CRYPTOGRAPHIC ALGORITHMS AND PROTOCOLS

PART I: CRYPTOGRAPHY

2.2. More Classical Ciphers

Playfair Cipher

- Not even the large number of keys in a monoalphabetic cipher provides security
- One approach to improving security was to encrypt multiple letters
- The Playfair Cipher is an example
- Invented by Charles Wheatstone in 1854, but named after his friend Baron Playfair

Playfair Key Matrix

- A 5X5 matrix of letters based on a keyword
- Fill in letters of keyword (sans duplicates)
- Fill rest of matrix with other letters
- eg. using the keyword ***MONARCHY***

M	O	N	A	R
C	H	Y	B	D
E	F	G	I/J	K
L	P	Q	S	T
U	V	W	X	Z

Encrypting and Decrypting

Plaintext is encrypted two letters at a time:

1. If a pair is a repeated letter, insert filler like 'X'
2. If both letters fall in the same row, replace each with letter to right (wrapping back to start from end)
3. If both letters fall in the same column, replace each with the letter below it (again wrapping to top from bottom)
4. Otherwise each letter is replaced by the letter in the same row and in the column of the other letter of the pair

Security of Playfair Cipher

- Security much improved over monoalphabetic
- Since have 26 x 26 = 676 digrams
- Would need a 676 entry frequency table to analyse (verses 26 for a monoalphabetic) and correspondingly more ciphertext
- Was widely used for many years
  - eg. by US & British military in WW1
- It can be broken, given a few hundred letters since still has much of plaintext structure

Vigenère Cipher

- Simplest polyalphabetic substitution cipher
- Effectively multiple caesar ciphers
- Key is multiple letters long $K = k_1 \ k_2 \ldots k_m$
- I^{th} letter specifies the I^{th} alphabet to use
- Use each alphabet in turn
- Repeat from start after m letters in message
- Decryption simply works in reverse

Example of Vigenère Cipher

- Write the plaintext out $P = p_0, p_1, \ldots\ldots, p_{n-1}$
- Write the keyword repeated above it.
- $K = k_0, k_1, \ldots\ldots, k_{m-1}$ such that $m<n$
- Encrypt the corresponding plaintext letter
- $Ci = (p_i + k_i \bmod m) \bmod 26$
- Ex: using keyword deceptive
  - key: deceptivedeceptivedeceptive
  - plaintext: wearediscoveredsaveyourself
  - ciphertext:ZICVTWQNGRZGVTWAVZHCQYGLMGJ

Security of Vigenère Ciphers

- Have multiple ciphertext letters for each plaintext letter
- Hence letter frequencies are obscured
- But not totally lost
- Start with letter frequencies, See if look monoalphabetic or not
- If not, then need to determine number of alphabets, since then can attack each

Kasiski Method

- Method developed by Babbage / Kasiski
- Repetitions in ciphertext give clues to period
- So find same plaintext an exact period apart which results in the same ciphertext
- e.g. repeated “VTW” in previous example suggests size of 3 or 9; of course, could also be random fluke
- Then attack each monoalphabetic cipher individually using same techniques as before

Autokey Cipher

- Vigenère proposed the autokey cipher.
- Ideally want a key as long as the message with a keyword prefixed to message as key.
- Knowing keyword can recover the first few letters, use these in turn on the rest of the message
- But still have frequency characteristics to attack.
- eg. given key deceptive
  - key: deceptivewearediscoveredsav
  - plaintext: wearediscoveredsaveyourself
  - ciphertext:ZICVTWQNGKZEIIGASXSTSLVVWLA

Codebook Cipher

- Literally, a book filled with "codewords"
- Modern block ciphers are codebooks!
- Zimmerman Telegram encrypted via codebook

Februar	13605
fest	13732
finanzielle	13850
folgender	13918
Frieden	17142
Friedenschluss	17149
:	:

Codebook Cipher: Additive

- Codebooks also (usually) use **additive**
- Additive — book of "random" numbers
  - Encrypt message with codebook
  - Then choose position in additive book
  - Add additives to get ciphertext
  - Send ciphertext and additive position (MI)
  - Recipient subtracts additives before decrypting
- Why use an additive sequence?

Claude Shannon

- The founder of Information Theory 1949
- Fundamental concepts
  - **Confusion**— obscure relationship between plaintext and ciphertext
  - **Diffusion**— spread plaintext statistics through the ciphertext
- Proved one-time pad is secure
- One-time pad is confusion-only, while double transposition is diffusion-only

Taxonomy of Cryptography

- **Symmetric Key**
  - Same key for encryption and decryption
  - Two types: Stream ciphers, Block ciphers
- **Public Key** (or asymmetric crypto)
  - Two keys, one for encryption (public), and one for decryption (private)
  - And digital signatures — nothing comparable in symmetric key crypto
- **Hash algorithms**
  - Can be viewed as "one way" crypto

Taxonomy of Cryptanalysis

From perspective of info available to Trudy

- Ciphertext only
- Known plaintext
- Chosen plaintext
- Protocols might encrypt chosen data
- Related key
- Forward search (public key crypto)
- And others…