

ICS 134

Homework 2

Due at NOON, Tuesday February 13.
Submission by email to the TA: plaintext or PDF only.

1. Suppose we have an encryption function $E()$ for which the encryption speed grows linearly with the length of the key. The only way to break $E()$ is by brute-force, i.e., by trying all possible keys. Now, suppose that advances in technology make computers twice as fast. Both the good guys and the bad guys can get faster computers. Does this advance work to the advantage of the good guy? the bad guy? or does it make no difference? Explain your answer...
2. Show that in an abelian group $(G, @)$:
 - a) The identity element is unique (i.e., there is only one identity)
 - b) For each element, the inverse of an element must be unique
3.
 - a) Compute the inverse of 113 mod 209
 - b) What is $\phi(209)$?
 - c) What is $\phi(208)$?
4. We define a new hash function as:
 $H(\text{student}) = 12\text{-digit student ID number}$
 - a) How many random students would you need to together in order to have a 50% chance of at least two of them having the same $H(\text{student})$ value?
 - b) How many random students would you need to get together in order to have a 50% chance of at least two students having inverted student ID-s? Two student ID-s are “inverted” if one of them (from left to right) is the same as the other (from right to left).
For example, 82345058 and 85054328 are inverted.
5. Alice sends many blocks of ciphertext to Bob. She is using OFB mode. What happens if there is an error in a single block of ciphertext? (In other words, what would happen on Bob’s side?)
6. Suppose that Alice and Bob communicate over a noisy and lossy channel. Alice needs to send Bob many blocks of ciphertext (e.g., encrypted real-time sports simulcast). Some blocks of ciphertext can be damaged and/or lost. Assume that, for each ciphertext block that Alice sends to Bob, one of three things might happen:
 - 1) The block arrives intact
 - 2) The block is lost (no bits of it arrive at Bob)
 - 3) The block arrives but it is damaged (some or all bits are changed)Design a way for Alice to encrypt data such that Bob can detect lost and damaged blocks and recover blocks that are not lost or damaged.