Intro to Cryptography

Youhan Cheery

24 April 2017

1 Introduction

- Cryptogrophy is not the same as cryptanalysis
- Goals:
  - Confidentiality
  - Integrity
  - Authentication
  - Non-repudiation - sender cannot deny sending the message
- Crypto primitives: building blocks of a crypto system.. unkeyed (0 keys, e.g. hashing), symmetric (1 key, e.g. block and stream ciphers), asymmetric (2 keys, e.g. RSA)
- Why keys? Easiest way to get secret after compromise is too have very few very little secrets. Changing the key is much easier than changing the entire system

2 Caesar Cipher

- Caesar cipher - classical cipher that involves shifting the alphabet
- Cardinality = number of keys you can use in a cipher
- Activity 1: key = 3, flag = "bruteforceisbestforce"

3 Substitution Cipher

- Substitution cipher is an alphabet mapping that is then used to encrypt

$$E_pi(i) = pi(i)D_pi(i) = pi^{-1}(j)$$

- Cardinality is 26!. This means brute force is probably not the way to go. Use frequency analysis instead.

- Frequency analysis only works when there is a lot of text to analyse. When there's less characters, frequencies of letters becomes more random than anything that follows a distribution
- "Unicity distance" = how much ciphertext you need to break something via brute force. For substitution cipher this is 28.
- Activity 2: solution: THE BREAKING OF CIPHERS IS CALLED CRYPTANALYSIS. CRYPTANALYSIS IS USED TO BREACH CRYPTOGRAPHIC SECURITY SYSTEMS AND GAIN ACCESS TO THE CONTENTS OF ENCRYPTED MESSAGES, EVEN IF THE CRYPTOGRAPHIC KEY IS UNKNOWN. IN ADDITION TO MATHEMATICAL ANALYSIS OF CRYPTOGRAPHIC ALGORITHMS, CRYPTANALYSIS INCLUDES THE STUDY OF SIDE-CHANNEL ATTACKS THAT DO NOT TARGET WEAKNESSES IN THE CRYPTOGRAPHIC ALGORITHMS THEMSELVES, BUT INSTEAD EXPLOIT WEAKNESSES IN THEIR IMPLEMENTATION.

4 Vigenere Cipher

- Vigenere cipher is r different Caesar ciphers applied periodically = polyalphabetic mono-substitution cipher

$$E_k(M_i) = (M_i + K_i) mod 26$$

$$D_k(X_i) = (X_i - K_i) mod 26$$

- Frequency can still work for Vigenere cipher
- Index of Coincidence, IC, is the probability of selecting two random letters of them being the same.
- Use the IC to first get the key length and then decrypt by "columns"