Exercise 8

1.

We have:

$$m_1 = 3, b_1 = 2; m_2 = 5, b_2 = 3; m_3 = 7, b_3 = 4$$

So we get $M = m_1 * m_2 * m_3 = 105$.

$$\Rightarrow M_1 = 35, M_1^{'} = 2; M_2 = 21, M_2^{'} = 1; M_3 = 15, M_3^{'} = 1$$

So we get:

$x = 2 * 35 * 2 + 3 * 21 * 1 + 4 * 15 * 1(\mod 3 * 5 * 7) \Rightarrow x = 263(mod105)$

Finally

$$x = 53 + 105k, k \in N$$

2.

$$\phi(24) = \phi(2^3 * 3^1) = 24 * (1 - \frac{1}{2}) * (1 - \frac{1}{3}) = 8$$

$$\phi(n) = n * (1 - \frac{1}{p_1}) * (1 - \frac{1}{p_2}) * (1 - \frac{1}{p_3})$$

3.

$$\begin{gathered} S = r^{-1}(m - x_a R)(\mod p - 1) \\ \Rightarrow m = Sr + x_a R(\mod p - 1) \\ \Rightarrow g^m = g^{Sr + x_a R}(\mod p) \\ \Rightarrow g^m = (g^r)^S * (g^{x_a})^R(\mod p) \\ \Rightarrow g^m = R^S y_a^R(\mod p) \end{gathered}$$

4.

(1) When r is used twice, the adversary can calculate the plaintexts m by $S = my_b^r(\mod p)$ since y_b is the public key.

(2) The adversary could calculate the S and R to fabricate the signature by knowing x_a since $x_a = R^{-1}(m - Sr)(\mod p - 1)$.

5.

(1) Confidentiality can be achieved. Since finding the discrete logarithm is a hard problem, so DH key exchange can achieve confidentiality.

(2) Authenticity can not be achieved. Because the g^a and g^b doesn't provide any information about the two ends. So adversary can send a fabricated key to one side and the receiver has no method to verify the source of the key.