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](#_Toc457493179)

[2. Криптографија 1](#_Toc457493180)

[2.1. Симетрични крипотсистеми 5](#_Toc457493181)

# Увод

*“Не постоји знање које није моћ.”*

* Ралф Валдо Емерсон

Информације су у савремено доба, поготово од популаризације интернета, постале врло одступне скоро свима.

# Криптографија

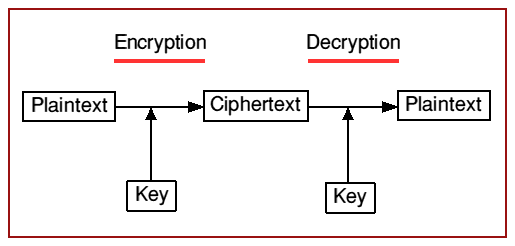
Криптографија је наука која се бави трансформацијом података тако да је њихово значење доступно само овлашћеним странам. Информације које се пренесе комуникационим каналом, који у општем случају није безбедан, могу услед прислушкивања да дођу до лица која не би требала да имају приступ тим информацијама. 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.

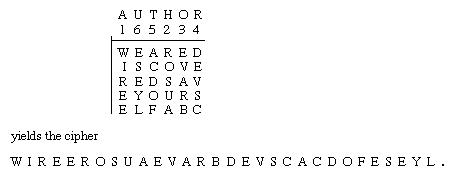
Шифарски систем је сигуран у колико је најефикасније напад потпуна претрага кључева. Простор кључева мора да буде довољно велики.

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*

Код шифре замене слова или групе слова се систематски мењају другим словима или групама слова. Постоје моноалфабетске шифре, код њих се слова мењају увек истим словима, хомофоне шифре, код њих се уводи елемнт случајности, полиграмске шифре, код којих се замена врши над већом групом слова, и полиалфабетске, код којих свако слово може да се мења већим бројем слова. Најпознатија шифра просте замене је, већ поменута, Цезарова шифра у којој се свако слово поруке мења словом које је од њега удаљено одређени број места у алвабету или азбуци, с' тим да последња слова долазе на места првих. Алгоритам шифровања је:

**pi** i-то слово отовореног текста

**ci** i-то слово шифрата

**KE** кључ, број помераја

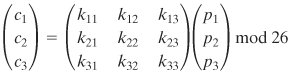
С' обзиром да је могуће померити за највише 26 места ова шифра има простор кључева од 26, што је врло мало, па је врло лако пробати све могуће вредности и доћи до отвореног текста. Због тога се дошло на идеју да кључ може бити било која премутација слова, што простор кључа повећава на 26! што је приближно 4\*1026. Међутим и даље је могуће разбити ову шифру коришћењем фрекфенцијске анализе. Наиме постоје на итернету јаве статитике фреквенције појављивања слова у неком произвољном тексту. Могуће је одрадити фреквенцијску анализу над шифратом и упоредити са неком другом анализом и на основу тога доћи до закључка којом логиком односно по ком правилу су слова мењана.

Због тога код хомофоне шифре шифат може да садржи више од 26 знакова а слова могу да се мењају већим бројем слова. У главном се слова са највећом фекфенцијом, односно са највећим бројем појављивања, предсатављају на више начина чиме се шири статистика шифрата. За правилан рад битно је пронаћи слова са највећом фрекфенцијом а затим одредити правило када доделити једну од две вредности за исто слово отовореног текста. С'обзитом на то да је шифрат треба да прикрије статистичке особине отовореног текста, он би требао да има особине случајног низа а постизање случајности. Шифрат је такође слаб на нападе познатог дела текста.

Код полиграмских шифара групе солва се шифрују заједно, а представници су плејфер шифра и Хилова шифра. Плејфер шифра шифрује по два слова заједно и код ње је могућа фрекфенцијска анализа али у дужим порукама. Хилова шифра је настала 1929. и осмислио ју је Лестер С. Хилл, користи блокове од три или више слова и заснована је на линеарним једначинама. Због оптужби да је његов систем због превелике компликованости неупотребљив, Хил је направио машину која шифрује користећи његов алгоритам али никада нију успео да је прода. Највећи његов допринос је уоптреба математике у осмишљању и анализирању криптографских система. Пример шифровања:

* Слова алфабета се представљају бројевим од 0 до 25.
* Текст се представи бројевима и подели на блокове дужине n. Сваки блок се обележи као р1,р2,р3,...рi где је i редни број блока, и запише као вектор димензија nх1.
* Шифрат блока се добије множењем по модулу 26 инвертибилне матрице А димензије nхn са вектором рi. A je кључ и њену вредност треба изабрати случајно из скупа инвертибилних матрица димензија nхn. Такође се мора водити рачуна да је могуће изтачунати инверзну матрицу, односно да детрминанта не сме да буде 0.
* Дешифровање се врши множењем блока шифрата инверзном матрицом матрице А (А-1) по модулу 26.

