

Vorteile

Sehr schnell für Ver- und  
Entschlüsselung der Nachricht

Bei langen Schlüssel eine  
Hohe Sicherheit

### Nachteile

Die Schlüsselübergabe: Es muss sichergestellt werden, dass der Schlüssel der beiden Teilnehmer über einen sicheren Kanal (zum Beispiel persönlich) ausgetauscht wird. Dies kann in der Praxis sehr schwer sein

Die Anzahl der benötigten Schlüssel:  
Für jedes Paar von Teilnehmern die verschlüsselte Nachrichten austauschen möchten, wird ein neuer Schlüssel benötigt