Учреждение образования

«БЕЛОРУССКИЙ ГОСУДАРСТВЕННЫЙ ТЕХНОЛОГИЧЕСКИЙ УНИВЕРСИТЕТ»

Исследование блочных шифров

Студент: Валдайцев А. Д.

ФИТ 3 курс 5 группа

Преподаватель: Савельева М. Г.

Минск 2023

# Алгоритм DES

Краткое описание самого алгоритма

# Зашифрование

Разделение на блоки

Дополнение блоков

Валидация ключа

# Расшифрование

# Лавинный эффект

Теория и скрины выполнения

# Алгоритм DES-EEE2

Пару строк: описание смысла и код

# Слабые и полуслабые ключи

Теория + **влияние ключей на лавинный эффект** (туду: реализовать это гавно в джаве)

# Время выполнения зашифрования и расшифрования

Просто графики

# Оценка степени сжатия шифротекста

+ пояснения почему так нахуй

# Вывод