CSE 594 : Modern Cryptography Date:01/24/17

Lecture 1: Introduction

Instructor: Omkant Pandey Scribe: Venkata Jyothsna Donapati,Him Kalyan Bordoloi

1 Introduction

Cryptography has many applications in modern day life. Almost every online service uses cryptography in some form. Some examples include

- Online banking
- E-commerce
- E-mail
- https browsing

The basic idea of cryptography is to have a mechanism of making secret communication between two parties such that an eavesdropper cannot understand the message being transferred even if he can read the text.

Definition 1 *Cipher : A cipher is defined by its 3 components.* $E(k,m) \rightarrow c$ *and* $m \leftarrow D(c,k)$ *are encryption and decryption algorithms, and k is the secret key. E can be randomized such that c changes every time*

Definition 2 *Symmetric Cipher: If k is same for E and D, it is called a Symmetric Cipher*

2 Historical Ciphers

2.1 Caesar Cipher

It was used by Julius Caesar to communicate with his generals and is thus named after him

- Encryption:
  The key(k) is a number between 1 to 25. The encrypted text is obtained by shifting each alphabet by 'k'
- Breaking the cypher:
  - Brute Force: Since the key space is just 25, each key can be tried to de-cypher the text.
  - Visible patterns and letter frequencies: Frequency of characters do not change in this cypher, they just shift by k letters. So a simple frequency analysis will break this cypher

2.2 Substitution Cipher

In Substitution Cipher random permutation of alphabets are chosen as following {A → T ,B → J, C → Z,....} (No repeating)

- Encryption:
  Plain text letters are mapped according to the substitution (key)
- Decryption:
  Decrypt using the same keys.
- Cannot break by brute forcing for the key since possible number of keys is 26! which is approximately 2^{88}
- Can be broken by frequency analysis.

2.3 Frequency Analysis

Following are frequencies of letters,bigrams and double letters in English:

Letters								
e	t	a	o	i	n	s	r	h
12.49%	9.28%	8.04%	7.64%	7.57%	7.23%	6.51%	6.28%	5.05%

Bigrams											
th	he	in	er	an	re	on	at	en	nd	ti	es
3.56%	3.08%	2.43%	2.05%	1.99%	1.85%	1.76%	1.49%	1.45%	1.35%	1.34%	1.34%

Double Letters										
ll	ss	ee	oo	tt	ff	pp	rr	mm	cc	nn
0.58%	0.41%	0.38%	0.21%	0.17%	0.15%	0.14%	0.12%	0.10%	0.08%	0.07%

How to break substitution cipher ?

- Collect a long ciphertext because frequency patterns will not change.
- Compute frequencies of various letters.
- Reconstruct the key using frequencies like the most frequent letter is "E" and the second most frequent letter is "T" and so on.Even bigrams and trigrams can be used.

2.4 Vignere Cipher

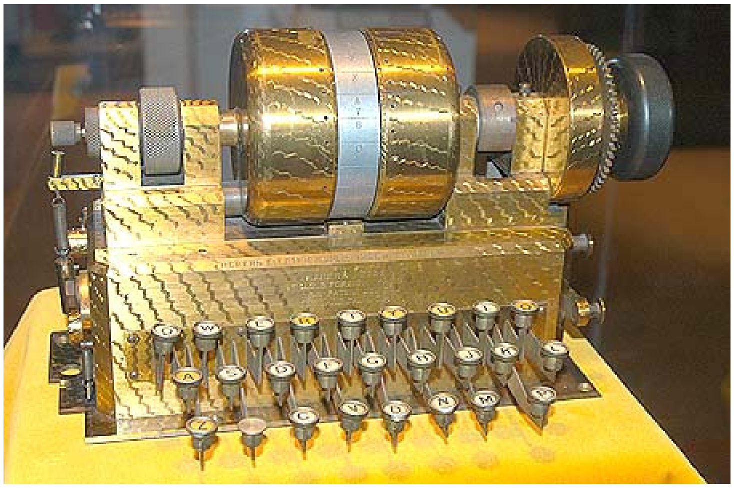
In Vigenere Cipher a random keyword is used to shift the letters.If the length of keyword is less than ciphertext repeat the process.

- let keyword be "CAB"

