Variante: Lauschangriff

	Integer
	Bitfolge
	Photonen
	Polscha
	unscharfe Photonen
	ASCII-Text
	Verschlüsselter Text
	Kommentar Alice
	Kommentar Eve
	Kommentar Bob

	Operator 1	Operator 2	Handlungschritt	Ergebnis		H	I	J	K
Beginn Phase 0			Text erzeugen	Str1 = "Hello World!"	Nachricht Alice-Bob [Alice]	A	1	Alice gibt einen zu verschlüsselnden Text Str1 ein	Beginn Phase 0
			Zahl erzeugen	Int1 = 32	Schlüssellänge Alice-Bob [Alice]	A	2	Alice berechnet die Schlüssellänge Int1 basierend auf der Nachricht	
		Int1 = 32	Nachricht über Bitübertragungskanal senden			A	3	Alice sendet die Schlüssellänge Int1 über den Bit-Kanal	
			Zug beenden			A	4	Alice beendet ihren Zug	
			Nachricht auf Bitübertragungskanal abhören	Int1 = 32	Schlüssellänge Alice-Bob [Alice]	E	5	Eve speichert sich die Schlüssellänge Int1	
			Zug beenden			E	6	Eve beendet ihren Zug	
			Nachricht auf Bitübertragungskanal empfangen	Int1 = 32	Schlüssellänge Alice-Bob [Alice]	B	7	Bob empfängt die Schlüssellänge Int1	
			Zug beenden			B	8	Bob beendet seinen Zug	
Ende Phase 0			Zug beenden			E	9	Eve ist dran, kann aber eigentlich nichts tun und beendet ihren Zug	Ende Phase 0
Beginn Phase 1		Int1 = 32	Bitfolge erzeugen	Bit1 = 0100 1111 1000 0101 1011 1101 0001 0001	Schlüsselbits Alice-Bob [Alice]	A	10	Alice erzeugt zufällige Schlüsselbits Bit1 entsprechend der Länge Int1	Beginn Phase 1
		Int1 = 32	Polschata erzeugen	Pol1 = xx+x +++x xxx+ ++xx x+xx x+++ ++x+ ++++	Polschata Alice-Bob [Alice]	A	11	Alice erzeugt die gleiche Anzahl zufälliger Polschata Pol1	
	Bit1 = 0100 1111 1000 0101 1011 1101 0001 0001	Pol1 = xx+x +++x xxx+ ++xx x+xx x+++ ++x+ ++++	Photonen erzeugen	Pho1 = /\\ -|| --|\\ --|\\//|-/-|\\// |--|\	Photonen Alice-Eve [Alice]	A	12	Alice erzeugt aus den Schlüsselbits Bit1 und Polschata Pol1 die Photonen Pho1	
		Pho1 = /\\ -|| --|\\ --|\\//|-/-|\\// |--|\	Nachricht auf Photonübertragungskanal senden			A	13	Alice überträgt die Photonen Pho1 über den Photonenübertragungskanal	
			Zug beenden			A	14	Alice beendet ihren Zug	
		Int1 = 32	Polschata erzeugen	Pol2 = xxx+ x+x+ x+xx +xx+ +x+ x+xx +x+ x+x	Polschata Eve [Eve]	E	15	Eve erzeugt ihre eigenen Polschata Pol2 anhand der Schlüssellänge Int1	
			-	VPh1 = **********	unscharfe Photonen Alice-Eve	-	16	Auf dem Photonenübertragungskanal befinden sich die Photonen VPh1 unbekannter Polarisation (Für Eve)	
	Pol2 = xxx+ x+x+ x+xx +xx+ +x+ x+xx +x+ x+x	VPh1 = **********	Nachricht auf Photonenübertragungskanal empfangen	Pho2 = /| //|--//|||\\//|\--||\\//|// -/-|\\	Photonen Eve-Bob [Eve]	E	17	Eve liest mithilfe ihrer Polschata Pol2 die unscharfen Photonen VPh1 aus und erhält die Photonen Pho2 (Die Polarisierung einiger Photonen wurde geändert)	
		Pho2 = /| //|--//|||\\//|\--||\\//|// -/-|\\	Photonen zu Bitfolge konvertieren	Bit2 = 1010 0101 0011 0110 1100 1101 0101 1001	Schlüsselbits Alice-Bob [Eve]	E	18	Kombinieren der Photonen Pho2 und Polschata Pol2 ergibt einen Bitstrom Bit2	
