http://crypto.fmf.ktu.lt/telekonf/archyvas/inf3047%20Kript.Duom.Sauga/

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

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

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

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

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

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

+	e	o
e	e	o
o	o	e

$e \equiv 0$, $o \equiv 1$ →

⊕	0	1
0	0	1
1	1	0

⊕ XOR Exclusive OR

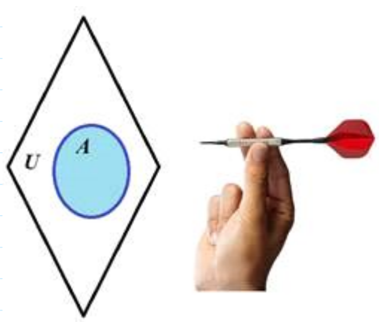
$1 \oplus 1 = 2 \bmod 2 = 0$

•	e	o
e	e	e
o	e	o

$e \equiv 0$, $o \equiv 1$ →

&	0	1
0	0	0
1	0	1

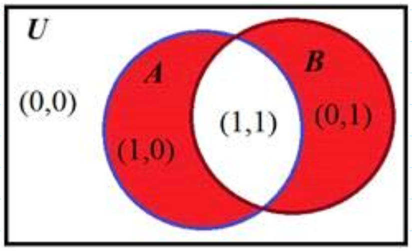
& AND Conjunction



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.

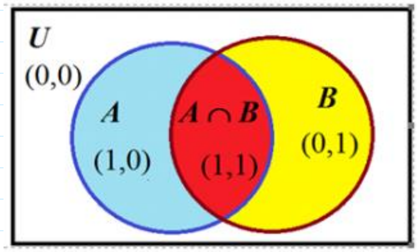
There are 16 Boolean functions defined for 2 variables and called binary functions.
Two of them XOR and AND are illustrated below.



Venn diagram of $A \oplus B$ operation.

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 **A&B** operation.

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

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

$\mathbb{Z}_{30} = \{0, 3, 6, 9, \dots\} \bmod 3 = 0$

$\mathbb{Z}_{31} = \{1, 4, 7, 10, \dots\} \bmod 3 = 1$

$\mathbb{Z}_{32} = \{2, 5, 8, 11, \dots\} \bmod 3 = 2$

$9 \div 3 = 3$, $9 - 9 = 0$; $\quad 9 \bmod 3 = 0$

$7 \div 3 = 2$, $7 - 6 = 1$; $\quad 7 \bmod 3 = 1$

$11 \div 3 = 3$, $11 - 9 = 2$; $\quad 11 \bmod 3 = 2$

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

$n \div n = 1$, $n - n = 0$

Let $n = p$ when p is prime; e.g. $p = 3, 5, 7, 11, \dots$

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

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

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

Exponent Tab Z11*

$9 \times 9 = 81$

$12 \div 11 = 1$, $12 - 11 = 1$

$12 \bmod 11 = 1$

set $\mathbb{Z}_n$ is closed with respect to $* \bmod 11$.

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

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

16 | 11

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

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

Let ***p*** is strong prime ***p*** = 2****q*** + 1, when ***q*** - is prime, then for all ***g***∈**Γ**
$g^q \neq 1$ **mod** ***p***; and $g^2 \neq 1$ **mod** ***p***.

$q = (p-1)/2$

$q = 5$

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

Discrete Exponent Function (12/14)

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 **Γ**={2, 6, 7, 8}.

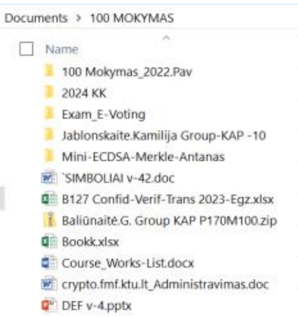
Public Parameters are **PP**=(**11**,**7**), Then $\mathbf{DEF}_g(x) = \mathbf{DEF}_7(x)$ is defined in the following way:

