Mathematics of Cryptography

Course Description : Cryptography deals with the study of making and breaking secret codes.

In this course we will be studying situations that are often framed as a game between three parties: a sender (e.g., an embassy), a receiver (the government office) and an opponent (a spy). We assume that the sender needs to get an urgent message to the receiver through communication channels which are vulnerable to the opponent. To do this communication, the sender and receiver agree in advance to use some sort of code which is unlocked by a keyword or phrase. The opponent will be able to intercept the message. Is he/she able to unlock the message without knowing the key?

In this course we will learn some probability theory, information theory and number theory to answer questions about how vulnerable the methods of sending secrets are. This has a great number of applications to internet credit card transactions, wireless communication and electronic voting. We will start by learning some classical codes (used up through WWI) and analyzing those. The last third of the course we will start to learn the methods that are used in modern cryptography.

The course web page can be found at

http://garsia.math.yorku.ca/~zabrocki/math4161w12/

The grades are based on the following components:

Quizzes (drop lowest 1 of 5)	65%
Computer assignment	5%
Final exam	30%
Total	100%

Please note that the grades will be based on a curve and will not use the absolute grading scale.

Below is a rough schedule of how I expect this class to proceed for the first few weeks and important dates. You can expect to see this schedule revised as the course develops. You are expected to show up for lectures and be aware of any changes to the **tentative** schedule that I am providing for you here.

Lecture Schedule	Topics	Remarks
Tuesday, January 3	Introduction-Caesar, Vigenere	
Thursday, January 5	classical ciphers- Rectangular transposition, homophonic, Playfair	
Tuesday, January 10		Quiz 1
Thursday, January 12	classical ciphers- Hill, Vernam, ADFGVX, snail	
Tuesday, January 17	probability theory and the game of craps	
Thursday, January 19	infinite monkeys	
Tuesday, January 24		Quiz 2

Early Ciphers
- Caesar
- Vigenere
- Rectangular Transposition
- Monoalphabetic Substitution
- Playfair
- ADFGVX
- Vernam's Two Tape System
- Hill Encipherment

Probability Theory
- Basics
- Statistical Models of English Text
- Random Number Generators

Codebreaking
- Breaking Vigenere
- Breaking Rectangular Transposition
- Breaking Monoalphabetic Substitution

Information Theory
- Basics on the concept of Information
- Entropy and Information
- Fundamental Identities
- Redundancy and Compression of Text
- Redundancy of English Text
- File and Text Compression
- The Huffman Code
- Perfect Secrecy Systems

Number Theory
- Euclidean Algorithm
- Chinese Remainder Theorem
- Residue Systems
- The Euler Phi Function
- Primitive Roots
- Quadratic Residues
- Quadratic Reciprocity Law
- The Jacobi Symbol
- Primality Testing
- The RSA Encipherment Scheme
- Knapsack
- Factoring Large Integers
- Public Key Systems

COMMON USES FOR CRYPTOGRAPHY

Phone Lines (voice) cell phones or secure phone line

Cable (TV signal, image)

Computer (data)

- e-mail
- internet shopping/ credit card data
- electronic signature
- subscriber protected data
- “rated” material
- password security
- encrypted l e s

Wartime Communications

Diplomatic Communications

Business Communications- Instustrial Espionage

Bank Communications

Love letters

Children’s games

Criminal Activity

THE JARGON OF CRYPTOGRAPHY

Cryptography: The art of secret writing

Plaintext: Text to be encoded for secrecy

Ciphertext: Encoded text. Short ciphertext is sometimes called a "cryptogram"

Cipher: A method of secret writing.

n-gram: A string of n-letters.

Encipherment, Encryption: The process of encoding plaintext into ciphertext.

Decipherment, Decryption: The process of decoding ciphertext back into plaintext.

Encrypt, Decrypt: These are the corresponding verbs.

Sender: The person or organization that is to send the encrypted message.

Receiver: The person or organization which is to receive and decrypt the message.

Opponent: The person or organization which intercepts the message and attempts the unauthorized decipherment.

Key: The information, usually a sequence of digits or symbols, used to determine the method by which plainext is to be transformed into ciphertext.

Cryptographic system, Encipherment scheme: A family of ciphers (transformations of plaintext into ciphertext to be used for encryption and decryption). Each member of the family is determined by a particular key.

Message space: The collection of all messages that may occur in a particular cryptographic transaction.

Key space: The collection of all keys that may occur in a given cryptographic system.

Cryptanalysis: The process by which the opponent attempts to recover the original plaintext from the intercepted ciphertext.

Code breaking: The process by which a cryptographic system is made vulnerable to cryptanalysis.

