

Homework 5

CS 460
Fall 2007
Craig A. Rich

- 1] Let p be a prime number and k be a positive number. Find an expression for $\phi(p^k)$ in terms of p and k , i.e., complete the statement of the following theorem and prove it:

Theorem. $\phi(p^k) =$

- 2] Corollary G.2.3 states that if n is a positive number and $e, d \in Z_{\phi(n)}^*$ such that $e \cdot d \equiv 1 \pmod{\phi(n)}$ and $X \in Z_n$, then $X^{e \cdot d} \pmod{n} = X$. Show that Corollary G.2.3 (as I stated it) is not true by finding n, e, d, X which satisfy the conditions of Corollary G.2.3, but do not satisfy $X^{e \cdot d} \pmod{n} = X$. Hint: consider how Corollary G.2.2 was misapplied in my proof of Corollary G.2.3.

- 3] Compute $106^{107} \pmod{11}$ without using a calculator. Show all work.

- 4] Compute the discrete inverse of 21 in Z_{100}^* without using a calculator. Show all work.

- 5] Generate public and private PGP keys using the GNU Privacy Guard (gpg), export your public key and e-mail it to `carich@csupomona.edu`:

```
% gpg --gen-key  
% gpg --armor --export
```

I will use your public key to encrypt a plaintext message and send the ciphertext to the e-mail address contained in your public key. You should recover the plaintext message, sign it with your private key, encrypt it with my public PGP key (which will be attached to the message you receive) and e-mail the resulting message to me so I know that you have seen it.