CS 161

Computer Security

Dawn Song

Fall 2012

Lab 3

Cryptography v.01

Due Date: October 10, 2012 by 11:59pm

Introduction

This lab consists of two components: a multiple choice questioner on cryptography and hands-on experience with code breaking improperly encrypted messages. As always, you are welcome to work with your lab partner for both parts. However, all students in a group must submit a solution! Solutions submitted after the deadline will not be graded.

Part 1

The first part of the lab consists of a multiple choice online exam in the form of a Google document, located at `http://bit.ly/QDEkpz`. There are 22 questions about cryptography, algorithms, and randomness. You may submit multiple times; only your final solution will be graded.

Part 2

Your country is at war with an evil empire. Their forces are closing in and it is only a matter of time before they wipe you out. Luckily for you, their military command and control system programmers did not take CS161, and as a result they were not properly trained in security like you. It turns out that they use the same AES key and IV for sending commands to their military divisions, although you don't know what the key and IV are.

You are a code breaker serving your country. Your military has just intercepted 3 different messages that the enemy command center sent to their divisions D1, D2, and D3 (a different message to each division). Each message is from the standard set of military commands listed below. If you can figure out which messages were sent to each division, your country will have a tactical advantage and win the war. It is up to you to save your homeland from tyranny. Good luck. Your solution and follow up questions should be submitted along with your solutions to Part 1 at `http://bit.ly/QDEkpz`

Details: Each message is encoded as a null terminated ASCII string. The message is then padded with random bytes so that its total length is 32 bytes. Each message is encrypted with the same AES-128 key and IV. The encryption is done with the CTR block cipher mode. You will probably need to write a short program to answer this question.

Below are the encrypted messages to each division. They are hex encoded one byte at a time.

Encrypted message to Division 1:
ABEAC9AD2CE382D7EE44A3A5C38E9FE8ACEAC9B50C9885EDA89C0741725325D8
Encrypted message to Division 2:
AEEDC0A078E0D0DCE943B6BB828C98F2A2F1A5F6F960B7A729CEAE94D668BB8F
Encrypted message to Division 3:
AFF0C8A369F7D0D9F444A3AA88EFEB1990DC172B9B01356DA437F9D03FCADDA8

The possible messages that could have been sent are:

- charge
- prepare ambush
- raid trenches
- tank attack
- bomber attack
- battleship attack
- submarine attack
- fire missiles
- sniper fire
- encircle enemy
- full frontal assault
- retreat
- feint retreat
- skirmish
- blockade
- lay mines
- fortify
- create distraction
- clear and hold
- split up
- set up a perimeter
- destroy bridges
- sabotage enemy missile defense
- restore formation
- launch the nukes