One-time pad: A key to be used only once.

In a typical cryptographic transaction the sender and receiver choose a cryptographic system and, at some time before the message is to be sent, the sender chooses the key. This determines which transformation of the system will be used to encrypt the message. The key is then sent to the receiver by some safe path (inaccessible to the opponent). Upon obtaining the key the receiver determines which transformation of the system is to be used to decrypt the message.

A number of assumptions are usually made without explicit mention about cryptographic transactions. It is assumed that safe paths between sender and receiver do exist though generally they may be impractical to use for the message itself (for instance the path may require hand carrying by an especially trusted messenger). While, for practical reasons (such as speed of delivery for instance) the path taken by the message itself may have to be "unsafe". Furthermore, security of the message is not usually expected to be achieved through the opponent's ignorance of the encryption system but rather from lack of knowledge as to which particular transformation of the family has been used in the encipherment. That is, the opponent's task usually consists of reconstructing the key from an analysis of the ciphertext. Security is achieved by assuring that the key space is too large for an exhaustive trial and error attack to be practical.

Of course, the basic goal of the opponent is to recover the original plaintext. This may not necessarily involve reconstructing the key.

The two main methods of encryption are Substitution and Transposition and most known modern methods are a mixture of both. These two methods may be described as follows:

Substitution: When individual letters or n-grams of plaintext are replaced by letters or n-grams of ciphertext.

```
THE END OF THE WORLD AS WE KNOW IT

WKH HQG RI WKH ZRUOG DV ZH NQRZ LW
```

Transposition: When the characters of the original message are rearranged according to some particular pattern.

```
FRANKLY MY DEAR

MADLA RKYEN FRY
```

A Cryptographic transaction may also be viewed as a two-person game between the sender-receiver on one side and the opponent on the other. This game may be played under different sets of rules. The most commonly used rules are dened as follows.

Ciphertext only attack: The opponent is to recover plaintext only through knowledge of ciphertext.

Known plaintext attack: The opponent may have access to some information concerning the original plaintext. This may include the knowledge of portions of the plaintext.

Chosen plaintext attack: The opponent is in a position to acquire ciphertext corresponding to plaintext of its selection.

Classical Cryptography: Usually this refers to a cryptographic transaction where the opponent is allowed Ciphertext-only or Known-plaintext attacks.

Modern Cryptography: Usually this refers to the game in which the opponent has access to an unlimited amount of corresponding plaintext-ciphertext pairs. That is, the opponent is capable of Chosen-plaintext attack. Usually, this is achieved by the opponent having access to all the encrypting transformations of the system. Security is to be achieved through secrecy of all the decrypting transformations.

DESIGN CONSIDERATIONS OF A CIPHER

There are ways of sending data so that is theoretically impossible to recover the message without knowing the key. Systems like this are rarely used because they are inconvenient. The key may only be used once and must be as long as the message that is being sent.

- Type of data (TV signal/voice/computer data/letter/telegram)
- Security
- Ease of Use
- Cost/ease of use vs. value of data
- Amount of data

Zimmermann Telegram

From Wikipedia, the free encyclopedia

The **Zimmermann Telegram** (or **Zimmermann Note**; German: *Zimmermann-Depesche*; Spanish: *Telegrama Zimmermann*) was a coded telegram dispatched by the Foreign Secretary of the German Empire, Arthur Zimmermann, on January 16, 1917, to the German ambassador in Mexico, Heinrich von Eckardt, at the height of World War I.

The telegram instructed the ambassador to approach the Mexican government with a proposal to form a military alliance against the United States. It promised Mexico land in the United States if they were to help. It was intercepted and decoded by the British, and its contents hastened the entry of the United States into World War I.

The Zimmermann telegram as it was sent from Washington to Mexico

Zimmermann's message was

> On the first of February, we intend to begin unrestricted submarine warfare. In spite of this, it is our intention to endeavour to keep the United States of America neutral.
>
> In the event of this not succeeding, we propose an alliance on the following basis with Mexico: That we shall make war together and make peace together. We shall give generous financial support, and an understanding on our part that Mexico is to reconquer the lost territory in New Mexico, Texas, and Arizona. The details of settlement are left to you.
>
> You are instructed to inform the President [of Mexico] of the above in the greatest confidence as soon as it is certain that there will be an outbreak of war with the United States and suggest that the President, on his own initiative, invite Japan to immediate adherence with this plan; at the same time, offer to mediate between Japan and ourselves.
>
> Please call to the attention of the President that the ruthless employment of our submarines now offers the prospect of compelling England to make peace in a few months.