Փուլ 1. Ինչ է պահանջվում նախագծել

Ծրագրային ապահովում (օպեր. համ.) հայտնի ռադիոսարքի համար որը փոխանցում և ընդունում է ձայնը այն գաղտնագրելով AES գաղտնագրման ալգորիթմով:

Պահանջներ.

- Գաղտնագրման կամ վերծանման արդյունքում տվյալների կորուստը պետք է չգերազանցի 0.01%-ը
- Ռադիոսարքի փոխանցման/ընդունման արագությունը պետք է չնվազի
- Ռադիոսարքի միջոցով հնարավոր չլինի գտնել գաղտնագրման բանալին
- Ծրագիրը աշխատի ոչ միայն ռադիոսարքի այլև համակարգչային (intel) ճարտարապետություններում
- Վերջնաժամկետը 3 ամիս:

Փուլ 2. Իրականացման միջոցները

- Ռադիոսարքի համար հնարավոր է գրել ծրագրեր միայն C ծրագրավորման լեզվով
- ***AES*** ալգորիթմը բավականին կդանդաղեցնի ռադիոսարքի աշխատանքը, այդ պատճառով անհրաժեշտ է օպտիմալացնել ռադիոսարքում օգտագործվող արդեն հայտնի ալգորիթմները
- Օգտագործել ուղղիչ կոդեր, տվյալների կորստից խուսափելու համար
- Մշակել համակարգ բանալիների փոփոխման և սինխրոնիզացման համար
- Մշակել ալգորիթմ որը թույլ կտա փոքրացնել տվյալների չափը ուղարկելուց առաջ
- Առավել օպտիմալ ուղղիչ կոդի ընտրում և օգտագործման թույլտվություն
- ***AES*** ալգորիթմը կիրառելու թույլտվություն

Փուլ 3. Կոդավորում

- Ձայնի փոխակերպում իրականացնող օպտիմալ ալգորիթմի մշակում
- Տվյալները արխիվացնող(և հակառակ) ֆունկցիայի մշակում
- Ուղղիչ կոդի ֆունկցիայի մշակում
- AES համակարգի մշակում
- Բանալիների փոփոխման ալգորիթմի մշակում