http://crypto.fmf.ktu.lt/telekonf/archyvas/inf5028-2025/

Today after the lecture we proceed with the other lecture instead of lab. Works.

Operation modulo n: $\bmod n$.

Pvz. 1. $137 \bmod 11 = 5$

$137 = 12 \cdot 11 + 5$

$$\begin{array}{r|l} 137 & 11 \\ -11 & 12 \\ \hline 27 & \\ -22 & \\ \hline 5 & \end{array} \qquad \begin{array}{r|l} 4 & 2 \\ -4 & 2 \\ \hline 0 & \end{array}$$

$2 \bmod 2 = 0$

$4 \bmod 2 = 0$

$\mathbb{Z} = \{\ldots, -3, -2, -1, 0, 1, 2, 3, 4, 5, 6, \ldots\}$

Pvz. 2. $n=2$: $\forall a \in \mathbb{Z} \longrightarrow a \bmod 2 = \begin{cases} 0, & \text{if } a \text{ even} \quad (e) \\ 1, & \text{if } a \text{ odd} \quad (o) \end{cases}$

$$\begin{array}{r|l} 5 & 2 \\ -4 & 2 \\ \hline 1 & \end{array}$$

$a \bmod 2 \in \{0, 1\}$

$\mathbb{Z} \bmod 2 = \{0,1\}$; $f_2 = \bmod 2 \longrightarrow f_2(\mathbb{Z}) = \{0,1\} = \mathbb{Z}_2$

$f_2: \mathbb{Z} \longrightarrow \mathbb{Z}_2 = \{0,1\}$

$\mathbb{Z}_2$ arithmetics : $< \mathbb{Z}_2, \overset{XOR}{\oplus}, \overset{AND}{\&} >$

+	e	o
e	e	o
o	o	e

$e \equiv 0$, $o \equiv 1$ $\longrightarrow$

$\oplus$	0	1
0	0	1
1	1	0

$\oplus$ XOR

Exclusive OR

$1 \oplus 1 = 2 \bmod 2 = 0$

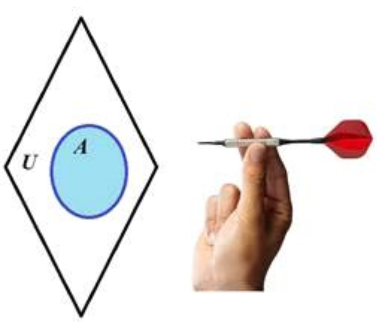
$\cdot$	e	o
e	e	e
o	e	o

$e \equiv 0$, $o \equiv 1$ $\longrightarrow$

&	0	1
0	0	0
1	0	1

& AND

Conjunction



XOR and AND logical operations in Boolean algebra can be illustrated by dartboard game.

Single Boolean variable can be represented by the set of 2 values {0,1} or {Yes,No} or {True,False}.

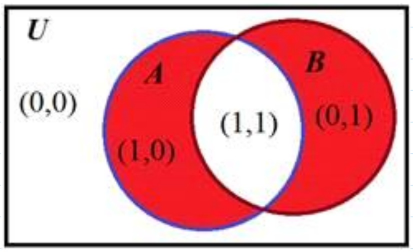
Let ***U*** is some universal set containing all other sets (we do not takke into account paradoxes related with ***U*** now).

Let ***A*** be a set in ***U***. Then with the set ***A*** in ***U*** can be associated a Boolean variable b_A=1 if area ***A*** is hit by missile

b_A=0 otherwise.

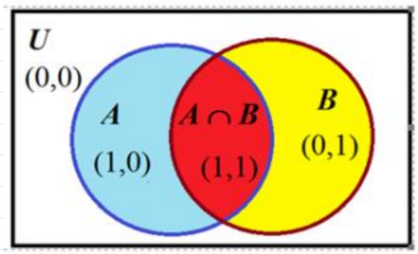
For this single variable b_A the negation (inverse) operation ` is defined:
$\boldsymbol{b_A}$`=0 if $\boldsymbol{b_A}$=1,
$\boldsymbol{b_A}$`=1 if $\boldsymbol{b_A}$=0.
Bollean operations are named also as Boolean functions.
Since negation operation/function is performed with the singe variable it is called a unary operation.

There are 16 Boolean functions defined for 2 variables and called binary functions.
Two of them XOR and AND are illustrated below.



A	B	$A \oplus B$
0	0	0
1	0	1
0	1	1
1	1	0

A	B	A&B
0	0	0
1	0	0
0	1	0
1	1	1



Venn diagram of $\boldsymbol{A \oplus B}$ operation.

Venn diagram of **A&B** operation.

