SPCS CRYPTOGRAPHY
HOMEWORK 10 (OPTIONAL)

Spend time on your project first - just do the ones in this p-set that interest you. You are strongly encouraged to work in groups, but you have to write up the solution on your own.

1. Try to design a signature scheme based on discrete log problem. Compare your design with ElGamal signature scheme.

2. Here is another method of doing key-exchange: the Needham-Schroeder protocol.
   Suppose Alice wants to establish a shared key with Bob. They have a trusted third party Steve. K_{AS} is an established shared key between Alice and Steve, and K_{BS} is an established shared key between Bob and Steve.
   - Alice tells Steve that she wants to communicate with Bob.
   - Steve generates a symmetric key K_{AB}, to be used between Alice and Bob.
   - Steve sends Alice K_{AB}, and also $(K_{AB}, Alice)_{BS}$, the encryption of K_{AB} (and the identity of Alice) using K_{BS}.
   - Alice sends Bob $(K_{AB}, Alice)_{BS}$.

   (a) How can Bob get the shared key?
   (b) What can Bob do to confirm that both of them has the right shared key?
   (c) Try to attack this system.

3. We mentioned PGP in class - there are other standards, such as GPG. Pick your favorite one and try to send an encrypted email. See https://emailselfdefense.fsf.org/en/ on how to do it.

4. Go to any website over https, and look at the certificates. Try to see how it matches up with the concepts we discussed today. You may see various modern standards being used nowadays, such as PKCS (public key cryptography standard), which would tell you the underlying cryptography method. For example, PKCS #1 is the standard published by RSA labs to tell you the format of public/private key in RSA, padding schemes, and signature scheme.

5. Random math fact: Quadratic reciprocity. Recall that Legendre symbol

$$\left(\frac{a}{p}\right) = \begin{cases} 0 & \text{if } p|a \\ 1 & \text{if } a \text{ is a square mod } p \\ -1 & \text{if } a \text{ is not a square mod } p \end{cases}$$

   The Jacobi symbol is defined similarly. For a positive integer n with prime factorization $n = p_1^{e_1} \cdots p_k^{e_k}$, the Jacobi symbol is

$$\left(\frac{a}{n}\right) = \left(\frac{a}{p_1}\right)^{e_1} \cdots \left(\frac{a}{p_k}\right)^{e_k}$$

   (a) Find $\left(\frac{2}{3}\right)$, $\left(\frac{2}{5}\right)$ thus $\left(\frac{2}{15}\right)$.
   (b) Show that if $gcd(a, n) = 1$ and a is a square mod n, then $\left(\frac{a}{n}\right) = 1$. Is the converse true?
   (c) The quadratic reciprocity law says that for any two primes $p, q > 2$,

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{\frac{p-1}{2}\cdot\frac{q-1}{2}}$$

   This is arguably Gauss' favorite theorem. In particular, if $q = 5$, this means that $\left(\frac{5}{p}\right) = \left(\frac{p}{5}\right)$, something you have seen in previous homework.
   Compute $\left(\frac{3}{11}\right)$ with quadratic reciprocity.

(d) Devise a way to quickly compute Jacobi symbols.