

# Моделирование шифровальной машины Энigma

Макаревич Арсений Рустемович

МГУ им. М.В. Ломоносова

2025

# Введение



# Создание шифровальной машины Энigma

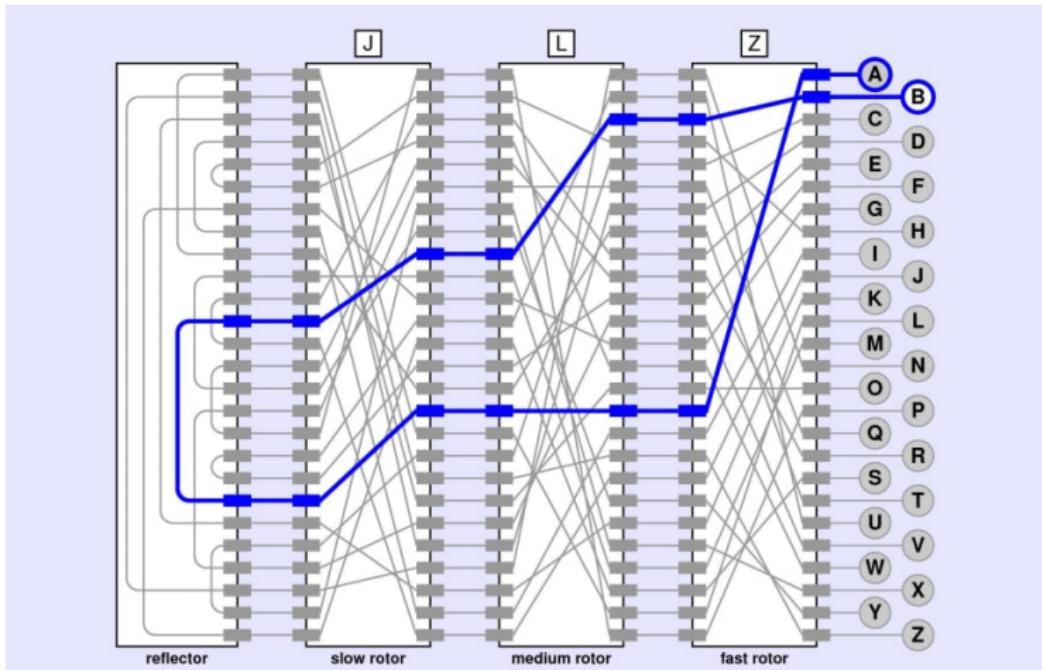


Рис.: Энигма с 4-мя роторами

# Компоненты

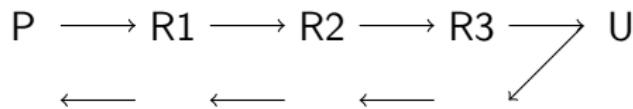


# Принцип работы

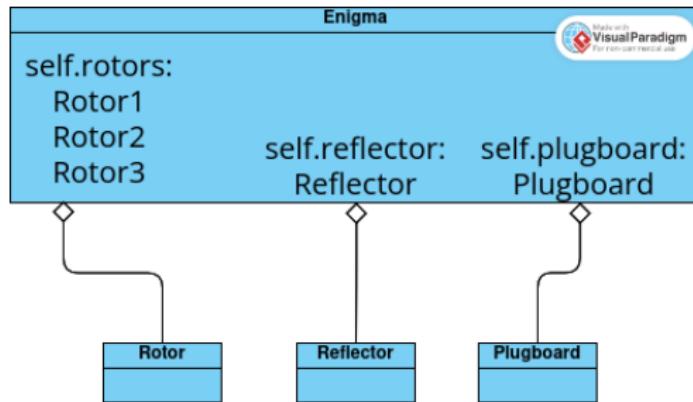


# Математическая модель

$$E(x) = P^{-1}(R_3^{-1}(R_2^{-1}(R_1^{-1}(U(R_1(R_2(R_3(P(x))))))))$$



# Программная реализация



Сообщение	Шифротекст
ATTACK	FAEMDM
SECRET	RKIVCW

# Криптостойкость

$1.58 \times 10^{20}$  вариантов

# Взлом через известные комбинации



- Частые слова: "EINS"
- Метод "меню"
- Перебор 17576 позиций

# Выводы

- 1 Точная модель
- 2 Уязвимость к атакам
- 3 Историческая значимость

# Спасибо за внимание!