Tanner Krebs, Gerardo Lopez, William Thornton
Math 314
9/7/17

Assignment 1

Problem 1: In a symmetric cryptosystem, Alice and Bob both know the e-key and the d-key. The cryptosystem is assumed to have no weakness and Alice and Bob are the only persons that ever know the secret keys. Alice sends some message m to Bob. Is it possible for Bob to prove to a judge that he really has received m from Alice (in other words, does a symmetric cryptosystem offer non-repudiation)? Say YES or NO and give a short and clear explanation.

Solution: A symmetric cryptosystem does not offer non-repudiation, meaning it does not provide authenticity unless an encrypted mode of operation is used. The shared e-key and d-key does not provide integrity, a message can be sent by an attacker, the receiver will decrypt and accept without knowing who encrypted it and/or legitimacy of the sender.

Problem 2 Ex.3: Encrypt howareyou using the affine function 5x + 7 (mod 26). What is the decryption function? Check that it works.

- h $= 7 : 5 * 7 + 7 \equiv 42 \equiv 16(mod 26)$
- o $= 14 : 5 * 14 + 7 \equiv 77 \equiv 25(mod 26)$
- w $= 22 : 5 * 22 + 7 \equiv 117 \equiv 13(mod 26)$
- a $= 0 : 5 * 0 + 7 \equiv 7(mod 26)$
- r $= 17 : 5 * 17 + 7 \equiv 92 \equiv 14(mod 26)$
- e $= 4 : 5 * 4 + 7 \equiv 27 \equiv 1(mod 26)$
- y $= 24 : 5 * 24 + 7 \equiv 127 \equiv 23(mod 26)$
- o $= 14 : 5 * 14 + 7 \equiv 16(mod 26)$
- u $= 20 : 5 * 20 + 7 \equiv 107 \equiv 3(mod 26)$

The phrase ‘howareyou‘ is encrypted to ‘qznhobxqd‘ .. Next we must find the decryption function.

- $y \equiv 5x + 7(mod 26)$
- $x \equiv 21(y - 7) \equiv 21y + 9$

Using the decryption function we will test the first few letters to see if it is correct.

- q $= 16 : 21 * 16 + 9 \equiv 345 \equiv 7(mod 26)$
- o $= 14 : 21 * 25 + 9 \equiv 534 \equiv 14(mod 26)$
- w $= 22 : 21 * 13 + 9 \equiv 282 \equiv 22(mod 26)$

As expected the numbers (7,14,22) correspond to ‘how‘ the first letters of the plaintext proving the decryption function works.

Problem 2 Ex.4: Consider an affine cipher (mod 26). You do a chosen plaintext attack using hahaha. The ciphertext is NONONO. Determine the encryption function.

Considering the ciphertext ‘NONONO‘ Let, $mx + n$ be the encryption function.

- h $= 7$ and N $= 13$, use the equation $m * 7 + n \equiv 13(mod 26)$
- and using the second letter a $= 0$, O $= 14$ we get $m * 0 + n \equiv 14$
- $7m \equiv -1(mod 26)$
- $m = 11$
- So the decryption function is $11x + 14$

Problem 2 Ex.6: Suppose you encrypt using an affine cipher, then encrypt the encryption using another affine cipher (both are working mod 26). Is there any advantage to doing this, rather than using a single affine cipher? Why or why not?

To start, let's take a look at the function $y = ax + b$ (mod 26) and encrypt this with another function...let's say $z = cy+d$. Now, if we solved for

z, the equation would be as follows: $cy + d = c(ax + b) + d = (ac)x + (cb + d)$ (mod 26). We see that x is now mapped to only one affine function, as a result, there is NO advantage to using 2 affine ciphers.

Problem 2 Ex.7: Suppose we work mod 27 instead of mod 26 for affine ciphers. How many keys are possible? What if we work mod 29?

For (mod 27) we need (α,27) = 1 such that we exclude all multiples of 3. As a result, that leaves us with 18 choices for α and 27 for β. Therefore....Possible Keys = $\alpha(\beta) = 18(27) = 486$ possible keys.

For (mod 29) we must note that this is a prime number. As a result, that leaves us with 28 choices for α and 29 for β. Therefore....Possible Keys = $\alpha(\beta) = 28(29) = 812$ possible keys.

Problem 3: The following ciphertext was produced with an affine cipher. Decrypt it and explain how you did it. There are a number of software tools available on the web (for example to count the frequency of letters, to do modular arithmetic, etc.) You can use such tools but not one that automatically provides the plaintext. You can also write a short program that does brute-force search. In case you use internet tools, you need to say what tool you have used and still explain what steps you did. In case you write your own program, include the code (which should have sufficient comments).

SQJRU UBEJN BAQJW BHEPS QBEFT PWJSQ RERTP EPRIA RCJSB NHDCH SBSDS BPEHB ENJJR NQAIR BESJK SNQRW RNSJW BHTRA AJYSP PEIVP EJNBA QJWSJ KSNQR WRNSJ WRHRW JHDIS SQJHR TJSPP IHSQR SHPIO JYSQJ XJVZP WYNBA QJWNP DIYCJ RAAIB JYSPS QJRUU BEJNB AQJWS QJPEI VYBUU JWJEN JBHSQ RSSQJ XJVHD CHSBS DSBPE ARSSJ WEBHE PSCRH JYPER XJVZP WY

Solution: Using frequency analysis the letter J appeared 35 times, or 13.11 percent of the entire cipher text. The letter S appears 32 times or 11.99 percent of the entire cipher text. Using deductive reasoning we can say that either the letter J or S will map to the letter E. Going with proven statistical data I will make the first guess of mapping J to E and S to T because they are the two most recurring letters in the English language.