δ

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. $137 \bmod 11 = 5$

$137 = 12 \cdot 11 + 5$

$137 : 11 = 12$, $27 - 22 = 5$

$4 : 2 = 2$, $4 - 4 = 0$

$2 \bmod 2 = 0$

$4 \bmod 2 = 0$

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

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

$5 : 4 = 1$, $5 - 4 = 1$

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

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

$f_2 : \mathcal{Z} \rightarrow \mathcal{Z}_2 = \{0, 1\}$

$\mathcal{Z}_2$ arithmetics : $< \mathcal{Z}_2, \oplus, \& >$ (XOR, AND)

+	e	o
e	e	o
o	o	e

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

⊕	0	1
0	0	1
1	1	0

⊕ XOR Exclusive OR

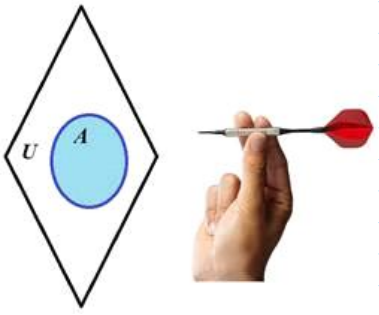
$1 \oplus 1 = 2 \bmod 2 = 0$

·	e	o
e	e	e
o	e	o

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

&	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}.

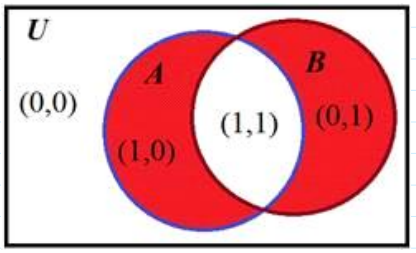
Let ***U*** is some universal set containing all other sets (we do not takke into account paradoxes related with ***U*** now).

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.

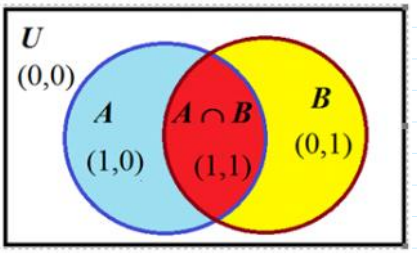
For this single variable b_A the negation (inverse) operation ` is defined:
b_A`=0 if b_A=1,
b_A`=1 if b_A=0.
Bollean operations are named also as Boolean functions.
Since negation operation/function is performed with the singe variable it is called a unary operation.

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 ⊕ 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 ***A*⊕*B*** operation.

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

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

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

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

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

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

$9 \bmod 3 = 0$

$7 \bmod 3 = 1$

$11 \bmod 3 = 2$

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

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 $\mathcal{I}_p = \{0, 1, 2, 3, \ldots, 10\}$; $p - 1 = 10$.

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

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	

$9 \times 9 = 81$

$12 \bmod 11 = 1$

set $\mathcal{Z}_{11}$ is closed with respect to $* \bmod 11$.

Pair of objects $\langle \mathcal{Z}_{11}^*, * \bmod 11 \rangle$ is called an agebraic group.

In general $\langle \mathcal{Z}_p^*, * \bmod p \rangle$

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

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

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 $\mathbf{Z_p^*}$ we must perform the following computatons.
1.Choose random number g in $\mathbf{Z_p^*}$ 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 example: $p = 11$, then $p = 2 \cdot 5 + 1 = 11$ and $q = 5$ is prime.

1) $p = 5$ – is prime, and it is a strong prime $p = 2 \cdot q + 1 = 2 \cdot 2 + 1 = 5$
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 $\mathbf{Z_{11}^*} = \{1, 2, 3, \ldots, 10\}$ and generator we choose g = 7 from the set $G = \{2, 6, 7, 8\}$.

Let as above p=11 and is strong prime in $\mathbf{Z}_{11}^*$ ={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:

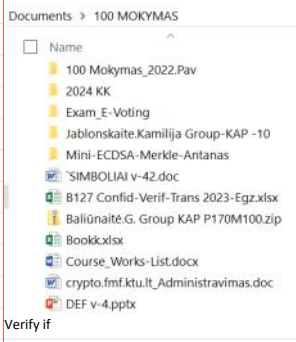
$$\mathbf{DEF}_7(x) = 7^x \bmod 11 = a;$$

$\mathbf{DEF}_7(x)$ 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
$7^x \bmod p = a$	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)



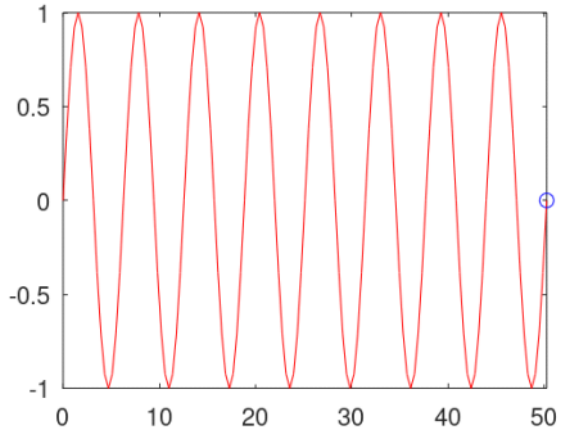
$2^8 \bmod 10$: >> mod_exp(2,8,10) = 6

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

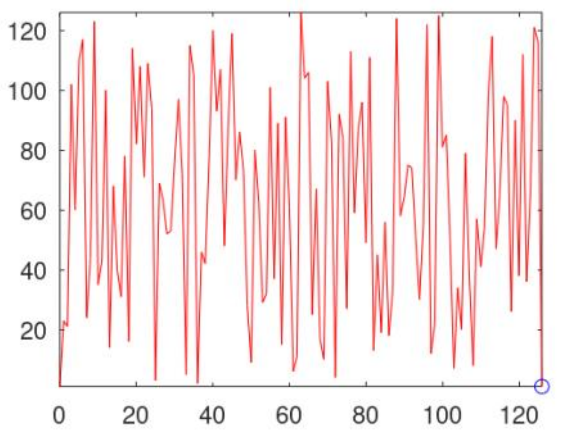
256 | 10 ; 20 ; 25 ; 56 ; 50 ; 6

```
>> 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 $\mathbb{Z}_p^* = \{1, 2, 3, \ldots, p-1\}$

```
>> q = (p-1)/2
>> g = 2
>> mod_exp(g, q, p)   % 1-st condition   g^q mod p ≠ 1
```

```
>> q = 2
>> mod_exp(q, q, p)      % I-st condition   q^q mod p ≠ 1
                         % If it is equal to 1 → choose the other q
                         % If no, then verify:
>> mod_exp(q, 2, p)      % II-nd condition
                         % If it is equal to 1 → choose the other q.
```

PP = (p, q)

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

```
>> x = int64(randi(2^28-1))
```

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

```
>> a = mod_exp(q, x, p)
```

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

The end of the 1-st Part