Криптологија и основне криптолошке методе

(криптос – тајно, графеин – писање, крипто-графија). Историја о криптологији је заиста пуна тајни. Разлог томе је врло једноставан – људи су чували тајне а криптографија им је помагала. Битни догађаји људске историје су увек под неким велом тајни.

Велики император Јулије Цезар (Јули 100 п.н.е – Март 44 п.н.е), настојао је да сачува своју империју. Знао је да сваког тренутка мора имати контролу над својом империјом. У том погледу најважнији део су биле информације које је слао и примао од својих војсковођа. Те информације су биле шифроване уз помоћ шифарског система који данас зовемо "Цезарова шифра". Цезар је узео алфабет отвореног текста и померио за 3 места и добио алфабет шифрованог текста.

Пример:

Отворени Текст: А Б Ц Д Е Ф Г Х И Ј К Л М Н О П Q Р С Т У В W Х Y З

Шифровани Текст: Д Е Ф Г Х И Ј К Л М Н О П Q Р С Т У В W Х Y З А Б Ц

Тако ће реч НАПАД постати QДСДГ (где је Н ⇒ Q, А ⇒ Д...). Ово је могао само да дешифрује онај ко је познавао овај шифарски систем. Прва справа за помоћ при шифровању је била скитала. Овде их спомињем јер је то први пут да људи користе справу како би шифровали. Касније ће доћи и до израде механичких справа као што су Лорензова машина, Енигма и многе друге.

Криптографија се највише развијала током 2. светског рата. У том периоду, поред развијања математике, телекомуникација и сличних области, дошло је до експлозије употребе шифарских система. Самим тим су се развијале области везане за употребу, слање и коришћење шифарских система.

Хладни рат је донео употребу сателитских система који су били заштићени Оне тиме пад шифарским системом. Такође, дошло је до појаве такозваних симетричних крипто-система и асиметричних крипто-система.

Иначе, криптографију која користи рачунаре, то јест шифарске системе (овде можемо рећи и алгоритам за рачунар) настале на рачунарима и прилагођене раду рачунара зовемо "Модерном криптографијом" а све раније шифарске системе стављамо под "Класична криптографија". Да разјаснимо: "криптологија" и "криптографија" – криптологија је наука о тајном, гђе имамо области:

криптографија – наука о тајном писању,

криптофонија – наука о заштити звука,

криптовизија – наука о заштити слике.

Другим речима , криптологија обухвата криптографију.

Терминологија Криптографије

У криптографији имамо две врсте информација: отворени текст и шифровани текст. Операција која отворени текст претвара у шифровани текст зове се шифарски систем. У модерној криптографији то се зове алгоритам. Сваки легалан процес обрнут од шифровања се зове дешифровање. Сваки процес који није легалан, односно користи непознавање шифарског система да би се дошло до текста, зове се декриптовање. Процес анализе, класификовање и друге радње над шифрованим текстом од стране треће стране се зове криптоанализа. Сваки знак отвореног текста има своју замену у виду шифарске замене или шифрованог знака.

Облици комуникације могу бити:

– уговорени облик комуникација (Београд – Дубровник);

– тајни облик комуникације (Брод креће са угљем – где је Брод – артиљерија, угаљ – гранатирање);

– шифровани облик комуникације (шифровани текст:АДФ ФДА – отворени текст: ВАН НАВ);

– невидљиви облик комуникације (невидљива мастила).

Ми ћемо се обазрети на тему шифрованог облика комуникације.

Поједини шифарски системи користе кључ. Кључ за шифровање може бити:

Према дужини:

– коначни

– бесконачни

Према типу кључа:

– логички (београд, сарајево...)

– нелогички (мАКОС12гоосе=)

– мнемонични (НАПАД = 62723 , ако узмемо бројеве са моб. телефона)

Криптографски Системи

Генерална подела:

1) Систем премештања

2) Систем замењивања

3) Комбинацијске шифре (премештање + замењивање)

Сви шифарски системи могу да имају АЛФАБЕТ: сређени или несређени (АБЦД.. , ДОЈА..)

Шифарски системи премештања:

– обично премештање

– премештање кључем

– премештање решеткама

– двоструко премештање

Шифарски систем замењивања се дели на:

1) Шифре просте замене

2) Шифре сложене замене

1 – Шифре просте замене (МОНОАЛФАБЕТСКЕ) се деле на:

– алфабетске шифре

– биграмске, Триграмске и полигамске шифре

– кодне таблице

– кодови

– шифре рашчлањивањем слова

2 – Шифре сложене замене (ПОЛИАЛФАБЕТСКЕ)

– шифре са сређеним алфабетом

– шифре са несређеним алфабетом

Цезарова шифра, ROT13

Једноставнији облик шифарског система јесте Цезар шифарски систем. То је обични супституцијски шифарски систем где је једно слово отвореног текста једнако слову шифарског текста.

Пример 1.(узимамо слова алфебета који се користи на рачунарима):

отв. текст: А Б Ц Д Е Ф Г Х И J K Л М Н О П Q Р С Т У В W Х Y З

шиф. текст: Ф Г Х И J K Л М Н О П Q Р С Т У В W Х Y З А Б Ц Д Е

Овде имамо срећени алфабет (гледа се шифарска замена у односу на отворени текст) а може бити и несређени облик алфабета (слова су у произвољном низу постављена).

Пример 2.

отв. текст: А Б Ц Д Е Ф Г Х И J K Л М Н О П Q Р С Т У В W Х Y З

шиф. текст: В Е K У Y Н Q Л J Т Р О А Б W Х П Ц Д Х Ф Г З И М С

Сада ћемо направити трансформацију текста у шифровану замену.

Алфабет из примера 1. :

отв. текст: МИ ЗЕЛИМО НАЗАД

шиф. текст: РО EJKQPT СФЕФИ

Урадимо кратку анализу Цезаровог шифровања које смо управо извршили.

Математички приказ ове трансформације је: Ф(х) ⇒ Ф(у), где имамо из првог скупа (отворени текст) копирање на други скуп (шифрована замена) – у којем нема таквог елемента првог скупа, који може имати више од једне замене у другом. Другим речима, све особине отвореног текста добија и шифарска замена. Практично то значи да неко ко познаје особине језика врло брзо може да "разбије" шифарску замену.

Под особинама језика спада:

– фреквенција појављивања слова

– фреквенција биграма, триграма, полиграма

– специфичност језика (рецимо, -АНА наставци у реченицама или -ОВА, -СКА и слично)

– број појављивања глагола, придева, именица и сл.

– просечна величина речи, реченице

– удаљеност слова (НАПАД, ђе је А удаљено од другог А тек једно место или Н од Д3 и слично)

– диференцијалност текста (текстови исте дужине, где имају поклапања или мимоилажења)

– јединственост речи (ускоро, следеће поглавље ...)

Ово спада под криптоанализу, о томе ћемо у наредном броју.

ROT13 има врло занимљиву историју. У ери интернета, постојао је обичај да ако желите да нешто ружно или неприклано кажете на newc групама, једноставно реч која не би била фина да се куца/чита, шифрујете ROT13 (енгл. ротате бу 13 плацес). Такође, он је супституцијски шифарски систем који користи сређени алфабет.

Напоменућу вам да Виндовс ХП, користи ROT13 да би "сакрио" у регистру-ју ваше активности.