O Grande Problema desta cifra se concentra na transmissão segura da chave pois para cada mensagem deve ser enviada uma chave por canal seguro porem ter que reenviar a chave a cada mensagem pode ser um risco.

Caso a mensagem estivesse em alemão por exemplo o atacante talvez não pudesse identificar o texto pois para ele não faria sentido o conteúdo da mensagem.