		Klartextsymbol			
		A	**B**	**C**	**D**
Schlüssel	**1**	A	B	C	D
	2	D	C	A	B
	3	C	A	D	B
	4	A	C	D	B

Alice verschlüsselt die Nachricht „ABC“ zuerst mit dem Schlüssel 2 und anschliessend das Ergebnis mit dem Schlüssel 3.

$$\text{"ABC"} \xrightarrow{E_2} \text{"DCA"} \xrightarrow{E_3} \text{"BDC"}$$

Der Angreifer kennt den Geheimtext „BDC“ und den dazugehörigen Klartext „ABC“. Seine Aufgabe ist es, die beiden Schlüssel zu erraten. Obwohl es für das Schlüsselpaar theoretisch $4^2 = 16$ Möglichkeiten gibt, muss er dazu maximal $2 \cdot 4 = 8$ Versuche durchführen.

$$\text{"ABC"} \xrightarrow{E_1} \text{"ABC"} \qquad \text{"BDC"} \xrightarrow{D_1} \text{"BDC"}$$

$$\text{"ABC"} \xrightarrow{E_2} \underline{\text{"DCA"}} \qquad \text{"BDC"} \xrightarrow{D_2} \text{"DAB"}$$

$$\text{"ABC"} \xrightarrow{E_3} \text{"CAD"} \qquad \text{"BDC"} \xrightarrow{D_3} \underline{\text{"DCA"}}$$

$$\text{"ABC"} \xrightarrow{E_4} \text{"ACD"} \qquad \text{"BDC"} \xrightarrow{D_4} \text{"DCB"}$$

Der Angreifer erkennt, dass die Verschlüsselung von „ABC“ mit dem Schlüssel 2 und die Entschlüsselung von „BDC“ mit dem Schlüssel 3 das gleiche Resultat, nämlich „DCA“, ergibt. Damit hat er das gesuchte Schlüsselpaar gefunden. ■

23.4 International Data Encryption Algorithm (IDEA)

Ein Verschlüsselungsalgorithmus, der aufgrund seiner seriösen Entwurfskriterien einen ausgezeichneten Ruf geniesst, wurde Ende der 80er Jahre am Institut für Signal- und Informationsverarbeitung der ETH Zürich durch Dr. Xuejia Lai und Prof. James Massey entwickelt [16]. Seit 1992 ist er unter der Bezeichnung IDEA (International Data Encryption Algorithm) bekannt. Ursprünglich trug IDEA die Bezeichnung „Improved Proposed Encryption Standard“ (IPES), da er durch eine kleine aber sehr wirkungsvolle Änderung aus dem PES von Massey und Lai hervorgegangen ist.

Als Entwurfskriterien nennt J. Massey die folgenden Punkte:

- Grosse Schlüssellänge. Der 128-Bit Schlüssel sollte eine genügend grosse Sicherheitsreserve gewährleisten.