		Pho2 = /| //|--//|||\\//|\--||\\//|// -/-|\\	Nachricht auf Photonübertragungskanal senden			E	19	Eve überträgt die Photonen Pho2 über den Photonenübertragungskanal zu Bob	
			Zug beenden			E	20	Eve beendet ihren Zug	
		Int1 = 32	Polschata erzeugen	Pol3 = x+x+ +x+x +++x +x+x +xx+ x+x+ +++x+ x+xx	Polschata Eve-Bob [Bob]	B	21	Bob erzeugt seine eigene Polschata Pol3 anhand der Schlüssellänge Int1	
			-	VPh2 = **********	unscharfe Photonen Eve-Bob	-	22	Auf dem Photonenübertragungskanal befinden sich die Photonen VPh2 unbekannter Polarisation (Für Bob)	
	Pol3 = x+x+ +x+x +++x +x+x +xx+ x+x+ +++x+ x+xx	VPh2 = **********	Nachricht auf Photonübertragungskanal empfangen	Pho3 = /| |--//\//|||/|\\|--||--/|/-||\\|-|	Photonen Eve-Bob [Bob]	B	23	Bob liest mithilfe seiner Polschata Pol3 die unscharfen Photonen VPh2 aus	
		Pho3 = /| |--//\//|||/|\\|--||--/|/-||\\|-|	Photonen zu Bitfolge konvertieren	Bit3 = 0110 1110 1010 1011 0010 1010 1001 0100	Schlüsselbits Alice-Bob [Bob]	B	24	Kombinieren der Photonen Pho3 und Polschata Pol3 ergibt einen Bitstrom Bit3	
Ende Phase 1			Zug beenden			B	25	Bob bestätigt erhalt der Nachricht durch Beenden seines Zuges	Ende Phase 1
Beginn Phase 2		Pol1 = xx+x +++x xxx+ ++xx x+xx x+++ ++x+ ++++	Nachricht auf Bitübertragungskanal senden			A	26	Alice gibt über den Bitübertragungskanal ihre Polschata Pol1 preis	Beginn Phase 2
			Zug beenden			A	27	Alice beendet ihren Zug	
			Nachricht auf Bitübertragungskanal abhören	Pol1 = xx+x +++x xxx+ ++xx x+xx x+++ ++x+ ++++	Polschata Alice-Bob [Alice]	E	28	Eve empfängt Alices Polschata Pol1	
	Pol2 = xxx+ x+x+ x+xx +xx+ +x+ x+xx +x+ x+x	Pol1 = xx+x +++x xxx+ ++xx x+xx x+++ ++x+ ++++	Vergleich Polschata (XOR)	Bit4 = 0011 1011 0101 0101 1001 0001 0110 1001	Bitmaske Alice-Eve [Eve]	E	29	Es entsteht eine Bitmaske Bit4, bei welcher "0" für gleich und "1" für ungleich steht	
			Zug beenden			E	30	Eve beendet ihren Zug	
			Nachricht auf Bitübertragungskanal empfangen	Pol1 = xx+x +++x xxx+ ++xx x+xx x+++ ++x+ ++++	Polschata Alice-Bob [Alice]	B	31	Bob empfängt die Polschata Pol1 von Alice	
	Pol3 = x+x+ +x+x +++x +x+x +xx+ x+x+ +++x+ x+xx	Pol1 = xx+x +++x xxx+ ++xx x+xx x+++ ++x+ ++++	Vergleich Polschata (XOR)	Bit5 = 1011 0101 0011 0001 1001 0110 0101 1001	Bitmaske Alice-Bob [Bob]	B	32	Durch Vergleichen der Polschata Pol3 und Pol1 entsteht eine Bitmaske Bit5, bei welcher "0" für gleich und "1" für ungleich steht	
	Bit3 = 0110 1110 1010 1011 0010 1010 1001 0100	Bit5 = 1011 0101 0011 0001 1001 0110 0101 1001	Streichen von Bits aus Bitfolge	Bit6 = 0101 0101 0111 0100 1011	Schlüsselbits Alice-Bob 2 [Bob]	B	33	Durch Streichen der Bits von Bit3, bei welchen die Bitmaske Bit5 nicht übereinstimmt, erhält man die neuen Schlüsselbits Bit6	
		Bit5 = 1011 0101 0011 0001 1001 0110 0101 1001	Nachricht auf Bitübertragungskanal senden			B	34	Bob schickt die Bitmaske Bit5 über den Bitübertragungskanal zu "Alice"	
			Zug beenden			B	35	Bob beendet seinen Zug	
	Bit5 = 1011 0101 0011 0001 1001 0110 0101 1001		Nachricht auf Bitübertragungskanal abhören	Bit5 = 1011 0101 0011 0001 1001 0110 0101 1001	Bitmaske Alice-Bob [Bob]	E	35	Eve empfängt die Bitmaske Bit5 von Bob	
