Matthew Austin

Principles of Cryptology

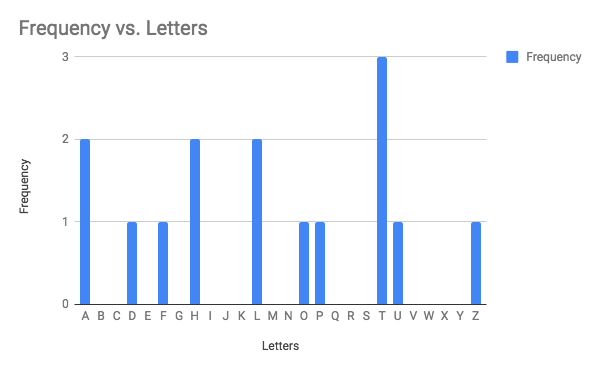
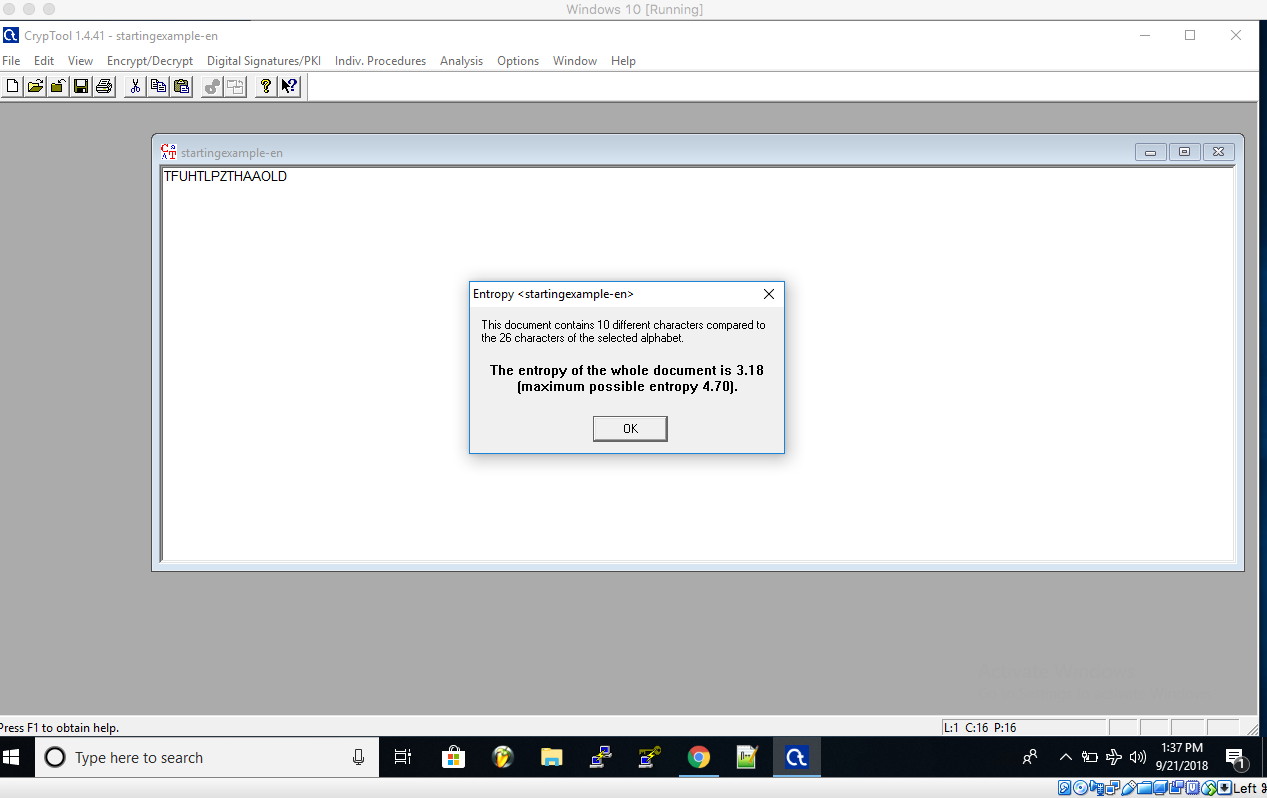
Anwar

