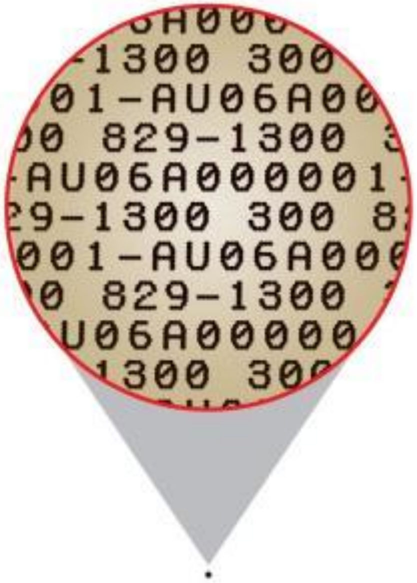
Secret writing



```
LIVITCSWPIYVEWHEVSRIQMXLEYVEOIEWHRXEXIP
FEMVEWHKVSTYLXZIXLIKIIXPIJVSZEYPERRGERI
MWQLMGLMXQERIWGPSRIHMXQEREKIETXMJTPRGEV
EKEITREWHEXXLEXXMZITWAWSQWXSWEXTVEPMRXR
SJGSTVRIEYVIEXCVMUIMWERGMIWXMJMGCSMWXSJ
OMIQXLIVIQIVIXQSVSTWHKPEGARCSXRWIEVSWII
BXVIZMXFSJXLIKEGAEWHEPSWYSWIWIEVXLISXLI
VXLIRGEPIRQIVIIBGIIHMWYPFLEVHEWHYPSRRFQ
MXLEPPXLIECCIEVEWGISJKTVWMRLIHYSPHXLIQI
MYLXSJXLIMWRIGXQEROIVFVIZEVAEKPIEWHXEAM
WYEPPXLMWYRMWXSGSWRMHIVEXMSWMGSTPHLEVHP
FKPEZINTCMXIVJSVLMRSCMWMSWVIRCIGXMWYMX
```

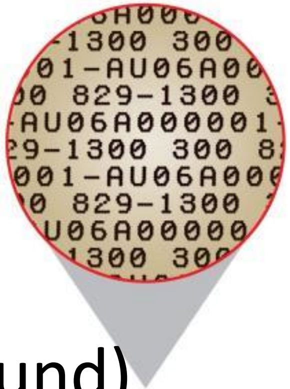
Overview

- Secret writing
  - Steganography
  - Cryptography
    - Keys, plaintext, ciphertext
    - Codes vs. Ciphers
    - Transposition ciphers
    - Substitution ciphers

DECODER
RING
Caesar
Cipher
C D E F G H I J K L M N O P Q R S T U V W X Y Z A B
S T U V W X Y Z A B C D E F G H I J K L M N O P Q R

Steganography vs. Cryptography

- Steganography
  - "covered writing"
  - Hide messages to keep them secret
  - Does not attract attention (if not found).



- Cryptography
  - "hidden writing"
  - Scramble messages so unintelligible
  - Screams: "Please try and decode me!"

- Not mutually exclusive:
  - e.g. Scrambled message in "invisible" ink

Physical hiding

- Ancient Chinese
  - Write message on thin silk sheet
  - Roll up → cover in wax → messenger eats
- 480 BC
  - Histiaeus wants Aristagoras of Miletus to revolt against the Persian King
    - Shaves head of messenger
    - Tattoos message on scalp
    - Waits for hair to grow back
    - Sends messenger to Aristagoras

Physical hiding

- 480 BC
  - Demaratus, Greek ex-pat living in Persia
  - Notices build up for attack on Greece
  - Sent secret messages:
    - Scraped wax of tablet
    - Wrote on wood
    - Covered up with wax
  - Persian ships attack, defeated by waiting Greeks

