## Course Works

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

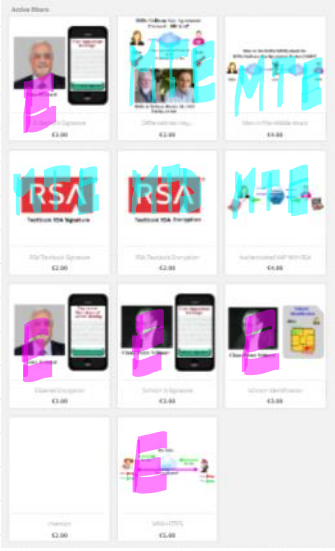
- Course_Work-Example.7z
- Course_Work-Requirements-2022.doc
- Course_Works-List.docx

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.

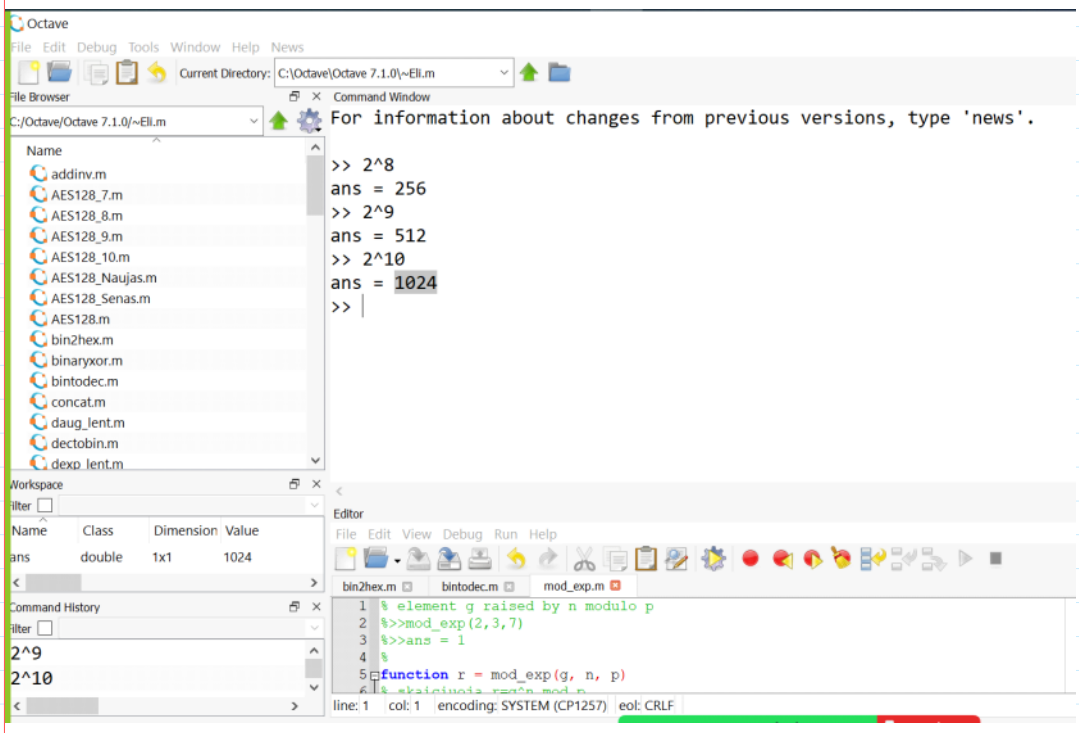
| Order reference | Date | Total price | Payment | Status | Invoice | |
|---|---|---|---|---|---|---|
| KTVWXUNJO | 01/24/2022 | €0.00 | Knowledge Bank | Payment accepted | PDF | Details Reorder |

## **Moodle:**

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

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

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




For our simulation we will use integers of 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=int64(152983475)
r = 152983475
>> rh=dec2hex(r)
rh = 91E57B3
>> rb=hex2bin(rh)
rb = 100100011110010101111110110011

>> p=genprime(28)
p = 265365371
```

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

$2^4\,2^3\,2^2\,2^1\,2^0$
$10000 = 1\cdot 2^4 + 0\cdot 2^3 + 0\cdot 2^2 +$
$+ 0\cdot 2^1 + 0\cdot 2^0 = 2^4 = 16$

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

| 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 |

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

>> ph=dec2hex(p)
ph = FD1277B
>> pb=hex2bin(ph)
pb = 1111110100010010011101111011

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

```
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
```

| | | |
|---|---|---|
| 14 | | E |
| 15 | 1111 | F |
| 16 | 10000 | 10 |