Problem Set 1

Christopher Seaman

2007-09-12

1

1.1 You obtain a string of characters from some alphabet. (An alphabet could be some letters - or symbols – or zeros and ones.) What steps would you take to see if the intercept was encrypted by a mono-alphabetic substitution method? Apply your answer to the ciphertext in the fifth problem on this set.

Mono-alphabetic substitutions are susceptible to attack through frequency analysis. To see if the intercept was encrypted using a mono-alphabetic cipher we should compare the symbol histograms from the intercept to those of other works in the alphabet. We could try assigning a map by the popularity rank of each letter (map most frequent ciphertext letter to most frequent plaintext letter) or finding the map that gives the smallest distance between the two frequency distributions by treating them as vectors.

1.2 You obtain a string of characters from some alphabet. What steps would you take to see if the intercept was encrypted? (This is a very hard question.)

Test for mono-alphabetic ciphers as above. Test for poly-alphabetic ciphers by breaking the intercept up mod n and performing n mono-alphabetic frequency comparisons. The intercept would obviously be encrypted if it were to have header information describing the type of cipher used. Apart from that, use statistical tests to compare the intercept with noise. Some symbols may appear more often than would likely occur by chance, or symbols may appear consecutively more often than would liekly occur by chance.

2

2.1 Solve for x: $5^x \equiv 7 \mod 65537$

Using the Baby-Step, Giant-Step algorithm (code attached): $5^{(217*257)+108} = 5^{55877} \equiv 7 \mod 65537$

2.2 Find, with proof, all n such that $\phi(n)|3n$

$$n = \Pi p_i^{\alpha_i}$$

$$\phi(n) = \Pi\phi(p_i^{\alpha_i}) = \Pi(p_i - 1)p_i^{\alpha_i - 1}$$

Suppose that $\phi(n)|3n$:

$$\Pi(p_i - 1)p_i^{\alpha_i-1}|3 \cdot \Pi p_i^{\alpha_i}$$

$$\Rightarrow \Pi(p_i - 1)|3 \cdot \Pi p_i$$

So $(p_i - 1)$ divides either 3 or some p_i. Any prime greater than 3 won't work because $(p_i - 1)$ would be non-prime and even, so it wouldn't divide any p_i on the right-hand side of the equation. $p_i = 2$ always works because (2 - 1) = 1 and 1 divides everything. $p_i = 3$ can work if there is a $p_j = 2$ because 3 - 1 = 2.

$$\therefore \phi(n) | 3n \text{ for } n = 2^a \cdot 3^b$$

$$a \geq 1, b \geq 0$$

2.3 Find x, y, z such that $35x + 55y + 77z = 1$

using the modulus to generate relations:

$$35x + 55y + 77z \equiv 35x \equiv 2x \equiv 1 \mod 11$$
$$35x + 55y + 77z \equiv 55y \equiv 6y \equiv 1 \mod 7$$
$$35x + 55y + 77z \equiv 77z \equiv 2z \equiv 1 \mod 5$$

Finding inverses for the coefficients gives us:

$$x = 6 \mod 11 \Rightarrow x = 11a + 6$$

$$y = 6 \mod 7 \Rightarrow y = 7b + 6$$

$$z = 3 \mod 5 \Rightarrow z = 5c + 3$$

so in linear algebra terms:

$$1 = \begin{pmatrix} 35 & 55 & 77 \end{pmatrix} \begin{pmatrix} x \\ y \\ z \end{pmatrix} = \begin{pmatrix} 35 & 55 & 77 \end{pmatrix} \begin{pmatrix} 6 + 11a \\ 6 + 7b \\ 3 + 5c \end{pmatrix}$$

$$1 = \begin{pmatrix} 35 & 55 & 77 \end{pmatrix} \left[\begin{pmatrix} 6 \\ 6 \\ 3 \end{pmatrix} + \begin{pmatrix} 11a \\ 7b \\ 5c \end{pmatrix} \right] = 771 + 385(a + b + c)$$

