ЖЕ МЕСТЕ».

Я хочу, чтобы моя подруга, которой поручено это сделать, не узнала содержание моего письма.

Как передать сообщение таким образом, чтобы исключить его прочтение посторонним лицом?

Криптографические методы защиты информации

ПРОСТЕЙШИЕ МЕТОДЫ ШИФРОВАНИЯ

Проблемой защиты информации путём её преобразования занимается криптология (kryptos – тайный, logos – наука)

Основные этапы развития криптологии

- 1. Эра донаучной криптологии, являвшейся ремеслом — уделом узкого круга искусных умельцев.
- 2. 1949 год, работа К. Шеннона «Теория связи в секретных системах», в которой проведено фундаментальное научное исследование шифров и важнейших вопросов их стойкости. Криптология оформилась как прикладная математическая дисциплина.
- 3. 1976 год, работа У. Диффи, М. Хеллмана «Новые направления в криптографии», где показано, что секретная связь возможна без предварительной передачи секретного **ключа.**

Криптология

Криптография	Криптоанализ
наука, занимающаяся поиском и исследованием математических методов преобразования информации.	наука, которая исследует возможности расшифровывания информации без знания ключа.

МЕТОДЫ КРИПТОГРАФИЧЕСКОГО ЗАКРЫТИЯ

- Шифрование – вид криптографического закрытия, при котором преобразованию подвергается каждый символ защищаемого сообщения.
- Кодирование – вид криптографического закрытия, когда некоторые элементы защищаемых данных (это не обязательно отдельные символы) заменяются заранее выбранными кодами (цифровыми, буквенными, буквенно-цифровыми сочетаниями).

Основные понятия

- Алфавит
- Открытый текст
- Закрытый текст
- Шифрование
- Дешифрование
- Ключ

Виды шифрования

- Замена
- Перестановка
- Аналитическое преобразование
- Гаммирование
- Комбинированные методы

Методы замены

- Метод моноалфавитной замены
- Метод полиалфавитной замены

Моноалфавитная замена

Алфавит открытого текста

АБВГДЕЖЗИЙКЛМНОПРСТУФХЦЧШЩЪЫЬЭЮЯ

Алфавит шифротекста

ЯЮЭЬЫЪЩШЧЦХФУТСРПОНМЛКЙИЗЖЕДГВБА

Символ алфавита открытого текста заменяется на стоящий под ним символ алфавита шифротекста

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 Ъ Ы Ь Э Ю Я _
_ Я Ю Э Ь Ы Ъ Щ Ш Ч Ц Х Ф У Т С Р П О Н М Л К Й И З Ж Е Д Г В Б А

ОТКРЫТЫЙ ТЕКСТ

ЗАВТРА_В_СЕМЬ_НА_ТОМ_ЖЕ_МЕСТЕ

З-Щ А-_ В-Ю Т-О Р-Р А-_ _-А В-Ю _-А С-П Е-Ы М-Ф Ь-Д _-А Н-У А-_ _-А Т-О О-Т М-Ф _-А Ж-Ъ Е-Ы _-А М-Ф Е-Ы С-П Т-О Е-Ы

Щ_ЮОР_АЮАПЫФДАУ_АОТФАЪЫАФЫПОЫ

ШИФРОТЕКСТ

Щ_ЮОР _АЮАП ЫФДАУ

АОТФ АЪЫАФ ЫПОЫ

Полиалфавитная замена
(Метод Вижинера)

