BONUS: INTRO TO CRYPTOGRAPHY

The art of secret writing!

BME 121 2016

Jeff Luo

Cryptography

- “Crypto”: secret
- “Graphy”: writing (like calligraphy, biography,…)
- From Greek words kryptós and graphein

- The necessities of politics, war, and governance have always included the need to keep communications secret and efficient between trusted friends
- At the same time, to gain advantage upon enemies, the art of Cryptanalysis came about: to break cryptographic systems

Cipher

- A single cryptographic system is called a cipher
  - Modern ones include RSA, DES, AES, Fiestel, and more… they are used to power up technologies like SSL, HTTPS, and secured e-commerce

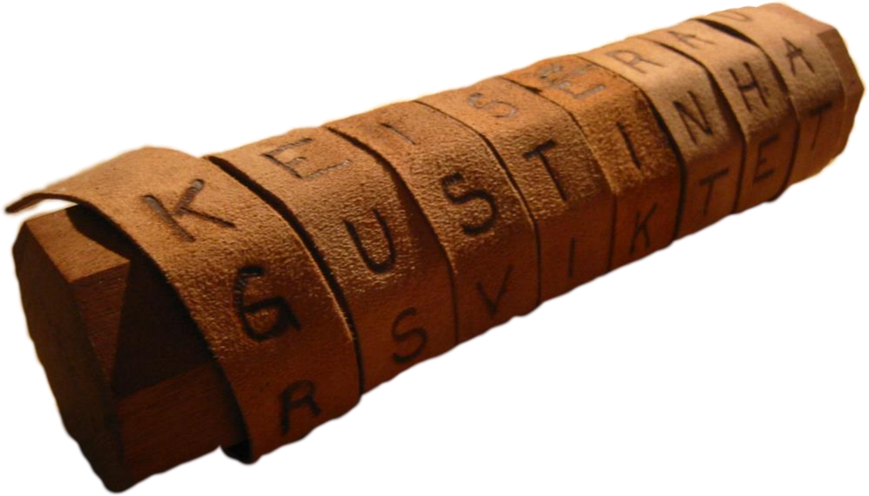
- We’ll look at two of the earliest ciphers in recorded history

Cryptography Basics

- **Plaintext**: the unencrypted, original message
  - `HELLO WORLD`
- **Ciphertext**: the encrypted message
  - `LAK$@#@EKJF`
- **Encryption**: the process of transforming plaintext into ciphertext, using a cipher
- **Decryption**: the process of transforming ciphertext into plaintext, using a cipher in reverse

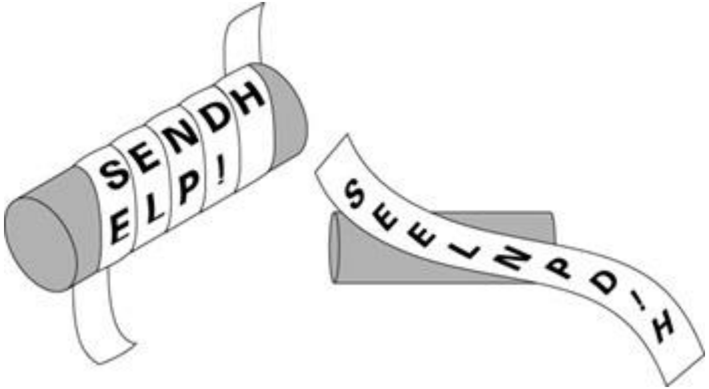
One of the Earliest Ciphers

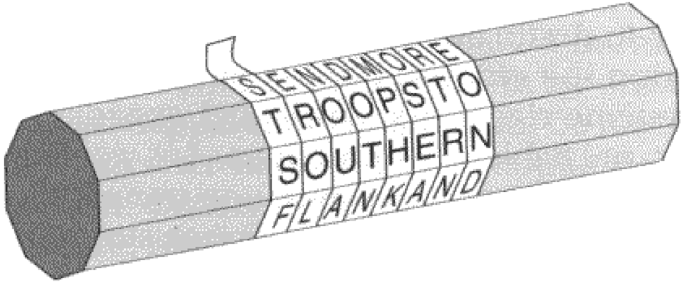
- In ancient Sparta, they used a Scytale (pronounced ska-teil) to wrap a piece of long paper or leather around to write secret messages



Spartan Scytale Cipher

- It is a Transposition Cipher
  - Letters are rearranged according to some “secret” order
- To properly decode the message, an friend or enemy must have a Scytale (or stick) with the same diameter, and wrap the paper according to the correct curvature





Breaking the Spartan Scytale Cipher

- Transposition Ciphertext exhibit a certain repeated rearrangement pattern, and its not too hard to recognize these:
- Can be broken in modern times by repeated trial and error, and the use of pattern finding and matching algorithms (including dictionaries)

T	I	I	S	A	T	H	S	S	P	R	A

THE CAESAR CIPHER!