Због линеарности је рањива на нападе познатог дела текста. У колико је су позанте димензије кључа А и довољан број блокова отвореног текста и шифрата онда:



***Слика 2.3.:*** *Принцип шифровања коришћењем Хилове шифре*

Шифре полиалфабетске замене корите више алфабета за шифровање, уопштено свако слово може да има своје правило за шифровање. Представник је Вижнерова шифра код које се свако слово помера за m, за које важи 0≤m≤25, места у десно.

Шифровање:

Дешифровање:

Отпорнија је на статистичку анализу али је и она могућа ако се погоди дужина кључа. У том случају се шифрат уписује у матрицу дужине m и над сваком колоном засебно се врши статистичка анализа.

Клод Шенон је 1949. увео појам „перфектна шифра“, који представља шифарски ситем код које шифрат не даје никакве информације о отвореном тексту или кључу. У простору отворених поруке *Р,* отворени текст *х* појављује се са вероватноћом *р(х),* у том случају постоји кључ који пресликава сваки отворени текст у сваки шифрат са подједнаком вероватноћом. Енторпија се користи као мера за количину информација садржаних у поруци. Количина информација зависи од вероватноће, што је нека порука вероватнија то је количина информација мања и обрнуто. Информациони садржај неке поруке *х* рачуна се по формули:

Пошто се користи логаритам са основом два, бинарни логаритам, количина информација поруке представља број бита који је потребан за опис поруке. У колико имамо поруку *Р* која садржи *хi* независних симбола са вероватноћом *рi*, i=0,…,n-1, ентропија предсавља просечну количину информација која је садржана у појединачним порукама и рачуна се формулом:

One-time pad су увели Гилбер Вернам и Џозеф Мауборгн 1917. и представља доказано сигурну шифру. Принцип рада шифре је крајње једноставан. Над отовреним текстом се изврши операција „ексклузивно или“ (XOR) кључем К, сви подаци су у бинарном формату. Поступак дешифровања је идентичан.

Шифровање:

Дешифровање:

Сигурност се заснива на случајности кључа као и на његовој једнократној употреби. У пракси је веом тешко генерисати чисто случајне низове и са становишта ктиптографије захтевано основно свјоство кључа се одређује ентропијом. Пжељна вредност ентропије је и она важи за вероватноћу појављивања нула и јединица , под условом да постоју униформа дистрибуција унутар бинарне секвенце. ОТР је оказано безбедна ако се користи по дефинисаним правилима:

* Шифрат не даје никакву информацију о отвореном тексту.
* Сваки отворени текст исте дужине подједнако је вероватан.
* Кључ мора бити „случајан“ и може се користити само једном.
* Кључ је познат само примаоцу и пошиљаоцу.
* Кључ је исте дужине као и порука.
* Механизам интегритета не постоји.

Због тешкоће генерисања и дистрибуције кључа ова шифра се не користи.

Кодна књига је скуп речи или фраза коју могу да се користе и доделе им се кодови. Постоје две једн за шифровање и друга за дешифровање, а кључ је сама кодна књига. Сигурност се заснива на самој физичкој сигурности књига. Цимерманов телграм је једна од најпознатијих кодних књига у историји а његово дешифровање било је повод за улазак САД у први сетски рат. Кодне књиге су подложне статистичкој анализи. Ради веће безбедности користе се и адитивне кодне књиге које садрже много случајних бројева који се сабирају са кодним речима и дају коначан шифрат. Почетно место из адитивне кодне књиге се договара док почетно место из кодне књиге одређује пошиљалац. Почетно место се назива индикатор порука или иницијализациони вектор.