Invisibility

http://www.instructables.com/id/Ghost-message-egg/

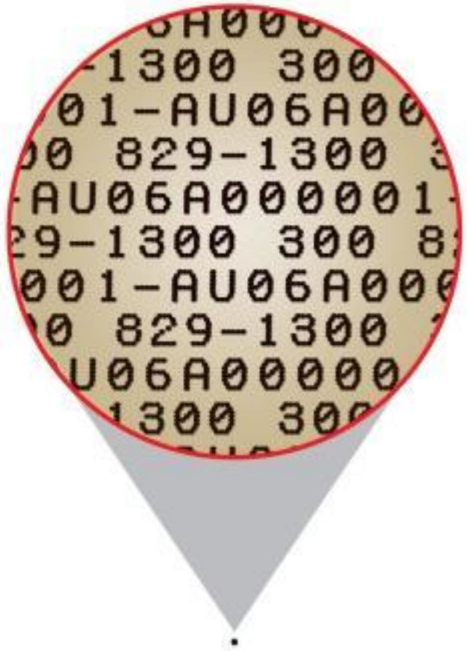
- Invisible writing
  - Invisible until heat/chemical/UV reaction
    - e.g. vinegar, ammonia, lemon juice, table salt, soap, milk, sunscreen, urine, saliva, wine, cola, …
  - 1500's, Italian scientist Giovanni Porta
    - Hard-boiled egg, alum+vinegar
    - Penetrates shell
    - Leaves message on egg
  - Invisible ink-jet printing

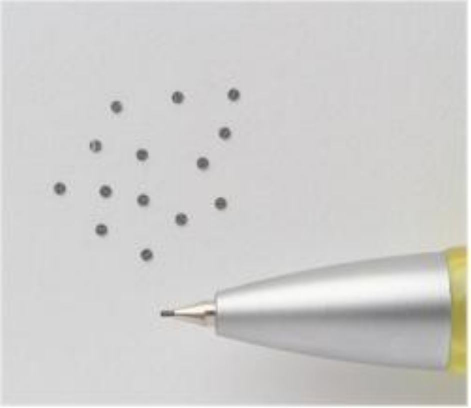
http://www.youtube.com/watch?v=oU2PkF9QLTQ

http://www.neomark.net/invisible.html

Really really small

- Microdots
  - Paris siege: via passenger pigeons
  - Germany between WW1 and WW2
  - Documents shrunk to size of a period.
  - Put in insecure postal mail
  - Modern usage
    - Tag vehicle or other asset with ID
    - Use lots of them: hard to find them all!

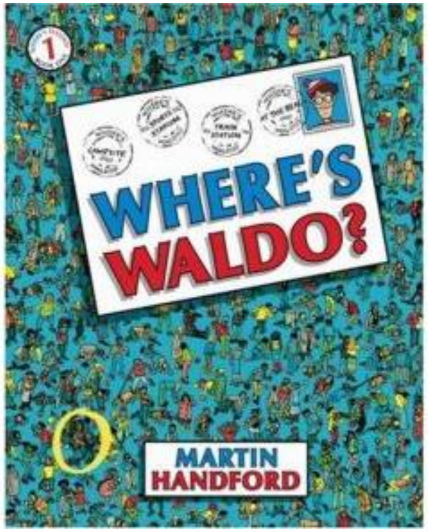




http://www.scienceinafrica.co.za/2005/november/microdot.htm

Digital steganography

- Digital steganography
  - Encode message in some digital media
    - e.g. text, image, audio file, video, executable files, …
  - Encode message in some other measurable thing
    - e.g. rate of network packets, timing of packets, DNA, …
  - Encode in unused areas
    - e.g. unused disk sectors, network packet fields, photo fields, …



Hiding text in text

- Hiding a message in text
  - German spy in WWII:
  - "Apparently neutral's protest is thoroughly discounted and ignored. Isman hard hit. Blockade issue affects pretext for embargo on by products, ejecting suets and vegetable oils."

