**Настя:** Здравствуйте, мы команда крафсед, в рамках первого творческого проекта нами была разработана скоростная криптографическая аппаратно-программная система шифрования.

Перед нами стояла задача создать описание для программируемой логической интегральной схемы на языке описания аппаратуры VHDL. Так же необходимо было разработать корпус устройства.

**Никита:**  Наша реализация “Кузнечика” аппаратная, она в разы быстрее программных аналогов. Мы можем выполнять несколько циклов и распараллеливать однотипные задачи, для достижения высокой скорости вычислений.

Так же алгоритм кузнечик является современным и часто используемым в отечественных разработках. Например он лежит в основе платёжной системы мир. Наше устройство миниатюрно, что так же является плюсом.

Основные потребители подобных продуктов это государственные струтуры и банковская сфера. Устройство подходит и для личного пользования но в ходе разработки проекта мы не учитывали данную перспективу так как отследить круг заинтересованных лиц представляется невозможным

Наша реализация является упрощённой, мы урезали количество раундов с 10 до 5 а также уменьшили размер блока данных и ключа до 16 и 32 бит соответственно.

**Даня.** Раунды состоят из трех основных функций. Побитовый ксор блока входных данных и раундового ключа, далее происходит замена блока данных в соответствии с таблицей подстановок, которая может быть модифицирована под каждое устройство. Последним шагом выполняется линейное преобразование, основанное на умножении подблоков в полях Галуа.

На этом слайде описан процесс создания раундового ключа. Он состоит из тех же этапов, что и процесс шифрования текста, за **исключением** использования других итерационных констант вместо раундовых ключей.

Перейдем к итогам работы. Мы создали модель в САПР там жто самое, напечатали ее на 3д принтере. устройство вышло миниатюрным.

**Я:** Для проверки работоспособности составленной схемы были произведены симуляционные тесты алгоритма. Успешные результаты представлены на слайде. Слева зашифровка справа расшифровка, строки совпадают, следовательно система работает.

На этом слайде представленна финальные архитектура устройсва, софт- процессор со всей обвязкой для коректной работы системы.

На данном слайде вы можете видеть электронные схемы отдельных ip-ядер шифрования и дешифрования, специализированных модулей для подключения к процессору.

Спасибо за внимание, по приложенным qr-кодам вы можете ознакомиться с исходным кодом проекта а так же прочесть статью о том как создавалось это устройство.