مقدمه برای داشتن یک ارتباط امن علاوه بر محرمانگی، می‌بایست اصالت سه چیز احراز شود: پیام، کلید و هویت عوامل برقرار کننده ارتباط. برای اینکه هویت عوامل ارتباط برای یکدیگر احراز شود می‌بایست بر سر موضوعات فراوانی از جمله موارد زیر توافق داشته باشند: (فرض کنیم پیام m بین عوامل رد و بدل شده باشد)

۱. چه کسی m را ساخته است؟

۲. چه زمانی m ساخته شده است؟

۳. به چه کسی m فرستاده شده است؟

۴. چند بار m فرستاده شده است؟

می‌توان به این موضوعات موارد دیگری نیز اضافه کرد:

۵. دو عامل در مورد پروتکلی که اجرا می‌کنند توافق داشته باشند

۶. دوعامل در مورد نقشی که در پروتکل بازی می‌کنند توافق داشته باشند

اگرچه اهمیت احراز هویت در رمزنگاری نامتقارن نمود بیشتری دارد و راه‌کارهایی از جمله امضای دیجیتال، مهر زمانی و ..برای آن معرفی شده است، در رمزنگاری متقارن نیز برای توزیع کلید بین عوامل با استفاده از یک سرور قابل اعتماد پروتکل‌های احراز هویت زیادی طراحی شده است.

در این مقاله ابتدا با استفاده از کتاب با آزمون و خطا تلاش می‌کنیم تا یک پروتکل توزیع کلید رمزنگاری متقارن بدست آوریم. این آزمون و خطا را تا جایی ادامه می‌دهیم که به صورت شهودی مطمین شویم که پروتکل بدست آمده امنیت لازم را دارد ولی هیچ اثبات صوری برای آن ارایه نمی‌دهیم. سپس برای اینکه بتوان امنیت پروتکل‌های احراز هویت را با استفاده از روش‌های صوری به صورت دقیق انجام داد به دنبال یافتن تعاریفی دقیق برای اینکه چه پروتکل‌هایی در این خاصیت صدق می‌کنند به مقاله‌ی مراجعه می‌کنیم که تعریف‌های ارایه شده در آن امروزه در اکثر مقالات پذیرفه شده است به طوری که اثبات‌های صوری خود را با استفاده از این تعاریف انجام می‌دهند.