http://crypto.fmf.ktu.lt/telekonf/archyvas/B111%20Kriptologija/B111%202024-P/

Course Works
http://crypto.fmf.ktu.lt/xdownload/

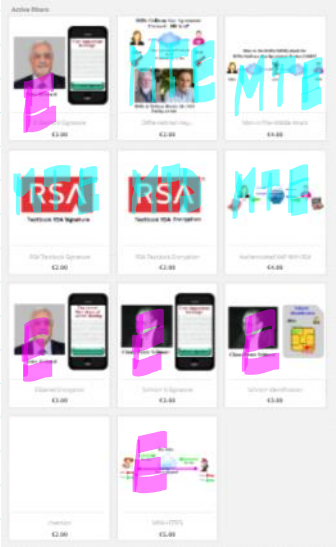
- Course_Work-Example.7z
- Course_Work-Requirements-2022.doc
- Course_Works-List.docx

Registracija bus pateikta mano Google drive.

Midterm Exam, Exam.

https://imimsociety.net/en/
https://imimsociety.net/en/16-intellect
Registration: **Jonas Petraitis** must register as [Surname: **Pe**] [Name: **Jonas**].
You must purchase only one problem at a time

https://imimsociety.net/en/14-cryptography



After successful problem You are invited to press a button [Get reward]
The result you can verify in Your account --> ORDER HISTORY AND DETAILS -->

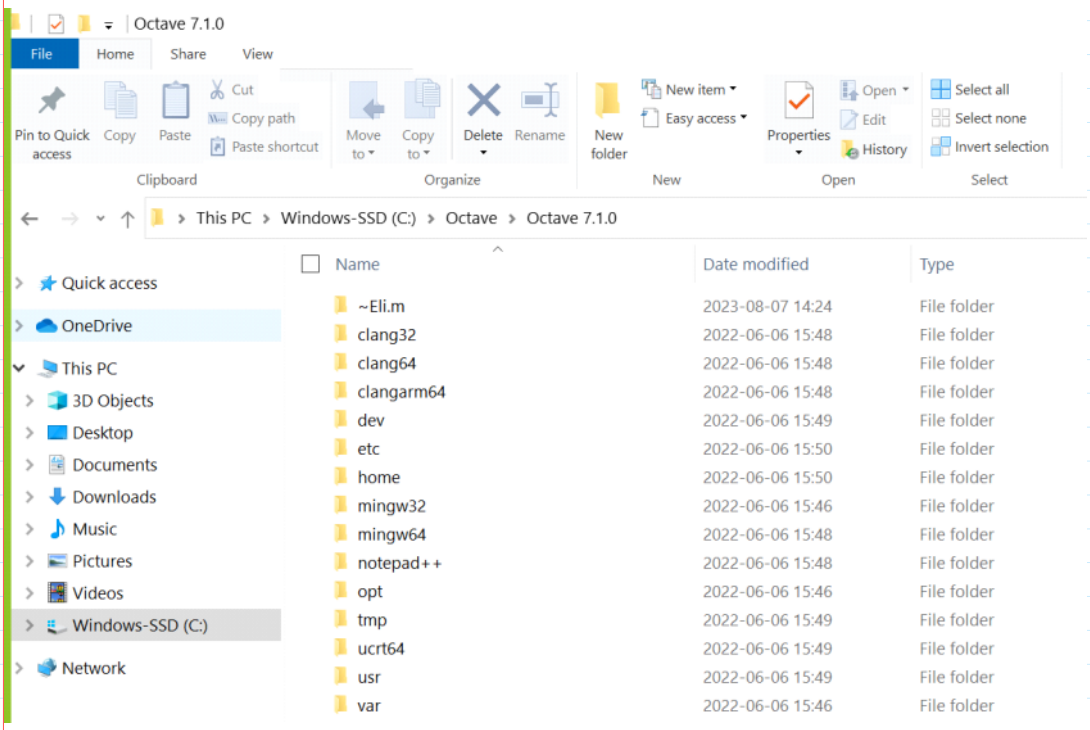
Here are the orders you've placed since your account was created.