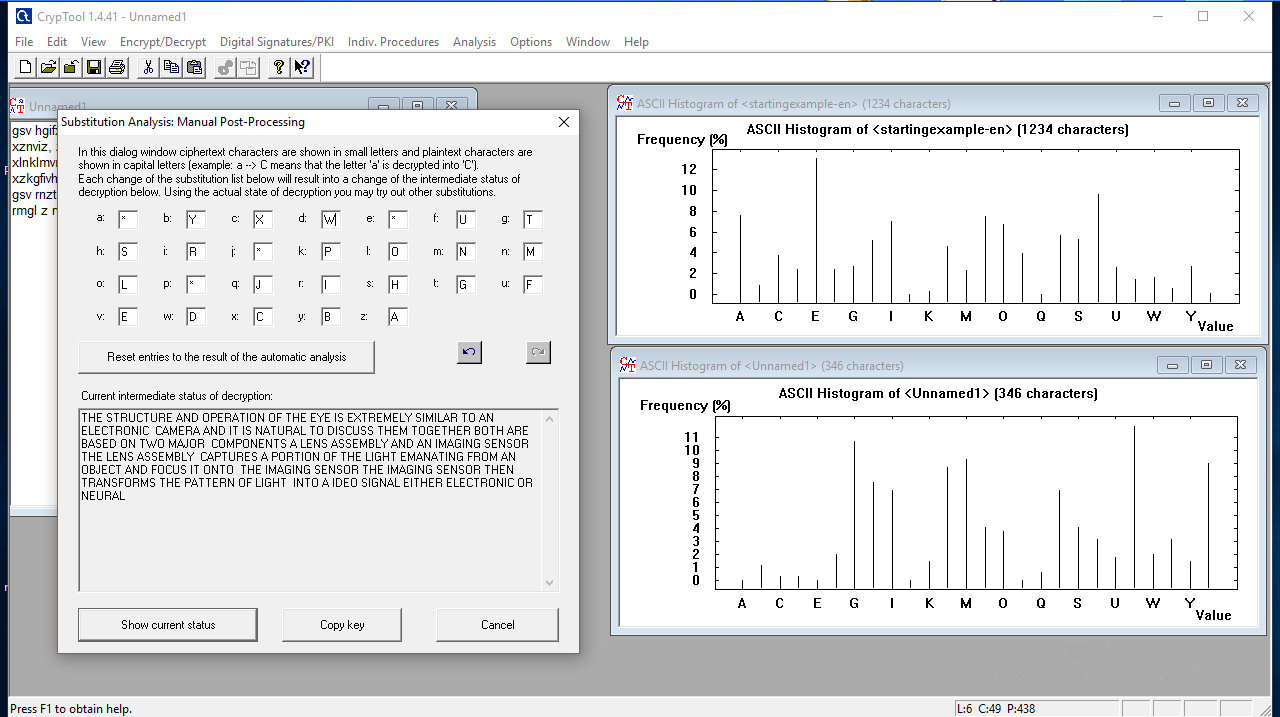
23 Sept 2018

HW1

1. Perform frequency analysis and entropy analysis using a spreadsheet on a small plaintext/ciphertext pair of your choosing. A sample procedure is provided [here](http://iccs.x10host.com/crypto/05classical/images/Class-Activity-Entropy.pdf). Then answer the following questions:
   * 1. Ceasar cipher: Shift 7
     2. PLAIN TEXT: MYNAMEISMATTHEW
     3. CIPHERTEXT: TFUHTLPZTHAAOLD

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Letters | Frequency | Probabilites | Entropy | English Entropy | Cross Entropy |
| A | 2 | 0.1333333333 | 0.3875854127 | 0.08167 | 7.228099924 |
| B |  | 0 | 0 | 0.01492 | 0 |
| C |  | 0 | 0 | 0.02782 | 0 |
| D | 1 | 0.06666666667 | 0.260459373 | 0.04253 | 4.555375335 |
| E |  | 0 | 0 | 0.12702 | 0 |
| F | 1 | 0.06666666667 | 0.260459373 | 0.02228 | 5.488106957 |
| G |  | 0 | 0 | 0.02015 | 0 |
| H | 2 | 0.1333333333 | 0.3875854127 | 0.06094 | 8.07293338 |
| I |  | 0 | 0 | 0.06966 | 0 |
| J |  | 0 | 0 | 0.00153 | 0 |
| K |  | 0 | 0 | 0.00772 | 0 |
| L | 2 | 0.1333333333 | 0.3875854127 | 0.04025 | 9.269734813 |
| M |  | 0 | 0 | 0.02406 | 0 |
| N |  | 0 | 0 | 0.06749 | 0 |
| O | 1 | 0.06666666667 | 0.260459373 | 0.07507 | 3.735619707 |
| P | 1 | 0.06666666667 | 0.260459373 | 0.01929 | 5.696003046 |
| Q |  | 0 | 0 | 0.00095 | 0 |
| R |  | 0 | 0 | 0.05987 | 0 |
| S |  | 0 | 0 | 0.06327 | 0 |
| T | 3 | 0.2 | 0.464385619 | 0.09056 | 10.39494669 |
| U | 1 | 0.06666666667 | 0.260459373 | 0.02758 | 5.180233733 |
| V |  | 0 | 0 | 0.00978 | 0 |
| W |  | 0 | 0 | 0.0236 | 0 |
| X |  | 0 | 0 | 0.0015 | 0 |
| Y |  | 0 | 0 | 0.01974 | 0 |
| Z | 1 | 0.06666666667 | 0.260459373 | 0.00074 | 10.40018711 |
|  | 15 |  | 3.189898095 |  | 2.693124642 |

