September 23, 2003

Math 65S
Cryptography and Society
Assignment 4

Due: Wednesday, September 29, 2003.

Journal: Write a one-page (12 pt, single-spaced) explication of the third chapter of Singh's book. Summarize what you feel are the major points made about the nature and use of cryptography.

1. Decrypt the passage sent to you by email which was encrypted with Vigenère. You may use the Maple commands defined in the Maple worksheet, available on the class website.

2. Decrypt the following passage

```
HGIGLGGIYKFGWHLQYNHEQTWHQXXWEXQN
DGXSYWQTFYLNGSUFHYLETYDYLKHFQTUJ
LEIWCFEEXOELMHEWYZRSHOFGHMKXGGIY
KNQNETFYLCEIPSHYLOGWSPHEFYLELGHX
YGWHSTHQXIWGIYKFYGLNHFGHHFYLYCEL
NQTNSWHLKOGWPXGTTQTUHEWSYQTHYLTY
HJQXYWOGPPYLWXGWHIETHFIWGIYKELNY
LYNMKXGHENYXYHYHFYWEJHOGLYWFYSWY
NHENEOTXEGNPEPSXGLWETUWOQHFESHPG
KQTUJELHFYIRSHQTHFYQLNYRGHYGRESH
ETXQTYWFGLQTUGTNWHYGXQTUIWGIYKWE
IYHQIYWJYYXWIELYCETJSWYNHFGTCETJ
QNYTH
```

which was encrypted using an affine cipher.

3. We derived in class the congruence (*Fermat's little Theorem*)

$$a^p \equiv a \pmod{p},$$

valid for any integer a and prime p, and concluded further that if $(a, p) = 1$ then

$$a^{p-1} \equiv 1 \pmod{p}.$$

This theorem can be used to compute many other powers of a mod p. Remember the *Rule for Exponents* (no modular arithmetic yet!):

$$a^{dq+r} = (a^d)^q \cdot a^r$$

Now suppose $(a, p) = 1$ and p is prime. Use Fermat's Little Theorem and the rule for exponents to derive the congruence $a^{(p-1)q+r} \equiv a^r \pmod{p}$.

4. Use the congruence in 3. to compute the following:

(i) $5^{100} \bmod 7$
(ii) $3^{999999999} \bmod 7$
(iii) $6^{2000} \bmod 11$