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

Operation modulo v	n: modn.
Puz. 1. 137 mod 11 = 5	$-\frac{137}{11}$ $-\frac{11}{12}$ $-\frac{11}{12}$
137 = 12.11 + 5	$-\frac{27}{22}$
4	5 2 mod 2 = 0
$d = f_{}, -3, -2, -1, 0$	, 1, 2, 3, 4, 5, 6, } 4 mod 2 = 0
Avz. 2. h=2: Va EZ -	$\Rightarrow a \mod 2 = \int 0, if a even (e)$
a mod 2 E f 0, 1 }	1, if a odd $(\sigma) - \frac{5}{4} \frac{1^2}{2}$
$I \mod 2 = \{0, 1\};$	$f_2 = mod 2 - f_2(I) = f_2(I) = I_2$
$f_{\mathbf{z}}: \mathcal{I} \twoheadrightarrow \mathcal{I}_{\mathbf{z}} = \{0, 1\}$	XOR AND
$\mathcal{I}_2$ arithmetics : < c	$\mathcal{I}_2, \oplus, \& >$
$\frac{+e}{e} = 0$	$\frac{\oplus 0}{2} \frac{1}{2} \oplus x0R$
e = 0 o = 0 = 1	1 1 0 1 0 1 0 1 0 1 0 0 0 0 0 0 0 0 0 0
• e o	KIOI NAND
$\begin{array}{c c} e & e \\ \hline e & e \\ \hline e$	> 000 Conjunction
DED DE	1   0 1
Λ	XOR and AND logical operations in Boolean algebra can be
	illustrated by dartboard game.

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.

 $(0,0) \begin{pmatrix} A & B & A &$ (0,0) A  $A \cap B$ **B** (0,1) Venn diagram of A&B operation. Venn diagram of  $A \oplus B$  operation. n=3: 2 mod 3 =  $L_3 = \{0, 1, 2\}$  $\mathcal{I}_3$  arithmetics :  $\mathcal{I} \mod 3 = \mathcal{I}_3 = \{0, 1, 2\}$  $J_{2n} = \{0, 3, 6, 9, \dots\} \mod 3 = 0$  $7_{31} = \{ 1, 4, 7, 10, \dots \} \mod 3 = 1$  $J_{32} = \{2, 5, 8, 11, \dots, 3 \mod 3 = 2\}$  $\mathcal{I}_n \quad \text{avithmetic} \ (n < \infty): \ \mathcal{I} \ \text{mod} \ N = \mathcal{I}_n = \{0, 1, 2, \dots, n-1\} \quad n \quad \prod_{n=1}^{n} f_n$ Let n=p when p is prime; e.g. p=3,5,7, 11, ... Let p = 11, Then  $Z_p = \mathcal{L}_0, 1, 2, 3, ..., 10$ ; p - 1 = 10.  $\mathcal{J}_{p}^{*} = \{1, 2, 3, \dots, p-1\}$   $\mathcal{J}_{p}^{*} = \{1, 2, 3, \dots, 10\}.$ 9×9 = 81 Multiplication Tab Z11\*  $12 \mod 11 = 1 = \frac{12}{-11} + \frac{11}{1}$ 9 10 9 10 2 4 8 10 3 6 set In is closed with respect. to \* mod 11. 5 10 Pair of objects < Im, \*mod 11> 7 3 10 is called an agebraic group. 2 10 9 7 In general < Ip\*, \* mod p> Z11\* Exponent Tab 16 111

$\begin{array}{c c c c c c c c c c c c c c c c c c c $																										
nent Tab $p = (1 + 1)^{2}$ 1 = 1 + 1 + 1 + 1 + 1 + 1 + 1 + 1 + 1 +																										
$\int_{1}^{6} 0 + \frac{1}{2} + \frac{2}{3} + \frac{3}{4} + \frac{5}{5} + \frac{7}{6} + \frac{8}{7} + \frac{9}{10} + \frac{1}{1} +$	nent Tab		Z	11*																			1	: 1	11	
$\frac{1}{2} \frac{1}{2} \frac{1}{2} \frac{1}{2} \frac{1}{4} \frac{1}{8} \frac{1}{5} \frac{1}{10} \frac{1}{9} \frac{1}{7} \frac{1}{3} \frac{1}{6} \frac{1}{1} \frac{1}{2}^{\mu} \mod 41 = 46 \mod 41 = 5$ $\frac{1}{4} \frac{1}{4} \frac{1}{5} \frac{1}{9} \frac{1}{3} \frac{1}{4} \frac{1}{5} \frac{1}{9} \frac{1}{3} \frac{1}{4} \frac{1}{5} \frac{1}{9} \frac{1}{3} \frac{1}{4} \frac{1}{7} \frac{1}{7} a set of generators$ $\frac{1}{5} \frac{1}{15} \frac{1}{5} \frac{1}{3} \frac{1}{4} \frac{1}{9} \frac{1}{15} \frac{1}{3} \frac{1}{4} \frac{1}{9} \frac{1}{9} \frac{1}{17} a set of generators$ $\frac{1}{5} \frac{1}{15} \frac{1}{5} \frac{1}{2} \frac{1}{3} \frac{1}{10} \frac$		Λ	0	1	2	2	4	5	6	7	8	9	10								_		4 C 1 N	> f	1	
$ \begin{array}{c c c c c c c c c c c c c c c c c c c $		4	4	-	4	4	7	1	1	,	4	1	10												•	
$\frac{1}{2} \frac{1}{2} \frac{2}{4} \frac{4}{8} \frac{8}{5} \frac{5}{10} \frac{9}{9} \frac{7}{3} \frac{3}{6} \frac{1}{1} \frac{2}{4} \frac{mutual}{4} \frac{2}{5} \frac{1}{6} \frac{mutual}{4} \frac{2}{5} \frac{1}{6} \frac{1}{9} \frac{3}{3} \frac{1}{1} \frac{4}{5} \frac{5}{9} \frac{3}{3} \frac{1}{1} \frac{1}{4} \frac{5}{5} \frac{9}{9} \frac{3}{3} \frac{1}{1} \frac{1}{4} \frac{1}{5} \frac{1}{6} \frac{1}{6} \frac{1}{6} \frac{6}{3} \frac{3}{7} \frac{9}{9} \frac{10}{10} \frac{5}{1} \frac{8}{8} \frac{4}{9} \frac{9}{1} \frac{1}{1} \frac{1}{10} \frac{1}{10$		1	1	1	1	1	L	T	T	1	1	1	1	H		111	_	. ,	11			à	5		N	