## Симетрични крипотсистеми

Крајем Другог светског рата почела је употреба рачунара у криптоанализи што је даље довело до употребе рачунара и за шифровање и дешифровање. Код модерне криптографије отворени текст се преставља низом битова и алгоритми за шифровање и дешифровање раде над њима. И даље се користе комбинације транспозиције и супстуције. Две највеће предности модерене криптографије у односу на класичну, односно две највеће предности које доноси употреба рачунара, јесу могућнос реализације много сложенијих алгоритама за шифровање и дешифоровање и много већа брзина шифровања и дешифровања.

Симетрични крипто системи користе исти кључ за шифровање и дешифровање, тако да обе стране које комуницирају морају пре почетка комуникације на неки сигуран и тајан начин да размене кључ. Постоје две врсте симетричних шифара а то су секвенцијалне и блоковске.

### Секвенцијалне шифре

Као што је већ споменуто ОТР представља беузсловно сигурну шифру, код које чак и потпуном претрагом кључева није могуће разбити шифрат, односно могуће је како резултат за различите кључеве добити различите отворене текстове и проблем је утврдити који је прави. Међитим због својих недостатака се не користи. Један од највећих проблема у коришћењу ОТР шифре јесте генерисање случајног низа, односно кључа. Један он начина јесте мерење неких природних појава као што су атмосферски шум, термички шум или остале ектерне електромагнетне и квантне појаве, на пример космичко позадинско зрачење или радиоктивни распад представљају добар извор случајности. Проблем код овог начина генерисања кључа јесте време које је потребно да се сакупи довољно мерења да би се добио кључ довољно велике дучине, јер кључ треба да буде исте дужине као и порука.

Због тога се у крпто системима као кључ у главном корисете псеудо случајни низови. Псеудо случајни низови су по својим статичким особинама исти као и прави случајни низови. Једина разлика јесте у томе што су преиодични, односно у неком моменту ће генератор псеудо случајних низова почети да генерише исте вредности. За иницијализацију генератора псеудослучајних низова се користи кључ К који је прави случајни низ, и који је много краћи од радног кључа, односно генерисаног низа.

Процес самог шифровања се своди на XOR операцију над отвореним текстом и радним кључем, а шифорвање потпуно исти процес само што се врши над шифратом и радним кључем. Функција секвенцијалне шифре је:

Где је К кључ, а S генерисани псеудослучајни низ.

За псеудослучајни низ , отоврени текст генерисање шифрата и затим дешифровање шифрата у отворени текст изгледа овако:

Сам алгоритам шифровања и дешифорвања сам по се би није у опште компликован. Снага ове шифре лежи у кључу. Постоји више решења за генераторе псеудослучајних бројева од којх је једао примена линеарних померачких регистара са повратном спрегом (ЛПР).

Линеарни померачки регистри обављају две функције. Прва је функција померачког регистра дужине n који сваки бит помера за једно место у десно. Друга функција је функција повратне спреге која на основу одређених бита у регисту одређује који ће се бит уписати на прво место. Излаз је најчешће један бит, најчешће крајњи десни, који је одређен почетним стањем и повратном спрегом. Периода померачког регистра је број бита излазне секвенце пре него што почне да се понавља. Померачки регистар дужине n може да има могућих почетних стања, не могу да буду све нуле, и правилним одабиром повратне спреге може се постићи пероида од бита. Непожељне особине линеарног померачког регистра су те што су првих n битаво јенднаки почетном стању. Такође је на основу бита излаза могуће реконструисати генератор.

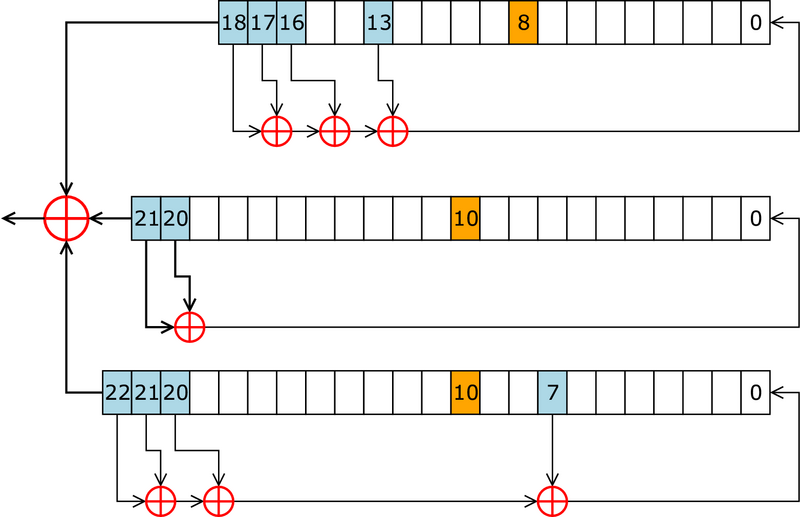
#### A5/1

Коришћен је у мобилној комуникацији за крипографску заштиту података код GSM заштитног протокола, тачније за безбедну комуникацију између телефона и базне сатанице. Алгоритам је чуван у тајности али је цурењем и реверзним инжењерингом доспео у јавност и показало се да алгоритам има озбиљних слабости.

