October 29, 2004

Math 65S
Cryptography and Society
Assignment 6

Due: Friday, November 5, 2004.

Journal: Write a one-page (12 pt, single-spaced) explication of the sixth chapter (*Alice and Bob Go Public*) of Singh's book, with emphasis on the process of discovery and impact of public-key cryptography and secure key-exchange.

1. Problems 13, 14, p. 65 in Beutelspacher

2. Solve each of the following congruences for x:

(i) $5^x \equiv 2 \pmod{23}$
(ii) $10^x \equiv 13 \pmod{23}$
(iii) $38x \equiv 7 \pmod{2317}$
(iv) $1673x \equiv 7 \pmod{2317}$ (*Warning:* 1673 is not invertible mod 2317.)
(v) $37x \equiv 1 \pmod{330}$

3. Bob and Alice communicate using the Pohlig-Hellman cipher. They agree on the prime $p = 331$ and using, say, Diffie-Hellman key exchange, generate the key $K = 37$. Bob wants to send a plaintext message unit P to Alice, so he computes $P^{37} \bmod 331$ and gets 103. Alice receives 103 from Bob. What was Bob's message P?