Hiding text in text

- Hiding a message in text
  - German spy in WWII:
  - "Apparently neutral's protest is thoroughly discounted and ignored. Isman hard hit. Blockade issue affects pretext for embargo on byproducts, ejecting suets and vegetable oils."
  - pershingsailsfromnyjunei
  - "Pershing sails from NY June 1"

Hiding text in text

- Hiding a message in text
  - Original text:

    "We explore new steganographic and cryptographic algorithms and techniques throughout the world to produce wide variety and security in the electronic web called the Internet."

Hiding text in text

- Hiding a message in text
  - Text with secret message:

"We explore new steganographic and cryptographic algorithms and techniques throughout the world to produce wide variety and security in the electronic web called the Internet."

Hiding text in text

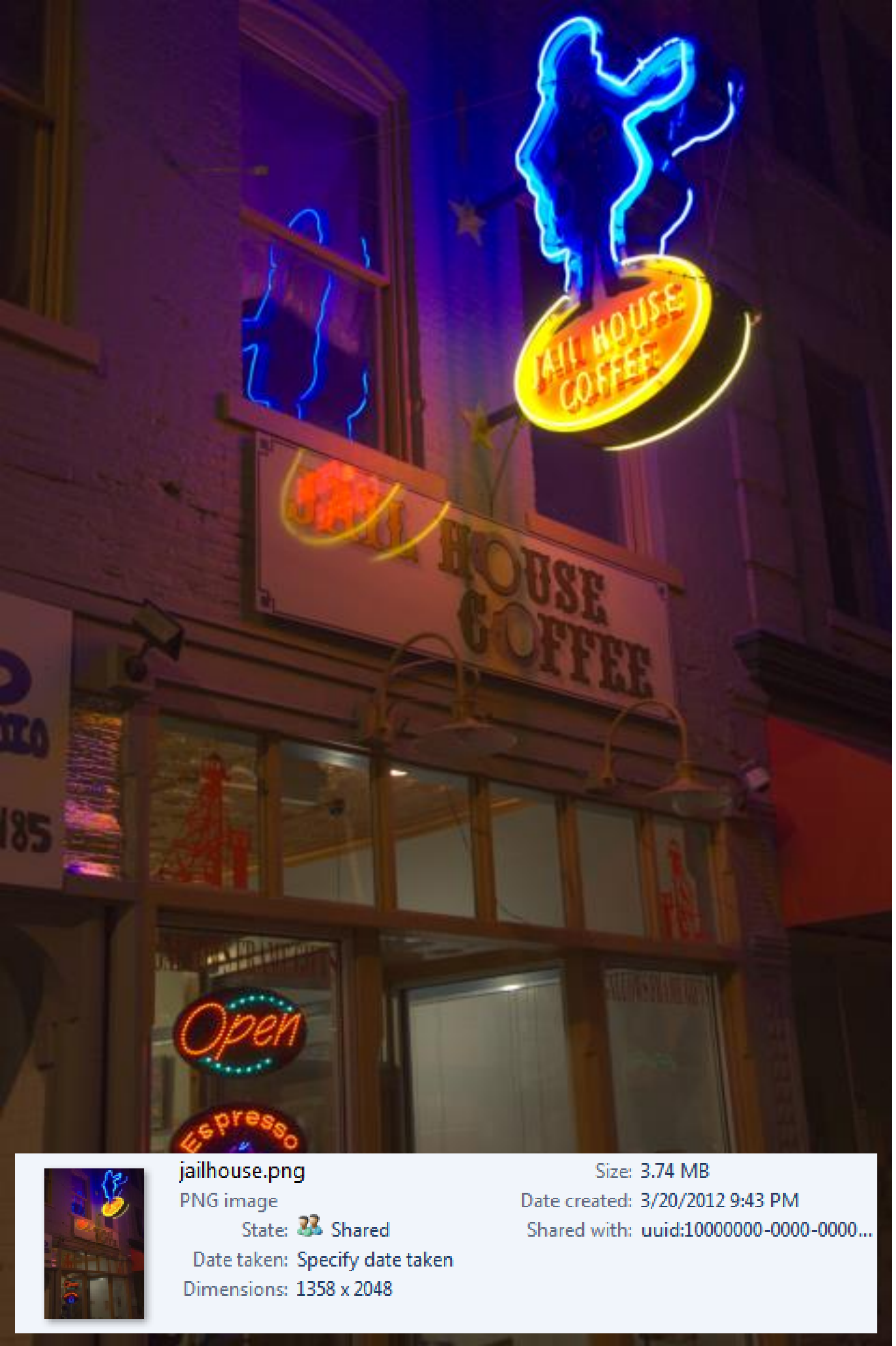
- Hiding a message in text
  - Text overlaid on each other:

