

## Список вопросов к к р 2

по курсу Теория автоматов и шифров. 2023/2024 уч год

- 1) Что такое шифр перестановки? На чем основан шифр перестановки?
- 2) Что такое шифр сцитала? На чем основывается шифр сцитала?  
Какой максимальный диаметр жезла мог быть использован для шифра сцитала? Каким образом предполагается расшифровывать шифр сцитала?
- 3) Что такое шифр магического квадрата, и каков принцип его действия?
- 4) На чем основывается принцип работы шифра Виженера? Что лежит в основе шифра Виженера?
- 5) Что такое шифр гаммирования? Кто предложил шифр гаммирования?
- 6) Что выбирается в качестве ключа в шифре гаммирования?
- 7) В чем отличие шифра Виженера от шифра гаммирования?
- 8) Какими методами обеспечивается конфиденциальность информации.
- 9) Что такое целостность информации.
- 10) Алгебраическая модель шифра.
- 11) Вероятностная модель шифра.
- 12) Математические модели открытого текста