- Named after Gaius Julius Caesar
- Formal Modern Name: Caesar Shift Cipher
- It is a Substitution Cipher

- For the majority of the 500 years of the Roman Empire, they used 1 cipher, in a basic or advanced configuration
- It fooled everyone!

THE CAESAR CIPHER!

1. Start with a plaintext alphabet
2. Shift the alphabet to the right by a number of positions to form the cipher alphabet (the amount of shift is the “password”, or Cryptographic Key)
3. Encryption: Replace each letter in the plaintext by its corresponding ciphertext in the alphabet
4. Decryption: Replace each letter in the ciphertext by its corresponding plaintext in the alphabet

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
x	y	z	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w

Example

- Plaintext: `grumpycat`
- Ciphertext: `dorjmvzxq`

- Try decrypting this: `kl`

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
x	y	z	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w

Breaking the Basic Caesar Cipher

- In Basic Caesar Cipher, the secret is the number of positions shifted
  - 26 letters: 26 shifts to try
  - One of them will look like correct legible language text, while the rest look like garbage text
- Not hard to break, but
- Literacy wasn't very common
  - This provided the actual security of using the Basic Caesar Cipher

Decryption shift	Candidate plaintext
0 (ciphertext)	`exxegoexsrgi`
1	`dwwdfndwrqfh`
2	`cvvcemcvqpeg`
3	`buubdlbupodf`
4	`attackatonce`
5	`zsszbjzsnmbd`
6	`yrryaiyrmlac`

Advanced Caesar Cipher

- Pick a word or phrase as a password:
  - EG: Biomedical
- Discard all repetitions of letters in the password:
  - Biomedcal
- This password begins the ciphertext alphabet, the rest of the alphabet follows in standard order, beginning at the last letter of the password

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
b	i	o	m	e	d	c	a	l	n	p	q	r	s	t	u	v	w	x	y	z	f	g	h	j	k

Example

- Plaintext: `grumpycat`
- Ciphertext: `cwzrujoby`

- Try decrypting this: `jex`

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
b	i	o	m	e	d	c	a	l	n	p	q	r	s	t	u	v	w	x	y	z	f	g	h	j	k

Breaking the Advanced Caesar Cipher

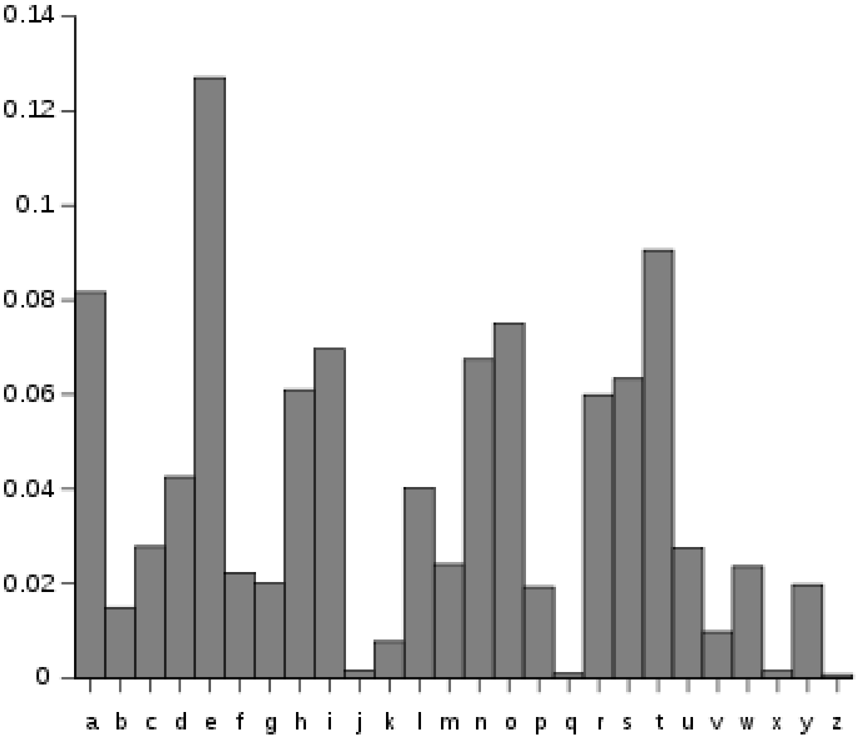
- Can’t simply shift and try, since the ciphertext alphabet is not in the same order as the plaintext…, but

