LING 120: Language and Computers

Semester: FALL 2017

Instructor: Sowmya Vajjala

Iowa State University, USA

16 October 2017

Outline

1. Language and ”secret writing” - an overview
   (based on the presentations by Jason Baldridge, Chris Brew and Marcus Dickinson)

Translation

1. Is translation something that can be thought of as secret writing? How many of you think so?

Translation

1. Is translation something that can be thought of as secret writing? How many of you think so?
2. Does anyone of you have parents who spoke a language you did not know?

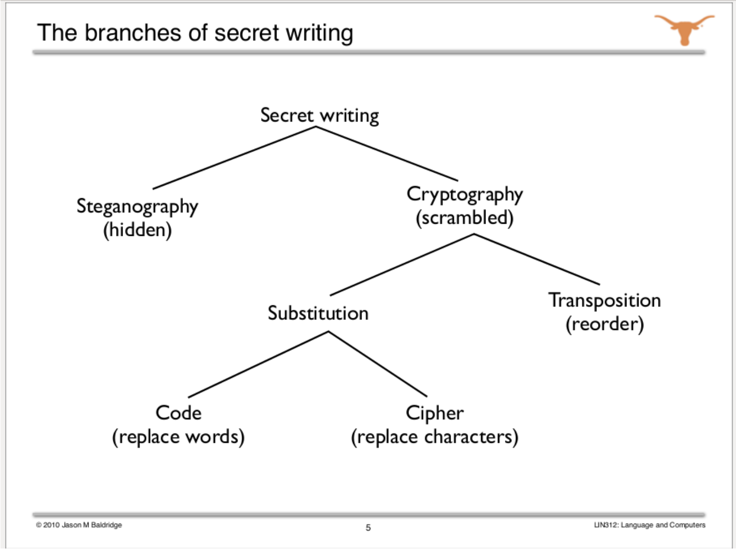
Translation

1. Is translation something that can be thought of as secret writing? How many of you think so?
2. Does anyone of you have parents who spoke a language you did not know?
3. Do you know about "Code Talkers"? `https://en.wikipedia.org/wiki/Code_talker`

Translation

1. Is translation something that can be thought of as secret writing? How many of you think so?
2. Does anyone of you have parents who spoke a language you did not know?
3. Do you know about "Code Talkers"? `https://en.wikipedia.org/wiki/Code_talker`
4. Cryptography has in some ways helped us crack forgotten writing systems.
5. communicate during war time.

Branches of secret writing



The branches of secret writing

Secret writing

Steganography (hidden)

Cryptography (scrambled)

Substitution

Transposition (reorder)

Code (replace words)

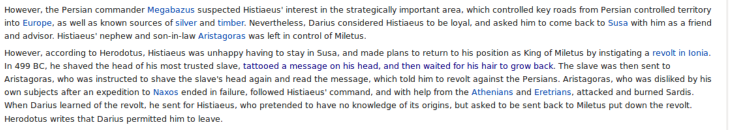
Cipher (replace characters)

Steganography

- No encryption, just hiding the message in something (e.g., invisible ink)

Steganography

- No encryption, just hiding the message in something (e.g., invisible ink)
- The story of Histiaeus:



However, the Persian commander Megabazus suspected Histiaeus' interest in the strategically important area, which controlled key roads from Persian controlled territory into Europe, as well as known sources of silver and timber. Nevertheless, Darius considered Histiaeus to be loyal, and asked him to come back to Susa with him as a friend and advisor. Histiaeus' nephew and son-in-law Aristagoras was left in control of Miletus.

However, according to Herodotus, Histiaeus was unhappy having to stay in Susa, and made plans to return to his position as King of Miletus by instigating a revolt in Ionia. In 499 BC, he shaved the head of his most trusted slave, tattooed a message on his head, and then waited for his hair to grow back. The slave was then sent to Aristagoras, who was instructed to shave the slave's head again and read the message, which told him to revolt against the Persians. Aristagoras, who was disliked by his own subjects after an expedition to Naxos ended in failure, followed Histiaeus' command, and with help from the Athenians and Eretrians, attacked and burned Sardis. When Darius learned of the revolt, he sent for Histiaeus, who pretended to have no knowledge of its origins, but asked to be sent back to Miletus put down the revolt. Herodotus writes that Darius permitted him to leave.

- provides some security, but once detected, anyone can read.

Modern Steganography

- Files (different forms of data) and Messages are hidden inside videos and pictures as well.

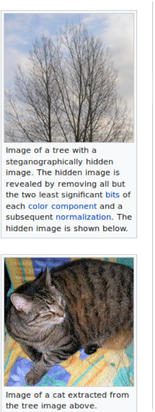


Image of a tree with a steganographically hidden image. The hidden image is revealed by removing all but the two least significant bits of each color component and a subsequent normalization. The hidden image is shown below.

Image of a cat extracted from the tree image above.

