Záver zimného semestra:

Získali sme dáta použitím RTL SDR zariadenie s pomocou softvéru GQRX, kde bol vysielaný signál nahratý. Signál pochádza z diaľkového ovládača na garážové dvere používajúci 'fixed + rolling code'. Obsahuje 2 tlačidlá, hodné a dolné, pričom obidve tlačidlá boli tri krát za sebou stlačené. Každé tlačidlo bolo nahraté samostatne. Nahrávky sme otvorili v Universal Radio Hacker, odkiaľ sme získali signáli prevedené na binárny zápis. Každé stlačenie bolo oddelené '\n'. Tým sme získali vstupné dáta pre analýzu. Keďže Universal Radio Hacker nepodporuje funkcie, ktoré sme potrebovali na ďalšiu analýzu, vytvorili sme vlastnú knižnicu pomocou, ktorej sme analyzovali dáta.

- Zistili sme, že každý bit je 'zabalený' zľava do 1 a sprava do 0. Tým bolo zabezpečené, aby boli za sebou vždy najviac dve jednotky alebo dve nuly. napr. signál 10001 bude 110100100100110

Nasledovné čísla bitov budú z 'odbaleného' signálu, t.j. bez 1 naľavo a 0 napravo. Ľahko by sme vedeli previesť dané čísla na čísla zo 'zabaleného' signálu. n -> (n-1)*3 + 2

- 3-4.bity : predpokladáme, že nesú vlastnosť čo sa má stať s garážovými dvermi. Keďže ale binárny zápis príkazu *zastav* v hornom tlačidle nie je rovnaký ako v dolnom tlačidle, na vykonanie príkazu potrebuje prijímacie zariadenie vedieť, ktoré tlačidlo bolo stlačené.

- 13., 21. bity : bity, ktoré delia signál na časti

- 27.bit, 61-62.bity : bity nesúce informáciu, ktoré tlačidlo bolo stlačené

- 32.-64.bity okrem 61.-62.bitov : identifikačné bity, sú rovnaké nezávisle na tlačidle a počte stlačení.

Ďalšie súvislosti medzi bitmi sme nenašli. Nastávajú pre ne dve možnosti:

1. sú to kľúče zo zoznamu, ktorý má ako vysielač, tak aj prijímač a pomocou zhody sa spustí operácia s dvermi.

2. postupne sa mení hodnota kľúča, podľa vnútornej funkcie, ktorú sme ešte neobjavili.

Fotky z analýzy – celá analýza na stránke: