Week 3 - Friday

COMP 4290

Last time

- What did we talk about last time?
- Modular arithmetic
- Shift ciphers
- Transposition ciphers
- Substitution ciphers
- Started Vigenère cipher

Questions?

Project 1

Giorgio Armani
1934 - 2025

Photo Credit: Fairchild Archive

Security tidbit of the day

- Cloudflare just defended against the biggest DDoS attack (ever?) over the Labor Day weekend
- Cloudflare is a tech company that provides content delivery networks (CDN) and security services to a big chunk of the Internet
- The attack is simple: send TONS of bad UDP packets, requiring servers to respond that a service can't be found that matches the UDP
- The hard part of doing an attack like this is controlling a large enough botnet to send all the packets
- This attack was 11.5 terabits per second
  - 5.1 billion packets delivered in 35 seconds
  - About 60% faster than the previous record-holder of 7.3 terabits per second
- The attack targeted one of Cloudflare's clients, but they haven't said who
- Follow the story:
  - https://www.zdnet.com/article/cloudflare-stops-new-worlds-largest-ddos-attack-over-labor-day-weekend/

Vigenère Cipher

Vigenère cipher

- The Vigenère cipher is a form of polyalphabetic substitution cipher
- In this cipher, we take a key word and repeat it, over and over, until it is as long as the message
- Then, we add the repetitions of keywords to our message mod 26

Vigenère example

- Key: BENCH
- Plaintext: A LIMERICK PACKS LAUGHS ANATOMICAL

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

Example continued

- Encrypt the following:
  - Plaintext: GENTLEMEN DINE AFTER SEVEN
  - Key: WILDE

- Decrypt the following:
  - Ciphertext: EOJKINOCQGEOJKI
  - Key: BOWIE

Cryptanalysis of Vigenère

- The index of coincidence measures the differences in the frequencies in the ciphertext
- It is the probability that two randomly chosen letters from the ciphertext are the same
- IC = $$\frac{1}{N(N-1)}\sum_{i=0}^{25} F_i(F_i-1)$$

Period	1	2	3	4	5	10	Large
Expected IC	0.066	0.052	0.047	0.045	0.044	0.041	0.038

Normalized index of coincidence

- Some systems look at a "normalized" index of coincidence, which is found by multiplying the formula given on the previous page by the number of letters in the language
  - 26 for English
  - When reading the literature, both normalized and unnormalized versions can be called index of coincidence
- Here are index of coincidence values for a few common languages

Language	Index
English	1.73
French	2.02
German	2.05
Italian	1.94
Portuguese	1.94
Russian	1.76
Spanish	1.94

Friedman test

- The Friedman test is a way to estimate the length of the key uses the following equation:
  - Length = $\frac{\kappa_p - \kappa_r}{\kappa_o - \kappa_r}$
  - κ_p = 0.067 (the probability that any two randomly chosen letters are the same in monocase English)
  - κ_r = 0.0385 = 1/26 (the probability of a coincidence from a uniform distribution of letters)
  - κ_o = $\frac{1}{N(N-1)} \sum_{i=0}^{25} F_i(F_i - 1)$ (the observed coincidence rate)

Kasiski method

- If the IC indicates that a period of more than 1 is being used, look for repeated sequences
- Look at the gaps between long sequences
- Try to find the GCD of gaps between long sequences
- If you have a reasonable guess for the length of the key, break the ciphertext into groups based on the corresponding letter of the key
- If the IC is high (in the range of a single letter), then you have probably found the key length

After the length is known…

- The rest is easy
- Try various shifts for each letter of the key so that high frequency letters (E, T, A) occur with high frequency and low frequency letters (Q, X, Z) occur with low frequency
- Guess and check

One-Time Pad

One-Time Pad

- A One-Time Pad is similar to the Vigenère cipher, except that the key is as long as the message
- What will this do to the index of coincidence?
- Any given ciphertext could be decrypted into any plaintext, provided that you have the right key

One-Time Pad example

- Key: THISISTHESECRETPASSWORD
- Plaintext: SOMEBODY SHOUTED MCINTYRE

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

- Now, use the key IFYOUDISSDRDRE to encrypt MELODY AND RHYME

One-Time Pad example continued

- Plaintext: SOMEBODY SHOUTED MCINTYRE

- Find a key (never done that before, have we?) that will encrypt the plaintext to YOUCOULDFINDTHEABSTRACT

Perfect secrecy

- A One-Time Pad has the property of **perfect secrecy** or **Shannon secrecy**
- Perfect secrecy means that $\mathbf{P}(M) = \mathbf{P}(M|C)$
  - Remember that it is possible to find a key that would decrypt a ciphertext to **any** plaintext
- Thus, learning the ciphertext tells you **nothing** about the plaintext (except a maximum bound on the length)

One-Time Pad weaknesses

- You can only use it one time
  - Otherwise, recovering the key is trivial
  - Completely vulnerable to known plaintext attack
- The key is as long as the message
- If you have a way of sending a key that long securely, why not send the message the same way?
- Generating keys with appropriate levels of randomness presents a problem

Secure Encryption Algorithms

How do you define good?

- Claude Shannon is the guy that invented Shannon secrecy and is considered the father of information theory
- He proposed 5 characteristics for a good cipher:

1. The amount of secrecy needed should determine the amount of labor appropriate for encryption and decryption
2. The set of keys and the enciphering algorithm should be free from complexity
3. The implementation of the process should be as simple as possible
4. Errors in ciphering should not propagate and cause corruption of further information in the message
5. The size of the enciphered text should be no larger than the text of the original message

A more modern view

- Shannon was focused on hand encryption
- Modern commercial users of cryptography want the following characteristics for their cryptosystems:
  - Based on sound mathematics
  - Analyzed by competent experts and found to be sound
  - Stood the test of time

Stream and Block Ciphers

Stream and block ciphers

- A common way of dividing ciphers is into **stream ciphers** and **block ciphers**
- Block ciphers divide messages into fixed length parts (or blocks) and encipher each part with the same key
- Stream ciphers encipher each message character by character
  - Some other authors define a stream cipher to be like a block cipher except that the key changes with each block based on the message

Self-synchronous stream ciphers

- Self-synchronous ciphers are stream ciphers that get the key from the message itself
- The simplest such cipher is an **autokey** cipher that uses the message itself for the key
- Essentially, this is similar to the Vigenère cipher with the key coming from the message
- Example:
  - Message: **`THISISTHEREMIX`**
  - Key: **`QTHISISTHEREMI`**
- Alternatively, the key can be drawn from the ciphertext
  - Message: **`THEBOYHASTHECAT`**
  - Key: **`XQXBCQOVVNGNRTT`**
  - Ciphertext: **`QXBCQOVVNGNRTTM`**

Confusion and Diffusion

- **Confusion** is the property of a cryptosystem that changing a single character in the plaintext should not have a predictable effect
- **Diffusion** is the property of a cryptosystem that each character in the plaintext should impact many characters in the ciphertext
- Examples:
  - Caesar cipher has poor confusion and no diffusion
  - One time pad has good confusion but no diffusion
  - Auto-key ciphers may have poor confusion but good diffusion
  - AES and DES have good confusion and diffusion within a block

Ticket out the Door

Upcoming

Next time…

- DES
- AES
- Jennifer Perez presents

Reminders

- Keep reading Sections 2.3 and 12.2
- Work on Project 1
  - Due next Friday
- Finish Assignment 1
  - **Due tonight by midnight!**