"We **explore** new steganographic and cryptographic algorithms and techniques throughout **the world** to produce **wide** variety and security in the electronic **web** called the Internet."

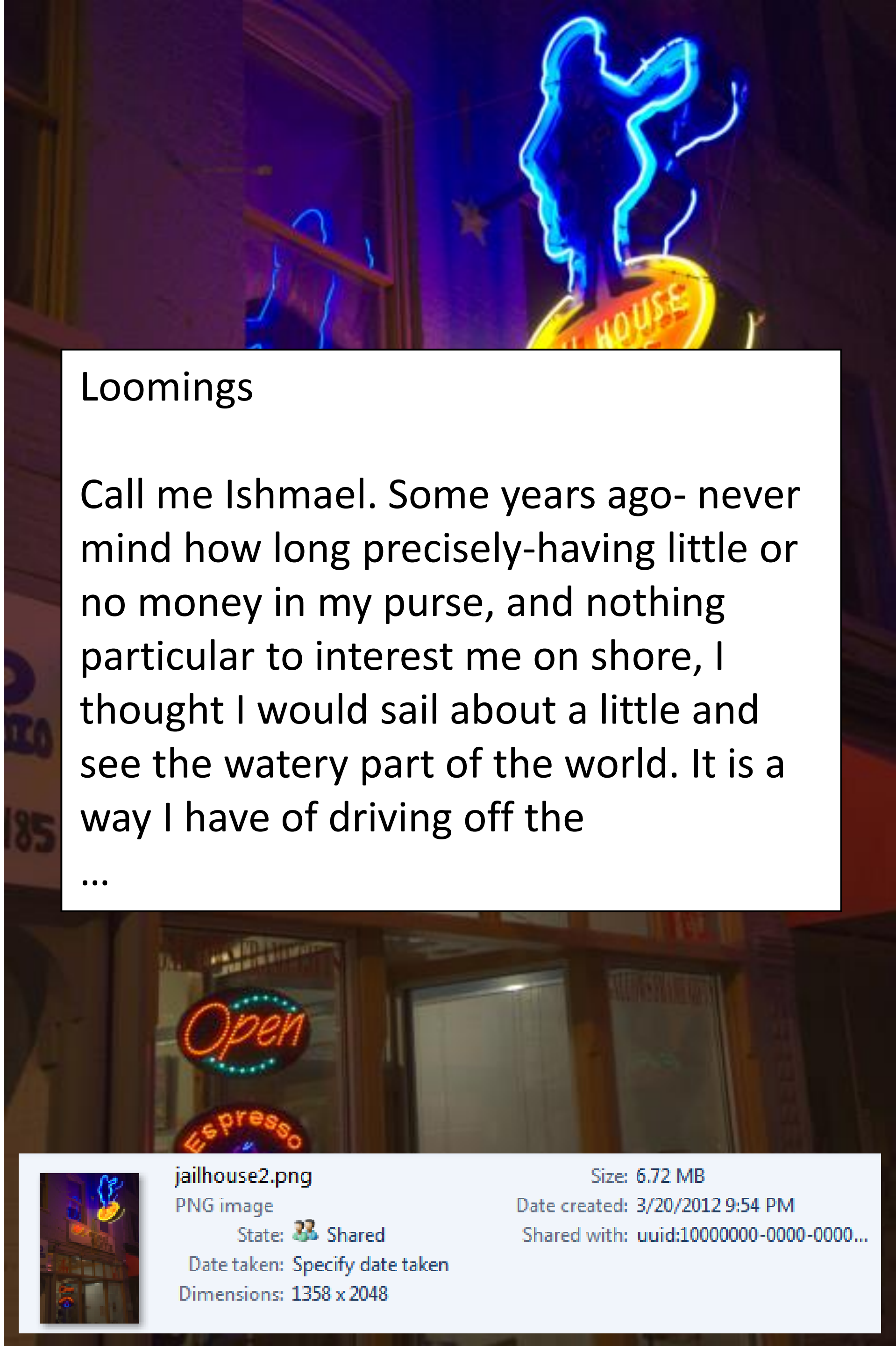
Hiding in images

- Images
  - High resolution image with 16M colors
    - You can change a lot of bits without perceptively altering the image's appearance
    - e.g. use 1-2 least significant bits in each pixel
  - Also useful for invisible watermarking
    - Prove somebody stole your photo
  - May not be robust to image alterations
    - e.g. changing compression level, brightness
    - Short messages (e.g. copyright) can be included many times in hopes of surviving