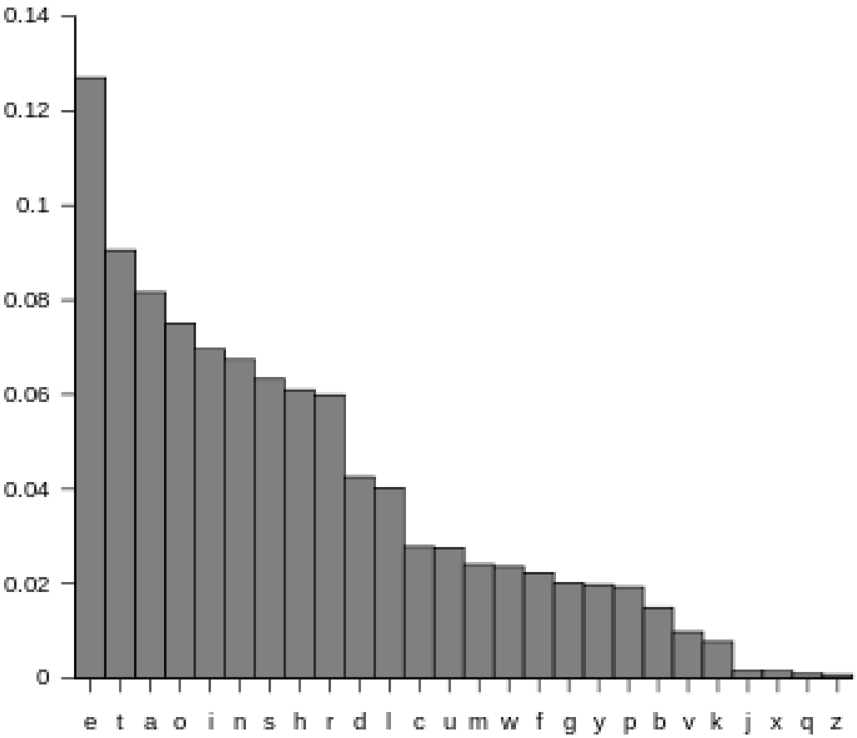
- Every language has a hidden statistical pattern:
  - The number of times each letter shows up in each word, message, essay … across collections and collections of documents

- Overall, the English language has the following relative frequencies:

a	**b**	**c**	**d**	**e**	**f**	**g**	**h**	**i**	**j**	**k**	**l**	**m**
8.17%	1.49%	2.78%	4.25%	12.70%	2.23%	2.02%	6.09%	6.97%	0.15%	0.77%	4.03%	2.41%
n	**o**	**p**	**q**	**r**	**s**	**t**	**u**	**v**	**w**	**x**	**y**	**z**
6.75%	7.51%	1.93%	0.10%	5.99%	6.33%	9.06%	2.76%	0.98%	2.36%	0.15%	1.97%	0.07%

