Modern Cryptography: Designing Ciphers and Securing the Internet
Vipul Goyal

Course Description:

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, and even in securing everyday apps like WeChat and Whatsapp.

Goals:

1. To gain a solid background in the basics of cryptography and cybersecurity.
2. To understand why all the classical ciphers were broken and the philosophy of modern cryptography
3. To work on a research project and write a report.

Prerequisites: There are no prerequisites for this course. However, we expect the students to have a basic background in mathematics.

Individual Evaluations: All the students will be evaluated on the basis of the following. Class participation will carry 20% weightage. This includes asking questions in the class, answering the questions asked by the Professor, and overall ability to follow the lectures. Homework assignments will consist of 40% of the weightage. Homework assignments will include exercises on the course material as well as programming assignments. The final project will carry 40% weightage as well. All students will be required to produce a report which will be evaluated on the basis of the overall quality of work done, demonstration of the understanding of the research topic, and, the quality of the write up in English language.

Course materials:

There is no required textbook. As we go along, we will provide web links, reading material and scribe notes as appropriate.

List of topics:

The topics covered will consist of the following: Classical ciphers vs modern cryptography, fixed-shift cipher, Caesar cipher, Vigenere cipher, Substitution cipher, Homophonic cipher, one-time pad and its security analysis, message-authentication codes, basics of modular arithmetic

and number theory, discrete log problem, factoring problem, one-way hash function, digital signatures, password-based authentication, symmetric key encryption, Diffie-Hellman key exchange, public-key encryption, El Gamal encryption, digital certificates, SSL and HTTPS protocols, Bitcoin and cryptocurrencies (time-permitting).

Research project:

All students will be required to work on a research project. Professor will suggest various topics from which the students can choose. Topics will include the following: digital signature, Bitcoin, encryption schemes, and, classical ciphers used in World War 2.

Detailed description of the course:

Cryptography is an ancient art with history going back thousands of years. Caesar cipher, for example, was used by Julius Caesar to communicate with his Generals during the wars that led to the rise of the Roman Empire. Germans used Enigma machine in World War 2 to encrypt their messages. A dedicated team of British mathematicians was successful in breaking the German code and decipher their messages. This is estimated to have shortened the duration of the war by more than a year. The team included Alan Turing, the father of computer science, who created a machine to try all possibilities for the secret key. The machine can be seen as a precursor to a modern computer.

Modern cryptography is much more than just the design of ciphers and encryption schemes. It includes things like digital signatures, cryptographic protocols for communicating securely over the internet, and digital certificates. We will study several of these topics and try to gain a basic understanding of cryptography.

The topics covered will consist of the following. We will start by trying to understand the difference between classical and modern cryptography. How is cryptography today different from cryptography 100 or even 1000 years ago? We will try to understand the various common classical ciphers including the fixed-shift cipher, Caesar cipher, Vigenere cipher, Substitution cipher, and, Homophonic cipher. All of these ciphers have been broken and we will try to understand why. We will study one-time pad and understand why it's a perfectly secure cipher. We will also cover the limitations of one-time pad. Next we will cover message authentication codes (MACs): the notion, its applications and how to build secure MACs.

We will then move to modular arithmetic and number theory: two basic mathematical subjects which are very important in cryptography. We will cover the basics of modular arithmetic. We will study the discrete log problem, the decisional Diffie-Hellman (DDH) problem, and, the

factoring problem. We will see how people have been try to break factoring and discrete log for hundreds of years but have been unsuccessfully.

We will cover one-way hash functions: definitions, applications and design. Hash functions are perhaps the most basic objects in modern cryptography and have played an important role in various applications. They are used for password authentication, verification, preventing tampering of data, and, even in designs of modern cryptocurrencies such as Bitcoin. We will touch upon many of their applications.

We will study the concept of digital signatures. Digital signatures are fascinating objects and can be much more secure compared to paper signatures which are relatively easy to forge. We will study what digital signatures are, where they can be used, and how to design digital signature schemes. We will also study authentication in general and how to design secure password-based authentication schemes.

We will cover symmetric key encryption: the modern equivalent of classical ciphers. Symmetric key encryption schemes can be used to secure communication between two-parties assuming the parties have a pre-shared secret key. We will see how to design such schemes securely.

We will cover key exchange protocols, and, in particular, Diffie-Hellman key exchange protocol. Key exchange protocols can be used to establish a key between two parties who have never communicated before. We will see how Diffie-Hellman key exchange works and why it is secure. We will also see the number theory behind the protocol. We will then move on to study public-key encryption. Public-key encryption was invented in 1976 and has changed our world forever. We will see the definition and applications of public-key encryption. We will also see how to design a secure public-key encryption scheme. In particular, we will see the El-Gamal public key encryption scheme which is also closely related to Diffie-Hellman key exchange.

Towards the end of the course, we will learn what digital certificates are and their applications. Digital certificates are the backbone of security of our present day Internet. We will also learn about certificate authorities and how they function. We will learn about SSL and HTTPS protocols used widely by every web browser for secure browsing today.

Course Schedule:

Following is the tentative course schedule.

Lecture 1: Applications of Modern Cryptography, Fixed-Shift cipher, Caesar cipher
Lecture 2: Classical ciphers continued: Vigenere cipher, Substitution cipher, Homophonic Cipher
Lecture 3: One-time pad, security analysis of one-time pad, tampering attacks on one-time pad
Lecture 4: One-time message authentication code (MAC), security analysis, moving towards computational cryptography
Lecture 5: Basics of number theory and modular arithmetic, discrete log problem, DDH problem, factoring problem

Lecture 6: One-way hash functions, design of one-way hash functions based on discrete log, password authentication
Lecture 7: Digital signatures, designing one-time digital signatures
Lecture 8: Symmetric key encryption, design based on DDH problem, problem of key management
Lecture 9: Diffie-Hellman Key exchange, Public-key encryption, Elgamal encryption
Lecture 10: Digital certificates, Certificate authorities, HTTPS/SSL protocol

Research topics: Professor will suggest various research topics from which the student can choose. Examples include the following:

Bitcoin: Bitcoin is not a physical currency like the US dollar or the Euro. Bitcoin is a cryptocurrency which has no involvement of any government or bank. Bitcoin has become widely popular in the last couple of years owning to its borderless and decentralized nature. We will explore how Bitcoin works, what its limitations are, and think about ideas to overcome those limitations.

Ethereum: Just like Bitcoin, Ethereum is a cryptocurrencies. While Bitcoin is the largest, Ethereum is the second largest such currency by market capitalization. We will explore how Ethereum works, its positive and negative points and try to come up ideas to make it better.

Digital Signature: Digital signatures are fascinating objects and can be much more secure compared to paper signatures (which are relatively easy to forge). However digital signatures require a lot of computation. We will explore some ideas to make digital signatures faster.

Classical ciphers: Codebreaking is always a lot of fun, and, can teach you interesting mathematics. We will write an article surveying the various classical ciphers such as those used in prehistoric times, used in World War I, World War II, etc. We will also try to break all of them.

The duration of each project will be 5 weeks. First week will be dedicated simply to understanding the problem and the background material. Weeks 2 to 4 will be used to carry out the required research. This will involve consulting various books, internet sources, and, published articles. The last week will be used to write the final report and polish it as much as possible.