**CS355: Cryptography** **Fall 2005**

# Homework #2

**Due date & time:** 10:30am on September 30, 2005. Hand in at the beginning of class (preferred), or email to the TA (wangq@purdue.edu) by the due time.

**The Late Policy and Additional Instructions for HW1 still apply. Ask for clarifications if you have questions about them.**

**Problem 1 (5 pts)** Exercise 19 in Section 2.13 of the textbook (On page 57).

**Problem 2 (5 pts)** Exercise 20 in Section 2.13 of the textbook (On page 57).

**Problem 3 (5 pts)** Exercise 11 in Section 3.13 of the textbook (On page 105).

**Problem 4 (10 pts)** Exercise 15 in Section 3.13 of the textbook (On page 105).

**Problem 5 (15 pts)** Exercise 16 in Section 3.13 of the textbook (on pages 105–106).

**Problem 6 (5 pts)** Calculate $\phi(64)$, $\phi(100)$, and $\phi(120)$.

**Problem 7 (15 pts)** Exercise 17 in Section 3.13 of the textbook (On page 106).

**Problem 8 (15 pts)** Exercise 20 in Section 3.13 of the textbook (On pages 106 – 107).

**Problem 9 (10 pts)** Let $a$ be a positive integer whose base-10 representation is $a = (a_{k-1} \cdots a_1 a_0)_{10}$. Let $b$ be the sum of the decimal digits of a; that is, let $b := a_0 + a_1 + \cdots + a_{k-1}$. Show that $a \equiv b \pmod 9$. From this, justify the usual "rules of thumb" for determining divisibility by 9 and 3: a is divisible by 9 (respectively, 3) if and only if the sum of the decimal digits of $a$ is divisible by 9 (respectively, 3).

**Problem 10 (15 pts)** We now describe a variation of the RC4 stream cipher, which instead of working with bytes, uses 2-bit blocks. The internal state `S` has 8 bits, and is maintained as 4 blocks of 2 bits each: `S[0],S[1],S[2],S[3]`. The initialization process divides the key into blocks of 2 bits each and stores them in `K[0],K[1],K[2],K[3]`. It then does the following:

```
for i:=0 to 3 do
    S[i] := i;
end for
j := 0;
for i:=0 to 3 do
    j := (j + S[i] + K[i mod L]) mod 4;
    swap (S[i], S[j]);
end for
```

**a.** Given the initial key such that `K[0]=3`, `K[1]=2`, `K[2]=3`, `K[3]=1`. What is the internal state in `S`, i.e., what are the values of `S[0], S[1], S[2], S[3]`.

**b.** Write out the algorithm that outputs the two-bit sequences to be used in encryption.

More on the back. Turn Over.

**c.** Give the first 8 blocks of outputs.

**d.** What is the number of possible internal states in the above cipher?

**e.** What is the number of possible internal states in the actual RC4 cipher?