$\frac{3}{4} \frac{1}{1} \frac{3}{4} \frac{9}{5} \frac{5}{4} \frac{4}{1} \frac{1}{3} \frac{9}{5} \frac{5}{4} \frac{4}{1} \frac{1}{1} \frac{3}{7} \frac{9}{5} \frac{5}{4} \frac{1}{4} \frac{1}{1} P^{*} \ \text{is a set of genurators} \\ 5 \frac{1}{5} \frac{5}{3} \frac{3}{4} \frac{9}{9} \frac{1}{1} \frac{5}{5} \frac{3}{3} \frac{4}{9} \frac{9}{1} \frac{1}{1} P^{*} \ \text{is a set of genurators} \\ P^{*} = \sqrt{2}, 6, 7, 8, 3;  P^{*}  = 4 \\ 7 \frac{1}{7} \frac{7}{5} \frac{5}{2} \frac{3}{3} \frac{10}{4} \frac{4}{6} \frac{9}{9} \frac{8}{8} \frac{1}{1} \\ 9 \frac{1}{10} \frac{9}{1} \frac{9}{10} \frac{4}{3} \frac{5}{5} \frac{1}{1} \frac{9}{4} \frac{4}{3} \frac{5}{5} \frac{1}{1} \\ 10 \frac{1}{10} \frac{1}{10}$		2	1	2	4	8	5	) 10	9	7	3	6	1	2	vvivi	( 1 1	_	/	10	Л	10	'U	11	-	5	
$\begin{array}{c ccccccccccccccccccccccccccccccccccc$		3	1	3	9	5	4	1	3	9	5	4	1	-					1							
$\frac{1}{1} + \frac{1}{2} + \frac{1}$		4	1	4	5	9	З	1	4	5	9	З	1	F	140	1 SI	1	oł	-	a	N	v	ri	at	tor	-5
$ \begin{array}{c} \mathbf{s} & 1 & \mathbf{s} & \mathbf{s} & 4 & 9 & 1 & 5 & \mathbf{s} & 4 & 9 & 1 \\ 1 & 1 & 5 & 2 & 3 & 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 \\ 9 & 1 & 9 & 4 & 3 & 5 & 1 & 9 & 4 & 3 & 5 & 1 \\ 10 & 1 & 10 & 1 & 10 & 1 & 10 & 1 & 10 & 1 & 10 & 1 \\ 10 & 1 & 10 & 1 & 10 & 1 & 10 & 1 & 10 & 1 \\ 10 & 1 & 10 & 1 & 10 & 1 & 10 & 1 & 10 & 1 \\ 10 & 1 & 10 & 1 & 10 & 1 & 10 & 1 & 10 & 1 \\ 10 & 1 & 10 & 1 & 10 & 1 & 10 & 1 & 10 & 1 \\ 10 & 1 & 10 & 1 & 10 & 1 & 10 & 1 & 10 & 1 \\ 10 & 1 & 10 & 1 & 10 & 1 & 10 & 1 & 10 & 1 \\ 10 & 1 & 10 & 1 & 10 & 1 & 10 & 1 & 10 & 1 \\ 10 & 1 & 10 & 1 & 10 & 1 & 10 & 1 & 10 & 1 \\ 10 & 1 & 10 & 1 & 10 & 1 & 10 & 1 \\ 10 & 1 & 10 & 1 & 10 & 1 & 10 & 1 \\ 10 & 1 & 10 & 1 & 10 & 1 & 10 & 1 \\ 10 & 1 & 10 & 1 & 10 & 1 & 10 & 1 \\ 10 & 1 & 10 & 1 & 10 & 1 & 10 & 1 \\ 10 & 1 & 10 & 1 & 10 & 1 & 10 & 1 \\ 10 & 1 & 10 & 1 & 10 & 1 & 10 & 1 \\ 10 & 1 & 10 & 1 & 10 & 1 & 10 & 1 \\ 10 & 1 & 10 & 1 & 10 & 1 \\ 10 & 1 & 10 & 1 & 10 & 1 & 10 & 1 \\ 10 & 1 & 10 & 1 & 10 & 1 & 10 & 1 \\ 10 & 1 & 10 & 1 & 10 & 1 & 10 & 1 \\ 10 & 1 & 10 & 1 & 10 & 1 \\ 10 & 1 & 10 & 1 & 10 & 1 & 10 & 1 \\ 10 & 1 & 10 & 1 & 10 & $		-	-	-	2	4	0	-		2	J	0	1	1		, _	0		,	g .	0		٨		1	-
$ \begin{array}{c ccccccccccccccccccccccccccccccccccc$		<b>-</b>	1	Э	3	4	9	T	С	3	4	9	T	1 2	= ~	2,	6,	+	1	X	J	ĵ	'	r		= '
$\frac{7}{10} \frac{1}{10} \frac{7}{5} \frac{5}{2} \frac{2}{3} \frac{10}{10} \frac{4}{4} \frac{6}{6} \frac{9}{9} \frac{8}{8} \frac{1}{1}$ $\frac{9}{9} \frac{1}{10} \frac{3}{10} \frac{5}{10} \frac{1}{9} \frac{4}{3} \frac{3}{5} \frac{5}{1} \frac{1}{9} \frac{9}{4} \frac{3}{3} \frac{5}{5} \frac{1}{1}$ $\frac{9}{10} \frac{1}{10} \frac{1}{$		6	1	6	3	7	9	10	5	8	4	2	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         9       1       0       4       3       5       1       9       4       3       5       1         9       1       0       1       10       11       10       11       10       11       12       13       14       14       14       14       14		7	1	7	5	2	3	10	4	6	9	8	1													
$\frac{9}{10} \frac{1}{10} \frac{9}{10} \frac{4}{10} \frac{3}{10} \frac{5}{10} \frac{1}{10} \frac{9}{10} \frac$		8	1	8	9	6	4	10	3	2	5	7	1													
$\frac{10}{10} \frac{1}{100} \frac{1}$		q	1	q	Δ	3	5	1	9	4	2	5	1													
p = (p-1)/2 $p = (p-1)/2$ $q = (p-1)/2$		10	1	10	-	10	1	10	1	10	1	10	1													
$y = (p-1)/2$ $y = (p-1)/2$ $y = (p-1)/2$ $y = 5$ $p = 2r \cdot 5 + 1 = nn$ Discrete Exponent Function (12/14) s above $p=11$ and is strong prime in $\mathbb{Z}_{4}^{*} = \{1, 2, 3,, 10\}$ and generator we choose $g = 7$ from the set $\Gamma = \{2, 6, 7, 8\}$ . c Parameters are $PP = (11,7)$ . Then $DEF_{g}(x) = DEF_{7}(x)$ is defined in the following way: $DEF_{7}(x) = 7^{*} \mod 11 = a;$ (x) provides the following 1-to-1 mapping, displayed in the table below. $\frac{x  0}{57} = \frac{1}{2} \cdot \frac{3}{3} \cdot \frac{4}{3} \cdot \frac{5}{6} \cdot \frac{6}{7} \cdot \frac{8}{9} \cdot \frac{9}{10} \cdot \frac{11}{7} \cdot \frac{12}{5} \cdot \frac{13}{2} \cdot \frac{14}{3}$ $\frac{7 \cdot 