
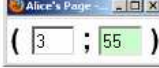
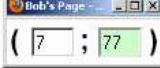




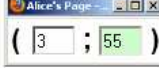
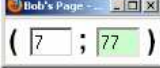

# Signieren und Verschlüsseln einer Nachricht in fünf Schritten

<input type="text"/>	<input type="text"/>	ab vier treffen an der uhr
Schlüssel auf Nachricht anwenden		Schlüssel auf Nachricht anwenden
<input type="text"/>	>>	<<
Hashwert		14 Hashwert
Signatur	<input type="text"/>	14 Signatur
Schlüssel auf Signatur anwenden		Schlüssel auf Signatur anwenden


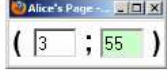

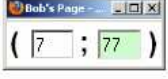

Der Hashwert der Nachricht wird mit dem Knopf „V“ in das Signatur-Feld kopiert ...

privater Schlüssel*: 	öffentlicher Schlüssel*: 		öffentlicher Schlüssel*: 	privater Schlüssel*: 
anzuwendender Schlüssel:			anzuwendender Schlüssel:	
<input type="text"/>	<input type="text"/>		<input type="text"/>	<input type="text"/>
Schlüssel auf Nachricht anwenden			Schlüssel auf Nachricht anwenden	
<input type="text"/>	>>	<<	<input type="text"/>	<input type="text"/>
Hashwert			14 Hashwert	
Signatur	<input type="text"/>	<input type="text"/>	49 Signatur	
Schlüssel auf Signatur anwenden			Schlüssel auf Signatur anwenden	


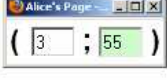



... und mit dem privaten Schlüssel des Absenders verschlüsselt.

privater Schlüssel*: 	öffentlicher Schlüssel*: 		öffentlicher Schlüssel*: 	privater Schlüssel*: 
anzuwendender Schlüssel:			anzuwendender Schlüssel:	
<input type="text"/>	<input type="text"/>		<input type="text"/>	<input type="text"/>
Schlüssel auf Nachricht anwenden			Schlüssel auf Nachricht anwenden	
ah+!nob+yno33o1+a1+iob+uqb	>>	<<	ah+!nob+yno33o1+a1+iob+uqb	
1, 8, 43, 33, 14, 15, 2, 43, 25, 2, 1			1, 8, 43, 33, 14, 15, 2, 43, 25, 2, 1	
5, 51, 51, 15, 49, 43, 1, 49, 43, 9,			5, 51, 51, 15, 49, 43, 1, 49, 43, 9,	
15, 2, 43, 21, 17, 2			15, 2, 43, 21, 17, 2	
Hashwert			26 Hashwert	
Signatur	<input type="text"/>	<input type="text"/>	49 Signatur	
Schlüssel auf Signatur anwenden			Schlüssel auf Signatur anwenden	

Die Nachricht mit dem öffentlichen Schlüssel des Empfängers verschlüsselt und mit dem Knopf „<<“ versendet.

privater Schlüssel*: 	öffentlicher Schlüssel*: 		öffentlicher Schlüssel*: 	privater Schlüssel*: 
anzuwendender Schlüssel: 27 55			anzuwendender Schlüssel: 7 77	
<div style="border: 1px solid gray; padding: 5px;"> <p>ab vier treffen an der uhr</p> <p>Schlüssel auf Nachricht anwenden</p> <p>1, 2, 32, 22, 9, 5, 18, 32, 20, 18, 5, 6, 6, 5, 14, 32, 1, 14, 32, 4, 5, 18, 32, 21, 8, 18</p> </div>	>>	<<	<div style="border: 1px solid gray; padding: 5px;"> <p>ah+!nob+yno33o1+a1+iob+uqb</p> <p>Schlüssel auf Nachricht anwenden</p> <p>1, 8, 43, 33, 14, 15, 2, 43, 25, 2, 15, 51, 51, 15, 49, 43, 1, 49, 43, 9, 15, 2, 43, 21, 17, 2</p> </div>	
Hashwert 14		49	Hashwert 26	
Signatur 49			Signatur 49	
Schlüssel auf Signatur anwenden			Schlüssel auf Signatur anwenden	

Der Empfänger entschlüsselt nun die Nachricht mit seinem privaten Schlüssel.

privater Schlüssel*: 	öffentlicher Schlüssel*: 		öffentlicher Schlüssel*: 	privater Schlüssel*: 
anzuwendender Schlüssel: 7 77			anzuwendender Schlüssel: 7 77	
<div style="border: 1px solid gray; padding: 5px;"> <p>ab vier treffen an der uhr</p> <p>Schlüssel auf Nachricht anwenden</p> <p>1, 2, 32, 22, 9, 5, 18, 32, 20, 18, 5, 6, 6, 5, 14, 32, 1, 14, 32, 4, 5, 18, 32, 21, 8, 18</p> </div>	>>	<<	<div style="border: 1px solid gray; padding: 5px;"> <p>ah+!nob+yno33o1+a1+iob+uqb</p> <p>Schlüssel auf Nachricht anwenden</p> <p>1, 8, 43, 33, 14, 15, 2, 43, 25, 2, 15, 51, 51, 15, 49, 43, 1, 49, 43, 9, 15, 2, 43, 21, 17, 2</p> </div>	
Hashwert 14		49	Hashwert 26	
Signatur 14			Signatur 49	
Schlüssel auf Signatur anwenden			Schlüssel auf Signatur anwenden	

Mit dem öffentlichen Schlüssel des Absenders entschlüsselt der Empfänger nun die Signatur: Sie ergibt den Hashwert der entschlüsselten Nachricht.

Wenn sich Absender und Empfänger darauf einigen, kann die Signatur auch durch den Hashwert der verschlüsselten Nachricht gebildet werden, dann muss die Signatur vor dem Entschlüsseln überprüft werden.