Сигурна комуникация между устройства с ограничени ресурси

Иван Николов

Под ръководството на:

Христо Стоянов

Лятна изследователска школа 2015

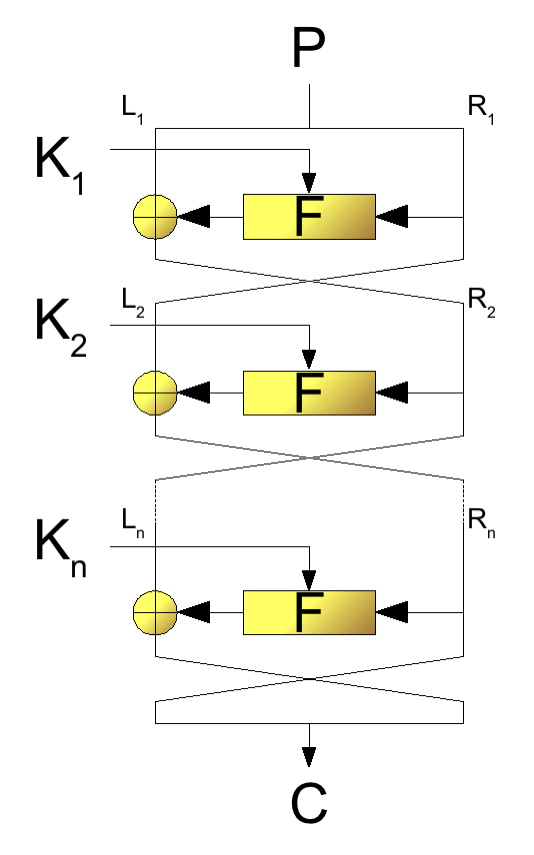
10 ноември 2015

# Въведение

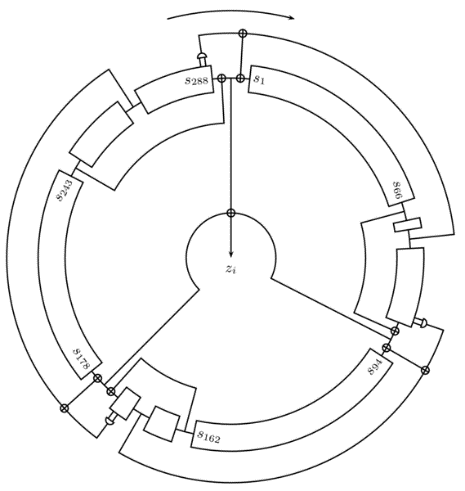
С развитието на безжичните мрежи и вградените системи се увеличава ползата на различни малки устройство, чиито функционалности често са ограничени. Тези устройства са широко разпространени в ежедневието ни, намират се както в кредитните и дебитните карти, така и във водомерите и електромерите. Срещат се под различни видове на чипове и платки. Устройствата комуникират едни с други чрез мрежа, която не винаги е защитена. Това налага използването на криптографска защита. Тъй като на малките устройства имат ограничен брой възможности(изчислителна мощ, батерия, памет) не може да се имплементират стандартните шифри. Данните от подобен тип устройства трябва да стига до компютър или сървър, който може да ги анализира, без да има как някой да наблюдава, променя или повтаря данни. Много „леки“ шифри предлагат сравнително сигурна защита, на ниска цена от гледна точка към хардуерни ресурси.

Целта на проекта е да илюстрира работата на различни видове шифри и как те използват различени видове ресурси. До сега проектът ми е стигнал до имплементирането на два шифъра. Първият е обикновен блок шифър - *DES(Data Encryption Standard)*, а другият е лек поточен шифър – *Trivium.*

# DES

*Data Encryption Standard* е типичния блок шифър – алгоритъм, който взима обикновен текст с фиксирана дължина и чрез поредица от сложни операции го трaнсформира в шифрован текст с дължината на първоначалния текст. В случаят на *DES,* размерът на блоковете е от 64 бита. Също така *DES* използва 64 битови ключ за да промени шифрования текст по такъв начин, че само тези който притежават ключа да могат да разберат първоначалния текст. Всъщност осем бита биват премахнати и за това може да кажем, че ключът е с големина от 56 бита. *DES* работи чрез „*Feisteal мрежа“*– разделя текста на две части, едната половина бива криптирана с ключа на съответния рунд и това се повтаря 16 пъти, като на всеки рунд двете половини се разменят. Също така *DES* притежава една първоначална функция за разместване на битовете на съответния блок и една обърната такава за края на шифъра.

# Trivium

Алгоритъма *Trivium* е хардуерно-ефективен, синхронно поточен шифър проектиран от *Christophe De Canniere* и *Bart Preneel.* Шифърът използва 80-битов ключ и 80-битова начална стойност; 288-битово временно състояние, състоящо се от три взаимосвързани, нелинейни регистъра с дължина от 93, 84 и 111 бита. Работата на шифъра се разделя на две части: да се настроят ключът и инициализационен вектор (*initialization vector*) и поточния генератор. Настройването на ключа е подобно на поточния генератор и прави 1152 стъпки от процедурата по часовника на *Trivium.* Потокът е генериран с повтарящо се въртене на шифъра, като на всяко въртене три временни бита се променят използвайки еднопосочна нелинейна функция и един бит от шифъра се произвежда на въртене. Спецификацията на шифърът показват, че от всяка двойка ключ/първоначалната стойност, може да се създаде 264 поток от битове.

# Бъдеще

Продължението на проекта включва проучване и имплементация на разнообразни видове по конструкция шифри. Осъществяване на сигурна комуникация между две хардуерни устройства с ограничени ресурси. Тестване на различните видове шифри. Анализиране на получените резултати.

# Благодарности

Искам да благодаря на моя ментор Христо Стоянов за напътствията и подкрепата през цялото време на съвместната ни работа. Искам да благодаря на учениците от Лятната изследователска школа, който търпеливо изслушваха идеите ми Василен Цветков и Антон Колов. Благодаря на Константин Делчев, Явор Папазов и Георги Койков за указаната помощ при затруднения. Изразявам своята най-дълбока благодарност към Лятната изследователска школа че даде начало на моят проект.