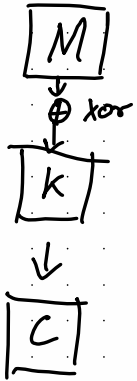


One Time Pad



- Message und Key sind gleich lang
- Key darf nur ein Mal benutzt werden
- Key muss absolut zufällig sein
- Key muss auf sicherem Weg ausgetauscht sein
- theoretisch absolut sicheres Verfahren
- Bei absolut zufälligem Key ist auch der ciphertext absolut zufällig