	Bit5 = 1011 0101 0011 0001 1001 0110 0101 1001	Bit2 = 1010 0101 0011 0110 1100 1101 0101 1001	Streichen von Bits aus Bitfolge	Bit7 = 0011 0110 1100 1101 0101 1001	Schlüsselbits Alice-Bob 2 [Eve]	E	36	Eve streicht die Stellen an Hand der Bitmaske Bit5 die Bob gelöscht hat aus ihren Schlüsselbits Bit2 und erhält somit ihre neuen Schlüsselbits Bit7	
	Bit5 = 1011 0101 0011 0001 1001 0110 0101 1001	Bit4 = 0011 1011 0101 0101 1001 0001 0110 1001	Streichen von Bits aus Bitfolge	Bit8 = 1111 0000 1111 0000 1111 0000	Bitmaske Richtige Bits Eve [Eve]	E	36	Eve streicht die Stellen ihrer Bitmaske Bit5 wo Bob falsch geraten hat und erhält die Bitmaske Bit8 mit den Bits die sie richtig geraten hat	
			Zug beenden			E	37	Eve beendet ihren Zug	
			Nachricht auf Bitübertragungskanal empfangen	Bit5 = 1011 0101 0011 0001 1001 0110 0101 1001	Bitmaske Alice-Bob [Bob]	A	38	Alice empfängt die Bitmaske Bit5 von Bob	
Ende Phase 2	Bit1 = 0100 1111 1000 0101 1011 1101 0001 0001	Bit5 = 1011 0101 0011 0001 1001 0110 0101 1001	Streichen von Bits aus Bitfolge	Bit9 = 1111 0000 1111 0000	Schlüsselbits Alice-Bob 2 [Alice]	A	39	Alice streicht die Stellen an denen Bob falsch geraten hat aus ihren Schlüsselbits Bit1 und erhält die neuen Schlüsselbits Bit9	Ende Phase 2
Beginn Phase 3			Zahl erzeugen	Int2 = 5	Prüfbitanzahl Alice-Bob [Alice]	A	40	Alice ermittelt aus der Länge der neuen Schlüsselbit Bit9 die Zahl Int2 der Bits, die angefordert werden sollen	Beginn Phase 3
		Bit9 = 1111 0000 1111 0000	Zahl erzeugen	Int3 = 16	Länge Prüfmaske Alice-Bob [Alice]	A	41	Alice bestimmt die Länge der Bitmaske Int3 anhand ihrer Schlüsselbits Bit9	
	Int3 = 16	Int2 = 5	Bitmaske erzeugen	Bit10 = 0110 0010 0100 1000	Prüfmaske Alice-Bob [Alice]	A	42	Alice generiert nun eine Bitmaske Bit10, welche angibt, welche Bits Bob schicken soll Ihre Länge ist bestimmt durch Int3 und die Anzahl der zu prüfenden Bits durch Int2	
	Bit10 = 0110 0010 0100 1000	Bit9 = 1111 0000 1111 0000	Streichen von Bits aus Bitfolge	Bit11 = 1 0101	Prüfbits Alice-Bob [Alice]	A	43	Alice erhält die Prüfbits Bit11 durch streichen der Schlüsselstellen aus Bit9	
	Bit10 = 0110 0010 0100 1000	Bit9 = 1111 0000 1111 0000	Streichen von Bits aus Bitfolge	Bit12 = 001 1110 1010	Schlüssel Alice-Bob [Alice]	A	44	Alice erhält den Schlüssel Bit12 durch streichen der Prüfmaske Bit10	
		Bit10 = 0110 0010 0100 1000	Nachricht auf Bitübertragungskanal senden			A	45	Alice sendet die Prüfmaske Bit10 an "Bob"	
			Zug beenden			A	46	Alice beendet ihren Zug	
			Nachricht auf Bitübertragungskanal abhören	Bit10 = 0110 0010 0100 1000	Prüfmaske Alice-Bob [Alice]	E	47	Eve erhält die Prüfmaske Bit10 von Alice	
	Bit10 = 0110 0010 0100 1000	Bit7 = 0011 0110 1100 1101 0101 1001	Streichen von Bits aus Bitfolge	Bit13 = 0 1111	Prüfbits Alice-Eve [Eve]	E	48	Eve erzeugt aus ihrem Schlüsselbits Bit6 und der Prüfmaske Bit10 von Alice die Prüfbits Bit13	