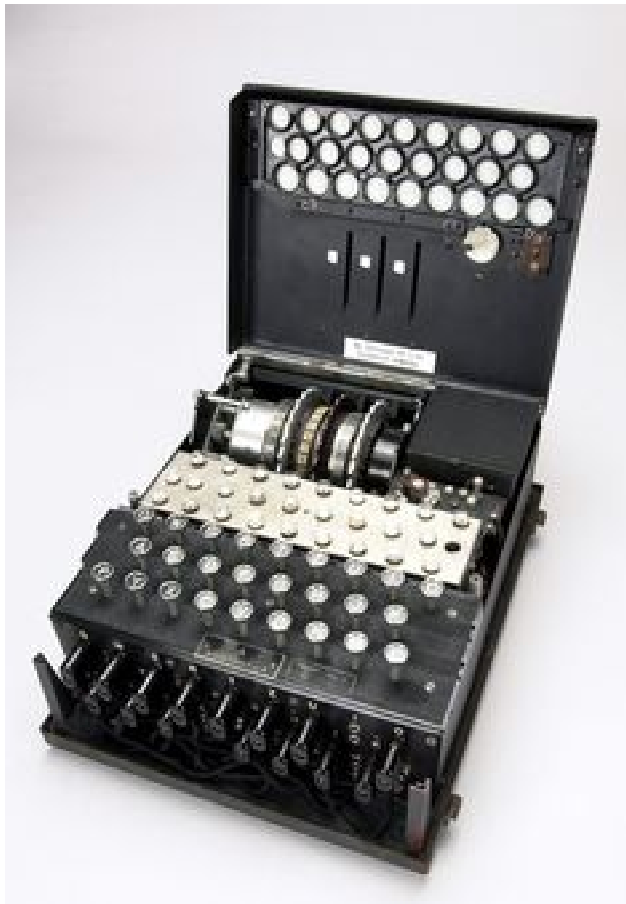
- Alphabets A-Z are mapped from 0 to 25
- shift using word "CAB" = 201
- For example lets take message "HELLO" key will be "CABCA" so it will be encrypted as H $\rightarrow$ J,E $\rightarrow$ E,L $\rightarrow$ M,L $\rightarrow$ N,O $\rightarrow$ O as "JEMNO"
- Even Vigenere Cipher can be broken by frequency analysis by guessing key length and analyzing frequencies.

2.5 Rotor Machines

Encryption based on rotor machines.
Following is a Hebern rotor.



- Rotor encodes the key
- Typed symbol is encrypted with the next symbol on the rotor
- As a letter is typed rotor moves changing the key each time.
- A Cycle is measured after which the key starts repeating
- Then came machines with more rotors, more rotors means bigger the key space.
  Following is Enigma rotor machine



- More rotors means more keys approximately 2^{36} in Enigma with 3 rotors.
- But these are susceptible to known cryptanalysis methods.
- Friedman had several important cryptanalysis methods for Hebern.
- Even improved and highly optimized by others.
- Turing designed a machine to search for Enigma key from known ciphertexts/plaintext pairs.

2.6 Digital Age

- In 1974 Data Encryption Standard (DES) was designed by IBM in response to governments call for a good encryption standard
- DES has roughly 256 keys and is not considered safe with todays computing powers.
- Advanced Encryption Standard (AES):
  - AES is designed by Vincent Rijmen and Joan Daemen in 1998 and is originally called Rijndael.
  - Selected and standardized by the US government through intense competition.

  - AES comes with different key sizes and other parameters (typical for such ciphers)

- There are many other ciphers today, for example Salsa, Twofish etc.,

2.7 As of today

- Even as of today design of such symmetric ciphers is an ongoing process.
- Ciphers like AES are not yet broken officially.
- Weaknesses created by replacing parameters with new parameters or using new ciphers are discovered.
- These ciphers are quite fast and practical to use.So practical applications will always rely on them as the main method. A different approach to designing ciphers will be:
  - Taking the cryptanalysis out of the equation altogether and proving the cipher is hard to break.
  - Although it is possible and practical, slow speed is its main drawback and might not be as fast as say AES.

2.8 Beyond Secret Communication

- In future classes study of encryption schemes that allow secret communication will be discussed in detail.
- Cryptography can do a lot more than secure communication.For example
  - Digital Signatures :
    A digital signature is a mathematical scheme for demonstrating the authenticity of digital messages or documents. A valid digital signature gives a recipient reason to believe that the message was created by a known sender (authentication), that the sender cannot deny having sent the message (non-repudiation), and that the message was not altered in transit (integrity).
  - Digital Cash:
    Digital cash mimics the functionality of paper cash. More technically, digital cash is a payment message bearing a digital signature which functions as a medium of exchange or store of value.
  - Electronic voting :
    An electronic voting system works as follows: before voting, a voter must first communicate with a registration authority, who provides the voter with a token. This token is used to vote: it is given to the party in charge of tabulation.
  - Zero Knowledge Proofs:
    A zero-knowledge proof or zero-knowledge protocol is a method by which one party (the prover) can prove to another party (the verifier) that a given statement is true, without conveying any information apart from the fact that the statement is indeed true.

- Secure multiparty computation:
  Secure multi-party computation is also known as secure computation, multi party computation/MPC, or privacy-preserving computation with the goal of creating methods for parties to jointly compute a function over their inputs while keeping those inputs private.

Always use Provable security approach and strive for constructions that are mathematically proven hard to break.

2.9 Cryptography as a rigorous science

- Functionality: Understanding what needs to be done.
- Threat Model: Who and what are we protecting from and propose a construction
- Proving that breaking the construction is either impossible, or at least as hard as solving some known "hard problem".

2.10 Useful Resources

http://norvig.com/mayzner.htm