http://www.digimarc.com/digimarc-for-images



jailhouse.png
PNG image
State: Shared
Date taken: Specify date taken
Dimensions: 1358 x 2048
Size: 3.74 MB
Date created: 3/20/2012 9:43 PM
Shared with: uuid:10000000-0000-0000...



Loomings

Call me Ishmael. Some years ago- never mind how long precisely-having little or no money in my purse, and nothing particular to interest me on shore, I thought I would sail about a little and see the watery part of the world. It is a way I have of driving off the

…

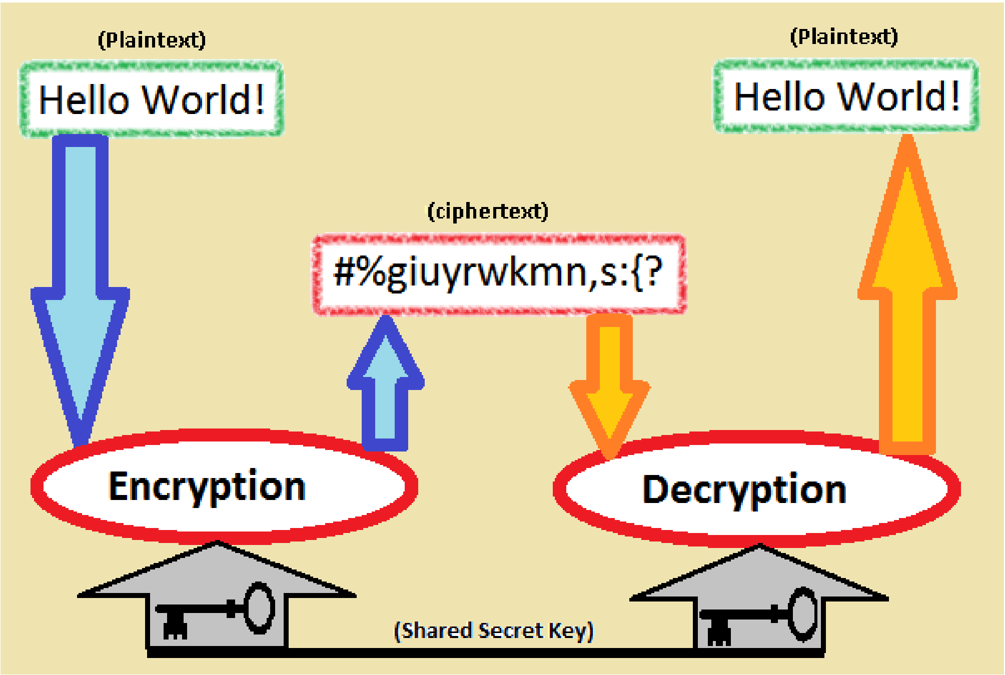
jailhouse2.png
PNG image
State: Shared
Date taken: Specify date taken
Dimensions: 1358 x 2048
Size: 6.72 MB
Date created: 3/20/2012 9:54 PM
Shared with: uuid:10000000-0000-0000...