	Bit10 = 0110 0010 0100 1000	Bit7 = 0011 0110 1100 1101 0101 1001	Streichen von Bits aus Bitfolge	Bit14 = 0110 1010 0001 0100	Schlüssel Alice-Bob [Eve]	E	49	Eve streicht die Stellen aus ihrem Schlüssel Bit6 die angefordert wurden	
			Zug beenden			E	50	Eve beendet ihren Zug	
			Nachricht auf Bitübertragungskanal empfangen	Bit10 = 0110 0010 0100 1000	Prüfmaske Alice-Bob [Alice]	B	51	Bob erhält die Prüfmaske Bit10 von "Alice"	
	Bit10 = 0110 0010 0100 1000	Bit6 = 0101 0101 0111 0100 1011	Streichen von Bits aus Bitfolge	Bit15 = 101 0111	Prüfbits Alice-Bob [Bob]	B	52	Bob streicht die Stellen aus seinem Schlüssel Bit6 die nicht angefordert wurden und erhält seine Prüfbits Bit15	
	Bit10 = 0110 0010 0100 1000	Bit6 = 0101 0101 0111 0100 1011	Streichen von Bits aus Bitfolge	Bit16 = 11 01101 0010	Schlüssel Alice-Bob [Bob]	B	53	Bob streicht die angefragten Prüfbits Bit10 aus seinem Schlüssel Bit6	
		Bit15 = 101 0111	Nachricht auf Bitübertragungskanal senden			B	54	Bob sendet die berechneten Prüfbits Bit15 an "Alice"	
			Zug beenden			B	55	Bob beendet seinen Zug	
			Nachricht auf Bitübertragungskanal abhören	Bit15 = 101 0111	Prüfbits Alice-Bob [Bob]	E	56	Eve empfängt die von Bob gesendeten Prüfbits Bit15	
	Bit13 = 0 1111	Bit15 = 101 0111	Bitfolgen auf Gleichheit prüfen (XOR)	Bit17 = 000 0000	Ergebnisbits Prüfung Alice-Bob-Eve [Eve]	E	57	Falls die Prüfbits Bit13 und Bit15 nicht übereinstimmen, so weiß Eve, dass sie erwischt wurde	
			Zug beenden			E	58	Eve beendet ihren Zug	
			Nachricht auf Bitübertragungskanal empfangen	Bit15 = 101 0111	Prüfbits Alice-Bob [Bob]	A	59	Alice empfängt die von "Bob" gesendeten Prüfbits Bit15	
Ende Phase 3	Bit11 = 1 0101	Bit15 = 101 0111	Bitfolgen auf Gleichheit prüfen (XOR)	Bit18 = 0 0000	Ergebnisbits Prüfung Alice-Bob [Alice]	A	60	Alice prüft ihre berechneten Prüfbits Bit11 mit den von "Bob" erhaltenen Prüfbits Bit15 auf Gleichheit	Ende Phase 3
Beginn Phase 4	Str1 = "Hello World!"	Bit12 = 001 1110 1010	Nachricht verschlüsseln	Cif1 = **********	Chiffre Alice-Bob [Alice]	A	61	Alice verschlüsselt den String Str1 mit ihrem Schlüssel Bit12 und erhält dadurch die Chiffre Chif1	Beginn Phase 4
		Cif1 = **********	Nachricht auf Bitübertragungskanal senden			A	62	Alice sendet die Chiffre Cif1 über den Bitübertragungskanal an Bob	
			Zug beenden			A	63	Alice beendet ihren Zug	
			Nachricht auf Bitübertragungskanal abhören	Cif1 = **********	Chiffre Alice-Bob [Alice]	E	64	Eve hört die Chiffre Chif1 ab	
	Cif1 = **********	Bit14 = 0110 1010 0001 0100	Nachricht entschlüsseln	Str1 = "Hello World!"	Nachricht Alice-Bob [Alice]	E	65	Eve entschlüsselt die Chiffre Chif1 mit dem Schlüssel Bit14	
			Zug beenden			E	66	Eve beendet ihren Zug	
			Nachricht auf Bitübertragungskanal empfangen	Cif1 = **********	Chiffre Alice-Bob [Alice]	B	67	Bob empfängt die Chiffre Cif1	
Ende Phase 4	Cif1 = **********	Bit16 = 11 01101 0010	Nachricht entschlüsseln	Str1 = "Hello World!"	Nachricht Alice-Bob [Bob]	B	68	Bob entschlüsselt mithilfe seines Schlüssels Bit16 die Chiffre Cif1 und erhält dadurch den String Str1	Ende Phase 4