توضیحات پروتکل سوال آخر:

در این سیستم تبادل از روش دفی هلمن برای مبادله کلید جلسه استفاده شده است. یک عدد اول P با تعداد بیت ۲۰۴۸ انتخاب می شود که هر بار کلید خصوصی از بازه ۲ تا P-1 گزینش شده G به توان کلید خصوصی در پیمانه P کلید عمومی هر طرف را می سازد سپس این کلید عمومی برای طرف مقابل ارسال شده و هرطرف کلید عمومی طرف دیگر را به توان کلید خصوصی خود رسانده و حاصل را در پیمانه P حساب می کند. به این ترتیب key حساب می شود. سپس برای اینکه کلید ۲۵۶ بیت شود و بتوان در رمز نگاری AES از آن استفاده کرد sha256(key) را محاسبه کرده و این حاصل به عنوان کلید جلسه استفاده می گردد.

به این ترتیب تمام پیام های مبادله شده ابتدا با کلید جلسه رمز می شوند. به علاوه برای اطمینان از صحت پیام های دریافتی لازم است قسمتی تحت عنوان امضا همراه با پیام ارسال شود در این پروتکل متن امضا از حاصل hmac پیام با کلید جلسه بدست می آید و با متن رمز شده ارسال می شود.

فرد دریافت کننده پس از دریافت پیام رمز شده بخش cipher را از sign جدا کرده و متن cipher را رمزگشایی کرده hmac پیام بدست آمده را با کلید جلسه محاسبه کرده و آن را با sign مقایسه می کند در صورت برابری یعنی متن دریافتی صحیح می باشد.

P با طول ۲۰۴۸ بیت انتخاب می شود چراکه باید طول بیت آن به اندازه ای باشد که مسئله لگاریتم گسسته قابل حل نباشد یعنی از روی کلید عمومی و P و G نتوان کلید خصوصی را محاسبه کرد. (متاسفانه سیستم من قادر به تولید P با ۲۰۴۸ بیت نبود و در داخل کد از یک P با ۱۵۰۳ بیت استفاده کرده ام ولی در حالت کلی تعداد بیت بیشتری برای امنیت لازم است)

تمامی کد ها با python3 نوشته شده است و با دستور python3 filename در ترمینال لینوکس قابل اجرا هستند.