Attack Methods

Alex Shaffer

Attack Methods Intro

- In the field of cryptanalysis, there are many different ways to try and break a cipher who's key you do not know.
- Many of these methods are a bit too complicated for the scope of this course but we will cover some basic ones, and what it takes for a cipher to be truly secure.

Attack types

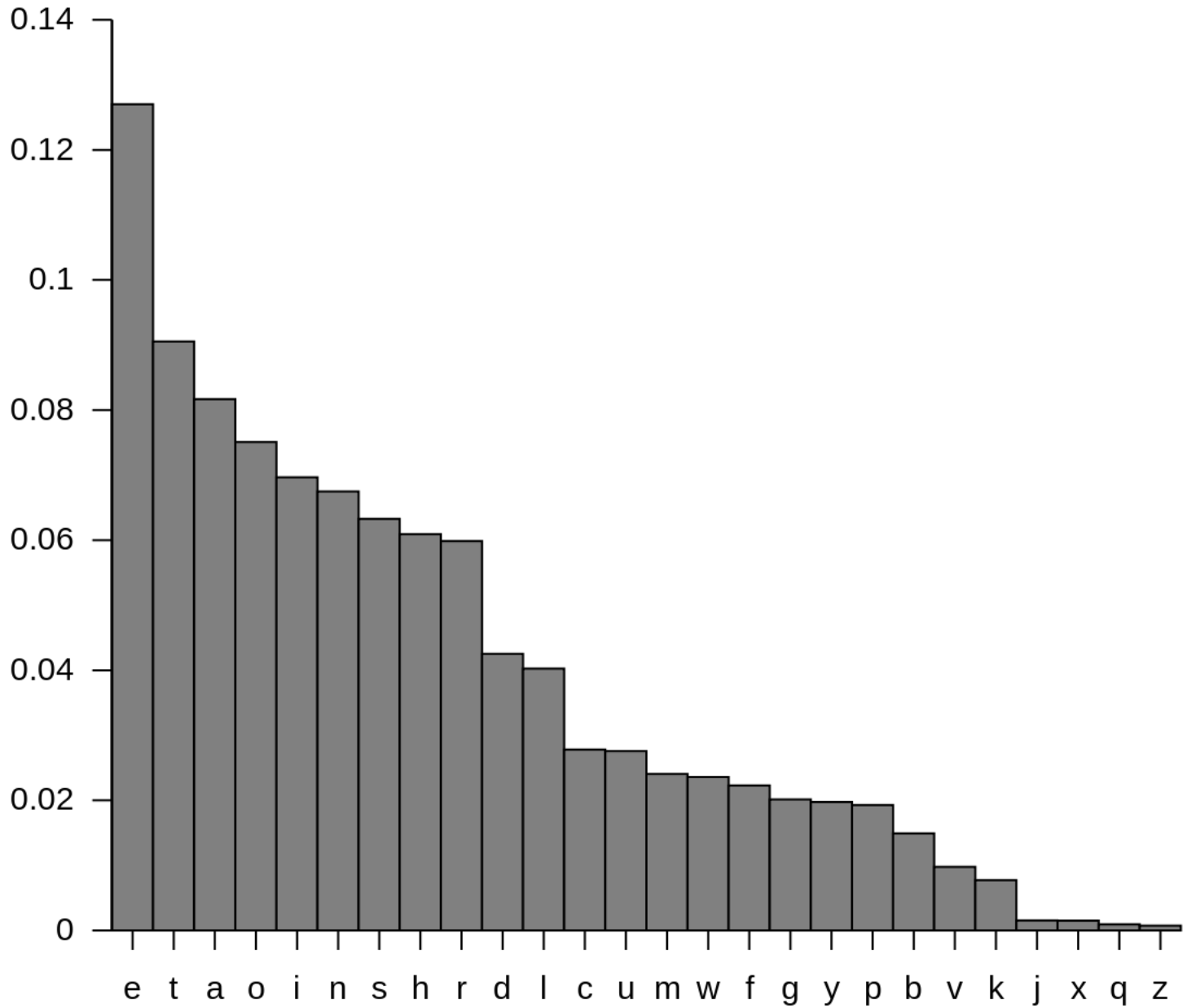
- Ciphertext only
  - Here the ciphertext is the only piece of information that the attacker has.
  - Typically, the most challenging to break.
  - The Caesar cipher was susceptible to this.
- Known plaintext
  - Here the attacker has information about the ciphertexts that correspond to plaintexts
- Chosen Plaintext
  - Here the attacker is able to supply plaintexts to an “oracle” which will provide corresponding plaintexts.

Breaking the Caesar Cipher

- The Caesar cipher, beautiful in its simplicity is not particularly secure.
- It’s first fault comes from its very low number of possible keys.
  - There are only 26 unique keys.
- If you know the language the message is written in then breaking it is as simple as trying 26 different keys.

Breaking the Caesar Cipher

- The second method for breaking the Caesar cipher is typically less work. It is called a frequency attack.
- The English language does not use every letter an equal number of times.
  - The letter ‘e’ is used far more often than the letter ‘z’.
- One can check the frequency with which letters appear in the cipher text, to determine which keys are the most likely.


0.14
0.12
0.1
0.08
0.06
0.04
0.02
0
e t a o i n s h r d l c u m w f g y p b v k j x q z

Breaking the Affine Cipher

- The Affine cipher may be broken in similar ways to the Caesar cipher.
  - Each letter is always encrypted to the same ciphertext letter.
    - Makes frequency analysis possible.
  - More keys that the Caesar cipher, but not a lot .
    - Makes brute forcing possible.
    - There are 312 key combinations (why?)

Further Reading

- Most of the more advanced attack methods are far too complicated for this course.
- If you are curious read from the following:
  - Linear cryptanalysis.
    - https://en.wikipedia.org/wiki/Linear_cryptanalysis
  - Differential cryptanalysis.
    - https://en.wikipedia.org/wiki/Differential_cryptanalysis
  - Integral cryptanalysis.
    - https://en.wikipedia.org/wiki/Integral_cryptanalysis