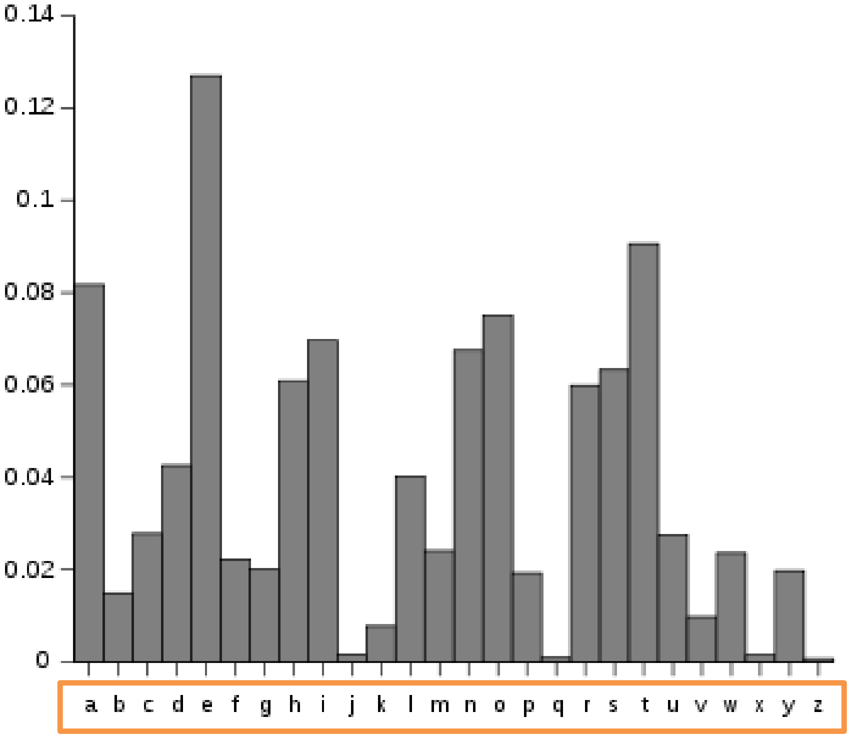
English Language Letter Frequency





Breaking the Advanced Caesar Cipher

- The Caesar Cipher simply reassigns the labels in the x axis of the histogram
- If you collect enough ciphertext (created with the same password), you can count the occurrence of each letter and then produce a histogram with the ciphertext letters as labels
- Match those labels with the ones in the plaintext language, and bingo!

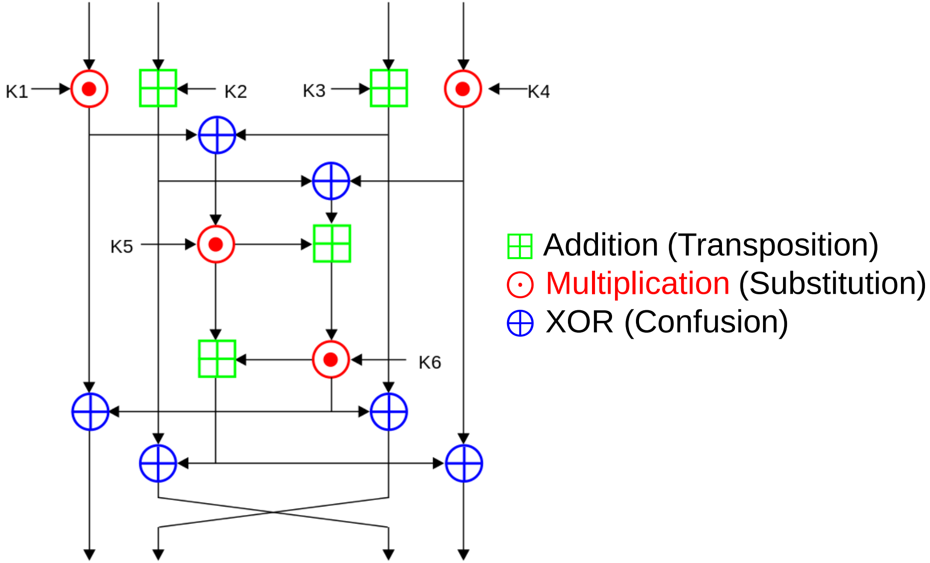


a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z
b	i	o	m	e	d	c	a	l	n	p	q	r	s	t	u	v	w	x	y	z	f	g	h	j	k

In Short

- Transposition Ciphers rearrange the plaintext to create the ciphertext
  - Vulnerable to guess work, or systematic trial and error
- Substitution Ciphers replace the plaintext using a specific alphabet to create the ciphertext
  - Vulnerable to Frequency Analysis
- Modern Ciphers do both at the same time, to stop both kinds of cryptanalysis and attacks

- They also have vulnerabilities of their own (Google DES attack cryptanalysis)



1 Round of a total of 8 in the IDEA Cipher

Summary / Practice: Encryption

- Strings are actually arrays of Chars
  - An array of Strings, is a 2D array of Chars…

- If string library methods cannot solve a string problem, then frame it as an array problem and solve it by converting the string into an array of characters:
  - someString.ToCharArray()

- With `EncryptionSkeleton.cs` as the starting point, study the code in method `Encrypt()` and then complete the method `Decrypt()`.