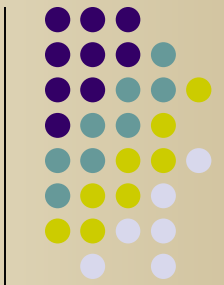
ENGR/CS 101 CS Session Lecture 5

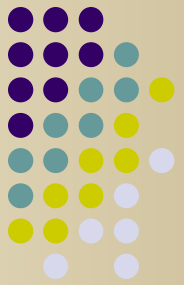


- No programming today
- Submission system will be demonstrated at the end of class.

Outline

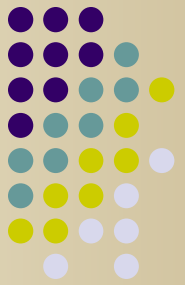
- Problem: How to send a secret message?
- Codes and ciphers
- Substitution ciphers

Problem:
How to send a secret message?



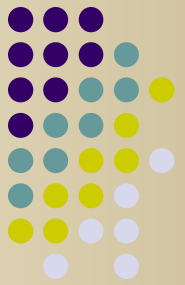
- ***Steganography*** ("concealed writing"): science of sending concealed messages. Includes physical concealment like invisible ink, microdots...
- ***Cryptography*** ("hidden writing"): how to obscure message so it cannot be read even if intercepted. Use codes and ciphers.

Codes & Ciphers



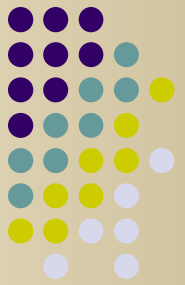
- ***Code***: whole words or phrases replaced by a word, letter, or a number. Like an alien language; uses translation code book.
- ***Cipher***: individual letters are replaced by other letters or symbols.
- ***Plaintext***: message in normal language
- ***Ciphertext***: message in secret form

Ciphers



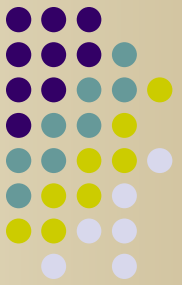
- Transposition cipher: rearrange letters of message.
  - Scytale: strip of writing material wrapped around a dowel; write message across dowel.
  - Block: arrange message into a block, rewrite vertical lines
- Substitution cipher: replace letters with other letters

Cipher = Algorithm + Key



- ***Algorithm***: a series of well-defined steps that can be followed as a procedure.
- ***Key***: auxiliary information used by an algorithm. Different keys produce different ciphers using the same algorithm.

Caesar Shift Cipher

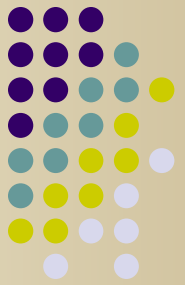


- Algorithm: substitute a letter with the letter *n* places to the right
- Key: letter to shift 'A' to that is n places to the right. E.g. A -> I is shifting 8 places to the right:

plain	A	B	C	D	E	F	G	H	I	J	K	L	M
cipher	I	J	K	L	M	N	O	P	Q	R	S	T	U

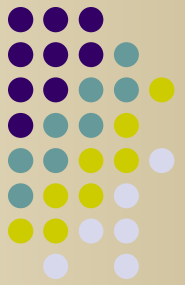
plain	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
cipher	V	W	X	Y	Z	A	B	C	D	E	F	G	H

In-class Exercise



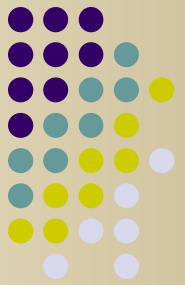
- Practice enciphering and deciphering using Caesar shift cipher.
- Turn in worksheet at the end of class.

What if the key is unknown?



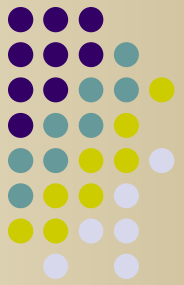
- How many possible keys are there for the Caesar Shift Cipher?
- How easy would it be to find the key?

Polyalphabetic Ciphers



- Make cipher harder to break by using multiple substitution alphabets
- Vigenere cipher: key is a "word" rather than just a single letter. Algorithm is to use the key letters to change the Caesar cipher shift key for each letter of plaintext.

