Massachusetts Institute of Technology
6.857: Network and Computer Security
Professor Ronald L. Rivest
Professor Yael T. Kalai

Handout 2
February 13, 2016
Due: February 27, 2016

Problem Set 1

This problem set is due on *Monday, February 27, 2016* at **11:59 PM**. Please note our late submission penalty policy in the course information handout. Please submit your problem set, in PDF format, on Gradescope. *Each problem should be in a separate PDF.* Have **one and only one group member** submit the finished problem writeups. Please title each PDF with the Kerberos of your group members as well as the problem set number and problem number (i.e. *kerberos1_kerberos2_kerberos3_pset1_problem1.pdf*).

You are to work on this problem set with your assigned group of three or four people. You should have received an email with your group assignments. If you have not been assigned a group, please email `6.857-tas@mit.edu`. Be sure that all group members can explain the solutions. See Handout 1 (*Course Information*) for our policy on collaboration.

Homework must be submitted electronically! Each problem answer must be provided as a separate pdf. Mark the top of each page with your group member names, the course number (6.857), the problem set number and question, and the date. We have provided templates for LaTeX and Microsoft Word on the course website (see the *Resources* page).

Grading: All problems are worth 10 points.

With the authors' permission, we may distribute our favorite solution to each problem as the "official" solution—this is your chance to become famous! If you do not wish for your homework to be used as an official solution, or if you wish that it only be used anonymously, please note this in your profile on your homework submission.

Our department is collecting statistics on how much time students are spending on psets, etc. For each problem, please give your estimate of the number of person-hours your team spent on that problem.

Problem 1-1. "The Growth of Cryptography" lecture

Professor Rivest gave a lecture titled "The Growth of Cryptography" as his Killian Award lecture in 2011. The lecture video is available on YouTube, here. Watch the video and answer the following questions.

(a) Who proved Fermat's Little Theorem?

(b) Two developments with major impact on the growth of cryptography were the radio and _____.

(c) What are the factors of 8616460799?

Note: This problem has been added to the problem set to "make up" for the missed lecture due to the snow day on Monday, February 13th. While we have included three trivia-style questions to accompany the video, *please watch it all the way through as if it were Monday's lecture*, not just to find the answers to the questions! It contains material that will be referenced in later lectures, and also is just an awesome lecture that we think will be well worth your time. :)

Problem 1-2. Security Policy for Amazon Echo

Amazon Echo is a useful AI/smart home device that allows users to conveniently play music, check the weather, set alarms, etc. It may also be used to do more personal tasks, such as check the personal calendar or buy products from Amazon.

Describe a security policy for Amazon Echo. Be sure to address the relevant principals, actions, and policies. The policies you come up should address each of the security goals discussed in class, though focus on the one(s) that are most relevant for AI devices like Echo.

Given time constraints and the complexity of the problem, we expect your solutions to be less than comprehensive. That being said, keep in mind that there are various parties or agents that may interact with

Echo, other than the user, and that some of these parties may act in an adversarial manner to cause some undesirable result.

(This problem is a bit open-ended, but should give you excellent practice in writing a security policy. Also, you may actually care about such security policies for designing systems used by large numbers of people—or if you use one yourself! We have included sample solutions from similar questions in previous years on the course website.)

Problem 1-3. Re-Using a One-Time Pad

It is well known that re-using a "one-time pad" can be insecure. This problem explores this issue, with some variations.

In this problem all characters are represented as 8-bit bytes with the usual US-ASCII encoding (e.g."A" is encoded as 0x41). The bitwise exclusive-or of two bytes x and y is denoted $x \oplus y$.

Let $M = (m_1, m_2, \ldots, m_n)$ be a message, consisting of a sequence of n message bytes, to be encrypted. Let $P = (p_1, p_2, \ldots, p_n)$ denote a pad, consisting of a coresponding sequence of (randomly chosen) "pad bytes" (key bytes).

In the usual one-time pad, the sequence $C = (c_1, c_2, \ldots, c_n)$ of ciphertext bytes is obtained by xor-ing each message byte with the corresponding pad byte:

$$c_i = m_i \oplus p_i, \text{ for } i = 1 \ldots n \ .$$

When we talk about more than one message, we will denote the messages as $M_1, M_2, \ldots, M_k$ and the bytes of message M_j as m_{ji}, namely $M_j = (m_{j1}, \ldots, m_{jn})$; we'll use similar notation for the corresponding ciphertexts.

