Asymmetrisch verschlüsseln ohne Austausch geheimer Informationen

Auch bei unknackbaren Verschlüsselungsverfahren besteht stets die Gefahr, dass jemand das geheime Schlüsselwort erfährt. Bevor Nachrichten verschlüsselt werden können müssen sich die Kommunikationspartner stets auf einen gemeinsamen Schlüssel einigen. Deshalb haben in der zweiten Hälfte des 20. Jahrhunderts einige Wissenschaftler erforscht, ob es nicht ein Verfahren geben kann, bei dem keine geheimen Schlüssel ausgetauscht werden müssen.

Stell dir folgende Situation vor:

Alice und Bob haben je ein Schloss mit Schlüssel.
Alice möchte Bob ein Geheimnis in einer verschlossenen Kiste übermitteln.

Wie kann Alice den Inhalt der Kiste sicher übermitteln, ohne Bob den Schlüssel für ihr Schloss zu geben?

Hinweis: Wie gesagt, *beide* haben je ein Schloss!