$n=3: \quad \mathcal{Z} \bmod 3 = \mathcal{Z}_3 = \{0,1,2\}$

$\mathcal{Z}_3$ arithmetics : $\mathcal{Z} \bmod 3 = \mathcal{Z}_3 = \{0,1,2\}$

$\mathcal{Z}_{30} = \{0, 3, 6, 9, \ldots\} \bmod 3 = 0$

$\mathcal{Z}_{31} = \{1, 4, 7, 10, \ldots\} \bmod 3 = 1$

$\mathcal{Z}_{32} = \{2, 5, 8, 11, \ldots\} \bmod 3 = 2$

$9 \,|\, 3$, 9, 3, 0 — $9 \bmod 3 = 0$

$7 \,|\, 3$, 6, 2, 1 — $7 \bmod 3 = 1$

$11 \,|\, 3$, 9, 3, 2 — $11 \bmod 3 = 2$

$\mathcal{Z}_n$ arithmetic $(n < \infty)$: $\mathcal{Z} \bmod n = \mathcal{Z}_n = \{0, 1, 2, \ldots, n-1\}$ $\quad 0 \equiv n$ $\quad n \,|\, n$, $-n$, 1, 0

Let $n = p$ when p is prime; e.g. $p \in \{3, 5, 7, 11, 13, 17, 19, 23, \ldots\}$
The primes are the number that can be divided only by 1 and by itself.
For ex. the first prime numbers are $\{2, 3, 5, 7, 11, 13, \ldots\}$

Let $p = 11$, Then $\mathcal{Z}_p = \{\cancel{0}, 1, 2, 3, \ldots, 10\}$; $p-1 = 10$.

$\mathcal{Z}_p^* = \{1, 2, 3, \ldots, p-1\}$ $\qquad \mathcal{Z}_p^* = \{1, 2, 3, \ldots, 10\}$.

Multiplication Tab		Z11*								

$9 \times 9 = 81$

Multiplication Tab		Z11*									
*	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**10**	
1	1	2	3	4	5	6	7	8	9	10	
2	2	4	6	8	10	1	3	5	7	9	
3	3	6	9	1	4	7	10	2	5	8	
4	4	8	1	5	9	2	6	10	3	7	
5	5	10	4	9	3	8	2	7	1	6	
6	6	1	7	2	8	3	9	4	10	5	
7	7	3	10	6	2	9	5	1	8	4	
8	8	5	2	10	7	4	1	9	6	3	
9	9	7	5	3	1	10	8	6	4	2	
10	10	9	8	7	6	5	4	3	2	1	

$9 \times 9 = 81$

$$\begin{array}{r|l} 12 & 11 \\ -11 & 1 \\ \hline 1 & \end{array}$$

$12 \bmod 11 = 1$

set Z_{11} is closed with respect to $*$ mod 11.

Pair of objects $< Z_{11}^*, * \bmod 11 >$ is called an agebraic group.

In general $< Z_p^*, * \bmod p >$

Exponent Tab		Z11*									
^	0	1	2	3	4	5	6	7	8	9	10
1	1	1	1	1	1	1	1	1	1	1	1
2	1	2	4	8	5	10	9	7	3	6	1
3	1	3	9	5	4	1	3	9	5	4	1
4	1	4	5	9	3	1	4	5	9	3	1
5	1	5	3	4	9	1	5	3	4	9	1
6	1	6	3	7	9	10	5	8	4	2	1
7	1	7	5	2	3	10	4	6	9	8	1
8	1	8	9	6	4	10	3	2	5	7	1
9	1	9	4	3	5	1	9	4	3	5	1
10	1	10	1	10	1	10	1	10	1	10	1

$$\begin{array}{r|l} 16 & 11 \\ -11 & 1 \\ \hline 5 & \end{array}$$

$2^4 \bmod 11 = 16 \bmod 11 = 5$

Γ is a set of generators

$\Gamma = \{2, 6, 7, 8\}; |\Gamma| = 4.$

$q = (p-1)/2$

$q = 5$

$p = 2 \cdot 5 + 1 = 11$

The prime number p is **strong prime** if $p = 2*q + 1$, when q - is prime as well.
To find agenerator in the set Z_p^* we must perform the following computatons.
1.Choose random number g in Z_p^* as a candidate of generator.
2.Verify if the following 2 conditions are satisfied:
for all $g \in \Gamma$ the following must hold $g^q \neq 1 \bmod p$; and $g^2 \neq 1 \bmod p$.

For examplee: $p = 11$, then $p = 2 \cdot \underset{q}{5} + 1 = 11$ and $q = 5$ is prime.

