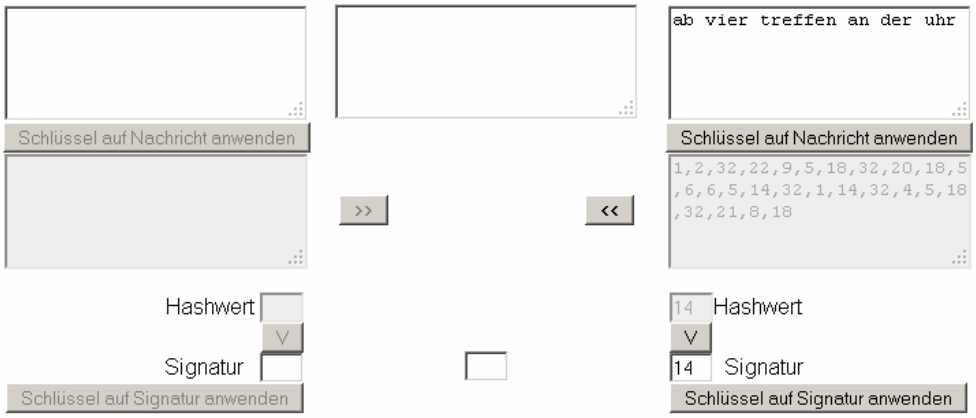
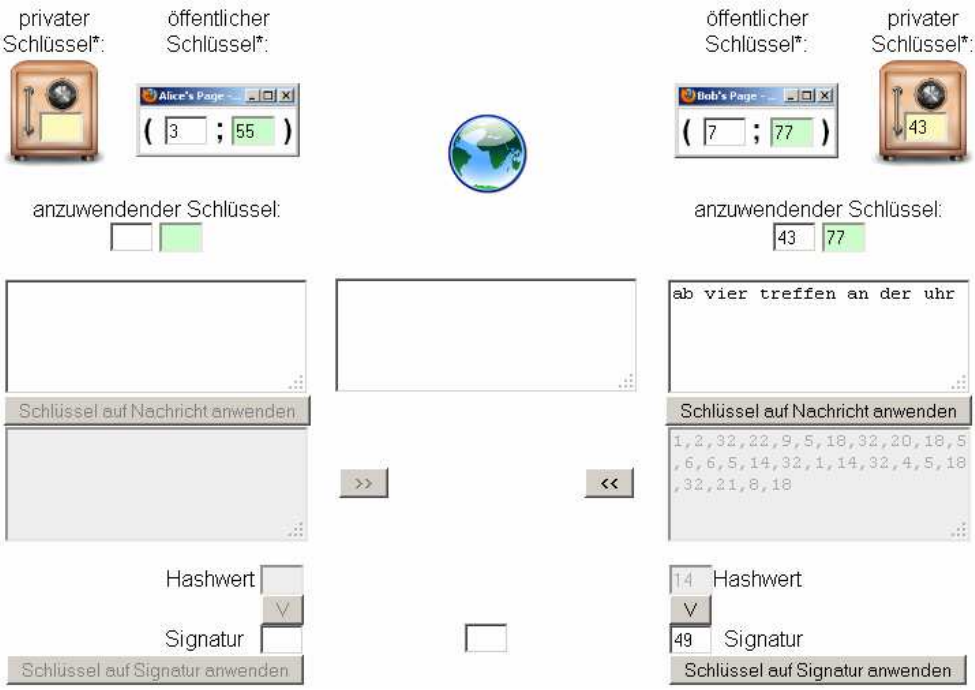
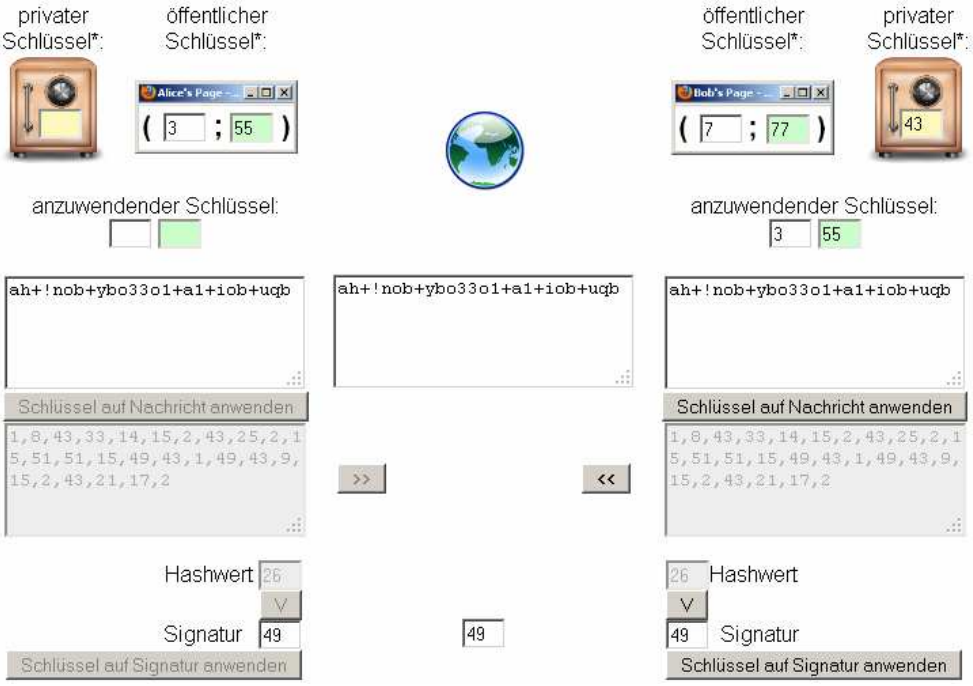
Signieren und Verschlüsseln einer Nachricht in fünf Schritten



