يمكن حل هذه المشكلة ، عن طريق جعل جميع الأشخاص يستخدموا مفتاح واحد ، لكن في حال مثلا خروج أحد العملاء منها فسوف تكون هناك مشكله لأنه يعرف المفتاح ، لذلك على الشركة أن تقوم بتغير المفتاح ، وإعطاء جميع العملاء المفتاح الجديد (من خلال مثلا الاجتماع) وهو حل "يبدو" جيد .

وتبدأ المشاكل في حال تمكن المخترق من كسر رسالة والحصول على المفتاح ، سوف يكون بإمكانه كسر جميع الرسائل (في حال كان طول المفتاح 128 بت والخوارزمية جيده ، فانه لن يمكن كسر المفتاح بسهوله) لكن اذا افترضنا انه قام بسرقة المفتاح (مثلا أخذه من عميل غشاش ، أو استخدم أسلوب التهديد) المهم حصل عليه ، فهنا يكون المخترق قد حصل على كشف الرسائل لأنه يملك المفتاح . وهذا ما لا يريده أحد ، لذلك حل "مفتاح واحد للجميع" حل غير عملي أيضا.

باختصار يكون حل إرسال المفتاح قبل عمليه الإرسال مناسب اذا كانت عمليه الإرسال بسيطة (بين شخصين أو ثلاثة مثلا) ، وإذا كانت أيضا عمليه الإرسال عبر الهاتف آمنه .

غير ذلك سوف نلجأ إلى الحل الثاني، و هو استخدام طرف ثالث في العملية TTP :

دعنا نوضح الآمر بمثال بسيط .

لنفرض محمد يريد أن يرسل رسالة لعلي ، والطرف الثالث هو سامي .

الآن في البداية يذهب محمد إلى الطرف الثالث سامي ويقوم سامي بتوليد مفتاح KEK ويقوم بتخزين المفتاح في جهازه ، واعطاء نسخه من الـ KEK إلى محمد. يأتي علي أيضا إلى الطرف الثالث سامي ، ويقوم بتوليد مفتاح KEK ويخزنه في جهازه ، ويعطي على نسخه من المفتاح.

هنا عندما يريد محمد إرسال رسالة إلى علي ، يقوم محمد بطلب مفتاح الجلسة من الطرف الثالث سامي ، يقوم سامي بتشفير مفتاح الجلسة بالمفتاح KEK الذي قام بتوليده هو و محمد في البداية ، ويقوم بإرسال المفتاح المشفر إلى محمد ، ويقوم بتشفير مفتاح الجلسة أيضا مره أخرى ولكن بمفتاح علي ويقوم بإرساله إلى علي.