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

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

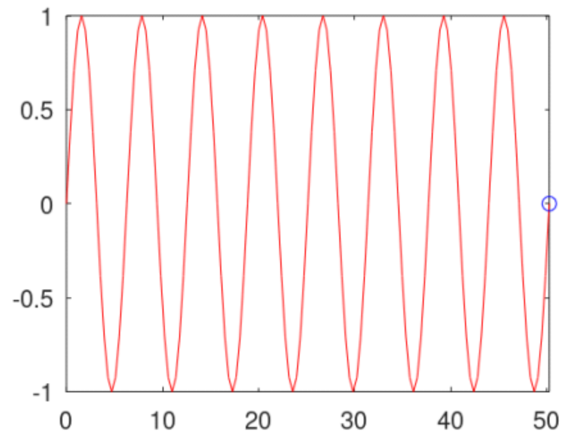
x	**0**	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	*10*	*11*	*12*	*13*	*14*
7^x **mod** ***p*** = ***a***	**1**	**7**	**5**	**2**	**3**	**10**	**4**	**6**	**9**	**8**	*1*	*7*	*5*	*2*	*3*

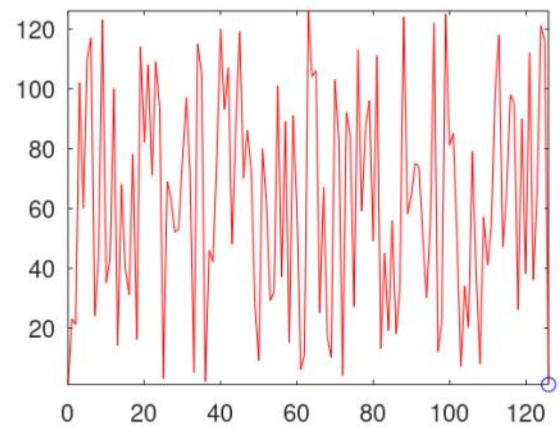
$$7 \cdot 7 = 49 \begin{array}{|l} 11 \\ \hline 4 \end{array}$$
$$\begin{array}{r} -44 \\ \hline 5 \end{array}$$



\>> 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) % I-st condition
% 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.

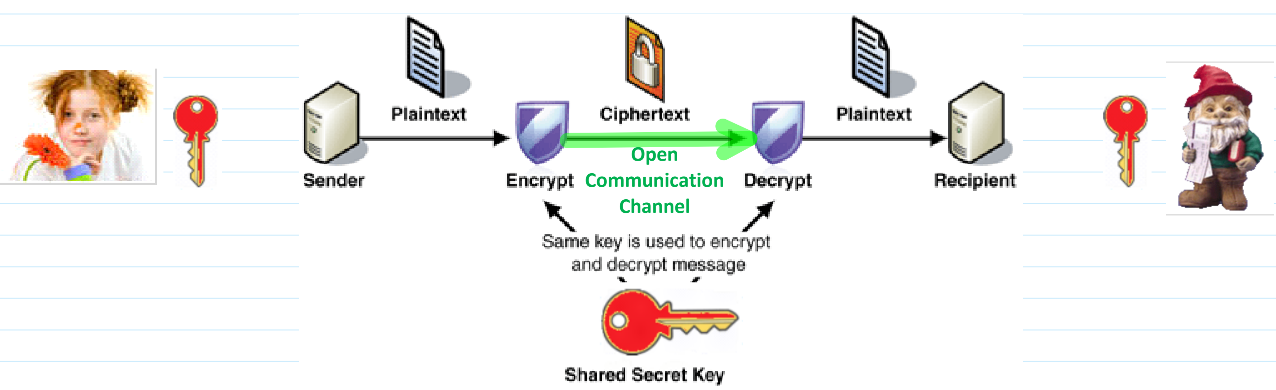
3) Generate $PrK = x$ using random number generator function randi

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

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

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

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



Diffie-Hellman Key Agreement Protocol (DH KAP)

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

$u \leftarrow rand(Z_p^*)$

$g^u \bmod p = t_A \longrightarrow t_A$

$v \leftarrow rand(Z_p^*)$

$t_B \longleftarrow t_B = g^v \bmod p$

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

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

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

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

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