Висока Школа Електротехнике и Рачунарства Струковних Студија

У Београду



Дипломски рад

Сигурнос Информационих Система

Анђелковић Милош НРТ-35/13 др.Зоран Бањац

Београд 2016.

Садржај

[1. Увод 1](#_Toc456976484)

[2. Криптографија 1](#_Toc456976485)

# Увод

*“Не постоји знање које није моћ.”*

* Ралф Валдо Емерсон

# Криптографија

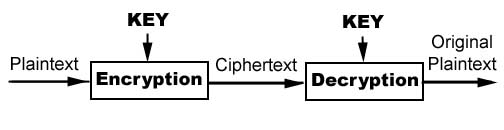
Криптографија је наука која се бави трансформацијом података тако да је њихово значење доступно само овлашћеним странам. Информације које се пренесе комуникационим каналом, који у општем случају није безбедан, могу услед прислушкивања да дођу до лица која не би требала да имају приступ тим информацијама. У колико су у питању финансијске, војне или државне тајне ово може да представља велики проблем, мада и злоупотреба приватних информација како би се нанела штета неком појединцу није занемарљив проблем. Употребом криптографије и одговарајућих криптографских система и алгоритама овај проблем је могуће превазићи.

Појавом писма појавила се и потреба да се сачува тајност садржаја неких писама, тада је и настала криптографија. Од самог почетка шифровање података користило се у војне сврхе. Међу првима је криптографију почео да користи Јулије Цезар, једна од најпознатијијх шифара приосте замене, Цезарова шифра, добила је име баш по њему. Он је све поруке које је слао својим војсковођама шифровао тако што је свако слово поруке замењивао, „померао“, словом које је 3 или више места после тог слова у абецеди. Тако шифровану поруку могли су да дешифрују и разумеју само они који су знали за колико места су слова померена, односно они којима је порука била намењена. Прву расправу о криптографији написао је Леоне Батиста Алберти 1467. Он је такође творац шифарског круга и неких других решења двоструког прикривања тексат која су прихватили усавршили немачки, енглески и француски бирои. Пола века након тога објављено дело Јоханеса Тритхемуса, прва књига о криптофгафији. У 16. веку значајан допринос дају милански доктор Гироламо Кардано, математичар Бартисто Порта и француски дипломата Блаисе де Вигенер.

Тек за време Другог светског рата појавила се машина која је шифровала поруке на до тада невиђен начин. Машину су направили немци и звала се Енигма. Међутим колико год да је она била револуционарана савезници су ипак успели да дешифрују поруке шифроване Енигмом. Оно шта је много више утицало на развој криптографије јесте употреба рачунара. Како су временом рачунари постајали све бржи и моћнији, број операција у секунди је скочио са неколико стотина на неколико милиона па чак и милијарди операција у секунди, 20. јуна. 2016. Sunway TaihuLight поставио је рекорд од 93 petaflops-a, што је 93\*1015 операција у секунди. Ово је потпуно променило начин шифровања и дешифровања порука, ове брзине омогућавају много брже разбијање шифрата што је довело да развијања нових сигурнијих и компликованијих алгоритама за шифровање.

Основни термини који се користе у криптографији су:

* Отворени текст (plaintext)- порука коју је потребно заштити.
* Шифровање (encryption)- операција којом се отворени текст мења тако да неовлашћеним странама буде потпуно неразумљив, односно да не могу извући никакве информације.
* Шифрат (ciphertext)- резултат шифровања, излазана вредост трансфорамације отвореног текста.
* Алгоритам шифровања- скуп правила који се користи за шифроавање отвореног текста.
* Кључ шифровања (key)- од њега зависе операције алгоритма шифровања, улазна вредност као и отворени текст.
* Дешифровање (decryption)- операција којом се из шифрата добија отворени текст
* Алгоритам дешифровања- скуп правила који се користи за дешифровање шифрата.



***Слика 2.1.:*** *Процес шифровања и дешифроавања*

Дужина кључа, односно број симбола којима је представљен, зависи од конкретне имплементације алгоритма и представља један од параметара сигурности система. Сигурност криптографског система почива искључиво на тајности кључа. Сам алгоритам је јаван, односно опште познат. Овакав принцип се користи јер у колико сигурност ситема зависи од алгоритам постоји могућност да неко украде или на неки други начин дође до алгоритам, што се у пракси показало као вероватно. У том случају потребно је мењани комплетан систем, док у колико сигурност система зависи искључиво од кључа у колико неко на неки начин дође до кључа довољно је само променити кључ и систем може да настави да се користи без икаквих већих промена. Такође јавни алгоритми су доступни великом броју криптографа који могу да открију и прије слабости.

