MATH 195: CRYPTOGRAPHY
HOMEWORK #13

Problem 6.20(a). *Suppose the ElGamal system is used with* $G = \mathbb{F}_{71}^*$, $g = 7$, *public key* $g^b = 3$ *and random integer* $a = 2$. *What is the cipher text of message* $x = 30$*?*

Problem 6.27. *Suppose the Diffie-Hellman method is used with group* $G = \mathbb{F}_{32}^*$ *(where* $\mathbb{F}_{32} = \mathbb{F}_2[X]/(X^5 + X^2 + 1)$*), primitive root* $g = X + 1 = 00011$, *and with secret exponents* $a = 8$ *(*X_A*),* $b = 12$ *(*X_B*). What is the common secret key* h *(*K*) that is exchanged?*

Problem 7.18. *Let* G, g *be as in Problem* 6.27. *Use the baby step-giant step method to compute* $\log_g(10101)$.

Problem 7.19. *Let* $G = \mathbb{F}_{131}^*$, *with primitive root* $g = 2$. *Use the Pohlig-Hellman method with* $m = 10 \cdot 13$ *(or* $13 \cdot 10$*) to find* $\log_2 3$.

Date: April 30, 2002.
6.20(a), 6.27, 7.18, 7.19.