

Lab. Works

- > Octave tools to learn Cryptography
- > Study materials
- > Other downloadable information

<https://crypto.fmf.ktu.lt/xdownload/>

Download these files:

- [octave-9.2.0-w64-installer.exe](#)
- [octave.Stud.7z](#)

>> 2^8	>> p=11	>> 2^8
ans = 256	p = 11	ans = 256
>> n=14	>> mod(25,11)	>>
n = 14	ans = 3	>> mod_exp(2,9,p)
>> n=14;	>> mod(25,p)	ans = 6
>> dec2bin(n)	ans = 3	>> mod(2*9,p)
ans = 1110	>>	ans = 7
>> dec2hex(n)	>> mod_exp(2,8,p)	>> mod(2^9,p)
ans = E	ans = 3	ans = 6
>> dec2hex(10)	>> mod(256,p)	>> 2^9
ans = A	ans = 3	ans = 512
		>> mod(512,p)
		ans = 6

>> 2*2	>> r=123456678	
ans = 4	r = 1.2346e+08	// float variable format
>> mod(15*5,10)	>> r=int64(123456789)	// integer format 64 bits
ans = 5	r = 123456789	
>> 15*5	>> dec2bin(p)	
ans = 75	ans = 1111111000000011011011000011	
>> mod(37,11)	>> g=randi(p)	
ans = 4	g = 1.0487e+08	
>> mod_exp(2,3,7)	>> g=int64(randi(p))	
ans = 1	g = 158646790	
>> p=genstrongprime(28)	>> a=mod_exp(g,r,p)	
p = 266352323	a = 196830972	
>> isprime(p)		
ans = 1		