KRIPTOGRAFIJA SA PRIMJENOM
VJEŽBA 1

LABORATORIJSKE VJEŽBE U MATLABU

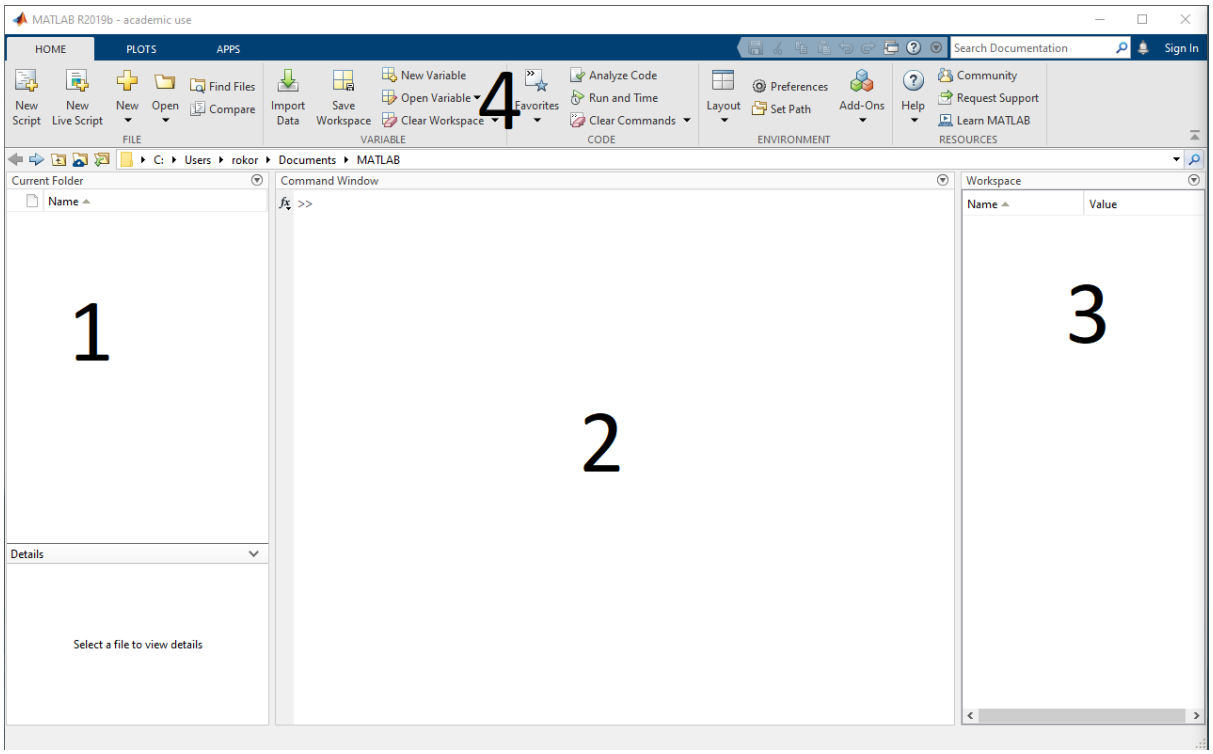
Roko Rogulj

UVOD U MATLAB

MATLAB je okružje s programskim jezikom namijenjeno tehničkim izračunima. Obuhvaća izračune, vizualizaciju i programiranje u okolini jednostavne uporabe. U okvirima kolegija „Kriptografija s primjenom“ MATLAB će se koristiti kao alat za simuliranje kriptoalgoritama te funkcija koje osiguravaju korištenje samih kriptoalgoritama.

Sučelje MATLAB programa pri samome otvaranju izgleda kao na slici 1. Sučelje se sastoji od sljedećih okvira:

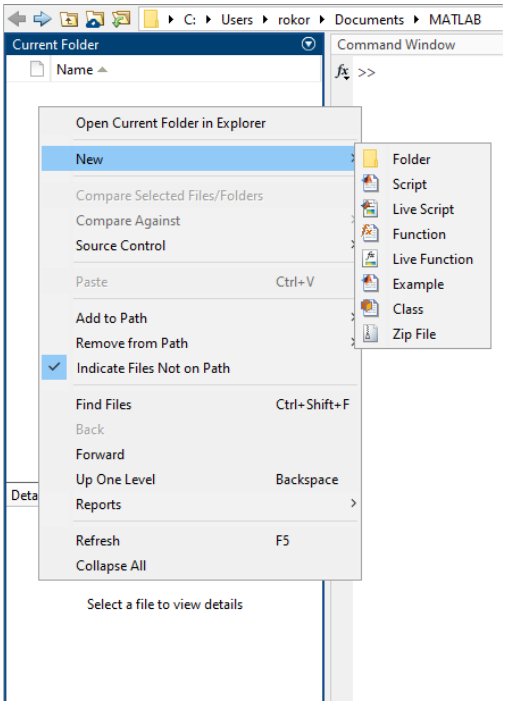
1. Datotečni sustav trenutnog direktorija,
2. Prostor za ispisivanje naredbi,
3. Korištene varijable,
4. Alatna Traka.