1) $p = 5$ – is prime, and it is a strong prime $p = 2 \cdot q + 1 = 2 \cdot \overset{q}{2} + 1 = 5$

2) $p = 7$ – is prime, and – – – – – $p = 2 \cdot q + 1 = 2 \cdot 3 + 1 = 7$

3) $p = 17$ – is prime, but it is not a strong prime $p = 2 \cdot q + 1 = 2 \cdot 8 + 1 = 17$
$q = 8$ – is not a prime

Discrete Exponent Function (12/14)

Let as above p=11 and is strong prime in $Z_{11}^* = \{1, 2, 3, \ldots, 10\}$ and generator we choose $g = 7$ from the set $G = \{2, 6, 7, 8\}$.

Let as above p=11 and is strong prime in Z_{11}^* ={1, 2, 3, …, 10} and generator we choose g = 7 from the set **G**={2, 6, 7, 8}.
Public Parameters are **PP**=(**11**,**7**), Then $\mathbf{DEF}_g(x) = \mathbf{DEF}_7(x)$ is defined in the following way:

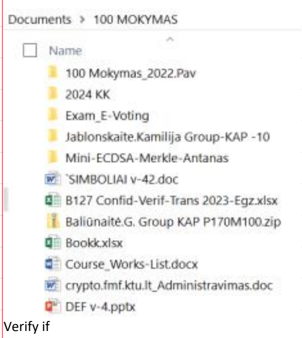
$$\mathbf{DEF}_7(x) = 7^x \mathbf{\ mod\ } 11 = a;$$

$\mathbf{DEF}_7(x)$ provides the following 1-to-1 mapping, displayed in the table below.

$7 \cdot 7 = 49$ | 11
-44 | 4
5

x	0	1	2	3	4	5	6	7	8	9	*10*	*11*	*12*	*13*	*14*
7^x **mod** p = a	1	7	5	2	3	10	4	6	9	8	*1*	*7*	*5*	*2*	*3*

Modular operations z mod p: >> mod(z,p)   DEF: >> mod_exp(2,8,p)



Verify if

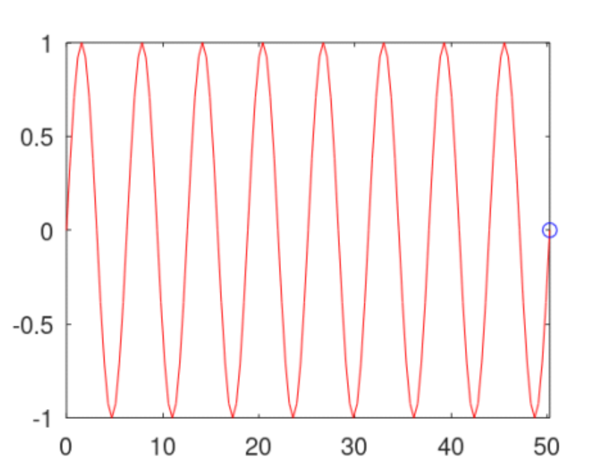
$2^8 \bmod 10$: >> mod_exp(2,8,10)=6

$2^8 = 256$: >> mod(256,10)=6

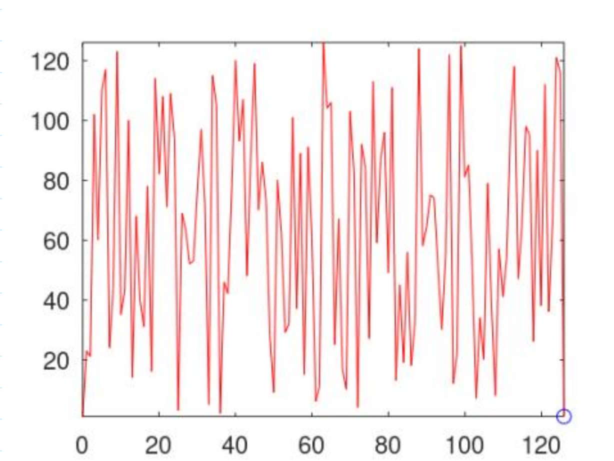
256 | 10
-20 | 25
56
-50
6

```
>> mod_exp(2,8,10)
ans = 6
>> 2^8
ans = 256
>> mod(ans,10)
ans = 6
```

>> p128sin



>> p128def



Private and Public Keys generation : PrK = x ; PuK = a ;

1) Generate strong prime number p.

>> p = genstrongprime(28) % generates 28 bit lenghts of p

2) Find a generator g in the set $Z_p^* = \{1, 2, 3, \ldots, p-1\}$

>> q = (p-1)/2

>> g = 2

>> mod_exp(g, q, p) % I-st condition $g^q \bmod p \neq 1$

$>> g = 2$

$>> mod\_exp(g, q, p)$ % I-st condition $g^q \bmod p \neq 1$
% If it is equal to 1 → choose the other g
% If no, then verify:

$>> mod\_exp(g, 2, p)$ % II-nd condition
% If it is equal to 1 → choose the other g.