Steganography summary

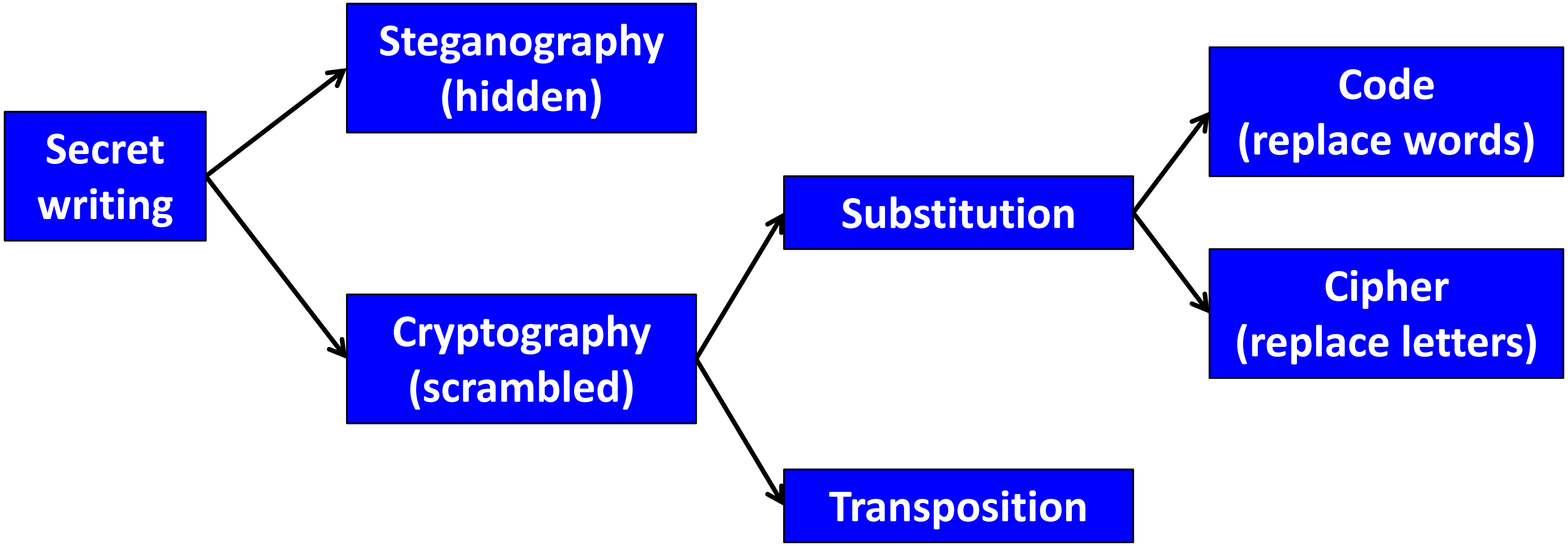
- Steganography
  - Hide messages via physical or digital means
  - Does not draw attention to itself
    - But if found, info revealed (unless also encrypted)
  - Steganalysis: trying to detect secret messages
- Uses:
  - Cloak and dagger stuff
  - Nefarious activities: terrorism, malware
  - Tagging assets: cars, photos, etc.
  - Not really what we need for e-commerce