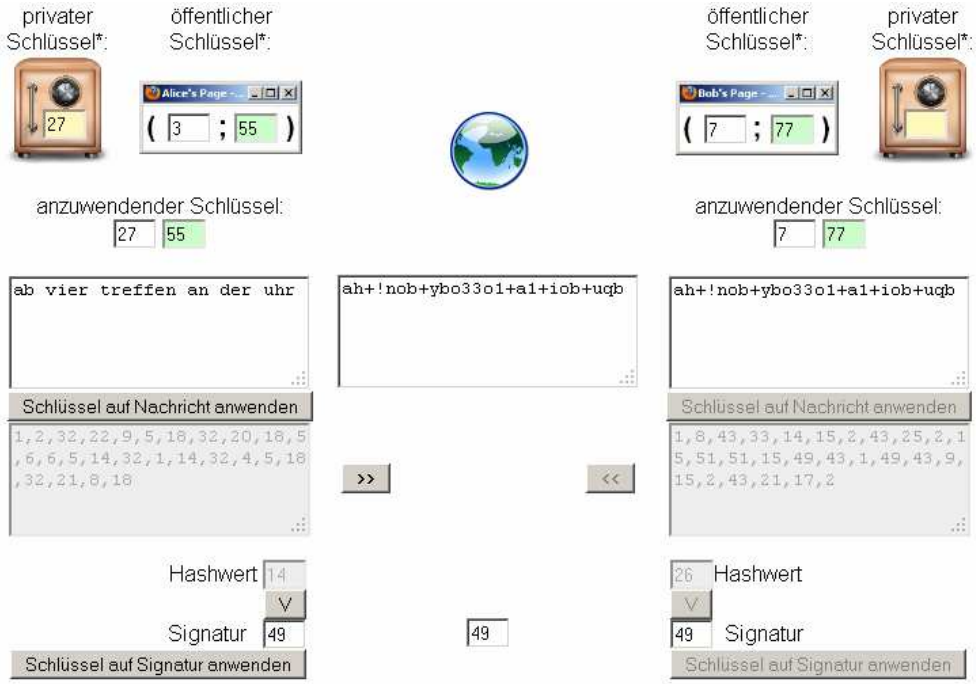
Der Hashwert der Nachricht wird mit dem Knopf „V“ in das Signatur-Feld kopiert …



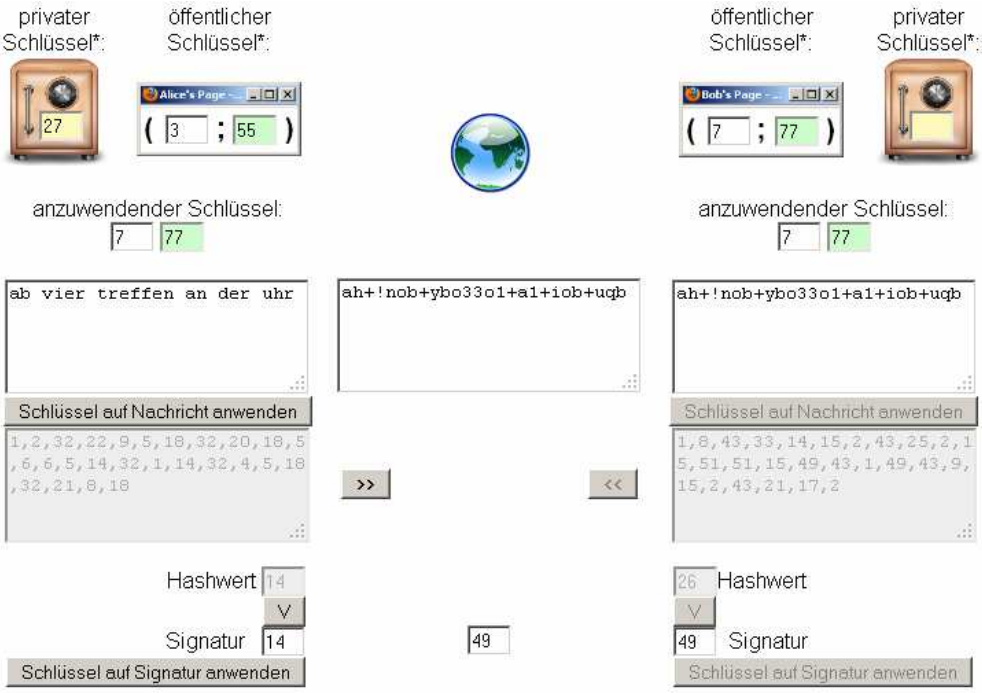
… und mit dem privaten Schlüssel des Absenders verschlüsselt.



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



Der Empfänger entschlüsselt nun die Nachricht mit seinem privaten Schlüssel.



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.