Jiping Zhang
CSE 207B: Applied Cryptography Due:

Homework 5

0. (a)(b) (I think these two questions are the same, so I answer them together) p-1 can be factored into the product of some smaller primes, and product the first several small prime factors has already exceeded 2^{128} (AES key area).

   So, after applying pohlig hellman algorithm to each of these prime factors, and applying Chinese remainder theory to the mod results of pohlig hellman, we can get that $kmodr = x$ where r is the product result of prime factors and $r > 2^{128}$.

   Now we can confirm k , it must be x. Then we can compute the AES key using k.

   (c) We should make sure that (p-1) can't be factored into some small prime factors, where the product of first several small factor is larger than or close to 2^{128} and we can run pohlig hellman algorithm on each of these small factor in acceptable short time

   To make things easier , we can just choose a big prime q , and use 2q+1 as p

1. (a) let's prove it's contrapositive proposition : If E is not semantically secure , then DDH assumption does not hold in G.

   if E is not semantic secure, that is, exist some F so that for two messages m_0 and m_1 , $|Pr(F(enc_{m_0}) == m_0) - Pr(F(enc_{m_0}) == m_1)| = 2\epsilon$ where $\epsilon > negligible$

   that is to say, for m_0 and m_1 , $|Pr(F(enc_{m_0}) == m_0) - \frac{1}{2}| = \epsilon$

   for two messages m_0 and m_1 , the enc_{m_0} and enc_{m_1} are $(g^b, g^{ab} \cdot m_0)$ and $(g^b, g^{ab} \cdot m_1)$ respectively.

   so, with this F, if we are given two triplets (g^a, g^b, g^{ab}) and (g^a, g^b, g^c) in random order,

   that is , we get (g^a, g^b, x) and (g^a, g^b, y), where one of x,y is g^{ab} and the other is g^c

   then, we generate a message m , calculate m multiplied by x and by y (of course multiply here is mod p multiply), and feed g^b, mx and g^b, my into F

   since $c \neq ab$, (g^b, mg^c) is not even a valid encrypted message, F applied to (g^b, mg^c) should behave randomly, that is $|F(g^b, mg^c) - \frac{1}{2}| = \delta$ where δ is negligible.

   $|F(g^b, mx) - F(g^b, my)| = |F(g^b, mg^{ab}) - F(g^b, mg^c)|$

   $\geq ||F(g^b, mg^{ab}) - \frac{1}{2}| - |F(g^b, mg^c) - \frac{1}{2}|| = |\epsilon - \delta|$

   ϵ is not negligible, δ is negligible, so $|\epsilon - \delta|$ is not negligible

   (b) if DDH assumption doesn't hold in G , that is we have a F so that $|F(g^a, g^b, g^{ab}) - F(g^a, g^b, g^c)| = \epsilon$ where ϵ is not negligible, then, if we have m_0 and m_1 given to challenger E and it outputs $(g^b, m_x g^{ab})$ where x is 0 or 1, and of course we know the public key g^a

   we apply F to $(g^a, g^b, m_0^{-1} m_x g^{ab})$ and $(g^a, g^b, m_1^{-1} m_x g^{ab})$

   if x=0 then $m_1^{-1} m_x g^{ab}$ behave like g^c and $m_0^{-1} m_x g^{ab} = g^{ab}$, and vise versa, so $|F(g^a, g^b, m_0^{-1}m_x g^{ab}) - F(g^a, g^b, m_1^{-1}m_x g^{ab})| = \epsilon > negligible$

E is not semantic secure

(c) $Enc_{pk}(m_1) = (g^b, m_1 g^{ab})$

$Enc_{pk}(m_2) = (g^b, m_2 g^{ab})$

we just multiply them and we will get $(g^{2b}, m_1 m_2 g^{a(2b)})$, which is an encryption cipher text of 2b

2. G generated by g is a subgroup of Z_p

   for m_0 and m_1 , where $m_1 \notin \{m_0 g^i | 0 \leq i < q\}$

   we can define such a Function F to identify whether a encrypted msg is produced from m_0 or m_1

   F takes $m_x g^{ab}$ from $(g^b, m_x g^{ab})$

   and see if there is a i so that $m_x g^{ab} = m_0 g^i$ (we can use babystep-giantstep here, and if q is small enough, this step runs in acceptable time.)

   if there is such i, output m_0 , else, output m_1

   This F is always going to win.