1ST MIDTERM, MATH 587/CSCE 557 - FEBRUARY 13, 2007

Nigel Boston

Answer all four questions below. Show your working. Full credit will not be given for just the answer without any justification. Make sure you answer each part of each question.

1. (a) How many keys are there for (i) shift ciphers, (ii) affine ciphers, (iii) general substitution ciphers, (iv) Viginere ciphers where the keyword has length 3?

Answers: (i) 26, (ii) 312, (iii) 26!, (iv) 26^3.

(b) An affine cipher has encryption function $e_k(x) = 3x + 1 \pmod{26}$. What is its decryption function?

Answers: suppose $d_k(x) = cx + d \pmod{26}$. Then $c(3x + 1) + d = x \pmod{26}$ implies $3c = 1$ and $c + d = 0 \pmod{26}$. Thus $c = 9$ and $d = -9 = 17$, so $d_k(x) = 9x + 17 \pmod{26}$.

2. (a) The ciphertext DRZNUO was produced by using a Vigenere cipher with keyword BABY. What is the blocklength of the cipher? What is the plaintext?

Answers: The blocklength is 4. Subtracting BABYBA (i.e. 1,0,1,-2,1,0) from DRZNUO gives CRYPTO.

(b) Encrypt BABY using the Hill cipher with key $\begin{pmatrix} 3 & 2 \\ 13 & 9 \end{pmatrix}$. What is the decrypting key?

Answers: BA encrypts as $3*1+2*0=3, 13*1+9*0=13$, i.e. DN. BY encrypts as $3*1+2*(-2)=-1, 13*1+9*(-2)=-5$, i.e. ZV. So DNZV. Since $3*9-2*13=1 \pmod{26}$, the decrypting key is $\begin{pmatrix} 9 & -2 \\ -13 & 3 \end{pmatrix}$

3. What are the three kinds of attack you have met so far? Define each one. Suppose we have an affine cipher and we know how A and B are encrypted - show that this is enough to find the key. Suppose that instead we only know how A and C are encrypted - show that this is not enough to find the key uniquely [hint: say A is encrypted as B and C encrypted as D - what two possible keys are there?]

Answers: Chosen-plaintext attack (you can obtain the output for any input you wish); known-plaintext attack (you know some input/output pairs); ciphertext-only attack (you just have some outputs). Suppose $e_k(x) = ax+b \pmod{26}$. If we know $e_k(0)$, i.e. b, and $e_k(1)$, i.e. $a+b$, then we can find a and b, so knowing how A and B are encrypted determines $e_k(x)$. On the other hand, if we know $e_k(0)$ and $e_k(2)$, say $e_k(0) = 1$ and $e_k(2) = 3$, then $e_k(x)$ could be $x+1$ or $14x+1$. (In fact the latter is not an acceptable key and since the $2a$ for $a \in \mathbf{Z}_{26}^*$ are all distinct, you can actually solve for a after all! Did anybody get that?)

4. Describe briefly how frequency analysis is used to break a monoalphabetic cipher. In particular, which of the three kinds of attack is this used for? The most commonly used letters in English are E and then T. The ciphertext PDAPAOP was produced using a shift cipher. Using frequency analysis find the plaintext (which should make sense in English).

Answers: In frequency analysis we see which letters occur most frequently in the ciphertext and guess that the most common letter stands for E, the 2nd most common for T, and so on. If that does not yield a sensible plaintext, then we try other guesses, such as that the most common letter stands for T. We keep going until we obtain a sensible decryption. Thus, this applies in a ciphertext-only attack. In the given ciphertext, the most common letter is P. If we assume this stands for E, then decrypting is shifting by -11=15 and PDAPAOP yields ESPEPDE, which does not make sense. Supposing P stands for T, decrypting is shifting by 4 and PDAPAOP yields THETEST, i.e. with a space inserted, THE TEST.