



<https://youtu.be/VNkmpuL7Ycc>

## EC-Diffie-Hellman Schlüsselaustausch<sup>a</sup>

Name: ..... Vorname: .....

Klasse: .....

Partner/in: Name: ..... Klasse: .....

Generatorpunkt:<sup>b</sup> Punkt Nr. ..... Dossier Nr. .....

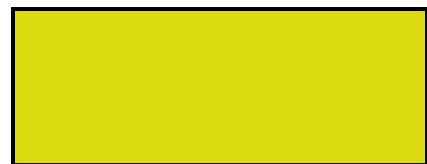
Gewählter Generatorpunkt:<sup>c</sup> Punkt Nr. .... Punkt: .....

Mein privater Schlüssel (Faktor):<sup>d</sup> .....

Mein öffentlicher Schlüssel (Punkt): ..... (an Partner)

Öffentlicher Schlüssel des Partners (Punkt): .....

Gemeinsamer geheimer Schlüssel:



Ist der geheime gemeinsame Schlüssel des Partners identisch mit deinem? .....

<sup>a</sup> Schriftliche Unterlagen auf <https://www.mathepauker.com/MustereX/Benedict/Projektarbeiten/EC-Diffie-Hellman.pdf>

<sup>b</sup> Für die verwendete diskrete elliptische Kurve gilt  $a = 2$ ,  $b = 132$  und  $p = 137$ .

<sup>c</sup> Beide Partner müssen mit demselben G-Punkt rechnen. Von beiden wird entweder "dein" G-Punkt oder derjenige des Partners verwendet. Der andere G-Punkt wird ignoriert.

<sup>d</sup> Eine Zahl zwischen 100 und 500. Als Online-EC-Rechner verwende z.B. <http://www.christelbach.com/ECCalculator.aspx>