$$-2 = a + b + c$$

For simplicity's sake set $a = -2, b = c = 0$. This give $x = 6 - 22 = -16, y = 6, z = 3$

$$35x + 55y + 77z = 35(-16) + 55(6) + 77(3) = 1$$

3 The rand() function gives consecutive values of 1, 2, and 3. What is the next value?

Given $x_1 = 1, x_2 = 2, x_3 = 3$. We know that the rand() function is a linear congruential generator, so we have some relations:

$$x_3 = A \cdot x_2 + B = 2 \cdot A + B \equiv 3 \mod n$$
$$x_2 = A \cdot x_1 + B = 1 \cdot A + B \equiv 2 \mod n$$
$$(x_3 - x_2) = (x_2 \cdot A + B) - (x_1 \cdot A + B) \equiv 3 - 2 \mod n$$
$$\Rightarrow (x_3 - x_2) = (x_2 - x_1) \cdot A = 1 \cdot A \equiv 1 \mod n$$

Noting that 1^{-1} is 1, this gives us $A \equiv 1 \mod n$. Plugging in to x_2 or x_3 gives us $B = 1$. Thus:

$$x_{i+1} = A \cdot x_i + 1 \mod n$$

$$x_4 = 1 \cdot 3 + 1 = 4$$

(really?)

4 The Diffie-Hellman key agreement protocol that we have discussed in class employs powers of a primitive root. Suppose that you were not allowed to use a base value (g) that was a primitive root. Redesign the protocol to make it work (if that is at all necessary) and discuss how to choose your (non-primitive) g and why you would do it this way – and quantify the security change in doing so.

The strength of the Diffie-Hellman protocol depends on the size of the group generated by g in the mutiplicative group G. When g is a primitive root, the group generated by g is the entire multiplicative group since primitive roots are generators of cyclic groups. For a non-primitive g', the powers of g' generate a subgroup of the multiplicative group. From Lagrange's theorem we know that the order of the subgroup divides the order of the entire group, $|G|$, thus the space of the group covered by powers of the non-primitive is $\frac{|G|}{n}$ for some integer $n = [< g' >: G]$. We can bound n, as $2 \leq n \leq \frac{|G|}{2}$ In this way, using a non-primitive leaves you $\frac{1}{n}$th as secure as using a primitive root.

5 Recover the plaintext from the following ciphertext:

To crack the cipher I treated the percentage frequencies of letters as vectors in $\mathbb{R}^{26}$. For each key length from 3 to 12 and for each position within that length key, I assigned a vector of percentage frequencies. Then, using the euclidean metric $d(a, b) = \Sigma(a_i - b_i)^2$, found the map for each position in the key with the minimum distance from the known-good frequency vector. In addition to giving me a mean distance for each key length (noting that this measure biases longer keys to shorter distances), this gave me a top-candidate map for each position in the key. The keys of length 6, 11, and 12 seemed good candidates - testing the key 'mzejbl' gave good results for most of the text (with one flub), but left the end of the text garbled. Inserting a spacer character just before the garble revealed the remaining text (one letter was skipped during the encryption).

mean distances and suggested keys for each length:
3: 0.0895741445761176 jel
4: 0.0816788887301825 ijbx
5: 0.0732026966033923 vbirm
6: 0.0565790835964783 mzejbl
7: 0.0610003814432948 mlmzpux
8: 0.0589581283859806 invvejbi
9: 0.0573040620261021 zzljelvbm
10: 0.0537237631567919 umirmxbiqj
11: 0.0484164238858958 dyeyfqmlekl
12: 0.047402670915008 zdfjblmmejbl
key: mzejbl

grim-visaged war hath soothed his [w]rinkled front and now instead of mounting barbed steeds to fright the souls of fearful adversaries he capers nimbly in a lady's chamber to the lascivious pleasing of a lute but i that am not shaped for sportive tricks nor made to court anamorous looking-glass i that am rudely stamped and want loves majesty to strut before a wanton ambling nymph i that am curtailed of this fair proportion cheated of feature by [d]issembling nature deformed unfinished sent before my time into this breathing world scarce half made up and that so lamely and unfashionable that dogs bark at me as i halt by them why i in this weak piping time of peace have no delight to pass away the time