(a) Here are two 11-character English words encrypted with a "one-time pad". Decide whether they were encrypted with the same pad or with different pads. If they are different pads, then explain why they cannot be the same pad. If they are the same pad, then decrypt the ciphertexts.

```
a2 6c 49 3f 20 81 c2 e4 da 16 c9
b1 71 4b 28 27 94 ce fd da 17 c0
```

(b) Ben Bitdiddle decides to fix this problem by making sure that you can't just "cancel" pad bytes by xor-ing the ciphertext bytes.

In his scheme g is a random-looking permutation of bytes. That is, g is a 1-1 function mapping $\{0,1\}^8$ to $\{0,1\}^8$. They can be represented as byte-valued array G of size 256. Ben chose this function in a random manner using dice; they indeed look "random" – there is no apparent structure. The array G is public and given in the file `gbox.txt`.

The sequence $C = (c_1, c_2, \ldots, c_n)$ of ciphertext bytes is obtained by

$$c_i = m_i \oplus g(p_i \oplus c_{i-1}), \text{ for } i = 1 \ldots n$$

where $c_0 = 0$.

Argue that Ben's scheme is decryptable. As part of your answer, explain how the recipient decrypts a ciphertext with Ben's scheme.

(c) Argue that Ben's scheme is like the OTP, "one-time secure": An adversary who hears one ciphertext, but doesn't have any information about the pad used, learns nothing about the message.

(d) Ben is confident that he can now re-use his pad, since there is no apparent way that one can "cancel" the effect of the pad on the message to obtain the ciphertext. For example, xor-ing ciphertexts doesn't seem to do anything useful for an adversary. So, he feels that he can now re-use a pad freely.

You are given the file `tenciphs.txt`, containing ten ciphertexts $C_1, C_2, \ldots, C_{10}$ produced by Ben, using the *same* pad P. You know that these messages are meaningful and contain only printable characters.

Submit the messages and the pad, along with a careful explanation of how you found them, and any code you used to help find the messages. The most important part is the explanation.

Problem 1-4. WhatsApp Retransmission Vulnerability WhatsApp is popular messaging app used by a billion users worldwide, which claims to secure users' messages using end-to-end encryption.

(a) Briefly explain what *end-to-end encryption* means. How would your expectations of privacy differ between two apps which make the following claims?

- App A: "We use encryption to secure your messages!"
- App B: "We use end-to-end encryption to secure your messages!"

Last year, a vulnerability was discovered in WhatsApp messaging protocol. The vulnerability is described in this blog post*. Read the blog post and answer the following questions.

(b) In light of the vulnerability, evaluate WhatsApp's claim that "only you and the person you're communicating with can read what is sent, and nobody in between, not even WhatsApp." In particular, consider *who else* apart from the sender and receiver might be able to read messages sent through WhatsApp? Phone companies? WhatsApp itself? Law enforcement? Your friends, neighbors, or boss? Discuss how difficult and/or likely you think it would be for these different parties to exploit the vulnerability to eavesdrop on people's messages.

(c) Are there any circumstances in which, despite the vulnerability, technically savvy users could be sure that their messages were not read by any third party?

WhatsApp's end-to-end encryption was allegedly implemented using the Signal protocol developed by Open Whisper Systems (in fact, the encryption feature was rolled out in collaboration with OWS). WhatsApp and Open Whisper Systems have been acclaimed for bringing end-to-end encryption to mainstream messaging, by integrating the encryption "seamlessly" so that the messaging experience does not add additional steps for the average user, or require any technical expertise.

(d) The vulnerability does not affect the Signal protocol itself, but only WhatsApp's implementation, as explained in the blog post. WhatsApp made an undisclosed design decision to deviate from the Signal protocol in how it retransmits undelivered messages. Can you think of any advantages to their decision?

The vulnerability was announced in April 2016, but it started receiving widespread media attention in January 2017, following an article published in The Guardian. The Guardian article was originally titled, "WhatsApp backdoor allows snooping on encrypted messages," and later revised to "WhatsApp vulnerability allows snooping on encrypted messages." The researcher who discovered the vulnerability had mixed to negative feelings about the ensuing publicity, as described in his blog post here*. Read the blog post and answer the following question.

(e) Imagine you were the reporter preparing this article for The Guardian—what considerations and concerns would you have about publicizing a vulnerability like this in a major newspaper with an international audience? With these considerations in mind, read the article* and briefly describe any changes you might make to the article (in terms of content, presentation, or other aspects), and why you think they would be beneficial.

**Note: You are not required to read all of the links in this problem: the required readings are marked with an asterisk. The other links are provided as relevant background and you may peruse them if interested.*