Andrew Johnson

CS 427

HW6

1) 410222175196

2) (a) Assuming we know the public key A and the group generator g. Given an ElGamal encryption of M, (B,C). Thus we have A, g, B, and C.

<u>DEC(a,(B,C))</u>
$K = B^a$
$M = CK^{-1}$
return M

We need to find a B' and C' such that when sent into the decryption we still get back M.
Let $B' = g \cdot B$ and $C' = A \cdot C$. When sent into the decryption we see that
$K' = (B')^a = (gB)^a = g^a \cdot B^a = A \cdot K$
Then $M' = C' \cdot (K')^{-1} = (A \cdot C) \cdot (A \cdot K)^{-1} = A \cdot A^{-1} \cdot C \cdot K^{-1} = C \cdot K^{-1} = M$ □

(b) Given two ElGamal encryptions of M_1 and M_2, we get (B_1,C_1) and (B_2,C_2). We need to find a B' and C' such that when decrypted we get $M_1 \cdot M_2$.
Let $B' = B_1 \cdot B_2$ and $C' = C_1 \cdot C_2$. When these are put into the decryption we see that
$K' = (B_1 \cdot B_2)^a = B_1^a \cdot B_2^a = K_1 \cdot K_2$
$M' = (C_1 \cdot C_2) \cdot (K')^{-1} = (C_1 \cdot C_2) \cdot (K_1 \cdot K_2)^{-1} = (C_1 \cdot K_1^{-1}) \cdot (C_2 \cdot K_2^{-1}) = M_1 \cdot M_2$ □

3) (a) If we take the case where x = 0 then we see that it is the same as the Lemma stated before. So what we are really checking is if $r_i - r_j \equiv x \pmod p$. So we are checking the distance between each r. In the former lemma we were checking a distance of 0. In the new Lemma, we can take any arbitrary x and will have the same probability instead of only looking at 0.

(b) Assume we know integers r and s, such that $g^r \equiv X \cdot g^s \pmod p$, We already know that g is a primitive root of Z^*_p, so we know that any power of g must have an inverse. Then we can use g^{-s} on our assumption to get, $g^r \cdot g^{-s} \equiv X \cdot (g^s \cdot g^{-s}) \pmod p \rightarrow g^{r-s} \equiv X \pmod p$. We can say $x = r - s$ and then we have proved $g^x \equiv X \pmod p$. □

(c) Let g be a primitive root of Z^*_p. From 3(a) we know with a *.6* probability that we can find an r and s that exist in Z^*_p such that $r - s = x$, for any fixed x, by only taking $\sqrt{2p}$ elements of g. This means we can find an r and s that satisfy above in $O(\sqrt{2p})$, or simplified $O(\sqrt{p})$. Thus, we see that by finding r and s, we have also satisfied 3(b) which is for finding the discrete logarithm. With both of these we can find x to solve the discrete logarithm in $O(\sqrt{p})$ time.