1 1. Observe that $\overset{(x_1,y_1)}{(6,2)}$ and $\overset{(x_2,y_2)}{(7,1)}$ are distinct points with distinct x-coordinates.

Then $\lambda = \frac{1-2}{7-6} = -1$, $x_3 = \lambda^2 - x_1 - x_2 = 1-6-7 = 10 \bmod 11$, $y_3 = (6-10)\cdot -1 - 2 = 2 \bmod 11$.

Hence, $P = (x_3, y_3) = (10, 2)$

$R = P + Q = (6,2) + (7,1) - (7,1) = (6,2) + O = (6,2)$

2. We want to show $\underbrace{(x_1,y_1) + (x_2,y_2)}_{P\ +\ Q} = \underbrace{(x_2,y_2) + (x_1,y_1)}_{Q\ +P}$.

Case 1: $x_1 \neq x_2$

Then $\lambda_{P+Q} = \frac{y_2-y_1}{x_2-x_1} = \frac{-(y_1-y_2)}{-(x_1-x_2)} = \frac{y_1-y_2}{x_1-x_2} = \lambda_{Q+P}$, call this value λ.

Consequently, $x_{3_{P+Q}} = \lambda^2 - x_1 - x_2 = \lambda^2 - x_2 - x_1 = x_{3_{Q+P}}$, call this x_3.

Now, we only need to show $y_{3_{P+Q}} = (x_1 - x_3)\lambda - y_1$ and $y_{3_{Q+P}} = (x_2 - x_3)\lambda - y_2$ are equal.

Observe that $y_{3_{P+Q}} = y_{3_{Q+P}} \iff (x_1 - x_3)\lambda - y_1 = (x_2 - x_3)\lambda - y_2$

$\iff \lambda x_1 - y_1 = \lambda x_2 - y_2$

$\iff y_2 - y_1 = \lambda(x_2 - x_1)$

$\iff \frac{y_2-y_1}{x_2-x_1} = \lambda$.

Since $\lambda = \frac{y_2-y_1}{x_2-x_1}$, we conclude $y_{3_{P+Q}} = y_{3_{Q+P}}$.

Case 2: $x_1 = x_2$. Similarly...

2 IK: Identity keys, EK: Ephemeral Keys, MK: Medium-term "backstop" keys

$k_1 = DH(IK_A, MK_B)$ → authenticates Alice to Bob

$k_2 = DH(EK_A, IK_B)$ → authenticates Bob to Alice

$k_3 = DH(EK_A, MK_B)$ → provides forward security and post-compromise security

③ 1. Verify(pk, m, σ) where $\sigma = (A, z)$ and $pk = g^s \bmod p$

$e = H(A, m)$

$$A \cdot S^e = g^a \cdot (g^s)^e = g^{a+s\cdot e} = g^z \bmod p$$

$A = g^a$ since σ is correctly generated & $S = g^s$ since pk is correctly generated

since $g \in \mathbb{Z}_p$ is of order q we can reduce the power mod q while the base is mod p & $z = a + s \cdot e$ since σ is correctly generated

Hence, Verify(pk, m, σ) outputs 1.

2. $\mathcal{B}$ picks $g \in \mathbb{Z}_p$ and computes $A = g^a \bmod p$. $\mathcal{B}$ runs $\mathcal{A}$ as a subroutine; inputs $g, A (= g^a)$, gets a and inputs $g, S (= g^s)$, gets s.

Then $\mathcal{B}$ can generate σ for any message using H.

④ 1. In $L_{ddhp\text{-}ideal}$, 2nd to last entries are independent but in $L_{ddhp\text{-}real}$, 5th entry is uniquely determined by 2nd and 3rd, 6th " 2nd and 4th.

2.

Algorithm $\mathcal{B}$:

1. Sample $\beta' \leftarrow \{0,1\}$
2. Sample $c, r \leftarrow \mathbb{Z}_q$
3. Take in (g, g^a, g^b, h) // $h = \begin{cases} g^{ab} & // \beta = 0 \\ g^r & // \beta = 1 \end{cases}$
4. if $\beta' = 0$: input $= (g, g^a, g^b, g^c, h, g^{ac})$
   else: input $= (g, g^a, g^b, g^c, h, g^r)$
5. Run $\mathcal{A}$ with input and forward its output $\hat{\beta}$.