Cryptography

- Cryptography
  - "hidden, secret"
  - Scramble text to hide its meaning
  - But intended recipient can read (hopefully)



Secret writing: branches



Secret writing

Steganography (hidden)

Cryptography (scrambled)

Substitution

Transposition

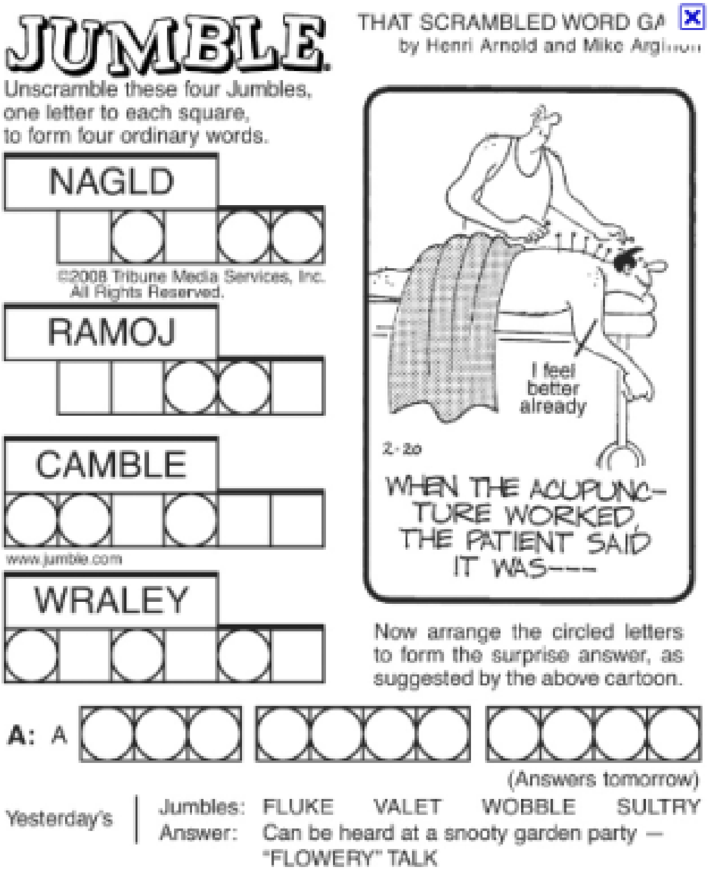
Code (replace words)

Cipher (replace letters)

Code word	Meaning
10-4	Acknowledgement (OK)
10-10	Fight in progress
10-11	Dog case
10-20	Location
10-30	Unnecessary use of radio
10-54	Livestock on highway

Transposition

- Transposition ciphers
  - Rearrange position of letters
  - OWC = ???
  - Exhaustively enumerate:
    - owc, cow, cwo, ocw, wco, woc
    - 3! = 6 ways



JUMBLE

THAT SCRAMBLED WORD GA
by Henri Arnold and Mike Arg

Unscramble these four Jumbles,
one letter to each square,
to form four ordinary words.

NAGLD

©2008 Tribune Media Services, Inc.
All Rights Reserved.

RAMOJ

CAMBLE

www.jumble.com

WRALEY

I feel
better
already

2-20

WHEN THE ACUPUNC-
TURE WORKED,
THE PATIENT SAID
IT WAS---

Now arrange the circled letters
to form the surprise answer, as
suggested by the above cartoon.

