Math 173A - Signatures

1. Sign a "document" with RSA and have your partner verify the signature. That is, pick two primes p and q and a verification key e coprime to $(p-1)(q-1)$. Publish $N = pq$ and e. Compute your signing key d with $de \equiv 1 \pmod{(p-1)(q-1)}$ and keep it secret.

   Now choose a document $D \pmod{N}$ and sign it by computing $S \equiv D^d \pmod{N}$. Have your partner verify your signature by computing $S^e \pmod{N}$ and making sure it's congruent to D.

2. Sign a "document" with ElGamal and have your partner verify the signature. That is, pick a prime p and a primitive root g modulo p. Choose a secret signing key $1 \leq a \leq p-1$ and publish the verification key $A \equiv g^a \pmod{p}$.

   Now choose a document $D \pmod{p-1}$ and sign it. Do this by picking a random $1 < k < p$ with $\gcd(k, p-1) = 1$. Compute the signature

   $$S_1 \equiv g^k \pmod{p} \qquad \text{and} \qquad S_2 \equiv (D - aS_1)k^{-1} \pmod{p-1}.$$

   Have your partner verify your signature by verifying that $A^{S_1} S_1^{S_2} \equiv g^D \pmod{p}$.

Here are some primes for RSA

23, 29, 31, 37, 41, 43, 47, 53, 59, 61, 67, 71, 73, 79, 83, 89, 97.

Here are some primes and primitive roots for ElGamal.

p	Primitive root modulo p
241	7
353	3
419	2
557	2
683	5