Course Overview

CMPUT 331

Singh’s Introduction

- epigraph: an inscription to suggest the theme
- the need for SECRET communication
- the battle between codemakers and codebreakers
- Singh’s objectives:
  - chart EVOLUTION of codes (bacteria, shields)
    - history is punctuated with codes
    - ancient scripts
  - show how cryptography is relevant today
    - phones, e-mail, networks, privacy, WikiLeaks
    - quantum computers and cryptography

Crypto Terms

- steganography vs. cryptography
- code vs. cipher
- plaintext vs. ciphertext
- encryption vs. decryption vs. cryptanalysis
- codemakers vs. codebreakers
- transposition vs. substitution

Terms are defined in Glossary at the end of Singh's book.

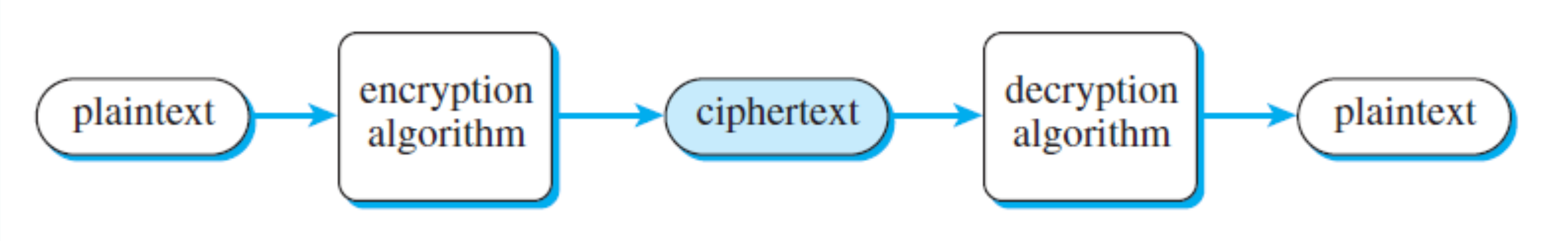
Definitions (1)

- **steganography** – the science of hiding a message
- **cryptography** – the science of encrypting a message
- **code** – a system for replacing each word with another word or string of characters, as specified in a **codebook**
- **cipher** – any general system for hiding the meaning of a message by replacing each letter with another letter
- **plaintext** – the original message before encryption
- **ciphertext** – the message (plaintext) after encipherment

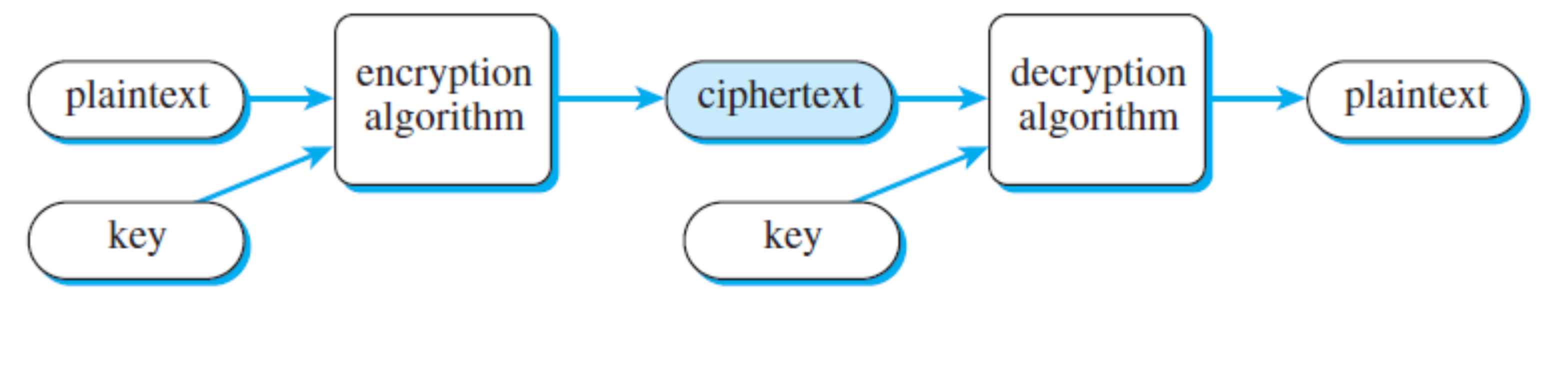
Definitions (2)