7}{5} = \frac{4}{6} \cdot \frac{9}{4} \cdot \frac{14}{4}$ b 1 50 MAXMAM $\frac{7}{100} = \frac{1}{7} \cdot \frac{7}{5} \cdot \frac{2}{2} \cdot \frac{3}{10} \cdot \frac{4}{4} \cdot \frac{6}{9} \cdot \frac{9}{8} \cdot \frac{17}{7} \cdot \frac{5}{2} \cdot \frac{2}{3}$ b 1 50 MAXMAM $\frac{7}{100} = \frac{1}{7} \cdot \frac{7}{5} \cdot \frac{1}{2} \cdot \frac{1}{3} \cdot \frac{14}{5} \cdot \frac{7}{5} \cdot \frac{9}{2} \cdot \frac{14}{3} \cdot \frac{14}{5} \cdot \frac{7}{5} \cdot \frac{9}{4} \cdot \frac{14}{4}$ $\frac{7}{57} \cdot \frac{7}{5} \cdot \frac{9}{4} \cdot \frac{14}{4} \cdot \frac{14}{5} \cdot \frac{11}{5} \cdot 1$		10	T	10	1	10	T	10	T	10	T	10	T													
p is strong prime $p = 2^{*}q + 1$ , when $q$ - is prime, then for all $g \in \Gamma$ 1 mod $p$ ; and $g^{2} \neq 1 \mod p$ . P = 2 · 5 + 1 = $M$ Discrete Exponent Function (12/14) s above $p=11$ and is strong prime in $\mathbb{Z}_{1}^{*} = \{1, 2, 3,, 10\}$ and generator we choose $g = 7$ from the set $\Gamma = \{2, 6, 7, 8\}$ . c Parameters are $\mathbb{PP}=(11,7)$ , Then $\mathbb{DEF}_{q}(x) = \mathbb{DEF}_{7}(x)$ is defined in the following way: $\mathbb{DEF}_{7}(x) = 7^{*} \mod 11 = a;$ (x) provides the following 1-to-1 mapping, displayed in the table below. $\frac{x = 0}{1}$ $\frac{1}{7}$ $\frac{2}{5}$ $\frac{3}{2}$ $\frac{3}{3}$ $\frac{10}{6}$ $\frac{4}{6}$ $\frac{8}{9}$ $\frac{9}{10}$ $\frac{11}{7}$ $\frac{12}{5}$ $\frac{13}{2}$ $\frac{14}{3}$ $\frac{7}{4}$ $\frac{7}{4}$ $\frac{4}{4}$ $\frac{1}{4}$ $\frac{1}{4}$ $\frac{1}{3}$ $\frac{1}{3}$ $\frac{1}{3}$ $\frac{1}{2}$ $\frac{1}{2}$ $\frac{1}{3}$ $\frac{10}{4}$ $\frac{1}{6}$ $\frac{9}{9}$ $\frac{10}{17}$ $\frac{11}{5}$ $\frac{12}{2}$ $\frac{13}{3}$ $\frac{14}{3}$ $\frac{7}{5}$ $\frac{7}{4}$ $\frac{9}{4}$ $\frac{1}{4}$ $\frac{1}{4}$ $\frac{1}{4}$ $\frac{1}{4}$ $\frac{1}{4}$ $\frac{1}{3}$ $\frac{1}{3}$ $\frac{1}{3}$ $\frac{1}{3}$ $\frac{1}{3}$ $\frac{1}{3}$ $\frac{1}{4}$ $\frac{1}{3}$ $\frac{1}$																E	2	-	(	þ	~	1)	) /	2		
p is strong prime $p = 2^{s}q + 1$ , when $q - is prime, then for all g \in I1 mod p; and g^{2} \neq 1 \mod p.p = 2^{s}5 + 1 = stDiscrete Exponent Function (12/14)s above p=11 and is strong prime in \mathbb{Z}_{11}^{*} = \{1, 2, 3,, 10\} and generator we choose g = 7 from the set \Gamma = \{2, 6, 7, 8\}.c Parameters are PP = (11, 7), Then DEF_{\pi}(x) = DEF_{7}(x) is defined in the following way:DEF_{7}(x) = 7^{x} \mod 11 = a;(x) provides the following 1-to-1 mapping, displayed in the table below.\frac{x}{100} = 0 = 1 = 2^{-3} = 3 = 4 = 5 = 6 = 7 = 8 = 9 = 10 = 11 = 12 = 13 = 14 = 7 = 4 = 1 = 14 = 7 = 4 = 1 = 12 = 12 = 12 = 12 = 12 = 12 =$	•			0.14		4						<b>c</b> 1		-		Ý	_		_	- V						
1 mod p; and $g^2 \neq 1 \mod p$ . $p = 2 \cdot 5 + 1 = M$ Discrete Exponent Function (12/14) s above p=11 and is strong prime in $Z_{11}^* = \{1, 2, 3,, 10\}$ and generator we choose $g = 7$ from the set $\Gamma = \{2, 6, 7, 8\}$ . c Parameters are $PP = (11,7)$ , Then $DEF_g(x) = DEF_7(x)$ is defined in the following way: $DEF_7(x) = 7^x \mod 11 = a$ ; (x) provides the following 1-to-1 mapping, displayed in the table below. $\frac{x}{10} = \frac{0}{1} \frac{1}{7} \frac{2}{5} \frac{3}{2} \frac{4}{3} \frac{5}{10} \frac{6}{4} \frac{7}{6} \frac{8}{9} \frac{9}{8} \frac{10}{17} \frac{11}{7} \frac{12}{5} \frac{13}{2} \frac{14}{3} \frac{7 \cdot 7}{4} = \frac{4}{4} \frac{14}{4} \frac{14}{4}$ 10 Mapping for $Q = 4$ 10 To 2 - 3 - 4 - 5 - 6 - 7 - 8 - 9 - 10 - 7 - 5 - 2 - 3 - 5 - 5 - 5 - 5 - 5 - 5 - 5 - 5 - 5	1s strong	, prim	e <b>p</b>	= 2*(	<i>q</i> +	1, W	hen	q - 18	s prii	ne, t	hen t	tor al	I <b>g</b> ∈.	Ľ		q	. 5	- 5	)							