Diskrete elliptische Kurve $y^2 = x^3 + 2x + 132 \pmod{137}$											
1.	$\begin{pmatrix} 1 \\ 51 \end{pmatrix}$	28.	$\begin{pmatrix} 23 \\ 120 \end{pmatrix}$	55.	$\begin{pmatrix} 50 \\ 39 \end{pmatrix}$	82.	$\begin{pmatrix} 73 \\ 107 \end{pmatrix}$	109.	$\begin{pmatrix} 93 \\ 38 \end{pmatrix}$	136.	$\begin{pmatrix} 116 \\ 75 \end{pmatrix}$
2.	$\begin{pmatrix} 1 \\ 86 \end{pmatrix}$	29.	$\begin{pmatrix} 24 \\ 21 \end{pmatrix}$	56.	$\begin{pmatrix} 50 \\ 98 \end{pmatrix}$	83.	$\begin{pmatrix} 74 \\ 11 \end{pmatrix}$	110.	$\begin{pmatrix} 93 \\ 99 \end{pmatrix}$	137.	$\begin{pmatrix} 117 \\ 60 \end{pmatrix}$
3.	$\begin{pmatrix} 2 \\ 12 \end{pmatrix}$	30.	$\begin{pmatrix} 24 \\ 116 \end{pmatrix}$	57.	$\begin{pmatrix} 52 \\ 62 \end{pmatrix}$	84.	$\begin{pmatrix} 74 \\ 126 \end{pmatrix}$	111.	$\begin{pmatrix} 94 \\ 37 \end{pmatrix}$	138.	$\begin{pmatrix} 117 \\ 77 \end{pmatrix}$
4.	$\begin{pmatrix} 2 \\ 125 \end{pmatrix}$	31.	$\begin{pmatrix} 26 \\ 19 \end{pmatrix}$	58.	$\begin{pmatrix} 52 \\ 75 \end{pmatrix}$	85.	$\begin{pmatrix} 75 \\ 34 \end{pmatrix}$	112.	$\begin{pmatrix} 94 \\ 100 \end{pmatrix}$	139.	$\begin{pmatrix} 119 \\ 44 \end{pmatrix}$
5.	$\begin{pmatrix} 3 \\ 24 \end{pmatrix}$	32.	$\begin{pmatrix} 26 \\ 118 \end{pmatrix}$	59.	$\begin{pmatrix} 53 \\ 14 \end{pmatrix}$	86.	$\begin{pmatrix} 75 \\ 103 \end{pmatrix}$	113.	$\begin{pmatrix} 95 \\ 25 \end{pmatrix}$	140.	$\begin{pmatrix} 119 \\ 93 \end{pmatrix}$
6.	$\begin{pmatrix} 3 \\ 113 \end{pmatrix}$	33.	$\begin{pmatrix} 27 \\ 2 \end{pmatrix}$	60.	$\begin{pmatrix} 53 \\ 123 \end{pmatrix}$	87.	$\begin{pmatrix} 76 \\ 60 \end{pmatrix}$	114.	$\begin{pmatrix} 95 \\ 112 \end{pmatrix}$	141.	$\begin{pmatrix} 122 \\ 17 \end{pmatrix}$
7.	$\begin{pmatrix} 5 \\ 33 \end{pmatrix}$	34.	$\begin{pmatrix} 27 \\ 135 \end{pmatrix}$	61.	$\begin{pmatrix} 54 \\ 47 \end{pmatrix}$	88.	$\begin{pmatrix} 76 \\ 77 \end{pmatrix}$	115.	$\begin{pmatrix} 98 \\ 59 \end{pmatrix}$	142.	$\begin{pmatrix} 122 \\ 120 \end{pmatrix}$
8.	$\begin{pmatrix} 5 \\ 104 \end{pmatrix}$	35.	$\begin{pmatrix} 29 \\ 59 \end{pmatrix}$	62.	$\begin{pmatrix} 54 \\ 90 \end{pmatrix}$	89.	$\begin{pmatrix} 77 \\ 46 \end{pmatrix}$	116.	$\begin{pmatrix} 98 \\ 78 \end{pmatrix}$	143.	$\begin{pmatrix} 123 \\ 10 \end{pmatrix}$
9.	$\begin{pmatrix} 7 \\ 30 \end{pmatrix}$	36.	$\begin{pmatrix} 29 \\ 78 \end{pmatrix}$	63.	$\begin{pmatrix} 55 \\ 5 \end{pmatrix}$	90.	$\begin{pmatrix} 77 \\ 91 \end{pmatrix}$	117.	$\begin{pmatrix} 99 \\ 11 \end{pmatrix}$	144.	$\begin{pmatrix} 123 \\ 127 \end{pmatrix}$