- **encrypt** – to encipher or encode (knowing the key)
- **decrypt** – to decipher or decode (knowing the key)
- **cryptanalysis** – deducing the plaintext from a ciphertext, <u>without knowing the key</u>
- **transposition** cipher – a system of encryption in which each character changes its position within the message
- **substitution** cipher – a system of encryption in which each character is replaced with another character

Encryption and decryption



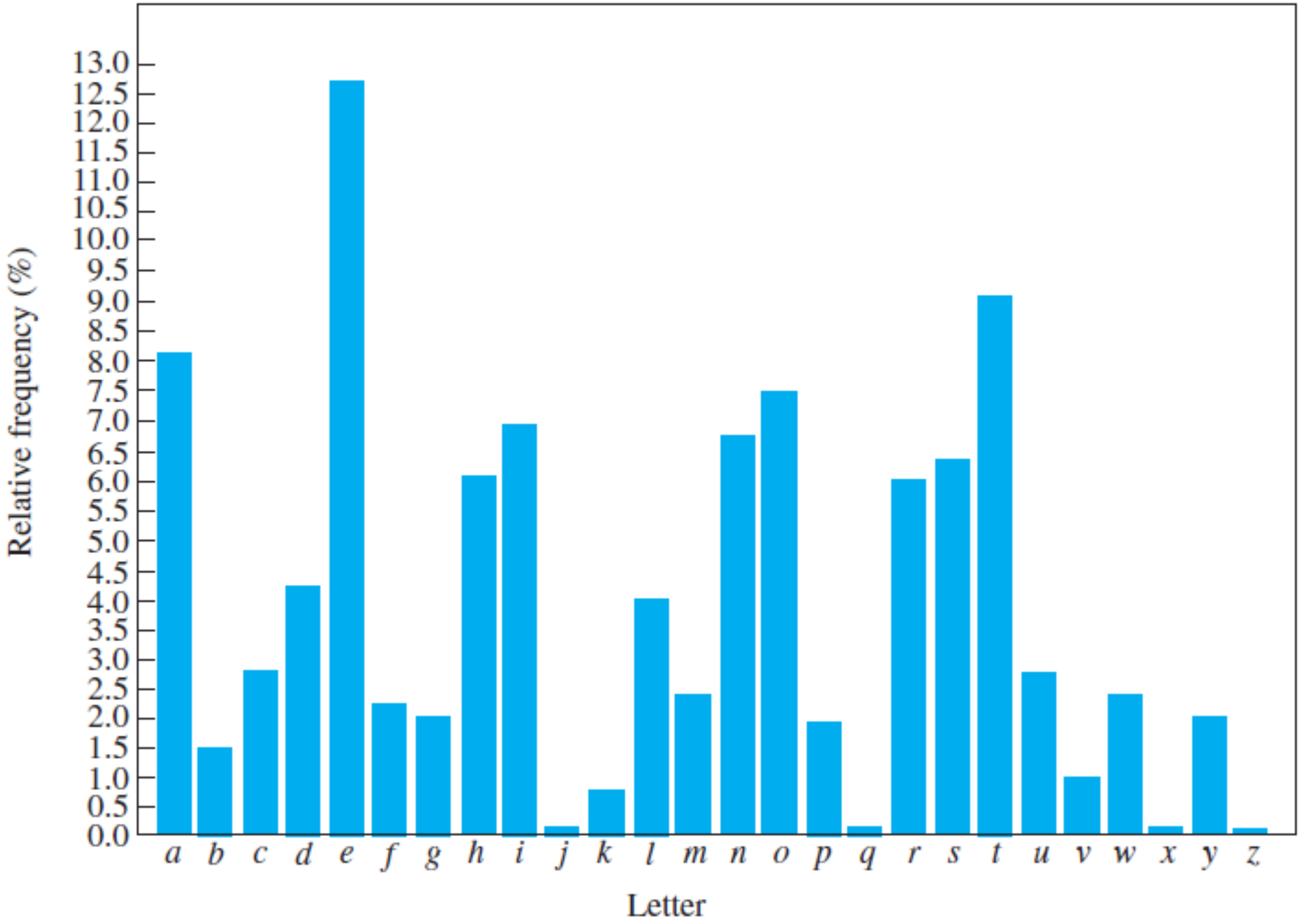
Encryption and decryption



