Chapter 2.3. Diffie-Hellman Key Exchange

Alice		Bob
sk: a		b
pk: g^a		g^b (Alice and Bob agree on a large prime p.)
	$\xrightarrow{g^a}$	
	$\xleftarrow{g^b}$	
computes $(g^b)^a = g^{ab}$		computes $(g^a)^b = g^{ab}$

Chapter 2.4. The ElGamal Public Key Cryptosystem

- KeyGen(1^n) ; chooses a large prime p and an element $g \in \mathbb{Z}_p^*$.
  chooses a secret key $1 \le a \le p-1$ and computes $A = g^a \bmod p$
  $pk = (p, g, A)$ $sk = (a)$

- Enc(pk, m) ; chooses a random r.
  computes $c_1 := g^r \bmod p$
  $c_2 := m \cdot A^r \bmod p$
  output (c_1, c_2)

- Dec$(sk, \vec{c})$; computes $(c_1^a)^{-1} \cdot c_2 =: m' \bmod p$
  output m'

- Mult(ct_1, ct_2) ; let $c_1 = (g^{r_1}, m_1 \cdot A^{r_1})$ and $c_2 = (g^{r_2}, m_2 \cdot A^{r_2})$
  Then, $c_1 \cdot c_2 = (g^{r_1} \cdot g^{r_2}, m_1 \cdot A^{r_1} \cdot m_2 \cdot A^{r_2})$
  $= (g^{r_1+r_2}, m_1 \cdot m_2 A^{r_1+r_2})$.