Академија струковних студија Западна Србија

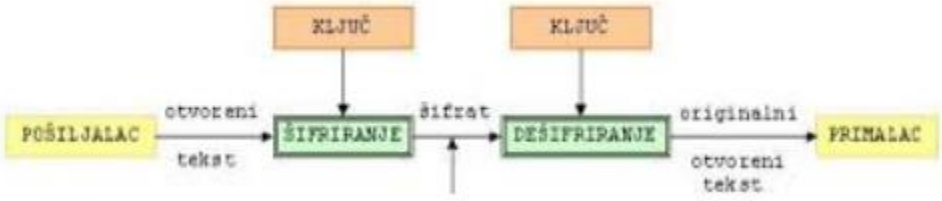
Мај месец математике

Цезарова шифра

Увод у криптографију и кратак историјски осврт

Криптографија је наука тајног писања, тј. наука наука чувања информација у оној форми коју разуме онај коме је та информација намењена, док ће осталима та информација бити неразумна. Са појавом шифри и криптографије појавила се и наука којој је циљ да те шифре преведе у разумљив језик и назива се криптоанализа.

Основни елементи криптографије су енкрипција, изворна порука, кључ и декрипција. Енкрипција је процес којим се почетна порука (*изворна порука*) уз помоћ алгоритама енкриптовања претвара у текст који није разумљив, осим онима који поседују алгоритам којим га претварају у разумљиву форму. Тај алгоритам се назива кључ. Процес враћања поруке у разумљиву форму назива се *декрипција* (Слика 1).



Слика 1. Процес криптовања поруке

Историја криптографије је мистична и тајна баш као што је и сама криптографија. Нема тачних података о томе када је први пут употребљена, али је једна од првих практично забележених употреба криптографије 2000 г.п.н.е у старом Египту где су коришћени нестандардни хијероглифи за украшавање гробница преминулих владара (слика 2).

Слика 2. Хијероглифи у старом Египту

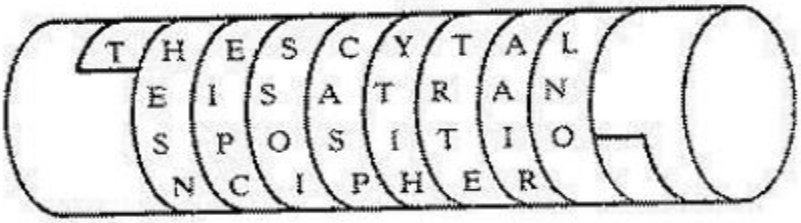
У старој Индији криптографија се употребљавала за комуникацију између владара и њихових шпијуна широм земље. У Месапотамији се употребљавало клинасто писмо које је по својој структури подсећало на египатско (Слика 3). Стари Кинези су користили идеографску природу свог језика и поруке претварала у идеограме које је могао да разуме само прималац поруке.

Слика 3. Клинасто писмо

У литератури постоји доста примера како се скривање порука и криптовање користило у време старих Грка. Према Херодотовим записима уметност писања тајних порука спасила је Грке од напада персијског владара Ксеркса. Наиме, Ксеркс је започео изградњу Персеполиса, нове престонице свог царства и поклони су стизали одасвуд, осим из Атине и Спарте. Како би казнио овакво показивање пркоса, следећих пет година Ксеркс је мобилисао највећу армију у историји и био спреман да крене у изненадни напад. Међутим, овим припремама био је сведок Демаратус, Грк протеран из домовине, мада још увек лојалан Грчкој.

Решио је да обавести своје сународнике на опасност, али је тешкоћа лежала у проналажењу начина да се таква порука достави без знања Персијанаца. Демаратус је састругао восак са дрвених таблица коришћених за писање, написао поруку и поново је прекрио воском, тако да су таблице деловале празно. Порука је несметано стигла до Грка, који су уклонили восак, прочитали упозорење и почели да се припремају за рат. Ксеркс је изгубио елемент изненађења и на крају, изгубио и сам рат.

Спартанци су у сврху шифровања порука користили лист папируса који се мотао око *скитале*. На папирусу је било написано слово испод слова а тајна порука се добијала у хоризонталном запису (слика 4) .