А Б В Г Д Е Ж З И К Л М Н О П Р С Т У Ф Х Ц Ч Ш Щ Ъ Ы Ь Э Ю Я _
_ А Б В Г Д Е Ж З И К Л М Н О П Р С Т У Ф Х Ц Ч Ш Щ Ъ Ы Ь Э Ю Я
Я _ А Б В Г Д Е Ж З И К Л М Н О П Р С Т У Ф Х Ц Ч Ш Щ Ъ Ы Ь Э Ю
Ю Я _ А Б В Г Д Е Ж З И К Л М Н О П Р С Т У Ф Х Ц Ч Ш Щ Ъ Ы Ь Э
Э Ю Я _ А Б В Г Д Е Ж З И К Л М Н О П Р С Т У Ф Х Ц Ч Ш Щ Ъ Ы Ь
Ь Э Ю Я _ А Б В Г Д Е Ж З И К Л М Н О П Р С Т У Ф Х Ц Ч Ш Щ Ъ Ы
Ы Ь Э Ю Я _ А Б В Г Д Е Ж З И К Л М Н О П Р С Т У Ф Х Ц Ч Ш Щ Ъ
Ъ Ы Ь Э Ю Я _ А Б В Г Д Е Ж З И К Л М Н О П Р С Т У Ф Х Ц Ч Ш Щ
Щ Ъ Ы Ь Э Ю Я _ А Б В Г Д Е Ж З И К Л М Н О П Р С Т У Ф Х Ц Ч Ш
Ш Щ Ъ Ы Ь Э Ю Я _ А Б В Г Д Е Ж З И К Л М Н О П Р С Т У Ф Х Ц Ч
Ч Ш Щ Ъ Ы Ь Э Ю Я _ А Б В Г Д Е Ж З И К Л М Н О П Р С Т У Ф Х Ц
Ц Ч Ш Щ Ъ Ы Ь Э Ю Я _ А Б В Г Д Е Ж З И К Л М Н О П Р С Т У Ф Х
Х Ц Ч Ш Щ Ъ Ы Ь Э Ю Я _ А Б В Г Д Е Ж З И К Л М Н О П Р С Т У Ф
Ф Х Ц Ч Ш Щ Ъ Ы Ь Э Ю Я _ А Б В Г Д Е Ж З И К Л М Н О П Р С Т У
У Ф Х Ц Ч Ш Щ Ъ Ы Ь Э Ю Я _ А Б В Г Д Е Ж З И К Л М Н О П Р С Т
Т У Ф Х Ц Ч Ш Щ Ъ Ы Ь Э Ю Я _ А Б В Г Д Е Ж З И К Л М Н О П Р С
С Т У Ф Х Ц Ч Ш Щ Ъ Ы Ь Э Ю Я _ А Б В Г Д Е Ж З И К Л М Н О П Р
Р С Т У Ф Х Ц Ч Ш Щ Ъ Ы Ь Э Ю Я _ А Б В Г Д Е Ж З И К Л М Н О П
П Р С Т У Ф Х Ц Ч Ш Щ Ъ Ы Ь Э Ю Я _ А Б В Г Д Е Ж З И К Л М Н О
О П Р С Т У Ф Х Ц Ч Ш Щ Ъ Ы Ь Э Ю Я _ А Б В Г Д Е Ж З И К Л М Н
Н О П Р С Т У Ф Х Ц Ч Ш Щ Ъ Ы Ь Э Ю Я _ А Б В Г Д Е Ж З И К Л М
М Н О П Р С Т У Ф Х Ц Ч Ш Щ Ъ Ы Ь Э Ю Я _ А Б В Г Д Е Ж З И К Л
Л М Н О П Р С Т У Ф Х Ц Ч Ш Щ Ъ Ы Ь Э Ю Я _ А Б В Г Д Е Ж З И К
К Л М Н О П Р С Т У Ф Х Ц Ч Ш Щ Ъ Ы Ь Э Ю Я _ А Б В Г Д Е Ж З И
И К Л М Н О П Р С Т У Ф Х Ц Ч Ш Щ Ъ Ы Ь Э Ю Я _ А Б В Г Д Е Ж З
З И К Л М Н О П Р С Т У Ф Х Ц Ч Ш Щ Ъ Ы Ь Э Ю Я _ А Б В Г Д Е Ж
Ж З И К Л М Н О П Р С Т У Ф Х Ц Ч Ш Щ Ъ Ы Ь Э Ю Я _ А Б В Г Д Е
Е Ж З И К Л М Н О П Р С Т У Ф Х Ц Ч Ш Щ Ъ Ы Ь Э Ю Я _ А Б В Г Д
Д Е Ж З И К Л М Н О П Р С Т У Ф Х Ц Ч Ш Щ Ъ Ы Ь Э Ю Я _ А Б В Г
Г Д Е Ж З И К Л М Н О П Р С Т У Ф Х Ц Ч Ш Щ Ъ Ы Ь Э Ю Я _ А Б В
В Г Д Е Ж З И К Л М Н О П Р С Т У Ф Х Ц Ч Ш Щ Ъ Ы Ь Э Ю Я _ А Б
Б В Г Д Е Ж З И К Л М Н О П Р С Т У Ф Х Ц Ч Ш Щ Ъ Ы Ь Э Ю Я _ А

ОТКРЫТЫЙ ТЕКСТ

ЗАВТРА В СЕМЬ НА ТОМ ЖЕ МЕСТЕ

КЛЮЧ – СОЛНЦЕ

А Б В Г Д Е Ж З И К Л М Н О П Р С Т У Ф Х Ц Ч Ш Щ Ъ Ы Ь Э Ю Я _
С Т У Ф Х Ц Ч Ш Щ Ъ Ы Ь Э Ю Я _ А Б В Г Д Е Ж З И К Л М Н О П Р
О П Р С Т У Ф Х Ц Ч Ш Щ Ъ Ы Ь Э Ю Я _ А Б В Г Д Е Ж З И К Л М Н
Л М Н О П Р С Т У Ф Х Ц Ч Ш Щ Ъ Ы Ь Э Ю Я _ А Б В Г Д Е Ж З И К
Н О П Р С Т У Ф Х Ц Ч Ш Щ Ъ Ы Ь Э Ю Я _ А Б В Г Д Е Ж З И К Л М
Ц Ч Ш Щ Ъ Ы Ь Э Ю Я _ А Б В Г Д Е Ж З И К Л М Н О П Р С Т У Ф Х
Е Ж З И К Л М Н О П Р С Т У Ф Х Ц Ч Ш Щ Ъ Ы Ь Э Ю Я _ А Б В Г Д

ЗА ВТ Р А_ В_С ЕМЬ_ НА _ТОМ_ЖЕ_ МЕСТЕ

СОЛНЦЕСОЛНЦЕСОЛНЦЕСОЛНЦЕСОЛНЦ

З-Ш А-О В-Н Т-Ю Р-Д А-Е _-Р В-Р . . .

ШИФРОТЕКСТ

ШОНЮ ДЕРР ....

Зашифровать методом Вижинера

выражение

«Ученье – свет, а неученье – тьма»

с помощью ключа – **школа**

А теперь **обратная задача**

Попробуйте расшифровать сообщение

«Щылнн стуто ч_хцс тцужп

кчз_ц оукьа клквд»

Ключ – **защита**

(обучающимся раздают таблицы Вижинера)

щылннстуточ_хцстцужпкчз_цоукьаклквд

з амен азаменазаменаз аменазаменазамен

Находим букву «щ» в алфавите, начинающемся на букву «з», поднимаемся вверх до пересечения с первой строкой. На пересечении получаем букву исходного текста «т».

Аналогично получаем

ы-ы л-_ н-з н-а с-с т-л у-у т-ж о-и ч-л _-_

х-о ц-ц с-е т-н ц-к у-у ж-_ п-п к-я ч-т з-ь…

Домашнее задание

Найти в интернете информацию и подготовить сообщение на тему «Случаи применения различных способов шифрования в истории»

Всем спасибо за урок!