Discrete Exponent Function (12/14) is above $p=11$ and is strong prime in $\mathbb{Z}_{11}^* = \{1, 2, 3,, 10\}$ and generator we choose $g = 7$ from the set $\Gamma = \{2, 6, 7, 8\}$ . is above $p=11$ and is strong prime in $\mathbb{Z}_{11}^* = \{1, 2, 3,, 10\}$ and generator we choose $g = 7$ from the set $\Gamma = \{2, 6, 7, 8\}$ . is above $p=11$ and is strong prime in $\mathbb{Z}_{11}^* = \{1, 2, 3,, 10\}$ and generator we choose $g = 7$ from the set $\Gamma = \{2, 6, 7, 8\}$ . is above $p=11$ and is strong prime in $\mathbb{Z}_{11}^* = \{1, 2, 3,, 10\}$ and generator we choose $g = 7$ from the set $\Gamma = \{2, 6, 7, 8\}$ . is a point $\mathbb{Z}_{11}$ by the point $\mathbb{Z}_{11}$ by the point $\mathbb{Z}_{12}$ by the point $\mathbb{Z}_{11}$ by the point $\mathbb{Z}_{11}$ by the point $\mathbb{Z}_{12}$ b	1 mod <i>p</i> ; a	and <b>g</b>	$^{2}\neq$	1 <b>m</b> o	od <b>p</b>	•										p	-	_	2.	5		+	1	-	- ,	11
Discrete Exponent Function (12/14)         s above $p=11$ and is strong prime in $Z_{11}^{*} = \{1, 2, 3,, 10\}$ and generator we choose $g = 7$ from the set $\Gamma = \{2, 6, 7, 8\}$ .         c Parameters are $PP=(11,7)$ , Then $DEF_{g}(x) = DEF_{7}(x)$ is defined in the following way: $DEF_{7}(x) = 7^{x} \mod 11 = a;$ (x) provides the following 1-to-1 mapping, displayed in the table below. $x$ $0$																t		1	<u> </u>			1	-	-	- 1	1
Discrete Exponent Function (12/14) s above $p=11$ and is strong prime in $\mathbb{Z}_{11}^{*} = \{1, 2, 3,, 10\}$ and generator we choose $g = 7$ from the set $\Gamma = \{2, 6, 7, 8\}$ . c Parameters are $PP = (11, 7)$ , Then $DEF_{g}(x) = DEF_{7}(x)$ is defined in the following way: $DEF_{7}(x) = 7^{x} \mod 11 = a;$ (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  7  2  4  9  141  4  7  7  5  2  3  7  5  2  3  7  5  2  3  7  5  2  3  7  5  2  3  7  5  2  3  7  5  2  3  7  5  2  3  7  5  2  3  7  5  2  3  7  5  2  3  7  5  2  3  7  5  2  3  7  5  2  3  7  5  2  3  7  5  7  8  9  10  11  12  13  14  7  7  7  7  7  7  7  7  7							_		_																	
s above $p = 11$ and is strong prime in $Z_{11}^{*} = \{1, 2, 3,, 10\}$ and generator we choose $g = 7$ from the set $\Gamma = \{2, 6, 7, 8\}$ . c Parameters are $PP = (11,7)$ , Then $DEF_{g}(x) = DEF_{7}(x)$ is defined in the following way: $DEF_{7}(x) = 7^{x} \mod 11 = a;$ (x) provides the following 1-to-1 mapping, displayed in the table below. $\frac{x}{mod} p = a 1 7 (5 2 3 4 5 6 7 8 9 9 10 11 12 13 14 7 5 2 3 9 10 4 6 9 8 1 7 5 5 2 3 9 10 1 7 5 2 3 9 10 1 1 7 5 2 3 9 10 1 1 7 5 2 3 9 10 1 1 7 5 2 3 9 10 1 1 1 7 5 2 3 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1$					Disc	crete	e Exp	oner	nt Fu	nctio	on (1)	2/14)														
$\begin{array}{c c c c c c c c c c c c c c c c c c c $	c Parameters	l and is are <b>P</b>	s stro P=(1	ong pr 1,7), '	ime i Then	in $Z_1$ DEI	$\mathbf{F}_{g}(\mathbf{x})$	1, 2, 3 = <b>DE</b>	5,, F <sub>7</sub> ( <i>x</i> )	10} a	and g	enerat in the	or we follo	choose	e <b>g</b> = 7 vay:	fron	1 th	e se	et I	[=	{2,	6,	7,	8}.		
imod p = a       1       7       5       2       3       10       4       6       9       8       1       7       5       2       3       4 <td< th=""><th>c Parameters <math>f(x)</math> provides</th><th>and is are <b>P</b></th><th>s stro P=(1 llow</th><th>ong pr 1,7), ' ing 1-</th><th>ime i Then to-1</th><th>in Z<sub>1</sub> DEI DEI mapj</th><th><math>1^* = \{</math> <math>F_g(x)</math> <math>F_7(x)</math> ping,</th><th>1, 2, 3 = <b>DE</b> = <b>7<sup>x</sup> 1</b> displa</th><th>,, F<sub>7</sub>(<b>x</b>) <b>nod</b> ayed</th><th>10} a is de 11 = a in the</th><th>and g fined r; table</th><th>in the below</th><th>or we follo<sup>v</sup> v.</th><th>choose</th><th>e <b>g</b> = 7 vay:</th><th>tron</th><th>1 th</th><th>e se</th><th>et I</th><th>[= </th><th>{2,</th><th>6,</th><th>7,</th><th>8}.</th><th></th><th></th></td<>	c Parameters $f(x)$ provides	and is are <b>P</b>	s stro P=(1 llow	ong pr 1,7), ' ing 1-	ime i Then to-1	in Z <sub>1</sub> DEI DEI mapj	$1^* = \{$ $F_g(x)$ $F_7(x)$ ping,	1, 2, 3 = <b>DE</b> = <b>7<sup>x</sup> 1</b> displa	,, F <sub>7</sub> ( <b>x</b> ) <b>nod</b> ayed	10} a is de 11 = a in the	and g fined r; table	in the below	or we follo <sup>v</sup> v.	choose	e <b>g</b> = 7 vay:	tron	1 th	e se	et I	[=	{2,	6,	7,	8}.		
