CS 1653: Applied Cryptography and Network Security
Fall 2020

Homework 2

Assigned: Wednesday, October 28 **Due:** Thursday, November 12, 11:59 PM

---

1 Background

In our semester project, you've been developing a set of protocols for secure communication between a group server, file servers, and clients. In this homework assignment, you'll write a brief discussion of an attack against the protocols used in VoLTE, a common method of transmitting voice calls in LTE.

To begin, read the following article and take some notes about what you learn. You will write a summary of the attack as a deliverable in this homework.

`https://blog.cryptographyengineering.com/2020/08/12/attack-of-the-week-voice-calls-in-lte/`

2 What do I need to do?

First, you should write up your approach to decrypting `rail.txt` and this PDF with the help of `pinyonjay.txt`. Name your writeup either `approach.txt` or `approach.pdf`. If you wrote any code to help you, you should commit that code and discuss it in your explanation. If you used existing tools, you should show that you understand what those tools did by discussing some technical details of how such a tool would work.

Then, write a short discussion of the article linked above. Your paper should be about a page in standard single-spaced layout (about 500 words), and no longer than two pages in total. In this paper, you should describe the attack, its impact, the mistakes made in implementations that enabled it, and improvements to the design that could have prevented it. Your intended audienci should be a fellow computer scientist who has studied the basics of cryptography and understands the relevant vocabulary. Submit your paper as `Revolte-abc123.pdf` (please do not submit other formats), where `abc123` is your Pitt username.

3 What do I turn in?

This homework is to be completed *individually*. A repository will be created for you via GitHub Classroom. Commit to this repository the following files:

- `approach.txt` or `approach.pdf` that describes your approach to cryptanalyzing in the first two steps of the assignment. If you wrote code, include that code as well.

- `Revolte-abc123.pdf`, where `abc123` is your Pitt username, in which you explain the ReVoLTE attack.

This homework is due at the precise date and time stated above. We will clone your repository immediately after the due date, so you will be graded on whatever changes have been committed **and pushed** to your repository's default branch by this time. No changes made after this point will be considered in grading your submission. Make sure your repository is created and you understand the submission process well in advance!