* + 1. 
    2. 
  1. Compare the two results. Do you notice any difference in entropy? Why or what not?
     1. Yes there is a difference in entropy. My entropy compared to the English entropy is drastically lower, this is due to my text being such a short sample and lacking a larger amount of text and letters for more precise calculations.
  2. What would happen to the entropy if all of the frequencies were the same? Turn in your spreadsheet along with your assignment report.
     1. If my entropy was the same as the english entropy, then I would have need to have the same amount of letters and letter usage (it doesn’t have to be an exact copy). This would make decrypting ciphertexts much easier as the observations will be more accurate and precise with frequency analysis.

1. Research and describe in your own words an interesting brute-force attack conducted in the history of cryptography. Describe the hardware used, the algorithm targeted, the motivation, the repercussions etc. A good starting point is to look at the famous RSA challenge. Also, discuss whether you think quantum computers are a reality or a hype.
   1. A brute-force attack on Github in 2013 was the largest brute force attack in recent history. They used a simple brute force password guessing software to break into several accounts of weak passwords. The other hardware they used was from another attack that obtained the username and passwords to put into the dictionary.txt of their brute force software. The specific names of the software were not stated. Through research it seems that Github uses AES encryption but with the added information the attackers had the work required was drastically reduced. The motivation behind the attack was to access any repositories they could get their hands on. There weren't any repercussions because the attackers are still yet to be identified, but the trust towards Github as far as information security has reduced.
2. Perform cryptanalysis of the following text encrypted using the substitution cipher:
   1. **gsv hgifxgfiv zmw lkvizgrlm lu gsv vbv rh vcgivnvob hrnrozi gl zm vovxgilmrx   
      xznviz, zmw rg rh mzgfizo gl wrhxfhh gsvn gltvgsvi. ylgs ziv yzhvw lm gdl nzqli   
      xlnklmvmgh: z ovmh zhhvnyob, zmw zm rnztrmt hvmhli. gsv ovmh zhhvnyob   
      xzkgfivh z kligrlm lu gsv ortsg vnzmzgrmt uiln zm lyqvxg, zmw ulxfh rg lmgl   
      gsv rnztrmt hvmhli. gsv rnztrmt hvmhli gsvm gizmhulinh gsv kzggvim lu ortsg   
      rmgl z rwvl hrtmzo, vrgsvi vovxgilmrx li mvfizo.**
   2. THE STRUCTURE AND OPERATION OF THE EYE IS EXTREMELY SIMILAR TO AN ELECTRONIC CAMERA AND IT IS NATURAL TO DISCUSS THEM TOGETHER BOTH ARE BASED ON TWO MAJOR COMPONENTS A LENS ASSEMBLY AND AN IMAGING SENSOR THE LENS ASSEMBLY CAPTURES A PORTION OF THE LIGHT EMANATING FROM AN OBJECT AND FOCUS IT ONTO THE IMAGING SENSOR THE IMAGING SENSOR THEN TRANSFORMS THE PATTERN OF LIGHT INTO A VIDEO SIGNAL EITHER ELECTRONIC OR NEURAL
   3. ****
3. In this question, we consider the life expectancy of the popular AES-128 cipher with regard to brute-force attacks.
   1. The attacker has a budget of $1M and has access to an ASIC that allows bruteforcing 5×1085×108 keys in one second. The cost of one ASIC is $50. Assume an overhead of the same cost of the ASIC itself just for configuration including PCB manufacturing cost, networking, power and cooling fans. Assuming ASICs can be run in parallel, how many can be used if we want to remain within the available budget? What is the average key search time? Compare your answer to the age of the Universe ≈1010≈1010 years.
      1. Each machine costs $100. Thus, $1,000,000÷$100=10,000𝗆𝖺𝖼𝗁𝗂𝗇𝖾𝗌
      2. Speed of our parallelised machines as: keys/seconds
      3. Length of time to find a key in the average case, The average case will be checks: 1.08×𝗒𝖾𝖺𝗋𝗌
      4. times longer than the elapsed age of the universe.
   2. Now take advances in computer technology into account. Using Moore’s Law calculate how long will it take to build a key-search machine for breaking AES-128 that takes about 24 hours of search time? Assume a budget of $1M.
      1. 1.08 ×Y𝖾𝖺𝗋𝗌 × = 1 D𝖺𝗒
      2. = 1.08 ×𝗒𝖾𝖺𝗋𝗌×365 𝖽𝖺𝗒𝗌
      3. Value of i which is 68.42.
      4. The number of years: 1.5 𝗒𝖾𝖺𝗋𝗌×69 𝗂𝗍𝖾𝗋𝖺𝗍𝗂𝗈𝗇𝗌 = 103.5 𝗒𝖾𝖺𝗋𝗌