Homework #1

UC Davis Students: Due April 14, 1997 at 11:59PM
NTU Students: Due April 21, 1997 at 11:59PM

1. (*40 points*) The entropy function $H(p_1, \ldots, p_n)$ must satisfy several properties, including the following (for which we assume $p_1 + \ldots + p_n = 1$):
   a. $H(p_1, \ldots, p_n)$ is a maximum when $p_1 = \ldots = p_n = 1/n$.
   b. For any permutation π of $(1, 2, \ldots, n)$, $H(p_1, \ldots, p_n) = H(p_{\pi(1)}, \ldots, p_{\pi(n)})$. In other words, H must be a symmetric function of the arguments $p_1, \ldots, p_n$.
   c. $H(p_1, \ldots, p_n) \geq 0$ and equals 0 only when one of the $p_i = 1$.
   d. $H(p_1, \ldots, p_n, 0) = H(p_1, \ldots, p_n)$.
   e. $H(\frac{1}{n}, \ldots, \frac{1}{n}) \leq H(\frac{1}{n+1}, \ldots, \frac{1}{n+1})$
   f. If m and n are positive integers, then $H(\frac{1}{mn}, \ldots, \frac{1}{mn}) = H(\frac{1}{m}, \ldots, \frac{1}{m}) + H(\frac{1}{n}, \ldots, \frac{1}{n})$ ..
   g. Let $p = p_1 + \ldots + p_m$ and $q = q_1 + \ldots + q_n$, where each p_i and q_j are non-negative; then, if p and q are positive, with $p + q = 1$, we must have
   $$H(p_1, \ldots, p_m, q_1, \ldots, q_n) = H(p, q) + pH(\frac{p_1}{p}, \ldots, \frac{p_m}{p}) + qH(\frac{q_1}{q}, \ldots, \frac{q_n}{q}) \quad .$$

   Please prove that the function $H(p_1, \ldots, p_n) = -\lambda\Sigma_k\, p_k \lg p_k$ (where the sum is over those k for which $p_k > 0$) meets these conditions.
2. (*20 points*)Let X be an integer variable represented with 32 bits. Suppose that the probability is 1/2 that X lies in the range $[0, 2^8-1]$ with all such values being equally likely, and 1/2 that X lies in the range $[2^8, 2^{32}-1]$, with all such values being equally likely. Please compute $H(X)$.
3. (*10 points*)Consider the following ciphertests:

   ```
   VZXYW
   ACRYZ
   QWERT
   ZZZZZ
   ```

   Which of these ciphertexts could result from enciphering five-letter words of English using:
   a. A substitution cipher, where each letter is replaced with some other letter, but the letters are not necessarily shifted as in the Caesar cipher (thus A could be replaced with X, B with U, *etc.*)?
   b. Any transposition cipher?
4. (*10 points*) Let n be a composite number. Please show there are integers x and y such that $xy \bmod n = 0$, but neither x nor y is 0 mod n. (This proves the cancellation law does not hold over the integers mod n with multiplication.)
5. (*40 points*) The following was enciphered with a Vigènere cipher. Please break it.

   ```
   TSMVM MPPCW CZUGX HPECP RFAUE IOBQW PPIMS
   FXIPC TSQPK SZNUL OPACR DDPKT SLVFW ELTKR
   GHIZS FNIDF ARMUE NOSKR GDIPH WSGVL EDMCM
   SMWKP IYOJS TLVFA HPBJI RAQIW HLDGA IYOUX
   ```

6. (*20 points*) Please determine the unicity distance of ciphers based on the affine transformation
   $$f(x) = (ax + b) \bmod 26$$
   assuming the keys a and b both generate complete sets of residues and that all such keys are equally likely.

7. (*10 points*) The ciphertext TKCXJ YMRES ATKMZ came from a message enciphered using the Playfair cipher with the following key:

```
I E N S B
R Y T O K
C P G A H
D F L M Q
U V W X Z
```

   Please decipher the ciphertext.

8. (*20 points*) If you are given two Playfair ciphers P_1 and P_2 which are applied one after the other to a string of text T, *i.e.*, $P_2(P_1(T))$, do you have a cipher which is more secure than using only P_1 or only P_2?

9. (*10 points*) Please compute the following:
   a. $2^{123}3^{456}5^{789}$ mod 4;
   b. 6^{512} mod 15

10. (*15 points*) Solve the following problems for x in the range $[0, n–1]$:
    a. $1234x$ mod $10001 = 1$
    b. $23x$ mod $57 = 1$
    c. $17x$ mod $100 = 10$.

11. (*5 points*) Find all solutions to the equation $15x$ mod $25 = 10$ in the range [0, 24].

Extra Credit

12. Given the additional requirement that $H(p_1, \ldots, p_n)$ is a continuous function of its arguments, prove that the *only* function meeting all these requirements is $H(p_1, \ldots, p_n) = -\lambda \Sigma_k \, p_k \lg p_k$ with λ any positive constant and where the sum is over those k for which $p_k > 0$.

13. Write a program to break a Caesar cipher automatically, assuming the plaintext is English. You may use any reasonable model of English (either single letter counts, *n*-gram counts, or a Markov model).