Johns Hopkins ■ CS600.424: Network Security ■ Spring 2012

Homework 6 – Assignment

Due Date – May 4 in class

Instructions: Please do not submit handwritten assignment.

1. Use Fermat's Theorem to find

   $(a) 3^{201} \bmod 11$

   $(b)\, a$ number x between 0 and 28 with $x^{85} \equiv 6 \bmod ulo\, 29$

2. (a) Determine $\Phi(n)$ for (a) n= 41, (b) 27, (c) 231 and (d) 440

   (b) Find primitive roots of 25.

   (c) Given 2 as the primitive root 0f 29, construct a table of discrete logarithms, and use it to solve the congruence $17x^2 \equiv 10 (\bmod 29)$

3. Users A and B use the Diffie-Hellman key exchange technique with a common prime q=71 and a primitive root α=7.

   (a) If user has A has private key X_A=5, what is A's public key Y_A?

   (b) If user B has the private key X_B=12, what is B's public key Y_B?

   (c) What is the shared secret key?

4. Consider a Diffie-Hellman scheme with a common prime q=11 and a primitive root α=2.

   (a) Show that 2 is the primitive root of 11

   (b) If user A has public key Y_A=9, What is A's private key X_A?

   (c) If user B has a public key Y_B=3, what is the secret key K shared with A?

5. Consider ElGamal scheme with a common prime q=71 and a primitive root α=7.

   (a) If user B has a public key Y_B = 3, and A chose the random integer k = 2, what is the ciphertext of M = 30?

   (b) If A now chooses a different value of k so that the encoding of M =30 is C = (59, C_2), what is the integer C_2?