s > 100 MOXYMAS  mm  Mo Molyma, 2022Pw 2024 K Eam F. Volin Jadiorskafats Kamilije Group-Vol-10 Mini-ECDSA-Merke-Antanas SMBOLM - V-2.00 Bitolards. Group KAP170M1002p Bookdasis Course Works-Listdooc CryptoIntElbult_Administravimas.dec DEF v-4.pptx  >> p128sin >> p128def	c Parameters $f(x)$ provides	and is are P	s stro P=(1 llow	ong pr 1,7), ' ing 1-	Then to-1	in Z <sub>1</sub> DEI DEI mapj	$1^* = \{$ $F_g(x)$ $F_7(x)$ ping,	$1, 2, 3$ $= DE$ $= 7^{x} 1$ displa	5,, F <sub>7</sub> ( <b>x</b> ) nod ayed	10} a is de 11 = a in the	fined ; table	in the below	or we follow.	e choose wing w	e <b>g</b> = 7 vay:	fron	n th	e se	et I		{2, 4	6, 9	7,	8}.	(1	
b > 100 MOXMAAS  me  Mo Molymas,2022Pw 2024 k  Eam,E-Voling Jablorskate Kamilijs Group-KAP-10 Mini-ECGS-Metkle-Antanas Mini-LocS-A Metkle-Antanas Bitolande G. Group KAP-10 Bi	c Parameters y(x) provides $\frac{x}{p(x)} = \frac{0}{1}$	and is are P	s stro P=(1 llow	ong pr 1,7), <sup>7</sup> ing 1- 3 2	Then to-1	in Z <sub>1</sub> DEI DEI mapj	$1^* = \{$ $F_g(x)$ $F_7(x)$ ping, 6 0 4	$1, 2, 3$ $= DE$ $= 7^{x} 1$ displa	<b>F</b> <sub>7</sub> ( <b>x</b> ) <b>nod</b> ayed <b>8</b> 9	10} a is de 11 = a in the 9 8	and g fined t; table	enerat in the below $2 \qquad 11 \\ 7 \qquad 7$	or we follow v.	e choose wing w 13 2	e <b>g</b> = 7 vay:	fron	n th	e so	et I		{2, 4	6, 9 4	7,	8}.	1	
Is > 100 MOKYMAS mme  T00 Mokymas_2022Pav 2024 KK Exam_F-VAdng JalonstarkExamJG Group-KAP-10 Mmi-ECGA-Merke-Antanas SMB0LM1 v-4.260 Exam_F-VAdnas Course_Works-Istadoox Course_Works-Istadoox Course_Works-Istadoox Course_Works-Istadoox SMB0LM1 - Sample Sam	c Parameters y(x) provides $\frac{x}{x} = 0$ $x \mod p = a$	and is are P	s stro P=(1 llow 2 5	ong pr 1,7), ' ing 1- 3 2	ime i Then to-1 4 3	in Z <sub>1</sub> DEI DEI mapj 5	$1^* = \{$ $F_g(x)$ $F_7(x)$ ping, 6 0 4	$1, 2, 3$ $= DE$ $= 7^{x} 1$ displate	F <sub>7</sub> (x) nod ayed 8 9	10} a is de 11 = a in the 9 8	and g fined v; table	in the below	or we follow v. 12 5	e choose wing w 13 2	e <b>g</b> = 7 vay:	fron	r th	e so	et I		{2, {4 {2,	6, 94	7,	8}.	11	
Is > 100 MOKYMAS  me	c Parameters x(x) provides x = 0 mod p = a 1	and is are P	s stro P=(1 llow 2 5	ong pr 1,7), <sup>7</sup> ing 1- 3 2	ime i Then to-1 4 3	in Z <sub>1</sub> DEI DEI mapj 5 1	$f_1^* = \{$ $F_g(x)$ $F_7(x)$ ping, 6 0 4	1, 2, 3 = $DE$ = $7^{x} 1$ displa	5,, F <sub>7</sub> ( <b>x</b> ) nod ayed 8 9	10} a is de 11 = a in the 9 8	and g fined t; table 10 1	eneration in the below $11$	or we e follow v. 12 5	e choose wing w 13 2	2 <b>g</b> = 7 7 7 7 8	fron	n th	e so	et I		{2, 4 4	6, 945	7,	8}.	11	
Ine CoSA-May Subset Real Subse	c Parameters y(x) provides $\frac{x}{mod p} = a$ 1	and is are P	s stro P=(1 llow 2 5	ong pr 1,7), ' ing 1- 3 2	Then to-1	in Z <sub>1</sub> DEI DEI mapj 5 1	$f_1^* = \{ F_g(x) \\ F_7(x) \\ ping, \\ 6 \\ 0 \\ 4 \\ 4 \\ 4 \\ 4 \\ 4 \\ 4 \\ 4 \\ 4 \\ 4$	1, 2, 3 = $DE$ = $7^{x}$ 1 displa	5,, F <sub>7</sub> (x) nod ayed 8 9	$10\} a$ is de is de $11 = a$ in the $9$ 8	and g fined t; table 10 1	in the below	or we c follow v. 12 5	e choose wing w 13 2	2 <b>g</b> = 7 7 7 8 7 8 7	fron	1 th		et I ۲		{2, 4	6, 94	7,	8}.	11	
100 Molyma, 2022Av Exam_E-Voling Jablonslate:Kamlija Group-KAP-10 Mini-EOSA-Merkei-Antanas SMBGUAI v-e:Aoc B127 Confid-Verif-Trans 2023-Egratax Balonalte:G. Group KAP P170M100.2p Bookdxiax Course Works List.doc crypto.fmf.ktult_Administravimas.doc DEF v-4.pptx >> p128sin >> p128def	c Parameters f(x) provides x = 0 $f \mod p = a$ 1 $f \mod p = a$	and is are P the fo 1 7	s strc P=(1 Illow 2 (5	ong pr 1,7), ' ing 1- 3 2	Then to-1	in Z <sub>1</sub> DEI DEI mapj 5 1	$f_1^* = \{$ $F_g(x)$ $F_7(x)$ ping, 6 0 4	$1, 2, 3$ $= DE$ $= 7^{x} 1$ displa	5,, F7( <b>x</b> ) nod ayed 8 9	10} a is de 11 = a in the 9 8	and g fined t; table	enerat in the below 7	or we follow v. 12 5	e choose wing w 13 2	14 3	fron	7		7		{2, 4 4	6, 94 5	7,	8}.	11	
Exam E-Voting Jablonskite Kamilij Group-KAP -10 Mini-ECDS-Merkle-Antanas SIMBOLIAI V-42.doc B127 Confid-Verif-Tans 2023-Egz.xlsx Balonate.G. (copus KAP P170M1002)p Bookkxlsx Course, Works-List.doc crypto.mfk.tutt, Administravimas.doc DEF v-4.pptx >> p128sin >> p128def	c Parameters f(x) provides x = 0 $f \mod p = a$ 1 $f \mod p = a$	and is are P the fo 1 7	s strc P=(1 110w 2 5	ong pr 1,7), ' ing 1- 3 2	Then tto-1	in Z <sub>1</sub> DEI DEI mapj 5 1	$f_{g}(x)$ F <sub>g</sub> (x) F <sub>7</sub> (x) ping, 6 0 4	1, 2, 3 = $DE$ = $7^{x} 1$ displa	5,, F7( <b>x</b> ) nod ayed 8 9	10} a is de 11 = a in the 9 8	and g fined table 10 1	eneration in the below $\frac{11}{7}$	or we follow v.	a choose wing w 13 2	2 g = 7 7 7 7 8 7 8 7 7	fron	7 7	e so	7 		{2, 4 4	6, 94 5	7,		11	
