7/26. ElGamal Encryption and Its Varaints.

ElGamal Encryption

- KeyGen(1^n); Choose a large prime p and $g \xleftarrow{\$} \mathbb{Z}_p^*$.
  Choose a secret key $s \xleftarrow{\$} \mathbb{Z}_p^*$
  Compute $y = g^s \bmod p$ (∵ Discrete Logarithm Problem)
  output $pk = (p, g, y)$ and $sk = (s)$

- Enc(pk, m); choose a random $r \xleftarrow{\$} \mathbb{Z}_p^*$.
  output $(g^r, m \cdot y^r)$

- Dec(sk, c); parse c as (c_1, c_2).
  output $c_2 \cdot (c_1^s)^{-1}$.
  finite field.

  $m \cdot y^r \cdot (g^r)^{-s} = m \cdot (g^s)^r \cdot (g^r)^{-s}$
  $= m$

- Mult(c_1, c_2); parse c_1 as $c(c_{11}, c_{12}) = (g^{r_1}, m_1 \cdot y^{r_1})$
  c_2 as $(c_{21}, c_{22}) = (g^{r_2}, m_2 \cdot y^{r_2})$
  output $c(c_{11} \cdot c_{21}, c_{12} \cdot c_{22}) = (g^{r_1} \cdot g^{r_2}, m_1 \cdot y^{r_1} \cdot m_2 \cdot y^{r_2})$
  $= (g^{r_1+r_2}, m_1 \cdot m_2 \cdot y^{r_1+r_2})$