

**Assignment 5**  
Computer Science 349  
Spring 2004

*Due: Start of class on Thursday March 4*

**Reading:** Stinson, Sections 2.4, 2.5

**Exercise 5.1. (Stinson 2.3a)**

Prove that the *Affine Cipher* achieves perfect secrecy if every key is used with equal probability  $1/312$ .

**Exercise 5.2. (Stinson 2.9)** Suppose  $X = \{a, b, c, d, e, \}$  has the following probability distribution;  $\Pr[a] = .32$ ,  $\Pr[b] = .23$ ,  $\Pr[c] = .20$ ,  $\Pr[d] = .15$ , and  $\Pr[e] = .10$ . Use Huffman's algorithm to find the optimal prefix-free encoding of  $X$ . Compare the length of this encoding to  $H(X)$ .

**Exercise 5.3.** Sending encrypted mail may keep the contents a secret, but in certain quarters it will raise red flags. Sometimes, knowledge that a communication took place at all, independent of its contents, is a problem. One possible solution is to send the message to everyone (and hence no one in particular), but in such a form that everyone but the intended recipient ignores it. David McKellar created a grammar that encodes messages in Spam-like phrases removed from his collection of Spam messages. You can see it in action at <http://www.spammimic.com>.

The CS349-Spr04 course conference has been spammed. The messages reads

Dear Friend , This letter was specially selected to be sent to you . This is a one time mailing there is no need to request removal if you won't want any more ! This mail is being sent in compliance with Senate bill 1618 ; Title 6 ; Section 304 ! This is NOT unsolicited bulk mail . Why work for somebody else when you can become rich in 38 days ! Have you ever noticed society seems to be moving faster and faster and more people than ever are surfing the web ! Well, now is your chance to capitalize on this ! WE will help YOU use credit cards on your website and turn your business into an E-BUSINESS . You are guaranteed to succeed because we take all the risk . But don't believe us . Mrs Ames of Nevada tried us and says "I was skeptical but it worked for me" . We assure you that we operate within all applicable laws . Because the Internet operates on "Internet time" you must act now . Sign up a friend and your friend will be rich too . Cheers . Dear Internet user ; Thank-you for your interest in our letter . If you no longer wish to receive our publications simply

reply with a Subject: of "REMOVE" and you will immediately be removed from our club ! This mail is being sent in compliance with Senate bill 1625 , Title 9 ; Section 304 ! This is not a get rich scheme ! Why work for somebody else when you can become rich within 46 weeks . Have you ever noticed people are much more likely to BUY with a credit card than cash plus people will do almost anything to avoid mailing their bills . Well, now is your chance to capitalize on this ! WE will help YOU deliver goods right to the customer's doorstep & SELL MORE . You can begin at absolutely no cost to you ! But don't believe us . Mrs Jones of New Jersey tried us and says "Now I'm rich, Rich, RICH" ! We assure you that we operate within all applicable laws ! We beseech you - act now ! Sign up a friend and you'll get a discount of 10% ! God Bless .

What does it really say? What is special about the plaintext?

**Exercise 5.4. (Stinson 2.10; Extra Credit)** Prove that  $H(\mathbf{X}, \mathbf{Y}) = H(\mathbf{Y}) + H(\mathbf{X} | \mathbf{Y})$ . Then show as a corollary that  $H(\mathbf{X} | \mathbf{Y}) \leq H(\mathbf{X})$ , with equality if and only if  $\mathbf{X}$  and  $\mathbf{Y}$  are independent.

**Exercise 5.5. (Stinson 2.11)** Prove that a cryptosystem has perfect secrecy if and only if  $H(\mathbf{P} | \mathbf{C}) = H(\mathbf{P})$ .

**Exercise 5.6. (Stinson 2.12)** Prove that, in any cryptosystem,  $H(\mathbf{K} | \mathbf{C}) \geq H(\mathbf{P} | \mathbf{C})$ . (Intuitively, this result says that, given a ciphertext, the opponent's uncertainty about the key is at least as great as his uncertainty about the plaintext.)

**Exercise 5.3. (Stinson 2.14)** Compute  $H(\mathbf{K} | \mathbf{C})$  and  $H(\mathbf{K} | \mathbf{P}, \mathbf{C})$  for the *Affine Cipher*. Interpret your results.