А5/1 користи три линеарна померачка регистра са повратном спрегом, означићемо их као X,Y и Z. Регистар X се састоји од 19 битова, Y од 22 и Z од 23, и укупан збир свих битова је 64, колика је и дужина кључа К. Кључ је иницијална вредност ови регистара након чега регистри генеришу псеудослучајни низ, односно радни кључ који се користи за шифровање и дешифровање. За ту дужину кључа очекивани низ случајних битова је , мада од самог дизајна померачких регистара са повратном спрегом зависи дужина радног кључа и величина периоде.

Поступак генерисања кључа:

* , maj представља маријотетну вредност односно „два од три“.
* Ако је онда се рачуна  и помера Х а на место првог бита се уписује вредност .
* Ако је онда се рачуна и помера Y a на место провг бита се уписује вредност .
* Ако је онда се рачуна и помера Z а на место првог бита се уписује вредност .
* Бит радног кључа се рачуна као .



***Слика 2.1.1.1.1:*** *А5/1 регистри*

Алогритам се врло лако имплементира у хардвер и генерише битове кључа пропорционално брзини такта процесора. Број бита радног кључа који се могу генерисати из једног кључа од 64 бита је практично неограничен, али ће се сигурно у једном тренутку поновити.

#### RC4

RC4 је секвенцијална шифра која софтверски имплементира и генерише један бајт кључа у сваком такту. У основи овај алгоритам садржи једну табелу са свим пермутацијама једног бајта 0-255, и сваки пут када се генерише бајт радног кључа табела се мења тако да увек садржи пемутацију од . Иначе комплетан алгоритам ради над бајтовима.

Прва фаза је инцијализација табеле коришћењем кључа. Ако је табела означена као Ѕ а кључ као кеy, онда псеудокод за иницијализацију табле изгледа овако:

**for** i **from** 0 **to** 255

S[i] := i

**endfor**

j := 0

**for** i **from** 0 **to** 255

j := (j + S[i] + key[i [mod](https://en.wikipedia.org/wiki/Modulo_operation) keylength]) mod 256

swap values of S[i] and S[j]

**endfor**

Ѕ[i] и key[i] су бајтови. Кључ може бити дужине онд 1 до 256 бајтова, најчешће је изеђу 5 и 40, и користи се само за иницијализацију пермутација.

Након овога се генеришу бајтови радног кључ. Псеудокод за генерисањ радног кључа изгледа овако:

i := 0

j := 0

**while** GeneratingOutput:

i := (i + 1) mod 256

j := (j + S[i]) mod 256

[swap values](https://en.wikipedia.org/wiki/Swap_(computer_science)) of S[i] and S[j]

K := S[(S[i] + S[j]) mod 256]

output K

**endwhile**

У свакој итерацији i се инкрементира, узима се i-ти елемент из табле, S[i], и додаје ј. Затим се мењају вредности i-тог и ј-тог елемента, S[i] и S[j], и њихов збир по модулу 256 се користи као идекс за узимање елемента који у ствари представља бајт радног кључа, К. Тај бајт се XOR-ује са бајтом отвореног текста у колико се шифрује, односно шифрата у колико се ради о дешифровању.

За правилан рад ове шифре неопходно је одбацити првих 256 бајтова радног кључа јер је на основу њих могуће реконструисати радни кључ. Такође је врло битно да кључ буде случајан.

Коришћен је у многим апликацијама укључујући заштитне протоколе SSL и WEP. Међутим од 2015. постоје спекулације да неке државне агенције могу да разбију RC4 када се користи у TLS протоколу. IETF (International Engineering Task Force) је објавио RFC 7464 којим забрањује употребу RC4 у TLS, Mozilla и Microsoft су објавили сличне препоруке.

### Блоковске шифре