

Homework is due at the *start of class*, on the date listed above. **Problems numbered G# need only be completed by graduate students.**

0. Read the posted handouts on algebra and discrete probability.
1. (a) Suppose  $a \in \mathbb{Z}_N^*$ , where  $N \geq 2$ . Show that  $a^{\Phi(N)} \equiv 1 \pmod{N}$ .  
(b) Suppose next that the integer  $a$  **does not** lie in  $\mathbb{Z}_N^*$ . Is it possible that  $a^{\Phi(N)} \equiv 1 \pmod{N}$ ?  
Justify your answer.
2. Consider private-key encryption, where each character of the plaintext is from the alphabet  $\{0, 1, \dots, m-1\}$  rather than  $\{0, 1\}$ . Derive an analog of the one-time pad, and prove that it is perfectly secure.
3. Stinson 2.1
4. Stinson 2.2
5. Stinson 2.4 – **PROBLEM WITHDRAWN**
- G1. Read Section 1.1.3 from Stinson.
- G2. Stinson 2.3, both [a] and [b].  
Note: on part [b], the probability of key  $(a, b)$  is  $\Pr[a]/26$ , NOT  $1/(26 \times \Pr[a])$ .