1082 作業七

繳交日期 109/05/22(五) 13:10

1. (a) In the Diffie-Hellman key exchange protocol, Alice and Bob choose a primitive root α in the integer multiplicative group Z_p^* for a large prime p. Alice sends $x_1 \equiv \alpha^a \pmod{p}$ to Bob, and Bob sends $x_2 \equiv \alpha^b \pmod{p}$ to Alice. Suppose Eve bribes Bob to tell her the values of b and x_2. However, he neglects to tell her the value of α. Suppose $\gcd(b, p-1) = 1$. Show how Eve can determine α from the knowledge of p, x_2, and b.

(b) In an ElGamal cryptosystem, Alice and Bob use $p = 17$ and $\alpha = 3$. Bob chooses his secret to be $a = 6$, so $\beta = 15$. Alice sends the ciphertext $(r, t) = (7, 6)$. Determine the plaintext m.