EC-Diffie-Hellman Schlüsselaustausch[a]

https://youtu.be/VNkmpuL7Ycc

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

Klasse: .....

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

Generatorpunkt:[b] Punkt Nr. ..... Dossier Nr. .....

Gewählter Generatorpunkt:[c] Punkt Nr. ..... Punkt: .....

Mein privater Schlüssel (Faktor):[d] .....

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

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

Gemeinsamer geheimer Schlüssel:

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

---

[a] Schriftliche Unterlagen auf https://www.mathepauker.com/Musterex/Benedict/Projektarbeiten/EC-Diffie-Hellman.pdf

[b] Für die verwendete diskrete elliptische Kurve gilt a = 2, b = 132 und p = 137.

[c] 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.

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

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

[a] Wendepunkte