Cryptography

- messages are not hidden - they can be seen by others, but they cannot make any sense out of it.
- messages are encrypted.
- How?: simple encryptions are - interchanging letters, having a substitution map, or having a simple code (replace a with b, b with c, c with d and so on)

Cryptography

- messages are not hidden - they can be seen by others, but they cannot make any sense out of it.
- messages are encrypted.
- How?: simple encryptions are - interchanging letters, having a substitution map, or having a simple code (replace a with b, b with c, c with d and so on)
- What is cryptography?

Cryptography

- messages are not hidden - they can be seen by others, but they cannot make any sense out of it.
- messages are encrypted.
- How?: simple encryptions are - interchanging letters, having a substitution map, or having a simple code (replace a with b, b with c, c with d and so on)
- What is cryptography? - study of writing and breaking codes?
- what is the purpose?

Cryptography

- messages are not hidden - they can be seen by others, but they cannot make any sense out of it.
- messages are encrypted.
- How?: simple encryptions are - interchanging letters, having a substitution map, or having a simple code (replace a with b, b with c, c with d and so on)
- What is cryptography? - study of writing and breaking codes?
- what is the purpose? - secure communication
- where is it useful?

Cryptography

- messages are not hidden - they can be seen by others, but they cannot make any sense out of it.
- messages are encrypted.
- How?: simple encryptions are - interchanging letters, having a substitution map, or having a simple code (replace a with b, b with c, c with d and so on)
- What is cryptography? - study of writing and breaking codes?
- what is the purpose? - secure communication
- where is it useful? - paying with credit card online, transmitting our data across internet, passwords, military communication etc. (beyond language encryption)

How does it work?

- Encryption: some way to produce the cipher text
- key: details of this encryption so that the receiver can decrypt
- e.g., Caeser cipher: substitution cipher, where each letter in the original message is replaced with another letter a few numbers ahead in the alphabet.
- i.e., a shift 3 Caeser cipher replaces a with d, b with e and so on.

How does it work?

- Encryption: some way to produce the cipher text
- key: details of this encryption so that the receiver can decrypt
- e.g., Caeser cipher: substitution cipher, where each letter in the original message is replaced with another letter a few numbers ahead in the alphabet.
- i.e., a shift 3 Caeser cipher replaces a with d, b with e and so on.
- If am not the intended receiver and I am trying to read your message, what are my options??

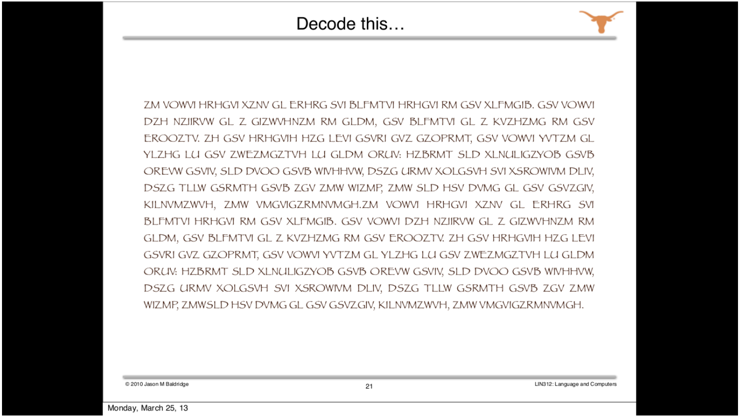
How does it work?

- Encryption: some way to produce the cipher text
- key: details of this encryption so that the receiver can decrypt
- e.g., Caeser cipher: substitution cipher, where each letter in the original message is replaced with another letter a few numbers ahead in the alphabet.
- i.e., a shift 3 Caeser cipher replaces a with d, b with e and so on.
- If am not the intended receiver and I am trying to read your message, what are my options??
- brute-force (try all possible combinations until I crack)

Encryption should be strong

- Weak encryption is worser than no-encryption.
- `https://www.simonsingh.net/The_Black_Chamber/maryqueenofscots.html`

how do we go about solving this?



Decode this…

ZM VOWVI HRHGVI XZNV GL ERHRG SVI BLFMTVI HRHGVI RM GSV XLFMGIB. GSV VOWVI DZH NZIIRVW GL Z GIZWVHNZM RM GLDM, GSV BLFMTVI GL Z KVZHZMG RM GSV EROOZTV. ZH GSV HRHGVIH HZG LEVI GSVRI GVZ GZOPRMT, GSV VOWVI YVTZM GL YLZHG LU GSV ZWEZMGZTVH LU GLDM ORUV: HZBRMT SLD XLNULIGZYOB GSVB OREVW GSVIV, SLD DVOO GSVB WIVHHVW, DSZG URMV XOLGSVH SVI XSROWIVM DLIV, DSZG TLLW GSRMTH GSVB ZGV ZMW WIZMP, ZMW SLD HSV DVMG GL GSV GSVZGIV, KILNVMZWVH, ZMW VMGVIGZRMNVMGH.ZM VOWVI HRHGVI XZNV GL ERHRG SVI BLFMTVI HRHGVI RM GSV XLFMGIB. GSV VOWVI DZH NZIIRVW GL Z GIZWVHNZM RM GLDM, GSV BLFMTVI GL Z KVZHZMG RM GSV EROOZTV. ZH GSV HRHGVIH HZG LEVI GSVRI GVZ GZOPRMT, GSV VOWVI YVTZM GL YLZHG LU GSV ZWEZMGZTVH LU GLDM ORUV: HZBRMT SLD XLNULIGZYOB GSVB OREVW GSVIV, SLD DVOO GSVB WIVHHVW, DSZG URMV XOLGSVH SVI XSROWIVM DLIV, DSZG TLLW GSRMTH GSVB ZGV ZMW WIZMP, ZMWSLD HSV DVMG GL GSV GSVZGIV, KILNVMZWVH, ZMW VMGVIGZRMNVMGH.