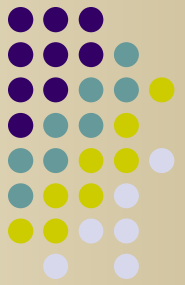
Vigenere Cipher Example



- For example, if the key word is "LION" and the plaintext message is "GO ACES", the ciphertext would be "RW OPPA", formed as shown to the right.

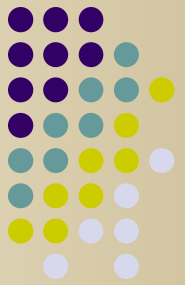
plain	key	cipher
G	L	R
O	I	W
A	O	O
C	N	P
E	L	P
S	I	A

Polyalphabetic Ciphers



- Suppose we allow any letter to be substituted by any other letter? E.g. a cryptoquip puzzle.
- The key would a substitution table mapping each letter to another letter.
- How many possible keys are there for this cipher?

400 Million Billion Billion

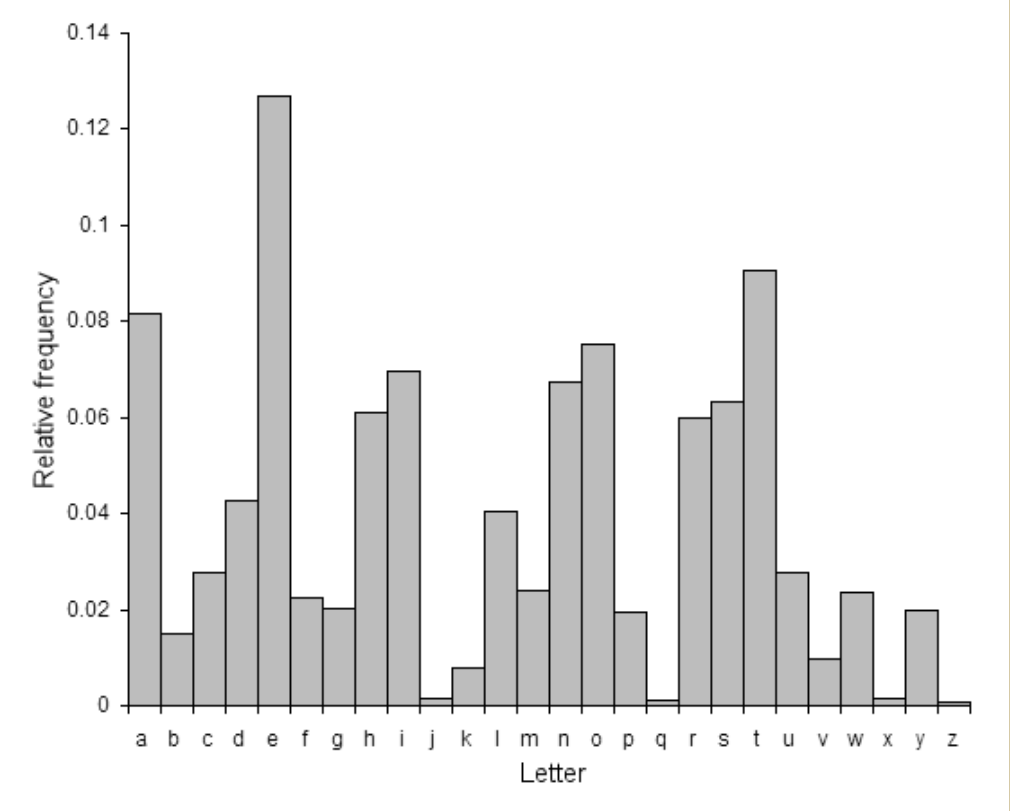


- Just how big is this number?
- 6.5 billion people on Earth; 31 million seconds in a year. If everyone on Earth checked one key per second, ...

- We can conclude that checking every possible key is not a feasible way of trying to decipher an arbitrary substitution cipher.

A Better Way to Decipher

- English letter frequency: E, T, A, O, ...
- One/two letter words: "I", "a", "to", "of", ...
- Common words: "the", "and", ...
- Repeated letters
- Context



Enigma Machine

- Random substitution cipher represented using a code wheel. Originally 3 code wheels, later 5 wheels.
- Instead of always starting with same letter on wheel as A, just encipher the current letter of plaintext with the next letter on wheel.