Slika 1. Sučelje MATLAB okruženja

U okviru ovih laboratorijskih vježbi programi unutar MATLAB-a će se izvršavati preko funkcija i skripti. Funkcije su dijelovi programa koji primaju argumente te na temelju tih argumenata računaju jednu ili više vrijednosti. Skripte su potpuni programi koji ne trebaju ulazne argumente a izvršavaju se samim programskim pozivom. Skripte i funkcije imaju datotečni nastavak „*ime.m*“.

Za početak rada potrebno je napraviti novi direktorij (*ime_prezime*) desnim klikom miša na datotečni sustav (slika 2.).

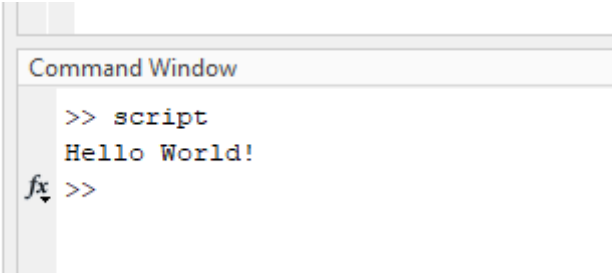


Slika 2. Izrada novog direktorija

Unutar direktorija potrebno je napraviti novu skriptu na **Home-> New -> Script**. Unesite sljedeću liniju koda u skriptu:

```
disp('Hello World!')
```

Spremite skriptu pritiskom **CTRL + S** i pokrenite je tako da upišete njeno ime unutar prostora za upisivanje naredbi (slika 3.). Ispisat će se poruka 'Hello World!'.



Slika 3. Pokretanje skripte u MATLAB-u

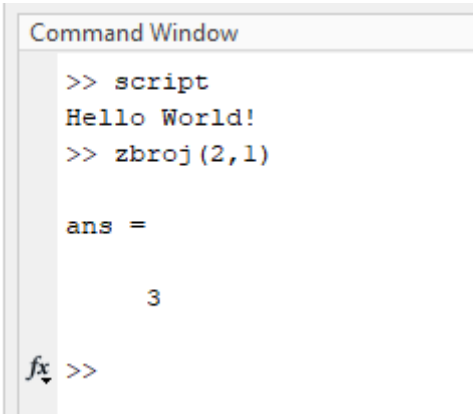
Funkcije u MATLAB-u se izrađuju pritiskom na **Home-> New-> Function.** Funkcije unaprijed dolaze sa sljedećim kodom:

```
function [outputArg1,outputArg2] = untitled5(inputArg1,inputArg2)
%UNTITLED5 Summary of this function goes here
%   Detailed explanation goes here
outputArg1 = inputArg1;
outputArg2 = inputArg2;
end
```

Funkcije (slično kao i u C++ programskom jeziku) primaju argumente i daju jedan ili više izlaza u ovisnosti o samoj strukturi programa. Pogledajmo primjer funkcije koja zbraja dva broja:

```
function [rezultat] = zbroj(a,b)
rezultat = a + b;
end
```

U funkcijama mora postojati minimalno jedan izlazni argument dok ulaznih argumenata može biti proizvoljan broj. Funkcija se poziva na isti način kao i skripta.



Slika 4. Poziv funkcije

OSNOVNE NAREDBE U MATLAB-U

U okviru ovoga kolegija bit će potrebno poznavati tri osnovne funkcije a to su:

IF, ELSEIF, ELSE

Sintaksa:

```
if izraz
      programski_kod
elseif izraz
      programski_kod
else
      programski_kod
end
```

Naredba *if* provjerava da li je uvjet u izrazu logički ispravan te izvršava programski kod ako je uvjet zadovoljen. Ukoliko izraz nije logički ispravan izvršava se programski kod u sljedećoj točnoj *elseif* ili *else* naredbi. Naredba *if* u Matlab-u završava *end* naredbom.