Monday, March 25, 13

How to solve systematically?-1

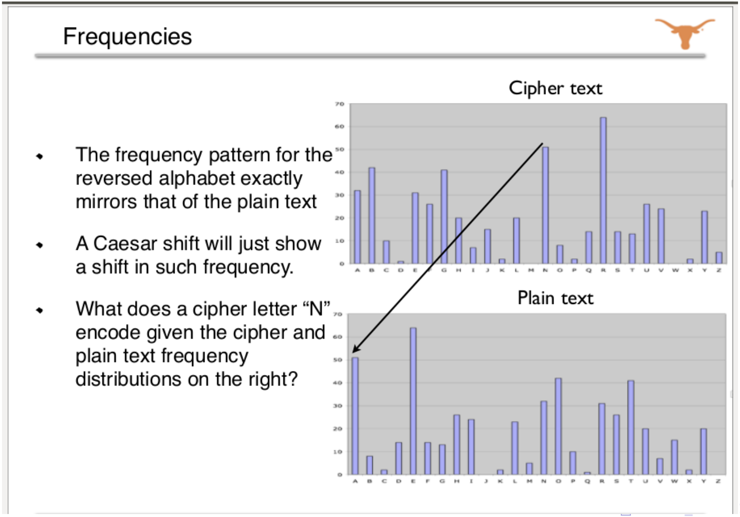
1. Make a table of characters
2. focus on a few common words, spot a few words. get a letter by letter mapping from there.
3. Chris Brew's slides (62–72)

How to solve systematically? -2

1. Calculate frequencies of characters in the cipher
2. Compare that with general frequency of characters in English.
3. Roughly, the order of frequencies should be the same.

How to solve systematically? -2

1. Calculate frequencies of characters in the cipher
2. Compare that with general frequency of characters in English.
3. Roughly, the order of frequencies should be the same.



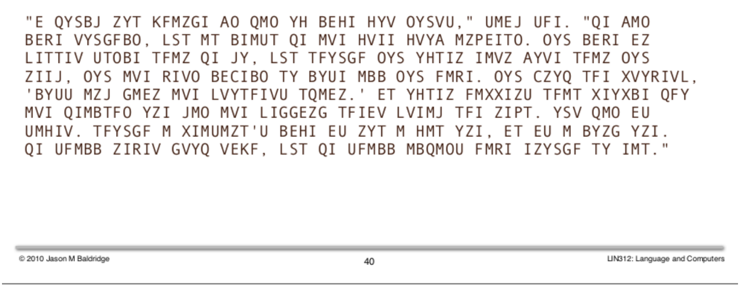
Frequencies

- The frequency pattern for the reversed alphabet exactly mirrors that of the plain text
- A Caesar shift will just show a shift in such frequency.
- What does a cipher letter “N” encode given the cipher and plain text frequency distributions on the right?

one-one mapping??

1. Assumption in previous slides is that we have a one-one mapping between letters in a language.
2. One-one mapping (mono alphabetic) based cipher is easy to decipher with word spotting and frequencies.
3. So, there are poly-alphabetic ciphers (where there is one-to-many mapping, depending on context!)
4. example: `https://goo.gl/D9dXIU`

Today’s attendance exercise



"E QYSBJ ZYT KFMZGI AO QMO YH BEHI HYV OYSVU," UMEJ UFI. "QI AMO BERI VYSGFBO, LST MT BIMUT QI MVI HVII HVYA MZPEITO. OYS BERI EZ LITTIV UTOBI TFMZ QI JY, LST TFYSGF OYS YHTIZ IMVZ AYVI TFMZ OYS ZIIJ, OYS MVI RIVO BECIBO TY BYUI MBB OYS FMRI. OYS CZYQ TFI XVYRIVL, 'BYUU MZJ GMEZ MVI LVYTFIVU TQMEZ.' ET YHTIZ FMXXIZU TFMT XIYXBI QFY MVI QIMBTFO YZI JMO MVI LIGGEZG TFIEV LVIMJ TFI ZIPT. YSV QMO EU UMHIV. TFYSGF M XIMUMZT'U BEHI EU ZYT M HMT YZI, ET EU M BYZG YZI. QI UFMBB ZIRIV GVYQ VEKF, LST QI UFMBB MBQMOU FMRI IZYSGF TY IMT."