Januardiante Antingia Undyr Faxe - 100 Mini-ECDS-Merke-Antana SIMBOLIAI Y-42.doc B127 Confid-Verif-Taria S023-Egz.kix Balonate.G. Group KAP P170M100.2p Bookkatsa Course, Worke-List.docx crypto.mfk.tut, daministravimas.doc DEF v-4.pptx >> p128sin >> p128def	c Parameters x 0 x = 0 x = 0 x = 1 x = 100  MOKYMAS ime 100 MoKymas_2022 Pav 2024 KK	and is are P the fo 1 7	s strc P=(1) 2 5	ong pr 1,7), ' ing 1- 3 2	Then to-1	in Z <sub>1</sub> DEI DEI mapj 5 1	$f_{1}^{*} = \{$ $F_{g}(x)$ $F_{7}(x)$ $f_{7}(x)$ $f_{9}(x)$	$1, 2, 3$ $= DE$ $= 7^{x} 1$ displating of a field of a f	8 (s,, s,, s,	10} a is de 11 = a in the 9 8	and g fined ; table 10 1	enerat in the below 7	or we follow v.	e choose wing w 13 2	2 g = 7 7ay: 14 3	Iron	7		et I ۲		{2,	6, 94 5	7,	8}.	11	
SiMBOLIA v-42.doc         B127 Confid-Verif-Trans 2023-Egz.kisx         Balionate G. Grups KAP P170M1002ip         Bookkxlsx         Course Works-Istdocx         crypto.fmf.ktult_Administravimas.doc         DEF v-4.ptx    >> p128sin >> p128def	c Parameters $r_{1}(x)$ provides x = 0 $r \mod p = a$ 1 ts > 100 MOKYMAS ame 100 Mokymas_2022.Pav 2024 KK Exam_E-Voting Liblorefaille formula	and is are P	2 5	ong pr 1,7), <sup>7</sup> ing 1-	Then to-1	in Z <sub>1</sub> DEJ DEJ mapj 5 1	$f_{g}^{*} = \{$ $F_{g}(x)$ $F_{7}(x)$ $f_{7}(x)$ $f_{7}(x)$	1, 2, 3 = <b>DE</b> = $7^{x}$ <b>i</b> displa	<b>F</b> <sub>7</sub> ( <b>x</b> ) <b>nod</b> <b>8</b> <b>9</b>	10} a is de 11 = a in the 9 8	and g fined ; table 10 1	enerat in the below 7	or we follow v.	a choose wing w 13 2	14 3	Iron	r th		¥.		{2,	6, 945	7,		11	
Ballonates Group KAP P170M100.2jp Bookksise Course, Works-List.docx crypto.fmf.ktult_Administravimas.doc DEF v-4.pptx  >> p128sin >> p128def	c Parameters $T_{x}$ 0 x 0 x mod $p = a$ 1 $T_{x}$ 0 $T_{x}$ 0 T	and is are P the fo 1 7	2 (5 0	ong pr 1,7), ' ing 1- 3 2	tto-1	in Z <sub>1</sub> DEJ DEJ mapj 5	$f_{g}^{*} = \{$ $F_{g}(x)$ $F_{7}(x)$ pping, 6 0 4	1, 2, 3 = $DE$ = $7^{x} 1$ displa	<b>F</b> 7( <b>x</b> ) <b>nod</b> <b>8</b> <b>9</b> <b>9</b>	10} a is de 11 = a in the 9 8	and g fined ; table 10	enerat in the below 7	or we follow v.	a choose wing w 13 2	2 g = 7 7 7 8 9 7 7 8 9		7 7		7		{2, 4	6, 94 5	7,	8}. [	11	
Bookkdsx Course_Works-List.docx crypto.fmf.ktult_Administravimas.doc DEF v-4.pptx >> p128sin >> p128def	c Parameters $T_{x}$ 0 x 0 x mod $p = a$ 1 $T_{x}$ 0 x method to the term of the term of the term of	and is are P the fo the fo 7	P=(1 lllow 5	ong pr 1,7), ' ing 1- 3 2	to-1	in Z <sub>1</sub> DEJ DEJ mapj 5 1	$f_{s}^{*} = \{$ $F_{g}(x)$ $F_{7}(x)$ ping, 6 0 4	1, 2, 3 = <b>DE</b> = $7^{x}$ 1 displa	F7(x) F7(x) nod ayed 9	10} a is de 11 = a in the 9 8	and g fined t; table	enerat in the below 7	or we follow v.	a choose wing w 13 2	14 3	Iron	7 7		₹ Ţ		{2, 4	6, 94 5	7,	8}.	<u>11</u>	
Course Works-Listdox         crypto.fmf.ktult_Administravimas.doc         DEF v-4.pptx         >> p128sin         >> p128def	c Parameters $T_{r}(x)$ provides x = 0 $x \mod p = a$ 10 MOKYMAS ame 100 MOKYMAS 100 MOK	and is are P the fo the fo 1 7	P=(1 lllow 2 5	ong pr 1,7), ' ing 1- 3 2	to-1	in Z <sub>1</sub> DEJ DEJ mapj 5 1	$f_{s}^{*} = \{$ $F_{g}(x)$ $F_{7}(x)$ pping, 60 4	1, 2, 3 = $DE$ = $7^{x} 1$ displa	<b>F</b> <sub>7</sub> ( <b>x</b> ) <b>mod</b> <b>8</b> <b>9</b> <b>9</b>	10} a is de 11 = a in the 9 8	and g fined t; table	enerat in the below 7	or we follow v.	a choose wing w 13 2	2 g = 7 7 7 7 8 7 8 7 7		7 7		et I		{2, 4	6, 94 5	7,	8}.	<u>-1</u>	
<pre>DEF v-4pptx &gt;&gt; p128sin &gt;&gt; p128def</pre>	c Parameters x 0 x 0 x mod $p = a$ 1 ts > 100 MOKYMAS ame 100 Mokymas_2022 Pav 2024 KK Exam_E-Voling Jablonskaite.Kamilija Gr Mini-ECDSA-Merkle-Ar SIMBOLIAI v-42.doc Bi27 Confid-VeriF.Trans Baliûnaite.G. Group KAF Bookkxisx	and is are P the fo the fo roup-KAP -1 ntanas	P=(1 lllow 2 5	ong pr 1,7), ' ing 1- 3 2	ime i Then	in Z <sub>1</sub> DEJ DEJ mapj 5 1	$f^* = \{$ $F_g(x)$ $F_7(x)$ ping, 6 6 0 4	1, 2, 3 = $DE$ = $7^{x} 1$ displa	<b>F</b> <sub>7</sub> ( <b>x</b> ) <b>F</b> <sub>7</sub> ( <b>x</b> ) <b>nod</b> <b>8</b> <b>9</b> <b>9</b>	10} a is de 11 = a in the 9 8	and g fined t; table	enerat in the below 7	or we follow v.	a choose wing w 13 2	2 g = 7 7 7 7 8 7 8 7 7		7 7		et I		{2, 4	6, 945	7,	8}.	11	