$PP = (p, g)$

3) Generate $PrK = x$ using random number generator function randi

$>> x = int64(randi(2^{28}-1))$

```
>> x=randi(2^28-1)
x = 1.9906e+08
>> x=int64(randi(2^28-1))
x = 256210849
```

4) compute $PuK = a$ using DEF, i.e. function

$>> a = mod\_exp(g, x, p)$

The end of the 1-st Part

PP = (***p***, ***g***) values In real cryptography are: $p \sim 2^{2048} \approx 10^{700}$ $|p| = 2048$ bits
In our simulation we use: $p \sim 2^{28}$ $|p| = 28$ bits

```
>> p=genstrongprime(28)
p = 215914079
>> pb=dec2bin(p)
pb = 1100 1101 1110 1001 0110 0101 1111
>> length(pb)
ans = 28

q = 107957039
>> isprime(q)
ans = 1
```

F

```
>> pb=dec2bin(p)
pb = 1100 1101 1110 1001 0110 0101 1111
      C    D    E    9    6    5    F
>> bin2hex(pb)
ans = CDE965F
```

Remark: if $z < p$
then $z \bmod p = z$

12321 < 215914079
mod(12321, 215914079) = 12321

$g^q \bmod p \neq 1$

```
>> g=2;
>> mod_exp(g,q,p)
ans = 1
>> g=3;
>> mod_exp(g,q,p)
...
>> g=11;
>> mod_exp(g,q,p)
ans = 1
>> g=111;
>> mod_exp(g,q,p)
ans = 215914078

>> mod_exp(g,2,p)
ans = 12321
```

PP = (***p***, ***g***) = (215914079, 111)

Prvate Key **PrK** = ***x*** and Public Key **PuK** = ***a*** generation and computation.

$x \leftarrow randi(\mathcal{Z}_{p-1})$

$\mathcal{Z}_{p-1} = \{0, 1, 2, ..., p-2\}$

$a = g^x \bmod p$

$>> int64(randi(2^{28}-1))$

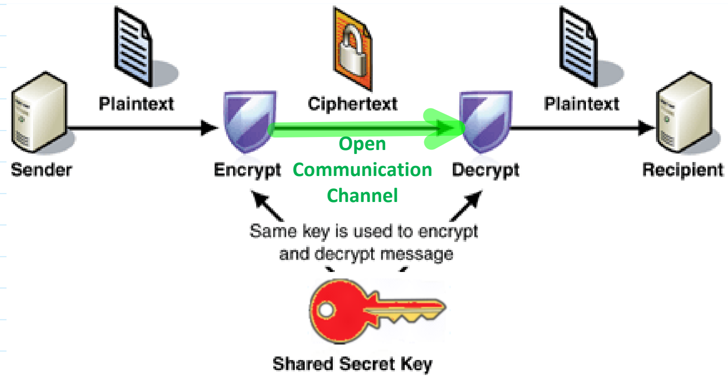
$>> a = mod\_exp(g, x, p)$

```
>> x=randi(2^28-1)
x = 8.0860e+07
>> x=int64(randi(2^28-1))
x = 193794955
>> a=mod_exp(g,x,p)
a = 168966198
```

$Z_{p-1}^* = \{1, 2, 3, \ldots, p-2\}$ | x = 1997...

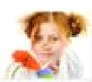
$a = g^x \bmod p$ | >> a=mod_exp(g,x,p)

>> a=mod_exp(g,x,p)
a = 168966198



Diffie-Hellman Key Agreement Protocol (DH KAP)

Public Parameters PP=(*p*,*g*)



$u \leftarrow rand(Z_p^*)$

$g^u \bmod p = t_A$ → t_A

$v \leftarrow rand(Z_p^*)$

t_B ← $t_B = g^v \bmod p$

$k_{AB} = (t_B)^u \bmod p =$
$= (g^v)^u \bmod p = g^{vu} \bmod p$

$k_{BA} = (t_A)^v \bmod p =$
$= (g^u)^v \bmod = g^{uv} \bmod p$

$k_{AB} = k = k_{BA}$

Security considerations: if someone can comput for example a secret param. u generated by A the he/she can compute secret key k by intercepting t_B

Adv.: $(t_B)^u \bmod p = k$.

If p is generated large enough, e.g. $p \sim 2^{2048} \approx 10^{700}$, $|p| = 2048$ bits the to find u when p, g and t_A are given is infeasible with classical computers.

It is ifeasible to compute u from the equation $g^u \bmod p = t_A$ by having p, g and t_A.

The problem to find u when p, g and t_A are given is called a discret logarithm problem — DLP

$dlog_g (g)^u \bmod p = u \cdot dlog_g (g) \bmod p = u \cdot 1 \bmod p = u$.

The end of the 2-nd Part