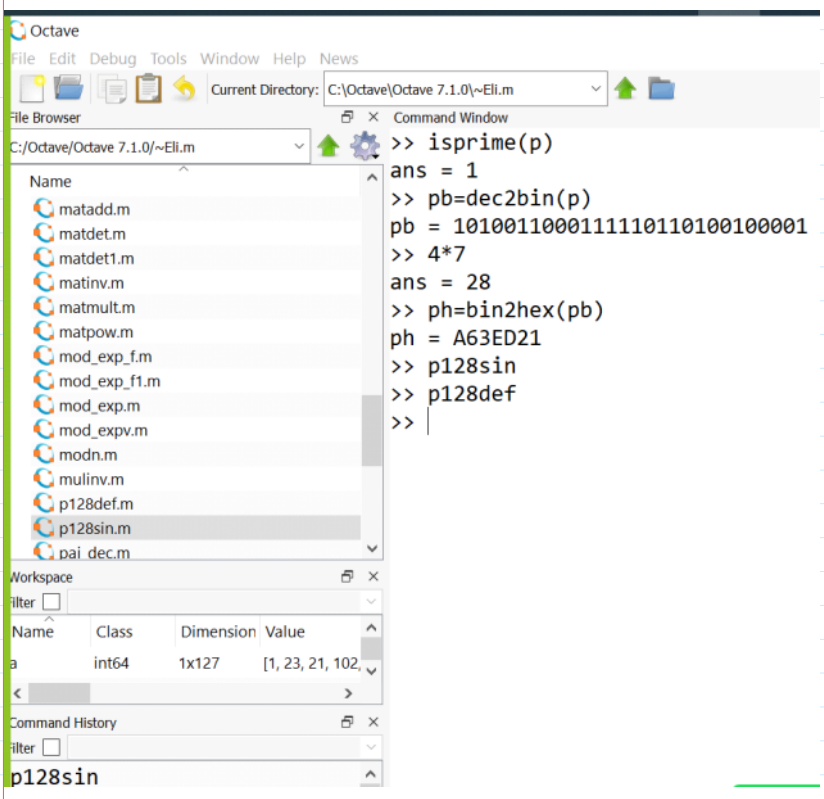
Order reference	Date	Total price	Payment	Status	Invoice	
KTVWXUNJO	01/24/2022	€0.00	Knowledge Bank	Payment accepted	PDF	Details Reorder

Moodle:

http://crypto.fmf.ktu.lt/xdownload/

- octave-7.3.0-w64-installer.exe
- octave.Stud.7z






```
>> concat(1234,abcd)
error: 'abcd' undefined near line 1, column 13
>> concat('1234','abcd')
ans = 1234abcd
```

dec	bin	hex
0	0	0
1	1	1
2	10	2

```
>> concat('1234','abcd')
ans = 1234abcd
>> x=randi(2^28-1)
x = 2.3294e+08
>> x=int64(randi(2^28-1))
x = 14516685
>> xb=dec2bin(x)
xb = 1101 1101 1000 0001 1100 1101

>> h1=bin2hex(1101)
error: base2dec: S must be a string or cellstring
error: called from
    base2dec at line 66 column 5
    bin2dec at line 64 column 5
    bin2hex at line 4 column 5
>> h1=bin2hex('1101')
h1 = D

>> xh=bin2hex(xb)
xh =  D  D  8  1  C  D
xb = 1101 1101 1000 0001 1100 1101
```