Криптографија мора да обезбеди следеће:

* Интегритет односно ведостојност података који који се шифрују, односи се на то да не дође до било какве неовлашћене измене или брисање податакака. У колико ипак некако дође до неовлашћене промене података неопходно је то детектовати, односно мора да постоји начин да се провери да ли су подаци мењани. Ову врсту напада могу да изврше и легални корисници који случајно или намерно покушавају да прекораче своја ограничења.
* Тајност, односи се на то да је садрђај података доступан само овалшћеним лицим односно онима који поседују кључ.
* Провера идентитета, оноси се на то да корисници пре приступа систему морају прво да се пријаве на систем.
* Немогућност избегавања одговорности, односи се на то корисник не може да порекне нешто за шта се зна да је баш он урадио. Врло битно код савремених система где велики број новчаних трансакција обавља преко интернета.

Крипто-анализа је процес којим се из шифрата долази до информација о отвореном тексту без познавање кључа, односно само на основу шифрата. У ширем смислу обухвата и проучава слабости крипотграфских елемеата, као што су, на пример, хеш функције или протоколи аутентификације. Технике криптоанализе називају се напади. Постоје два типа напада потпуна претрага кључева и скраћени напади. Потпуна претрага кључева представља испобавање сваке могуће вредности кључа из птостора кључева. Простор кључева је скуп свих могућих вредности кључева. Скраћени напади захтевају мање времена и обраде од потпуне претраге кључева. Неки од скраћених напада су:

* Напада на основу познавање шифтаза- у колико алогритам шифровања има слабости могуће је доћи до поруке само анализом шифрата.
* Напада на основу познатог дела отвореног текста- поруке које се шаљу најчешће имају унапред познате делове, као што су заглавља или слично. То може да се искористи за дешифроваењ остатка шифрата.
* Напад на основу изабраног отвореног текста- нападач себи шаље одређену поруку док корисник није за рачунаром(lunchbreak attack). Како нападач зна отворени текст и шифрат може да дође до кључа и дешифрује остале шифрате.
* Напда на основу адаптивно одабраног отвореног текста- нападач бира отворени текст, уради анализу, затим изабере нови текст на основу резулата. У колико добије очекиване резултате значи да је на добром путу.

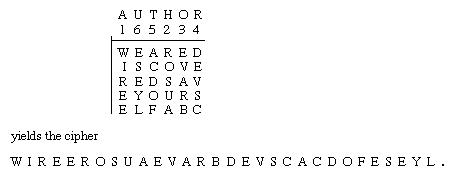
Шифарски систем је сигуран у колико је најефикасније напад потпуна претрага кључева. Простор кључева мора да буде довољно велики.

Постоје две врсте сигурности: рачунска и безусловна. Систем је рачунски сигуран у колико је цена разбијања шифрата већа од вредности шифроване информације или ако је време разбијања дуже од времена које информација треба да буде тајна. Систем је безусловно сигуран у колико не може да буде разбијен ни уз неограничене ресурсе и неограничено време.

Безусловно сигурна шифра је шифра код које се ни потпуном претрагом кључева не може доћи до отворене поруке.

Класичне шифре које су коришћене у далекој историји су: шифре транспозиције, шифре супституције, One-time pad и кодне књиге. Оне су коришћене само за шифровање порука док се савремене шифре користе и за друге ствари, између осталог и проверу интегритета поруке, проверу идентитета пошиљаоца или примаоца и слично.

Шифре транспозиције заснивају се на замени редоследа слова у тексту. Први пут је коришћена у Спарти и звала се Скитала. Текст поруке је писан на кожној траци обмотаној око дрвеног штапа. Кад је порука написан штап се одмота и добије се текст у којем је редослед слова испремештен. Такву поруку је могао да дешифрује или прочита само онај који има штап исте дебљине или зна дебљину штапа. У данашње време се за ову врсту шифровања котисте матрице и посте транспозиција колона и редова. Код транспозиције колона текст се пише редом у матрицу одређених димензија, у колико нема довољно слова да се попуне сви редови додају се док матрица није скорз попуњена. Затим се текст чита из колона, да би се проширио простор кључева додаје се тајна реч која која одређује којим редоследом се читају колоне. Код двоструке транспозиције се користи исти принцип с' тим што се премутују и редови. Међутим ова врста шифровања је веома слаба. Кључ представљају димензије матрице, а димензије морају бити такве да њихов производ треба да буде једнак или већи дужини поруке. Шифрат садржи само симболе из отвореног текста и исте је дужине, а не би требао да садржи никакве информације из отвореног текст јер оне олакшавају крипто аналитичарима претрагу кључева. Крипто-анализ овако шифрованих порука се заснива на принципу „подели па владај“. Могуће је из шифрата сазнати тајну реч, што одмах даје једу од две димензије матрица, након чега је лако доћи до отвореног текста јер се лако могу одредити димензије матрице и зна се редослед којим се читају колоне. Чак и без тога уз довољан број покушаја могу да се сазнају димензије матрице и након тога тајана реч па и отворен текст. Чак и само коришћењем оловке и папира уз довољно времена и труда је могуће разбити овакву шифру, док је употребом рачунара то занемарљиво лако.



***Слика 2.2.:*** *Пример шифре транспозиције*

Шифре замене