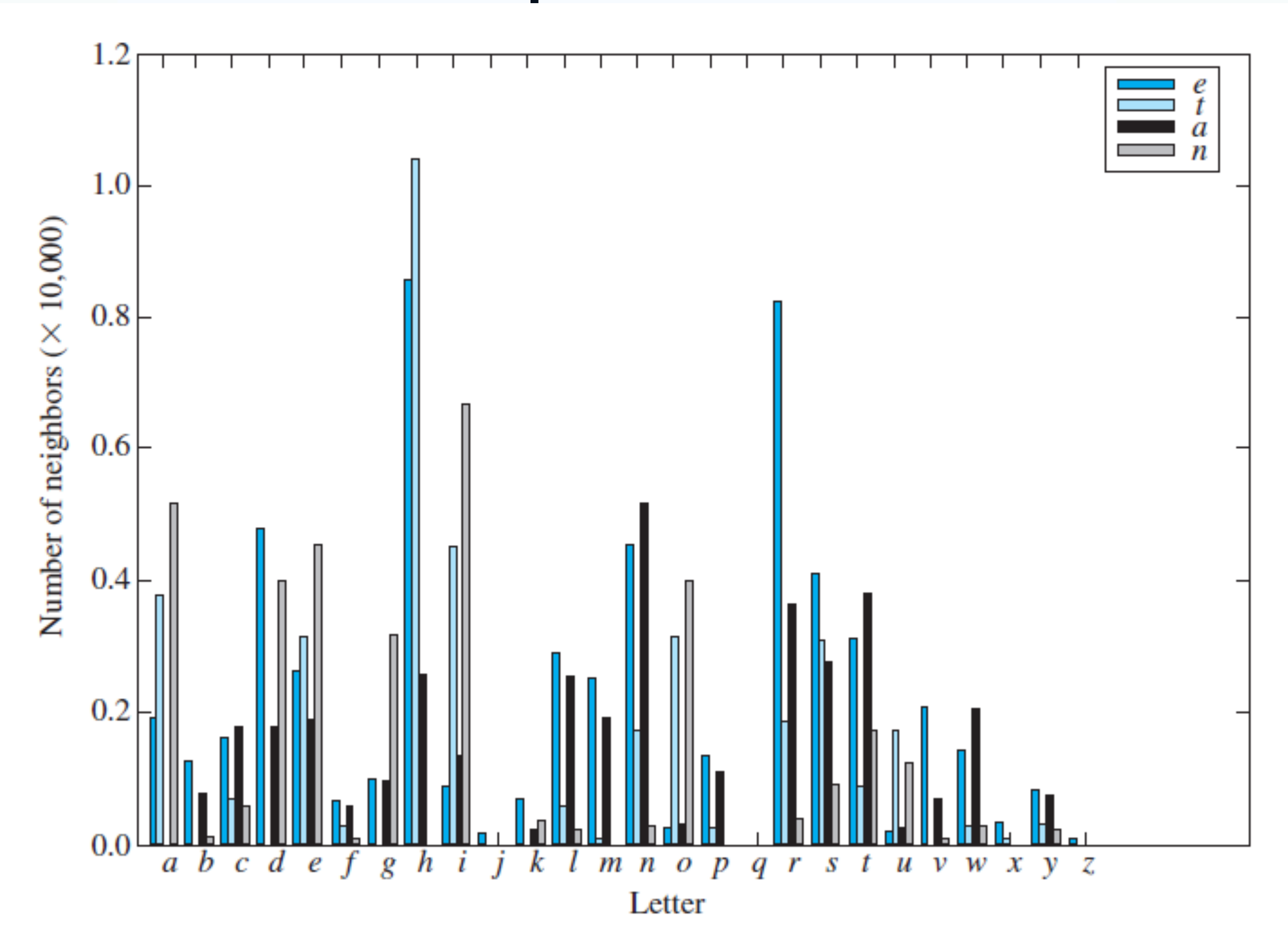
Code breaking

- Brute force: try all possible keys
- Letter frequency analysis
- Word dictionary matching
- Guessing parts of ciphertext
- Regular expressions
- Language models
- Spying

Relative letter frequencies



Some letter pair frequencies



Regular Expressions

Expression	Interpretation
.	match any character
[abc]	match *a* or *b* or *c*
[^abc]	match any character other than
[abc]+	match one or more occurrences
[abc]*	match zero or more occurrences
(*regex*)	create a capture group