10.	$\begin{pmatrix} 7 \\ 107 \end{pmatrix}$	37.	$\begin{pmatrix} 31 \\ 16 \end{pmatrix}$	64.	$\begin{pmatrix} 55 \\ 132 \end{pmatrix}$	91.	$\begin{pmatrix} 78 \\ 51 \end{pmatrix}$	118.	$\begin{pmatrix} 99 \\ 126 \end{pmatrix}$	145.	$\begin{pmatrix} 124 \\ 52 \end{pmatrix}$
11.	$\begin{pmatrix} 8 \\ 48 \end{pmatrix}$	38.	$\begin{pmatrix} 31 \\ 121 \end{pmatrix}$	65.	$\begin{pmatrix} 57 \\ 30 \end{pmatrix}$	92.	$\begin{pmatrix} 78 \\ 86 \end{pmatrix}$	119.	$\begin{pmatrix} 101 \\ 11 \end{pmatrix}$	146.	$\begin{pmatrix} 124 \\ 85 \end{pmatrix}$
12.	$\begin{pmatrix} 8 \\ 89 \end{pmatrix}$	39.	$\begin{pmatrix} 35 \\ 14 \end{pmatrix}$	66.	$\begin{pmatrix} 57 \\ 107 \end{pmatrix}$	93.	$\begin{pmatrix} 79 \\ 35 \end{pmatrix}$	120.	$\begin{pmatrix} 101 \\ 126 \end{pmatrix}$	147.	$\begin{pmatrix} 129 \\ 17 \end{pmatrix}$
13.	$\begin{pmatrix} 10 \\ 59 \end{pmatrix}$	40.	$\begin{pmatrix} 35 \\ 123 \end{pmatrix}$	67.	$\begin{pmatrix} 58 \\ 51 \end{pmatrix}$	94.	$\begin{pmatrix} 79 \\ 102 \end{pmatrix}$	121. <sup>a</sup>	$\begin{pmatrix} 102 \\ 43 \end{pmatrix}$	148.	$\begin{pmatrix} 129 \\ 120 \end{pmatrix}$
14.	$\begin{pmatrix} 10 \\ 78 \end{pmatrix}$	41.	$\begin{pmatrix} 37 \\ 13 \end{pmatrix}$	68.	$\begin{pmatrix} 58 \\ 86 \end{pmatrix}$	95.	$\begin{pmatrix} 80 \\ 7 \end{pmatrix}$	122. <sup>a</sup>	$\begin{pmatrix} 102 \\ 94 \end{pmatrix}$	149.	$\begin{pmatrix} 130 \\ 7 \end{pmatrix}$
15.	$\begin{pmatrix} 11 \\ 65 \end{pmatrix}$	42.	$\begin{pmatrix} 37 \\ 124 \end{pmatrix}$	69.	$\begin{pmatrix} 59 \\ 35 \end{pmatrix}$	96.	$\begin{pmatrix} 80 \\ 130 \end{pmatrix}$	123.	$\begin{pmatrix} 106 \\ 62 \end{pmatrix}$	150.	$\begin{pmatrix} 130 \\ 130 \end{pmatrix}$
16.	$\begin{pmatrix} 11 \\ 72 \end{pmatrix}$	43.	$\begin{pmatrix} 41 \\ 19 \end{pmatrix}$	70.	$\begin{pmatrix} 59 \\ 102 \end{pmatrix}$	97.	$\begin{pmatrix} 81 \\ 60 \end{pmatrix}$	124.	$\begin{pmatrix} 106 \\ 75 \end{pmatrix}$	151.	$\begin{pmatrix} 133 \\ 34 \end{pmatrix}$
17.	$\begin{pmatrix} 12 \\ 68 \end{pmatrix}$	44.	$\begin{pmatrix} 41 \\ 118 \end{pmatrix}$	71.	$\begin{pmatrix} 64 \\ 7 \end{pmatrix}$	98.	$\begin{pmatrix} 81 \\ 77 \end{pmatrix}$	125.	$\begin{pmatrix} 107 \\ 46 \end{pmatrix}$	152.	$\begin{pmatrix} 133 \\ 103 \end{pmatrix}$
18.	$\begin{pmatrix} 12 \\ 69 \end{pmatrix}$	45.	$\begin{pmatrix} 42 \\ 18 \end{pmatrix}$	72.	$\begin{pmatrix} 64 \\ 130 \end{pmatrix}$	99.	$\begin{pmatrix} 84 \\ 43 \end{pmatrix}$	126.	$\begin{pmatrix} 107 \\ 91 \end{pmatrix}$	153.	$\begin{pmatrix} 134 \\ 28 \end{pmatrix}$
