September 8, 2004

Math 65S
Cryptography and Society
Assignment 3

Due: Wednesday, September 15, 2004.

1. Express 241, 187 and 511 in binary form. Express $(101011101)_2$, $(10101)_2$ and $(11111111)_2$ in decimal form.

2. Use the method of successive squaring to compute

(i) 5^{13} mod 23
(ii) 2^{32} mod 50
(iii) 53^{19} mod 47

3. Let $\mathbb{Z}/15$ denote the set of congruence classes (buckets) mod 15. Which $\bar{x}$ in $\mathbb{Z}/15$ have a multiplicative inverse? For each such $\bar{x}$, find the inverse.

4. For each of the following pairs of integers x, y

(i) 15, 35
(ii) 0, 111
(iii) -12, 18
(iv) 99, 100
(v) 19, 26
(vi) -27, -45
(vii) 233, 144

find integers a, b such that $ax + by = \gcd(x, y)$.

5. It is not true that integers a, b such that $ax + by = \gcd(x, y)$ are unique. For each of your answers a, b in 3., find a different pair a', b' such that $a'x + b'y = \gcd(x, y)$.

6. Let a and b be given integers. We have seen that, in order for $E(\bar{p}) = \bar{a}\bar{p} + \bar{b}$ to be an encryption function, a must be relatively prime to 26. How many different such encryption functions are there? Be sure to explain your reasoning.

7. Cryptographers commonly try to make a cryptosystem stronger by combining (composing, in mathematical terminology) two encryption functions. This procedure is called *super-encipherment*. For instance, in Cryptosurvivor Team P combined a shift cipher with a transposition cipher. Suppose you combine two affine ciphers, say $E_1(\bar{p}) = \bar{a_1}\bar{p} + \bar{b_1}$

with $E_2(\bar{p}) = \bar{a_2}\bar{p} + \bar{b_2}$. Then the super-encipherment has encryption function $E(\bar{p}) := E_2(E_1(\bar{p}))$. Find a formula for E. What is its advantage over a single affine encipherment?

8. An affine cipher is monoalphabetic: the encryption function defines a one-to-one correspondence between plaintext letters and ciphertext letters. Moreover, this encryption function has a specific form. Alternatively, we could choose a random (but still monoalphabetic) one-to-one correspondence between plaintext letters and ciphertext letters as our encryption function. Briefly discuss the advantages and disadvantages of this sort of cryptosystem over an affine cipher, from both the user's and cryptanalyst's point of view.

9. An affine cipher was used to produce the following ciphertext

```
USLELJUTCCYRTPSURKLTYGGFVELYUS
LRYXDJURTUULVCUURJRKQLLQLYXSRV
CYREKLVEXBRYZDGHRGUSLJLLMLYPDJ
LJTJUFALGUPTGVTJULYUSLDALTJRWU
SLJFEOLPU
```

Decrypt it. (Explain all your steps.)