# Group Workshop Syllabus

## 1. Overview

| | | | |
|---|---|---|---|
| **Title** | **Cryptography, Cybersecurity and Blockchains** | | |
| **Mode** | **Online lectures and mentor sessions** | | |
| **Hours** | **4*2 hours lecture +2*2 hours final project preparation session+ 1*2 hours final presentation session+ 6*1.5 hours mentor sessions (conducted by mentor)** | | |
| **Targeted Students** | *(Please indicate as detailed as possible, as that will help us to better recruit targeted prospective students)* | | |
| **Prerequisites** | **High School Students** | Required course/Knowledge | **General math background is sufficient** |
| | | Recommended Materials for preparing for the course | **Basics of number theory and modular arithmetic** |
| | **College Students** | Required course/Knowledge | **None** |
| | | Recommended Materials for preparing for the course | **Programming background is helpful for the final project** |

## 2. Program Introduction and Objectives

| | |
|---|---|
| **Course Description**<br>In a paragraph, please specify：What kind of program is it? What field is the program based in? What knowledge/concepts does the program include? What is the final outcome of the program (types of projects/ What did the students do to demonstrate their learning outcome, etc.) | What happens when you try to purchase something using your credit card over the Internet? How do we make sure that online banking systems remain secure? Can we design a cipher which cannot be broken? This course deals with Cryptography and Cybersecurity: an area which is playing an increasingly important role in our daily lives. The applications of cryptography range from financial applications, to military domain, to Bitcoin, and even in securing everyday apps like WeChat and Whatsapp. |
| **Software/Tools (if any)** | **None** |

### 3. Program Schedule

| Week | | Lecture | Mentor Session<br>(lab/case study, etc.) | Assignment | Reading Materials |
|---|---|---|---|---|---|
| 1 | Topic | **Classical Ciphers** | | | |
| | Detail | Caesar cipher, Vigenere cipher, Substitution cipher, and, why they are all insecure. One-time pad and perfect security. | | | |
| 2 | Topic | **Modular exponentiation and Basics of Modern Cryptography** | | | |
| | Detail | Basics of number theory and modular arithmetic, discrete log problem, DDH problem, factoring problem, One-way hash functions, design of one-way hash functions based on discrete log, storing passwords, digital signatures, public key encryption, digital certificates, | | | |
| 3 | Topic | **Bitcoin and Blockchains** | | | |
| | Detail | How Bitcoin works, mining coins, achieving consensus, the difference between proof-of-work and proof-of-stake based blockchains. limitations of Bitcoins and current active areas of research | | | |
| 4 | Topic | **RSA and Zero-Knowledge Proofs** | | | |
| | Detail | RSA Encryption, RSA digital signatures, how to flip a fair coin over the phone or the internet, cryptographic commitment schemes, zero-knowledge proofs, graph 3-coloring problem | | | |
| 5 | **Final Project Preparation Session** | | | | |

| | |
|---|---|
| **6** | **Final Project Preparation Session** |
| **7** | **Final Written Reporting and Oral Presentation** |

## 4. Problem Sets/Written Assignments/Quizzes

| | | |
|---|---|---|
| **Total Number of Assignments** | **__5_ times** | |
| **Submission Deadline** | ____5____Days after class | |
| Is Mentor needed to review and grade assignment? | Yes (x) | No ( ) |
| Will a standard answer be provided? | Yes (x) | No ( ) |
| **Will there be Quizzes? How often/how many?** | 1 Quiz | |
| **Other Requirements (if any)** | | |

## 5. Final Oral and Written Project

### 5.1 Final Written Report

The students have to prepare a final report of about 5-7 pages. The report will be about the project which the student takes up as part of the class. The students can decide the project on their own in consultation with the professor, or, the professor can suggest a topic.

### 5.2 Oral Presentation

To successfully complete this course, students are required to prepare a 10-minute oral presentation about their project. Students will choose the final project from a list of possible projects. The students can do the projects in the groups but each student is still required to do an oral presentation individually.

## 6. Suggested Future Research Fields/Direction/Topics

*Some of our students may continue and extend their study based upon the online program they learn, and some may even would like to choose a topic/direction to write an academic manuscript. Therefore, if you have some suggestions on the direction/topic/hot trend in the related fields students can consider for their extended study, please advise here.*
*A number of topics include: Blockchains including proof-of-stake based ones, Zcash, zero-knowledge proofs and secure multi-party computation and, homomorphic encryption. Information regarding these will be provided in the class.*

## 7. Instructor Introduction

7.1 Instructor Title *Prof Vipul Goyal*
7.2 Instructor Bio

Vipul Goyal is an Associate Professor in the Computer Science Department at CMU. Previously, he was a researcher in the Cryptography and Complexity group at Microsoft Research. He received his PhD in Computer Science from University of California, Los Angeles in Dec 2009. Dr. Goyal is a winner of several honors including a 2016 ACM CCS test of time award, a JP Morgan Faculty Fellowship, a Microsoft Research graduate fellowship, and, a Google outstanding graduate student award. He was named to the Forbes magazine 30 under 30 list of people changing science and healthcare in 2013. His research has received media coverage at popular science publications such as MIT technology reviews, Slashdot, and, Nature news. He has published over 80 technical papers at top conferences in cryptography such as at Crypto, Eurocrypt, STOC, FOCS, and, ACM CCS. He is one of the highest cited cryptographers of his generation. Many of the students who he supervised are now at professors at top US universities, or, in leading positions in the software industry.