$$\left[\begin{array}{l} \text{if } \beta=0 \ \& \ \beta'=0 \Rightarrow \text{ input} = (g, g^a, g^b, g^c, g^{ab}, g^{ac}) \\ \text{if } \beta=1 \ \& \ \beta'=1 \Rightarrow \text{ input} = (g, g^a, g^b, g^c, g^z, g^{z'}) \end{array}\right]$$

$$Pr[B \text{ wins}] = Pr[\hat{\beta} = \beta] = \sum_{i,j \in \{0,1\}} \underbrace{Pr[\hat{\beta} = \beta \mid \beta = i \wedge \beta' = j]}_{A_{ij}} \cdot Pr[\beta = i \wedge \beta' = j]$$

$$\left[\begin{array}{l} \text{Observe: } Pr[A_{00}] = Pr[A \text{ wins} \mid \mathcal{L}_{ddhp\text{-real}}] \\ \qquad Pr[A_{11}] = Pr[A \text{ wins} \mid \mathcal{L}_{ddhp\text{-ideal}}] \end{array}\right]$$

$$\begin{aligned} Pr[B \text{ wins}] &= \frac{1}{4}\left(Pr[A \text{ wins} \mid \mathcal{L}_{ddhp\text{-real}}] + Pr[A \text{ wins} \mid \mathcal{L}_{ddhp\text{-ideal}}]\right) \\ &\quad + \frac{1}{4}\left(Pr[A_{01}] + Pr[A_{10}]\right) \\ &\geq \frac{1}{4}\left(Pr[A \text{ wins} \mid \mathcal{L}_{ddhp\text{-real}}] + Pr[A \text{ wins} \mid \mathcal{L}_{ddhp\text{-ideal}}]\right) \\ &= \frac{1}{2} Pr[A \text{ wins dist game } \mathcal{L}_{ddhp\text{-real}} \text{ vs } \mathcal{L}_{ddhp\text{-ideal}}] \end{aligned}$$

$\Rightarrow$ a factor of $1/2$

3. We are given $Pr(A \text{ win}) = \alpha$. We know $Pr(A \text{ win}) = \frac{Adv(A)}{2} + \frac{1}{2} = \alpha$,

where $Adv(A) = |Pr[A \Rightarrow \text{real} \mid L = L_{ddhp\text{-real}}] - Pr[A \Rightarrow \text{real} \mid L = L_{ddhp\text{-ideal}}]|$.

Observe that one of these terms is at least $Adv(A)$

Hence, $Pr(B \text{ win}) \geq Adv(A) \cdot \frac{1}{2} + \frac{1}{2} \cdot \frac{1}{2} = \frac{1}{2}\left(Adv(A) + \frac{1}{2}\right) \geq \frac{\alpha}{2}$.

5) An adversary can choose $m_0 = 0$ and $m_1 = 1$. By getting $c = g^{m_i}$ mod p the adv. can easily determine the message used. Indeed $g^{m_0} = g^0 = 1$ and $g^{m_1} = g^1 = g$ and $g \neq 1$.

1. Assume we have an algo. $\mathcal{A}$ that, on input p, q, g, h generates values m, m', c, r, r' s.t. $g^m h^r = g^{m'} \cdot h^{r'}$ mod p where $m \neq m'$. In particular, we know that $g^{m-m'} = h^{r'-r}$ mod p. We know that $\exists a \in \mathbb{Z}_q \setminus \{0\}$ s.t. $g^a = h$ mod $p \Rightarrow g^{m-m'} = (g^a)^{r'-r}$ mod p. Since g is an elt. of order q, we have $m - m' = a(r-r')$ mod q. We know that $m, m' \in \mathbb{Z}_q$ and $m \neq m' \Rightarrow m - m' \neq 0$ mod $q \Rightarrow$ also $a(r'-r) \neq 0$ mod $q \Rightarrow (r'-r) \neq 0$ mod q. Since q is a prime $(r'-r)$ is invertible mod $q \Rightarrow$ we can define $a = \frac{m-m'}{r'-r}$ mod q as disc. log. of h for the base g.

2. We want to show that $\forall (m, r) \in \mathbb{Z}_q \times \mathbb{Z}_q$ $\exists (m', r') \in \mathbb{Z}_q \times \mathbb{Z}_q$ s.t. $m \neq m'$, $r \neq r'$ and $g^m h^r = g^{m'} \cdot h^{r'}$ mod p.
We fix $m' \in \mathbb{Z}_q / \{m\}$. We want to find r' s.t. $g^m \cdot h^r = g^{m'} \cdot h^{r'}$ mod p. By using $h = g^a$ mod p, we write $g^{m+ar} = g^{m'+ar'}$ mod $p \Leftrightarrow m + ar = m' + ar'$ mod $q \Leftrightarrow m - m' + ar = ar'$ mod q. Since both g and h have order q, a must be invertible mod q. Then $m - m' + ar = ar'$ mod q $\Leftrightarrow (m - m' + ar)a^{-1} = r'$ mod q. We have just shown that $\forall m' \in \mathbb{Z}_q$ $\exists r' \in \mathbb{Z}_q$ s.t. $r \neq r'$ and $g^m h^r = g^{m'} h^{r'}$ mod p.