19.	$\begin{pmatrix} 15 \\ 48 \end{pmatrix}$	46.	$\begin{pmatrix} 42 \\ 119 \end{pmatrix}$	73.	$\begin{pmatrix} 65 \\ 32 \end{pmatrix}$	100.	$\begin{pmatrix} 84 \\ 94 \end{pmatrix}$	127.	$\begin{pmatrix} 109 \\ 27 \end{pmatrix}$	154.	$\begin{pmatrix} 134 \\ 109 \end{pmatrix}$
20.	$\begin{pmatrix} 15 \\ 89 \end{pmatrix}$	47.	$\begin{pmatrix} 43 \\ 26 \end{pmatrix}$	74.	$\begin{pmatrix} 65 \\ 105 \end{pmatrix}$	101.	$\begin{pmatrix} 85 \\ 16 \end{pmatrix}$	128.	$\begin{pmatrix} 109 \\ 110 \end{pmatrix}$	155.	$\begin{pmatrix} 135 \\ 42 \end{pmatrix}$
21.	$\begin{pmatrix} 18 \\ 66 \end{pmatrix}$	48.	$\begin{pmatrix} 43 \\ 111 \end{pmatrix}$	75.	$\begin{pmatrix} 66 \\ 34 \end{pmatrix}$	102.	$\begin{pmatrix} 85 \\ 121 \end{pmatrix}$	129.	$\begin{pmatrix} 110 \\ 64 \end{pmatrix}$	156.	$\begin{pmatrix} 135 \\ 95 \end{pmatrix}$
22.	$\begin{pmatrix} 18 \\ 71 \end{pmatrix}$	49.	$\begin{pmatrix} 45 \\ 67 \end{pmatrix}$	76.	$\begin{pmatrix} 66 \\ 103 \end{pmatrix}$	103.	$\begin{pmatrix} 88 \\ 43 \end{pmatrix}$	130.	$\begin{pmatrix} 110 \\ 73 \end{pmatrix}$	157.	$\begin{pmatrix} 136 \\ 35 \end{pmatrix}$
23.	$\begin{pmatrix} 21 \\ 16 \end{pmatrix}$	50.	$\begin{pmatrix} 45 \\ 70 \end{pmatrix}$	77.	$\begin{pmatrix} 68 \\ 55 \end{pmatrix}$	104.	$\begin{pmatrix} 88 \\ 94 \end{pmatrix}$	131.	$\begin{pmatrix} 114 \\ 48 \end{pmatrix}$	158.	$\begin{pmatrix} 136 \\ 102 \end{pmatrix}$
24.	$\begin{pmatrix} 21 \\ 121 \end{pmatrix}$	51.	$\begin{pmatrix} 46 \\ 4 \end{pmatrix}$	78.	$\begin{pmatrix} 68 \\ 82 \end{pmatrix}$	105.	$\begin{pmatrix} 90 \\ 46 \end{pmatrix}$	132.	$\begin{pmatrix} 114 \\ 89 \end{pmatrix}$		
25.	$\begin{pmatrix} 22 \\ 1 \end{pmatrix}$	52.	$\begin{pmatrix} 46 \\ 133 \end{pmatrix}$	79.	$\begin{pmatrix} 70 \\ 19 \end{pmatrix}$	106.	$\begin{pmatrix} 90 \\ 91 \end{pmatrix}$	133.	$\begin{pmatrix} 115 \\ 20 \end{pmatrix}$		
26.	$\begin{pmatrix} 22 \\ 136 \end{pmatrix}$	53.	$\begin{pmatrix} 49 \\ 14 \end{pmatrix}$	80.	$\begin{pmatrix} 70 \\ 118 \end{pmatrix}$	107.	$\begin{pmatrix} 92 \\ 61 \end{pmatrix}$	134.	$\begin{pmatrix} 115 \\ 117 \end{pmatrix}$		
27.	$\begin{pmatrix} 23 \\ 17 \end{pmatrix}$	54.	$\begin{pmatrix} 49 \\ 123 \end{pmatrix}$	81.	$\begin{pmatrix} 73 \\ 30 \end{pmatrix}$	108.	$\begin{pmatrix} 92 \\ 76 \end{pmatrix}$	135.	$\begin{pmatrix} 116 \\ 62 \end{pmatrix}$		

<sup>a</sup> Wendepunkte