Classical Encryption Techniques

Basic Terminology

- **Plaintext:** original message
- **Ciphertext:** coded message
- **Cipher:** algorithm for transforming plaintext to ciphertext
- **Key:** information (usually a string of characters) used in cipher, to encrypt plaintext, known only by the sender and the receiver
- **Encipher (encrypt):** the process of converting plaintext to ciphertext
- **Decipher (decrypt):** the process of recovering ciphertext from plaintext
- **Cryptography:** the study of encryption principles/methods
- **Cryptanalysis (codebreaking):** the study of principles/ methods of deciphering ciphertext *without* knowing key
- **Cryptology:** field of both cryptography and cryptanalysis

Symmetric Encryption

Also known as conventional / private-key / single-key

- sender and recipient share a common key
- all classical encryption algorithms are private key
- was the only type prior to invention of public-key in 1970's
- and by far the most widely used

Symmetric Cipher Model

Requirements

There are two requirements for secure use of symmetric encryption:

1) a strong encryption algorithm
2) a secret key known only to sender / receiver

- Mathematically have:
- $Y = E(K, X)$
- $X = D(K, Y)$
- assume encryption algorithm is known
- implies a secure channel to distribute key

Cryptography

- can characterize cryptographic system by:
  - type of encryption operations used
- substitution
- transposition
- product
  - number of keys used
- single-key or private
- two-key or public
  - way in which plaintext is processed
- block
- stream

Cryptanalysis

- objective to recover key not just message
- general approaches:
  - cryptanalytic attack
  - brute-force attack
- if either succeed all key use compromised

Cryptanalytic Attacks

- **ciphertext only**
- only know algorithm & ciphertext, is statistical,
- know or can identify plaintext
- **known plaintext**
- know/suspect plaintext & ciphertext
- **chosen plaintext**
- select plaintext and obtain ciphertext
- **chosen ciphertext**
- select ciphertext and obtain plaintext
- **chosen text**
- select plaintext or ciphertext to en/decrypt

More Definitions

- **unconditional security**
- no matter how much computer power or time is
- available, the cipher cannot be broken since the
- ciphertext provides insufficient information to
- uniquely determine the corresponding plaintext
- **computational security**
- given limited computing resources (eg time
- needed for calculations is greater than age of
- universe), the cipher cannot be broken

Brute Force Search

- • always possible to simply try every key
- • most basic attack, proportional to key size
- • assume either know / recognise plaintext

Classical Substitution Ciphers

- where letters of plaintext are replaced by
- other letters or by numbers or symbols
- or if plaintext is viewed as a sequence of bits,
- then substitution involves replacing plaintext
- bit patterns with ciphertext bit patterns

Caesar Cipher

- earliest known substitution cipher
- by Julius Caesar
- first attested use in military affairs
- replaces each letter by 3rd letter on
- example:
- meet me after the toga party
- PHHW PH DIWHU WKH WRJD SDUWB

Caesar Cipher

- can define transformation as:
- a b c d e f g h i j k l m n o p q r s t u v w x y z
- D E F G H I J K L M N O P Q R S T U V W X Y Z A B C
- mathematically give each letter a number
- a b c d e f g h i j k l m n o p q r s t u v w x y z
- 0 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25
- then have Caesar cipher as:
- $c = E(k, p) = (p + k) \bmod (26)$
- $p = D(k, c) = (c - k) \bmod (26)$

Cryptanalysis of Caesar Cipher

- only have 26 possible ciphers
- A maps to A,B,..Z
- could simply try each in turn
- a **brute force search**
- given ciphertext, just try all shifts of letters
- do need to recognize when have plaintext
- eg. break ciphertext "GCUA VQ DTGCM"

Monoalphabetic Cipher

- rather than just shifting the alphabet
- could shuffle (jumble) the letters arbitrarily
- each plaintext letter maps to a different random
- ciphertext letter
- hence key is 26 letters long
- Plain: abcdefghijklmnopqrstuvwxyz
- Cipher: DKVQFIBJWPESCXHTMYAUOLRGZN
- Plaintext: ifwewishtoreplaceletters
- Ciphertext: WIRFRWAJUHYFTSDVFSFUUFYA

Monoalphabetic Cipher Security

- now have a total of 26! = 4 x 1026 keys
- with so many keys, might think is secure
- but would be **!!!WRONG!!!**
- problem is language characteristics

Language Redundancy and Cryptanalysis

- human languages are **redundant**
- eg "th lrd s m shphrd shll nt wnt"
- letters are not equally commonly used
- in English E is by far the most common letter
- followed by T,R,N,I,O,A,S
- other letters like Z,J,K,Q,X are fairly rare
- have tables of single, double & triple letter
- frequencies for various languages

English Letter Frequencies

Use in Cryptanalysis

- key concept - monoalphabetic substitution ciphers
- do not change relative letter frequencies
- discovered by Arabian scientists in 9th century
- calculate letter frequencies for ciphertext
- compare counts/plots against known values
- if caesar cipher look for common peaks/troughs
- peaks at: A-E-I triple, NO pair, RST triple
- troughs at: JK, X-Z
- for monoalphabetic must identify each letter
- tables of common double/triple letters help

Example Cryptanalysis

- given ciphertext:
- UZQSOVUOHXMOPVGPOZPEVSGZWSZOPFPESXUDBMETSXAIZ
- VUEPHZHMDZSHZOWSFPAPPDTSVPQUZWYMXUZUHSX
- EPYEPOPDZSZUFPOMBZWPFUPZHMDJUDTMOHMQ
- count relative letter frequencies (see text)
- guess P & Z are e and t
- guess ZW is th and hence ZWP is the
- proceeding with trial and error finally get:
- it was disclosed yesterday that several informal but
- direct contacts have been made with political
- representatives of the Viet Cong in Moscow

One-Time Pad

- if a truly random key as long as the message is used,
- the cipher will be secure
- called a One-Time pad
- is unbreakable since ciphertext bears no statistical
- relationship to the plaintext
- since for **any plaintext** & **any ciphertext** there exists
- a key mapping one to other
- can only use the key **once** though
- problems in generation & safe distribution of key

Summary