The University of North Carolina at Greensboro
CSC 580: Cryptography and Security in Computing
Prof. Stephen R. Tate

Handout 3
January 19, 2016

Assignment 1 – Due Tuesday, February 2

Chapters 1–3

Note: Remember that one of the main goals of this class is to develop your skills in reasoning about security, so show your work and explain your reasoning on all problems – for homework problems, your thought process is as important as the final answer!

1. This question looks into the problem of malware inside point-of-sale systems (systems that you use to pay for a purchase in a store), which is a huge problem for retailers.

   (a) Do some Internet research and learn how traditional (magnetic stripe) credit card point-of-sale systems work, and draw a diagram of how a credit card purchase works in such a system. You don't have to be very detailed, but show all the major components (including the magstripe reader, the merchant's computers/network, and the payment authorizer) and indicate whether sensitive data is encrypted in each system or communication link.

   (b) Read about the infamous 2013 attack on Target stores in the following two stories (note: the links are live on the class web site, so you can just click)

   - A First Look at the Target Intrusion, Malware — Krebs on Security
     http://krebsonsecurity.com/2014/01/a-first-look-at-the-target-intrusion-malware/
   - A Closer Look at the Target Malware, Part II — Krebs on Security
     http://krebsonsecurity.com/2014/01/a-closer-look-at-the-target-malware-part-ii/

   Write a brief summary (less than a page), being careful to use proper terminology. In particular, what *assets* were compromised in this *attack*? (Hint: Think broadly: stolen information is certainly an asset, but so is company infrastructure.) For these assets, what are *confidentiality*, *integrity*, and *availability* goals, and were they compromised? Where was a *vulnerability* used as an *attack vector*? (This is complex: there were certainly multiple attack vectors, some of which are not publicly known – just summarize the ones described in the stories referenced above.) Describe specifically where the adversary (malware) was in your picture from part (a).

   (c) Find information on how newer, chip-card, point-of-sale systems work, and give a modified version of your diagram from part (a) showing this newer system. Would an adversary in the same position as in part (b) be successful in the newer system? Explain why or why not.

2. Textbook, page 56, Problem 2.1.

3. In this problem, we generalize the affine Caesar cipher from the previous problem to work over bytes (with values $0..255$) rather than letters of the alphabet.

   (a) If we did all operations mod 256 instead of mod 26, describe which keys $[a, b]$ (where $0 \leq a, b \leq 255$) would be valid and which would be invalid.

(b) What if we performed operations mod 257. What are the invalid keys now?

4. For this problem, you are to experiment with recognizing English text in a program, using that to break by brute force an affine cipher with operations performed mod 256 (as in part (a) of the previous problem). It turns out that almost all English text files are made up of pure ASCII characters, and satisfy the following three properties:

   - All ASCII characters have values between 0 and 127 (inclusive).
   - Between 13% and 18% of the characters are a space.
   - Between 8% and 12% of the characters are an 'E' (upper or lower case).

   On the class web page with this assignment, you will find example encryption code in C++, Java, and Python (with the plaintext missing) as well as a stub for each of these languages that defines your challenge ciphertext as a string constant. Answer the following questions:

   (a) How many valid keys are there for this cipher (i.e., what is the size of the keyspace)?

   (b) When you try all valid keys with the challenge ciphertext, how many keys result in decrypted plaintext that satisfies all three of the "typical English message" properties listed above?

   (c) What is the plaintext for this message?

5. Professor Alice had to leave town on a clandestine mission before sending in the final grade for student Mallory, who is taking her class pass/fail. She arranges to use a one-time pad, as described on pages 47–48, giving the one-time pad key to the registrar (Bob) before she leaves. Finally, she sends a message to the registrar that gives Mallory's final grade. Mallory can intercept and modify the message, and while she doesn't know exactly what the plaintext is (and obviously doesn't know the key) she knows that it starts with the plaintext word "fail." Mallory intercepts the ciphertext message "`SXMHYOCZWITVBLA`". What can she replace this with so that the plaintext message that Bob decrypts starts with the word "pass" rather than "fail?"

6. Textbook, page 81, Exercise 3.2

7. Textbook, page 82, Exercise 3.5

8. Consider a company in which only the company president (Alice) has the combination to the safe, but in case something happens to Alice she would like it so that her two vice-presidents, Bob and Carol, can learn the combination if they work together (this is a form of "key escrow"). The combination can be specified in 64 bits, so they will use DES to accomplish this. Alice shares a secret key K_{AB} with Bob and a secret key K_{AC} with Carol, but can't just encrypt the combination with K_{AB} or K_{AC} because then either one could decrypt the safe's combination without cooperating with the other. Devise a solution so that Alice can leave a ciphertext with them so that they can decrypt the combination if and only if they cooperate with each other.

   Describe your solution carefully, saying exactly what operations Alice must perform to create the ciphertext, and the operations Bob and Carol will use to decrypt the ciphertext and learn the safe's combination. Use clear, mathematical notation (so, for example, $E(K_{AB}, M)$ uses DES to encrypt message M using key K_{AB}). In your description clearly state how large the ciphertext is.