>> p128sin >> p128def	c Parameters (x) provides x 0 r mod p = a 1 ts > 100 MOKYMAS ame 100 Mokymas_2022.Pav 2024 KK Exam_E-Voting Jabionskaite.Kamilija Gr Mini-ECDSA-Merkle-AA SIMBOLIAI v-42.doc B127 Confid-Verif-Trans Baliūnaitė.G. Group KAF Bookksias Course_Works-List.docx Course_Works-List.docx	and is are P the fo the fo roup-KAP-1 ntanas is 2023-Egz.x P P170M100 x	P=(1 lllow 2 5	ong pr 1,7), ' ing 1- 3 2	Then to-1	in Z <sub>1</sub> DEI DEI mapj 5 1	$f_{g}^{*} = \{$ $F_{g}(x)$ $F_{7}(x)$ $f_{7}(x)$ $f_{7}(x)$	1, 2, 3 $= DE$ $= 7^{x} 1$ displa $7$ 6	F7(x) F7(x) nod	10} a is de 11 = $a$ in the 9 8	and g fined t; table	enerat in the below 7	or we follow v.	a choose wing w 13 2	2 g = 7 7 7 7 8 7 8 7 7		7 7		et I ۲		{2,	6, 94 5	7,	8}.	<u>-1</u>	
>> p128sin >> p128def	c Parameters (x) provides x 0 r mod p = a 1 ts > 100 MOKYMAS ame 100 AKK ts > 100 AKK ts AKK ame 100 AKK ts AKK ame 100 AKK ts AKK ame 100 AKK ts AKK ame 100 AKK	and is are P the fo the fo 7 roup-KAP -1 ntanas s 2023-Egz.x P P170M100 x	P=(1 lllow 5	ong pr 1,7), ' ing 1- 3 2	tto-1	in Z <sub>1</sub> DEI DEI mapj 5 1	$f_{g}^{*} = \{$ $F_{g}(x)$ $F_{7}(x)$ $f_{7}(x)$ $f_{7}(x)$	1, 2, 3 = DE = $7^{x}$ 1 displa 6	<b>F</b> 7( <b>x</b> ) <b>F</b> 7( <b>x</b> ) <b>nod</b> <b>a</b> yed <b>8</b> <b>9</b>	10} a is de 11 = a in the 9 8	and g fined table	enerat in the below 7	or we follow v.	a choose wing w 13 2	2 g = 7 7 7 7 8 7 8 7 7		7 7		et I		{2,	6, 94 5	7,	8}.	-1	
	c Parameters x 0 f mod $p = a$ 1 f mod $p = a$ 1 ts > 100 MOKYMAS ime 100 M	and is are P a the fo a the fo a the fo a a the fo a a the fo a a the fo a the followed a the follo	P=(1 lllow 5	ong pr 1,7), <sup>7</sup> ing 1-	tto-1	in Z <sub>1</sub> DEJ DEJ mapj 5	$f_{g}^{*} = \{$ $F_{g}(x)$ $F_{7}(x)$ ping, 6 0 4	1, 2, 3 $= DE$ $= 7^{x} 1$ displa $7$ 6	<b>F</b> <sub>7</sub> ( <b>x</b> ) <b>nod</b> <b>8</b> <b>9</b> <b>9</b>	10} a is de 11 = a in the 9 8	and g fined table	enerat in the below 7	or we follow v.	a choose wing w 13 2	2 g = 7 7 7 8 9 7 7 7 8 9		7 7		et I			6, 94 5	7,	8}.	11	
	c Parameters x = 0 f mod $p = a$ 1 f mod $p = a$ 1 ts > 100 MOKYMAS ts > 100 MOKYMAS ts > 100 MOKYMAS ts > 100 MOKYMAS to the transformation of transformation	and is are P the fo the fo 1 7 inoup-KAP -1 ntanas s 2023-Egz.x P P170M100 x iistravimas.de	P=(1 lllow 5	ong pr 1,7), ' ing 1- 3 2	to-1	in Z <sub>1</sub> DEJ DEJ mapj 5 1	$f_{g}^{*} = \{$ $F_{g}(x)$ $F_{7}(x)$ ping, 6 0 4	1, 2, 3 = $\mathbf{DE}$ = $7^{x} 1$ displa	F7(x) F7(x) nod ayed 8 9	10} a is de 11 = $a$ in the 9 8	and g fined table	enerat in the below 7	or we follow v.	28dof	14 3		7 7		et I			6, 945	7,	8}.	<u>11</u>	
	c Parameters x 0 f mod $p = a$ 1 f mod $p = a$ 1 ts > 100 MOKYMAS ts = 100 M	and is are P the fo the fo 1 7 roup-KAP -1 ntanas s 2023-Egz.x p P170M100 x sistravimas.du	P=(1 lllow 2 5	ong pr 1,7), ' ing 1- 3 2	ime i Then to-1	in Z <sub>1</sub> DEJ DEJ mapj 5 1	$f_{s}^{*} = \{$ $F_{g}(x)$ $F_{7}(x)$ pping, 60 4	1, 2, 3 = <b>DE</b> = 7 <sup>x</sup> 1 displa	<b>F</b> 7( <b>x</b> ) <b>nod</b> <b>8</b> <b>9</b> <b>9</b>	10} a is de 11 = $a$ in the 9 8	and g fined table	enerat in the below 7	or we follow v. 12 5 >> p12	28def	2 g = 7 7 7 7 7 7 7 7 7		7 7		et I			6, 94 5	7,	8}.	11	
	c Parameters (x) provides x 0 x mod p = a 1 x mod p =	and is are P the fo the fo 1 7 roup-KAP -1 ntanas s 2023-Egz.x P P170M100 x sistravimas.du	P=(1 lllow 2 5	ong pr 1,7), ' ing 1- 3 2	ime i Then to-1	in Z <sub>1</sub> DEJ DEJ mapj 5 1	$f_{g}^{*} = \{$ $F_{g}(x)$ $F_{7}(x)$ pping, 60 4	1, 2, 3 = <b>DE</b> = 7 <sup>x</sup> 1 displa	<b>F</b> 7( <b>x</b> ) <b>F</b> 7( <b>x</b> ) <b>nod</b> <b>8</b> <b>9</b> <b>9</b>	10} a is de 11 = a in the 9 8	and g fined t; table	enerat in the below 7	or we follor v. 12 5 	28def	2 g = 7 7ay: 14 3		7 7		et I		{2,	6, 945	7,		<u>-1</u>	
	c Parameters (x) provides x 0 x mod p = a 1 x mod p = a 1 x mod p = a 1 00 Mokymas_2022.Pav 2024 KK Exam_E-Voting Jabionskaite.Kamilija Gr Mini-ECDSA-Merkle-Ar SIMBOLIAV-42.doc B127 Confid-Verif-Trans Baliūnaitė.G. Group KAF Bookkstax Course_Works-List.docx Course_Works-List.docx Course_Works-List.docx SP128Si	and is are P the fo the fo 7 roup-KAP -1 ntanas s 2023-Egz.x p P170M100 x iin	P=(1 lllow 5	ong pr 1,7), ' ing 1- 3 2	ime i Then to-1	in Z <sub>1</sub> DEI DEI mapj 5 1	$f_{g}^{*} = \{$ $F_{g}(x)$ $F_{7}(x)$ $f_{7}(x)$	1, 2, 3 = $DE$ = $7^{x} I$ displa 7 6	<b>F</b> 7( <b>x</b> ) <b>F</b> 7( <b>x</b> ) <b>nod</b> <b>8</b> <b>9</b> <b>9</b>	10} a is de 11 = a in the 9 8	and g fined t; table	enerat in the below 7	or we e follor v. // 5 // 5 // 5 // 5 // 5 // 5 // 5 //	e choose wing w 13 2 2 28def	2 g = 7 7ay: 14 3		7 7		et I ۲		{2,	6, 94 5	7,		-1	