1	1	1
2	10	2
3		
4		
5		
6		
7	111	7
8	1000	8
10	1010	A
11	1011	B
12		C
13	1101	D
14		E
15	1111	F

```
>> factor(15)
ans =    3   5

>> p=genprime(28)
p = 194865859
>> factor(p)
ans = 194865859
>> isprime(p)
ans = 1
>> isprime(15)
ans = 0
>> pb=dec2bin(p)
pb = 10111001110101101010011000011
>> ph=dec2hex(p)
ph = B9D6AC3
```

The number p is strong prime if p = 2*q+1, when p and q are primes: q = (p-1)/2.

```
>> p=genprime(28)
p = 194865859
>> q=(p-1)/2
q = 97432929
>> isprime(q)
ans = 0

>> p=genstrongprime(28)
p = 201318479
>> isprime(p)
ans = 1
>> q=(p-1)/2
q = 100659239
>> isprime(q)
ans = 1
```

Operations mod p

Pvz. 23 mod 19 = 4

$23 \mid 19$, $19 \mid 1$, 4

$a \bmod n: \quad a = kn + r \rightarrow 23 = 1 \cdot 19 + 4$

$DEF\ (a,x,p) = a^x \bmod p: \quad (a^x)^y \bmod p = a^{xy} \bmod p$

$(a^x \cdot a^y) \bmod p = a^{x+y} \bmod p$

```
>> mod(23,19)
ans = 4
```

```
>> 2^4-1
```

```
> n=5
```

```
>> mod(23,19)
ans = 4
>>
>> 2^8
ans = 256
>> 2^13
ans = 8192
>> n=1234
n = 1234
>> mod(2^13,n)
ans = 788
>>
>> mod_exp(2,13,n)
ans = 788
```

```
>> 2^4-1
ans = 15
>> 2^28-1
ans = 2.6844e+08
>> int64(2^28-1)
ans = 268435455

>> (2^3)^4
ans = 4096
>> 2^12
ans = 4096
```

```
> n=5
n = 5
>> e3=mod_exp(2,3,n)
e3 = 3
>> e34=mod_exp(e3,4,n)
e34 = 1
>> ee34=mod_exp(2,12,n)
ee34 = 1
```

Till this place

For our simulation we will use integers o 28 bit length.
In cryptography we will use random generated integers, prime numbers, strong prime numbers.

```
>> r=randi(2^28-1)
r = 1.0235e+08
>> r=int64(randi(2^28-1))
r = 97878448
>> r=int64(randi(2^28-1))
r = 129372293
>> rb=dec2bin(r)
rb = 111101101100001000010000101
>> rh=bin2hex(rb)
rh = 7B61085
```

```
r = 129 372 293
rb = 111 1011 0110 0001 0000 1000 0101
rh =  7   B   6   1   0   8   5

r = 152983475
rb = 1001 0001 1110 0101 0111 1011 0011
rh =  9   1   E   5   7   B   3
```

$10000_{(2} = 1\cdot 2^4 + 0\cdot 2^3 + 0\cdot 2^2 + 0\cdot 2^1 + 0\cdot 2^0 = 2^4 = 16$

Dec	Bin	Hex
0	0000	0_h
1	0001	1_h
2	0010	2_h
3	0011	
4	0100	
5		
6		
7	0111	
8	1000	8
9		
10	1010	A_h
11	1011	B
12		C
13		D
14		E
15	1111	F
16	10000	10

```
>> r=int64(152983475)
r = 152983475
>> rh=dec2hex(r)
rh = 91E57B3
>> rb=hex2bin(rh)
rb = 10010001111001010111110110011

>> p=genprime(28)
p = 265365371
>> isprime(p)
ans = 1

>> ph=dec2hex(p)
ph = FD1277B
```

```
p = 265365371
>> isprime(p)
ans = 1
pb = 1111 1101 0001 0010 0111 0111 1011
ph =  F   D   1   2   7   7   B

>> max=int64(2^28-1)
max = 268435455
```

```
ph = FD1277B
>> pb=hex2bin(ph)
pb = 11111101000100100111101111011

>> ps=genstrongprime(28)
ps = 210821363
```