Слика 4. Порука на скитали

Цезарова шифра

Прва забележена употреба шифровања у време старих Римљана била је Цезарова шифра. Назив је добила по римском војсковођи Гај Јулију Цезару (100. п.н.е.-44. п.н.е) који је употребљавао шифровану комуникацију у размени војних информација у току Галских ратова. Римски писац Светоније наводи у својим списима да је Цезар, у својој војној комуникацији, заменом слова, правио записе који се нису могли разјаснити уколико би се она пресрела. Оригинална Цезарова шифра подразумевала је померај алфабета за три слова унапред па би се тада слово А мењало са словом D, слово B са словом E и тако редом. Математичка дефиниција Цезарове шифре дата је на следећи начин.

Дефиниција 1. Нека је (P ,C ,K ,*ек*,*дк*) уређена петорка при чему је P коначан скуп свих могућих отворених текстова, C коначан скуп свих могућих шифрата, K коначан скуп свих могућих кључева, *ек* алгоритам енкриптовања, а *дк* алгоритам декриптовања. Ако је $P=C=K=Z_{26}=\{0,1,2,3…25\}$ и нека је

ек(x)=x+K (mod)26

алгоритам енкриптовања, тада је алгоритам декриптовања дат са

dk(y)=y-K (mod) 26.

Из претходне дефиниције примећујемо да сваком слову придрижујемо неки цео број из скупа од 0 до 25. Кључ K може такође да буде из скупа од 0 до 25 и означава за колико ће се места вршити померање слова приликом шифровања. Шифровање сваког слова се врши тако што бројевној вредности слова додамо вредност кључа и тражи остатак при дељењу са 26. Декрипција се врши тако што од броја који одговара шифрованом слову одузме вредност кључа а затим се тражи остатак приликом дељења са 26.

Пример 1. Оригиналном Цезаровом шифром шифрирати поруку *Математика је лепа*.

Решење:

Отворена абецеда:	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
Бројевна вредност:	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25

Оригинална Цезарова шифра подразумева померај за вредност кључа 3 па се абецеда за шифровање помера за три места удесно. Тј. слову А одговара нумеричка вредност 0 у отвореној абецеди. Да би добили слово у шифрованој абецеди примењујемо алгоритам шифровања тј.

0+3 (mod) 26,

што даје вредност 3. Броју 3 одговара слово D, па се А шифрује са D. Примењујући поступак за свако слово додијамо шифровану абецеду.

Шифрована абецеда:	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C

Сада можемо шифровати текст.

Оригинална порука:	M	A	T	E	M	A	T	I	K	A	J	E	L	E	P	A
Шифрована порука:	P	D	W	H	P	D	W	L	N	D	M	H	O	H	S	D.

Пример 2. Дешифруј поруку A J S N A N I N A N H N шифровну Цезаровом шифром са вредношћу кључа 5.

Решење:

Приликом дешифровања користимо шифровану абецеду. Кључ 5 подразумева померај отворене абецеде за 5 места удесно. Добијамо,

Отворена абецеда: A B C D E F G H I J K L M N O P Q R S T U V W X Y Z
Шифрована абецеда: F G H I J K L M N O P Q R S T U V W X Y Z A B C D E

Сада можемо да дешифрујемо поруку.

Шифрована порука: A J S N A N I N A N H N
Оригинална порука: V E N I V I D I V I C I .

Уместо дељења са остатком често се примењује и тзв. круг коло (слика 5), који се састоји из два концентрична круга на којима си написана сва слова абецеде. Спољни круг је фиксиран док је унутрашњи могуће померати и на тај начин добити кључ за енкрипцију.

Слика 5. Коло

Цезарова шифра са кључном речи

Приликом коришћења Цезарове шифре са нумеричком вредношћу кључа имамо 26 потенцијалних могућности за декодирање текста. Да би повећали број могућности, уместо нумеричке вредности, могуће је узети кључну реч или фразу која ће представљати кључ. Приликом кодирања и декодирања неопходно је да пошиљалац и прималац знају кључну реч. Шифрована абецеда се формира тако што се на почетак стави кључна реч или фраза без размака, празнина и дуплих слова а остатак се попуни словима абецеде која се не налазе у кључу и то редом од почетка абецеде.

Пример 3. Ако је вредност кључа реч *тајна*, шифруј реч МАТЕМАТИКА.

Решење:

Да би шифровали реч математика потребно је направити шифровану абецеду по претходно описаним правилима.