	c Parameters (x) provides x 0 x mod p = a 1 x mod p =	and is are P the fo the fo 1 7 v v v v v v v v v v v v v v v v v v	P=(1 lllow 2 5	ong pr 1,7), <sup>7</sup> ing 1-	tto-1	in Z <sub>1</sub> DEJ DEJ 1	$f_{g}^{*} = \{$ $F_{g}(x)$ $F_{7}(x)$ $f_{7}(x)$	1, 2, 3 $= DE$ $= 7^{x} 1$ displa $7$ 6	<b>F</b> 7( <b>x</b> ) <b>nod</b> <b>ayed</b> <b>8</b> <b>9</b>	10} a is de 11 = a in the 9 8	and g fined table	enerat in the below 2 11 7	or we e follor v. 5 >> p12	28def	2 g = 7 7ay: 14 3		7 7		₹		{2, 4	6, 945	7,	8}.	<u>11</u>	
	c Parameters x = 0 x = 0	and is are P a the fo a the followed a the	P=(1 lllow 2 5	ong pr 1,7), <sup>7</sup> ing 1-	to-1	in Z <sub>1</sub> DEJ DEJ 1	$f_{g}^{*} = \{$ $F_{g}(x)$ $F_{7}(x)$ ping, 6 0 4	1, 2, 3 = <b>DE</b> = 7 <sup>x</sup> 1 displa	<b>F</b> 7( <b>x</b> ) <b>nod</b> <b>8</b> <b>9</b> <b>9</b>	10} a is de 11 = a in the 9 8	and g fined table	enerat in the below 2 11 7	or we follow v. >> p12	28def	2 g = 7 7ay:		7 7		2 .		{2, 4	6, 94 5	7,	8}.	11	
	c Parameters x 0 x 0 x mod $p = a$ 1 x mod p = a 1 x me 0 x me 0 x me 0 x me 0 x me 0 x me 0 x me 10 x me 0 x me 0 x me 0 x me 0 x me 0 x mod p = a 1 x me 0 x me	and is are P the fo the fo 1 7 v v roup-KAP -1 ntanas is 2023-Egz.x p P170M100 x istravimas.de	P=(1 lllow 5	ong pr 1,7), <sup>7</sup> ing 1-	ime i Then to-1	in Z <sub>1</sub> DEJ DEJ 1	$f_{g}^{*} = \{$ $F_{g}(x)$ $F_{7}(x)$ ping, 6 0 4	1, 2, 3 = <b>DE</b> = 7 <sup>x</sup> 1 displa	F7(x) F7(x) nod 1 ayed 1 8 9	10} a is de 11 = $a$ in the 9 8	and g fined timed table	enerat in the below 7	or we follow v.	28def	14 3		7 7		2 .		{2, 4	6, 94 5	7,	8}.	11	
	c Parameters $r_{x}$ 0 r mod $p = a$ 1 r mod p = a 1 r m mod p = a 1 r mod p = a 1 r m mod p = a	and is are P the fo the fo 1 7 inup-KAP -1 ntanas s 2023-Egzx p P170M100 x iin	s strc P=(1 lllow 2 5	ong pr 1,7), ' ing 1-	ime i Then to-1	in Z <sub>1</sub> DEJ mapj 5 1	$f_{g}^{*} = \{$ $F_{g}(x)$ $F_{7}(x)$ ping, 6 0 4	1, 2, 3 = <b>DE</b> = 7 <sup>x</sup> 1 displa	<b>F</b> 7( <b>x</b> ) <b>F</b> 7( <b>x</b> ) <b>nod</b> <b>8</b> <b>9</b> <b>9</b>	10} a is de 11 = $a$ in the 9 8	and g fined t; table	enerat in the below 7	or we follow v.	28def	2 g = 7 7ay:		7 7		2 .		{2, 4 (	6, 945	7,	8}.	<u>11</u>	
	c Parameters (x) provides x 0 r mod p = a 1 rs > 100 MOKYMAS rme 100 Mokymas_2022.Pav 2024 KK Exam_E-Voting Jablonskaite.Kamilija Gr Mini-ECDSA-Merkle-An SIMBOLIAI v-42.doc Bli27 Confid-Verif-Trans Baliūnaitė.G. Group KAF Bookkslas Course_Works-List.docx crypto.fmf.kut_Admini DEF v-4.pptx >> p128si	and is are P the fo the fo 1 7 roup-KAP -1 ntanas is 2023-Egz.x s 2023-Egz.x istravimas.do	P=(1 lllow 2 5	ong pr 1,7), ' ing 1- 3 2	ime i Then to-1	in Z <sub>1</sub> DEJ mapj 5 1	$f_{g}^{*} = \{$ $F_{g}(x)$ $F_{7}(x)$ ping, 6 6 0 4 	1, 2, 3 = <b>DE</b> = 7 <sup>x</sup> 1 displa	<b>F</b> 7( <b>x</b> ) <b>nod</b> <b>8</b> <b>9</b> <b>9</b>	10} a is de 11 = a in the 9 8	and g fined t; table	enerat in the below 7	or we follow v.	28def	2 g = 7 7ay:		7		¢.		{2,	6, 94 5	7,	8}.	<u>- 1</u>	

120 100 0.5 80 0 60 40 -0.5 20 -1 0 20 40 60 80 100 120 10 20 30 40 50 Private and Public Keys generation: PrK=X; PuK=a; 1) Genorate strong prime number P. >> p = genstrongprime (28) % genorates 28 bit lenghts of p 2) Find a generator g in the set Ip = f 1, 2, 3, ---, p-1] >> q = (p-1)/2>> q=2 >> mod\_exp(g, q, p) % I-st condition % If it is equal to 1 - anoose the other q % If no, then vority: >> mod\_exp (g, g, p) % II-nd condition % If it is equal to 1 - choose the other g. 3) Generate PrK=x using random number generator function randi  $\gg x = int 64 (ranoli(2<sup>28</sup>-1))$ >> x=randi(2^28-1) x = 1.9906e+08 4) compute Puk=a using DEF, i.e. function >> x=int64(randi(2^28-1)) x = 256210849 >> a = mod\_exp(g,x,p) Plaintext Ciphertex Plaintext **Encrypt Communication** Decrypt Channel Same key is used to encrypt and decrypt message Shared Secret Key

Diffie-Hellman Key Agreement Protocol (DH KAP) Public Parameters **PP**=(*p*,*g*)  $w = rand(Z_{p}^{*})$   $g^{u} \mod p = t_{A}$   $t_{B} = (t_{B})^{u} \mod p = t_{A}$   $k_{AB} = (t_{B})^{u} \mod p = g^{vu} \mod p$   $= (g^{v})^{u} \mod p = g^{vu} \mod p$   $k_{AB} = k = k_{BA}$   $v = rand(Z_{p}^{*})$   $t_{B} = g^{v} \mod p$   $= (g^{u})^{v} \mod p = g^{uv} \mod p$