Sample Test 2006

CRYPTOGRAPHY (CS402)

Time allowed: *one* hour.
Answer *four* questions.

1. Find $3^{20} \bmod 7$.

2. You intercept the following ciphertext

   SKPNPNBSVNS

   which was encrypted using the affine encryption function

   $$y \equiv 5x + 1 \mod 26.$$

   Recover the plaintext.

3. Find $\varphi(5096)$.

4. Suppose that the 27-symbol alphabet A-Z␣ is used for all plaintext and ciphertext messages in an RSA cryptosystem. Suppose also that plaintext message units are length 2 and ciphertext units are length 3. A user `A` has public key (1189, 3).

   (i) Encrypt for transmission to `A` the message

   NEW␣TEST

   (ii) Break this RSA cryptosystem by factorizing n.