Отворена абецеда: A B C D E F G H I J K L M N O P Q R S T U V W X Y Z
Шифрована абецеда: T A J N B C D E F G H I K L M O P Q R S U V W X Y Z

Оригинална реч: M A T E M A T I K A
Шифрована реч: K T S B K T S F H T.

Начин разбијања Цезарове шифре

За разбијање Цезарове шифре са нумеричким кључем, користе се два начина, метода грубе силе и метода френкфенцијске анализе.

Метода грубе силе

Метода грубе силе подразумева испитивање свих могућих кључева док се не добије неки смислени текст. Нека је, на пример, потребно дешифровати реч OCOCE.
За вредност кључа 0, реч OCOCE није смислена па тај покушај занемарујемо, и настављамо даље. За вредност кључа 1, оригинална реч је NBNBD што опет није смислено па настављамо даље.
За вредност кључа 2, добијамо реч MAMAC што представља смислену поруку па је самим тим шифра „разбијена“.

Метода фрекфенцијске анализе

Метод фрекфенцијске анализе заснива се на учесталости одређених слова абецеде у појединим језицима. Рецимо, у енглеском језику најфрекфентнија слова су E, T, A, O, I. У српском језику то су слова A, I, T, R , O, E. У немачком језику слова која се највише пнављају су E, I, N, R, S. Ова метода спада у теоријске методе и није увек делотворна у пракси. Код кратких речи фрекфенца не мора да буде у складу са фрекфенцијом у одговарајућем језику па резултат неће бити добар. Такође, да би спречили потенцијални напад, стране се могу договорити да не користе најфрекфентнија слова. Ипак, илустроваћемо ову методу простим примером.
Пример 4. Дешифровати поруку GFSFSF ако је текст писан на српском језику.
Решење: Прво се направи фрекфенцијска анализа слова у шифрованој поруци. Приметимо да је слово F најучесталије и да се појављује три пута. Уколико претпоставимо, да је то слово A онда шифрована абецеда изгледа F G H I J K L M N O P Q R S T U V W X Y Z A B C D E. Ако сада заменимо шифрате оригиналном абецедом добијамо реч BANANA, чиме смо дешифровали поруку.

Уместо закључка-Имплементација Цезарове шифре у програмском језику Python

Програмски језик Python је један од најпопуларнијих програмских језика. Због своје једноставности користи се за учење програмирања у основним и средњим школама у Србији. Задатак имплементације алгоритма енкрипције Цезаровом шифром може бити занимљив задатак у настави програмирања. У наставку је представљено једно решење поменутог проблема.

```
#Program za implementaciju Cezarove šifre
def encrypt(text,s):
    result = ""
    # prolaženje kroz tekst
    for i in range(len(text)):
        char = text[i]
        # Enkripcija velikih slova
        if (char.isupper()):
            result += chr((ord(char) + s-65) % 26 + 65)
        # Enkripcija malih slova
        else:
            result += chr((ord(char) + s - 97) % 26 + 97)
    return result
#check the above function
text = "ATTACKATONCE"
s = 4
print ("Tekst : " + text)
print ("Pomeraj : " + str(s))
print ("Šifra: " + encrypt(text,s))
```

Слика 6. Програмска имплементација Цезарове шифре у Python

Иако се сматра да Цезарова шифра спада у најједноставније шифре, она је била основ на ком су настали многи други кокплекснији начини шифровања као што су рецимо Vigenère-ova или Playfair-ova шифра као и многи други. Једноставност алгоритама енкрипције, идеалан је начин да се уђе у тајанствени свет криптографије.

Аутор спец. Бранко Гавриловић
предавач

Литература

[1] https://vladimirbozovic.net/univerzitet/bozovic/wp-content/uploads/2019/06/kripto-vlan-milica-joks.pdf

[2] Јовановић,М., Историја криптографских алгоритама и паметних картица, ETF Journal of Electrical Engineering, Vol. 18, No. 1, November 2009

[3] https://www.mg.edu.rs/uploads/files/images/stories/dokumenta/maturski/jelena-trisovic.pdf

[4] https://www.history.com/news/ciphers-secret-codes-enigma-morse

[5] https://kriptografijazapocetnike.wordpress.com/cezarova-sifra/

[6] http://enigmagika.blogspot.com/2020/09/nefrekventna-slova.html

[7] https://www.geeksforgeeks.org/caesar-cipher-in-cryptography/