6 A passage of prose was encrypted by a method presented in class. Break the cipher and recover the plaintext.

key: ANDSKOTTIN

For this problem I used the same method as in problem 5, additionally I noticed that the 10-length key (ANDSKOTTIN) and the 20-length key (AEDSKOTTINANDSKOTTIN) were strikingly similar. Noting that the 20-length key partitions the 10-key's letters into two sets, and that those sets need not be related for an incorrect key length (length of the test key not a multiple of proper key), it seemed likely that the 10-length key was correct. Also, checking for iceland words in the text yielded good results. I don't have a proper translation of the decrypted text, but I am reasonably confident that I do have the proper plaintext.

3: 0.0790533442717652 ÞNI

4: 0.0704049094123582 INAN

5: 0.0612859610246687 ATDSN

6: 0.0605801025365441 KNAÞAÉ

7: 0.0550641104822397 NÉYATAX

8: 0.0547953930400856 IÉTTÝNAÞ

9: 0.0503163506927287 TNMÝSÉJTT

10: 0.0459518674486886 ANDSKOTTIN

11: 0.0458065299614503 IÉSVTNNJAMF

12: 0.0477673715145068 UNAUÍSXNIOTÉ

13: 0.0479729082235253 FXGNOXJUNVJNÞ

14: 0.0464983496147282 IÉIYXYDVPYAÞAN

15: 0.0466610325456328 AIDJKAOUIKAJDSÉ

16: 0.0445278177396793 IÉTÝÝNÞXRSAÍYOAN

17: 0.0420857198523754 ONNIÞÓÉTVTNÉVÆITÐ

18: 0.0442024195545584 XNDÞÉÉJRATASUSANBÉ

19: 0.0421237156216871 VNÞNNOTNYAITAYIBNÉÁ

20: 0.0428028712197989 AEDSKOTTINANDSKOTTIN

21: 0.0414967095162893 KKOTÖTNNÉAFÉUSIÝSYUYM

plaintext:

IALLAFALLÞAÐVAREINUHVERJUSINNIAÐHÖSKULDURHAFÐIVI
NABOÐOGÞARVARHRÚTURBRÓÐIRHANSOGSATHIÐNÆSTAHONU
MHÖSKULDURÁTTISÉRDÓTTURERHALLGERÐURHÉTHÚNLÉKSÉ
RÁGÓLFIVIÐAÐRARMEYJARHÚNVARFRÍÐSÝNUMOGMIKILVEXT
IOGHÁRIÐSVOFAGURTSEMSILKIOGSVOMIKIÐAÐÞAÐTÓKOFAN
ÁBELTIHÖSKULDURKALLARÁHANAFARÞÚHINGAÐTILMÍNSAGÐ
IHANNHÚNGEKKÞEGARTILHANSHANNTÓKUNDIRHÖKUNAOGKY
SSTIHANASÍÐANGEKKHÚNÍBRAUTÞÁRÆDDIHÖSKULDURTILHR
ÚTSHVERSULÍSTÞÉRÁMEYÞESSAÞYKIRÞÉREIGIFÖGURVERAHRÚ
TURÞAGÐIVIÐHÖSKULDURTALAÐITILANNAÐSINNHRÚTURSVA
RAÐIÞÁÆRIÐFÖGURERMÆRSJÁOGMUNUMARGIRÞESSGJALDAEN
HITTVEITEGEIGIHVAÐANÞJÓFSAUGUERUKOMINÍÆTTIRVORAR