Two main drawbacks with Protocol 1:

* This is susceptible to middleman attacks. If the connection were interrupted, another person could act as Alice or Bob and send another OTP key to both and conversate with Bob and Alice while blocking Alice from directly communicating with Bob.
* Since the OTP key must be the same size (or larger) than the message and Is only used once, effectively the file that is sent is twice as large which can greatly affect performance.