PRIMJER:

```
if 5>6
    disp('Prvi uvjet tocan')
else
    disp('Drugi uvjet tocan')
end
```

FOR petlja

Sintaksa:

```
for index = vrijednost
    programski_kod
end
```

For petlja izvršava programski kod određeni broj puta određen vrijednosti *index* člana. Vrijednost *index* člana može poprimiti sljedeće oblike:

početna_vrijednost : krajnja_vrijednost
početna_vrijednost : inkrement : krajnja_vrijednost

Ova petlja završava *end* naredbom. Iz petlje se može izaći naredbama *break* i *continue.*

PRIMJER: Ispis brojeva od 0 do 10 koristeći *for* petlju.

```
for i=0:10;
    disp(i)
end
```

Slika 5. Izvršavanje *for* petlje

WHILE PETLJA

Sintaksa:

```
while izraz
    programski_kod
end
```

While petlja izvršava programski kod dok je izraz logički ispravan. Iz petlje se može izaći naredbama *break* i *continue*. Petlja završava *end* naredbom.

PRIMJER: Ispis brojeva od 0 do 10 koristeći *while* petlju.

```
i=0;
while i<11
    disp(i);
    i=i+1;
end
```

TEORIJA CIJELIH BROJEVA

1.Djeljivost brojeva

Jedno od najvažnijih svojstava cijelih brojeva je djeljivost.

Definicija: *Neka su* a *i* b *cijeli brojevi tako da je* a≠0*. Kažemo da* a **dijeli** b *ako postoji takav cijeli broj* k *tako da je* b = ak*. Ovo svojstvo se označava s* a|b*.*

Neka svojstva djeljivosti su:

(1) Za svaki a ≠ 0 *vrijedi* a|0 *i* a|a*. Također vrijedi* 1|b *za svaki* b*.*

(2) Ako je a|b *i* b|c*, tada je i* a|c*.*

(3) Ako je a|b *i* a|c *tada vrijedi* a|(sb+tc) *za svaki* s *i* t *is skupa cijelih brojeva.*

2.Prosti brojevi

Definirajmo broj *p > 1* na skupu cijelih brojeva. Svaki broj p koji je djeljiv samo s 1 i sa samim sobom nazivamo prostim brojem. Svaki drugi cijeli broj *n* nazivamo složenim brojem, što znači da se može izraziti kao umnožak cijelih brojeva *ab* tako da je *1 < a,b < n.*

Teorem prostih brojeva: *Neka je* π(x) *ukupan broj prostih brojeva manjih od* x*. Tada vrijedi*

$$\pi(x) \approx \frac{x}{\ln x},$$

ako promatramo omjer π(x)/(x/lnx) → 1 *ako* x→ ∞*.*

Bitno je naglasiti da prostih brojeva ima beskonačno te u raznim područjima kriptografije trebat će nam veliki prosti brojevi. S ovom jednadžbom možemo odrediti koliko prostih brojeva postoji na nekom intervalu.

Primjer: *Koliko postoji prostih brojeva na intervalu od 10^99 do 10^100?*

$$\pi\left(10^{100}\right) - \pi\left(10^{99}\right) \approx \frac{10^{100}}{\ln 10^{100}} - \frac{10^{99}}{\ln 10^{99}} \approx 3.9 \times 10^{97}$$

3.Najveći zajednički djelitelj

Najveći zajednički djelitelj cijelih brojeva *a* i *b* je najveći cijeli broj koji dijeli i a i b. U nastavku najveći zajednički djelitelj ćemo označavati kao *nzd(a, b)* (*eng. Greatest Common Divisor*).

Primjer: nzd(6, 4) = 2, nzd(5, 7) = 1, nzd(24, 60) = 12.

Definicija: *Za cijele brojeve* a *i* b *za koje vrijedi* nzd(a, b) = 1 *kažemo da su* ***relativno prosti.***

VJEŽBE U MATLABU

Napišite sljedeće zadatke koristeći funkcije i skripte u Matlab-u.

ZADATAK 1

Napišite funkciju koja prima jedan cijeli broj te provjerava da li je taj broj prost. Ako je broj prost funkcija vrača vrijednost 1 u suprotnome vraća vrijednost 0.

ZADATAK 2

Napišite skriptu ispisuje sve proste brojeve na intervalu [a,b]. Interval unosi korisnik.

ZADATAK 3

Napišite skriptu koja ispisuje sve proste faktore unesenog broja.

ZADATAK 4

Napišite funkciju koja prima dva cijela broja a i b. Funkcija ispisuje najveći zajednički djelitelj brojeva a i b.