Дополнительные задания к экзамену

Вместо практических занятий

(Контроллер освещения, 5 баллов за практические занятия; в общей оценке учитывается с коэффициентом 0,4) В выданном вам комплекте присутствуют микроконтроллер STM32L151CC с радиомодулем SX1276 (на отладочной плате `unwd-range-l1-r3`) и датчик освещенности OPT3001. Напишите программу, опрашивающую датчик с периодичностью 1 раз в 120 секунд и отправляющую сообщение в сеть LoRaWAN с текущим значением освещенности в люксах, упакованным в пакет формата `caynne-lpp` (тип данных - Illuminance Sensor, датчик освещенности; используйте функцию `cayenne_lpp_add_luminosity`). Кроме того, устройство должно работать в сети LoRaWAN, как устройство класса C, и при получении от сервера пакета с двумя байтами "ON" (ASCII-коды символов `0x4F`, `0x4E`) включать светодиод, подключенный к выводу `LED0_PIN`, а при получении пакета с тремя байтами "OFF" (`0x4F`, `0x46`, `0x46`) - выключать его.

«AES устарел, длина ключа всего 128 бит»

(10 баллов за весь курс, как и было обещано на одной из лекций) Ниже приведены 10 пар «открытый текст - шифротекст», шифрование во всех случаях осуществлялось с использованием алгоритма AES-128, с одним и тем же ключом в режиме ECB (electronic codebook). Назовите использованный ключ шифрования (до 21:00 по московскому времени 29.03.2022).

`ff6bab4a1b22af536a4bdd1bb64efd38` — `67760c155699907f360367533eef2f9d`
`4ce53c48b4cd8f90c1c53c7c1472d0c7` — `6c3de4e26f18a694afb2a381a409175e`
`6378d1172dabeb849ad56d760e4a09c9` — `4fab6ae789f2f248d51cc30c166e3311`
`11c9b33c9aac0cf28b2d29001dd30f39` — `db05dec7deee62ab195417746e9ec350`
`ec2069ab39c170794d1f12ab259c102a` — `a9d8fe33aa84fd986dbcc35a564c9fc5`
`4c2c67b19b483bdf7277f5331f4a2fa3` — `4150a5f78cbf740c6209da66acae2f37`
`a0c67ad8542e3c5c319c0b4447c8bf6a` — `01e6d0c0f6390df0ca6396d99184f59c`
`928aaf5271aea59300964bf47e19b56e` — `9f8ad9e1a6f3fa33a8fe84dc05cfd739`
`be5bf0662069660cbab86f7074bdf061` — `a6c43f5e1e4b2c0805d96a904c1e1990`
`760ff57bce6fdc0b9850e8dbb608abe2` — `b2288dec837e9685fa1bbd36c6b7b289`

Разрешено использование любых средств — от каких угодно вычислительных кластеров до подсказки «звонок другу» в ФСБ или АНБ.