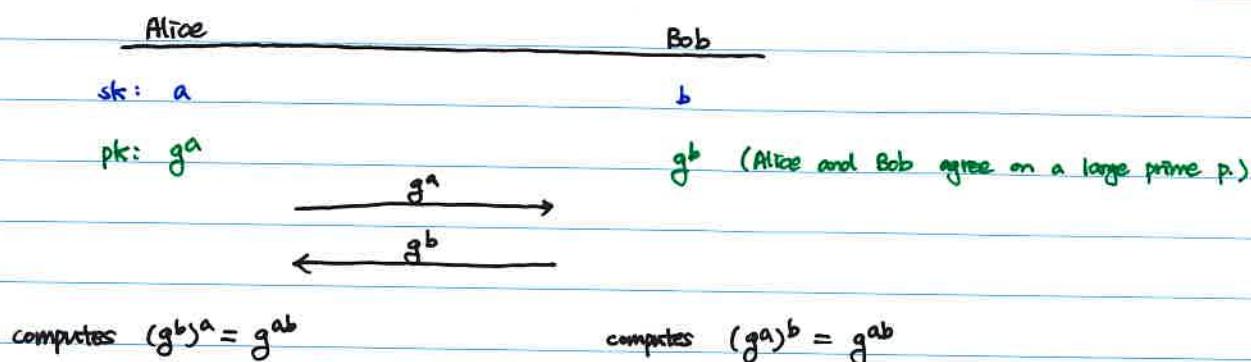


Chapter 2.3. Diffie-Hellman Key Exchange



Chapter 2.4. The ElGamal Public Key Cryptosystem

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

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

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

- $\text{Mult}(c_{t1}, c_{t2})$; 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, $c_1 \cdot c_2 = (g^{r_1} \cdot g^{r_2}, m_1 \cdot A^{r_1} \cdot m_2 \cdot A^{r_2})$
 $= (g^{r_1+r_2}, m_1 \cdot m_2 \cdot A^{r_1+r_2})$.