

# СЕТИ. БЕЗОПАСНОСТЬ

Урок № 24

Простые алгоритмы шифрующего кодирования.

## Memory line

Кодирование vs  
Шифрование vs  
Стеганография



# Три кита

---

**Кодирование** — Как записать, чтобы потом можно было прочитать



# Три кита

---

**Кодирование** — Как записать, чтобы потом можно было прочитать

**Шифрование** — Как записать, чтобы другие не могли прочитать



# Три кита

---

**Кодирование** — Как записать, чтобы потом можно было прочитать

**Шифрование** — Как записать, чтобы другие не могли прочитать

**Стеганография** — Как записать, чтобы другие не нашли, ЧТО читать



Немного разогреем мозг

Нмнз оеоа гггр рзое оемм

# Виды шифрования

Представьте, что вы ученик 3-го класса...

Как изменить сообщение, чтобы его не прочитали?

# Виды шифрования

Представьте, что вы ученик 3-го класса...

Как изменить сообщение, чтобы его не прочитали?

Сдвиг по  
алфавиту

Замена  
алфавита

Перестановка



# «Сникерс» - Простая перестановка

---

Окм оргь сетйемсоп - иетьнатс в ьтатичорпг (омсотк).



«Сникерс»

Онжолск ати лежуен?

# «Цезарь» - Простой сдвиг // Замена алфавита

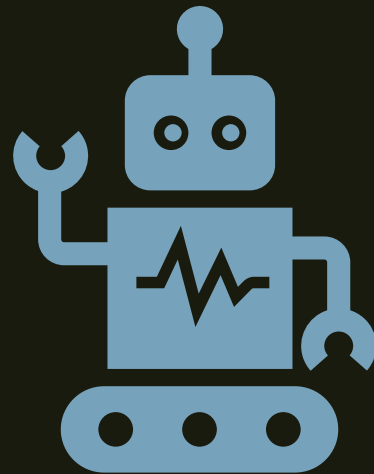
Бажашц, ода яц гэашяа!

Юъгщъ! Врульз - эънэрш ыъъэюъх лчощфюш.

Йоуёсётоп, лбл юуп нпзоп бгупнбуйийспгбуэ?

# Практика

---





# Простой анализ

оТежм ена анил!з- Д вайаетс олнжееу еж!




«Сибирский»

Побу пое рм ...

Чтал оаг? зом рт и

Чтумрир! оанпда зиюум ктмш эао лК ?





«Сибирский»

БОЛЬШАЯ подсказка:

абеёно вджмп гзлр икс йт

# «Сибирский» - схема

Этлгтр оаооу трпд имн те е

Этлгтр  
оаооу  
трпд  
имн  
те  
е

Этот алгоритм потруднее



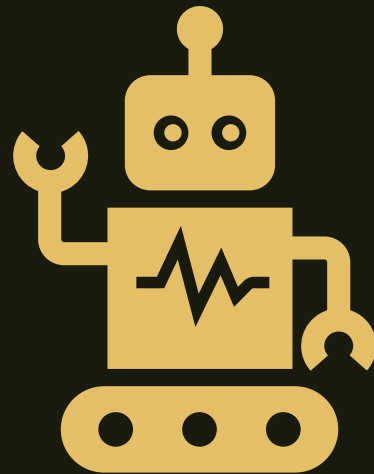
# «Сибирский» - задачи

---

- Знлгабол ааороге яр,тог иманч ттме ьа н
- Глоетивы аннстк впуьу рпнб оой до н
- Умощтелся еяу,отътнм нщепапеае еирвради неаовнн пдсеаа  
отдмд озиа иэз тм и

# Практика

---



# Простой Анализ. «СибирскийХард»

Этиш тоол кс!с оомр п

Тоне ал!ж м,ми еепу уирд снил еонж

Маза яоыэ нем, бнбб тепа ееро ишлр матм ьайт чалв !н,н оиио  
ьблг яииз кмоо ми

# «СибирскийХард+»

Крди муоо ле к сг- во л !оав

Гоь сну твше ов-о увйо б , лву о .а где укхв о

Кл у Кт еки , ля ааку аевф т ни чд р р рн фаи еит саал  
рса иино ммла ао о сза оя л ситс лммд гкти еео оочо нерч  
тжве ягги пеон оаме тди ол яйкс ь . лтня уиаи жкна аз