A: A ○○○ ○○○○ ○○○○

(Answers tomorrow)

Yesterday's | Jumbles: FLUKE VALET WOBBLE SULTRY
Answer: Can be heard at a snooty garden party — "FLOWERY" TALK

Transposition

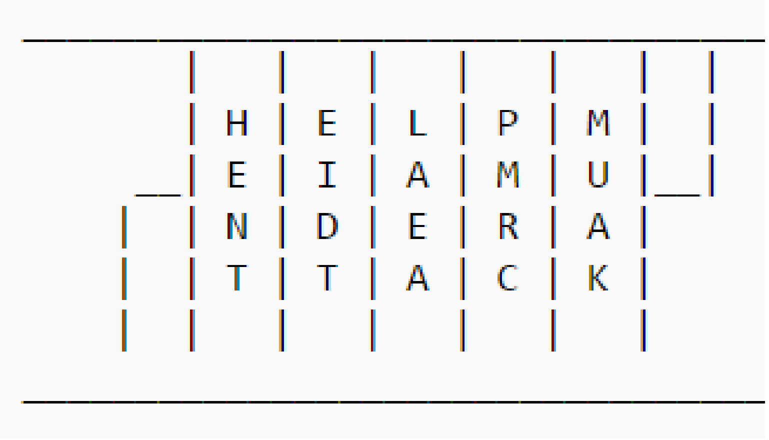
- Transposition ciphers
  - Rearrange position of letters
  - OBDTRPCLTEEUSEO = ???????????????
  - May be multiple words, with spaces deleted
  - Exhaustively enumerate:
    - obdtrpclteeuseo, obdtrpclteeusoe, obdtrpclteeueso, …
    - 15! = 1,307,674,368,000
- Random transposition impractical
  - Sender/receiver follow some sort of rule

http://www.counton.org/explorer/codebreaking/transposition-ciphers.php

Scytale

- Scytale
  - – Encode: message written on strip of leather
    - While wrapped around staff of certain diameter
    - When removed unreadable
    - Also wearable as a fashionable belt (steganography)
  - – Decode: wrap around staff of same diameter

HENTEIDTLAEAPMRCMUAK



```
____________________________________
         |   |   |   |   |   |   |
         | H | E | L | P | M |   |
      ___| E | I | A | M | U |___|
     |   | N | D | E | R | A |
     |   | T | T | A | C | K |
     |   |   |   |   |   |   |
____________________________________
```

Rail fence cipher

- Rail fence cipher
  - Transposition cipher
  - Used during Civil War
  - DULTPERTOBEOSCE

Rail fence cipher

- Rail fence cipher
  - Transposition cipher
  - Used during Civil War
  - DULTPERTOBEOSCE

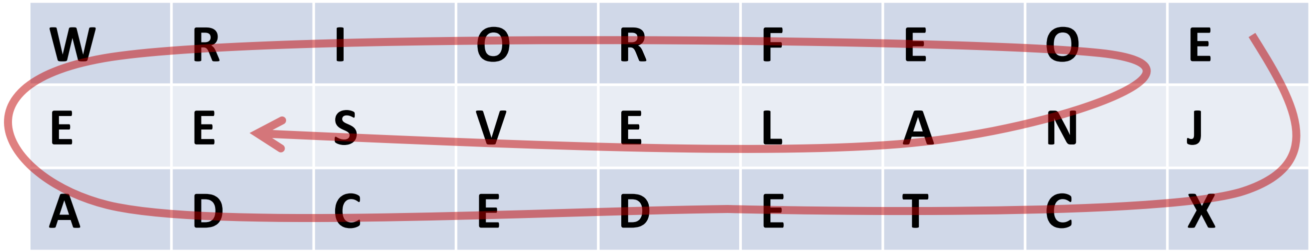
d		u		l		t		p		e		r		t
	o		b		e		o		s		c		e	

  - DBTSROLOEEUEPCT

d			b			t			s			r		
	o			l			o			e			e	
		u			e			p			c			t

Route cipher

- Route cipher
  - Transposition cipher
  - Like rail fence but with more keys
  - Ciphertext: EJXCTEDECDAEWRIORFEONALEVSE
  - Key = 9 x 3 grid, spiral in, clockwise, start top-right



W	R	I	O	R	F	E	O	E
E	E	S	V	E	L	A	N	J
A	D	C	E	D	E	T	C	X

  - We are discovered flee at once (jx)

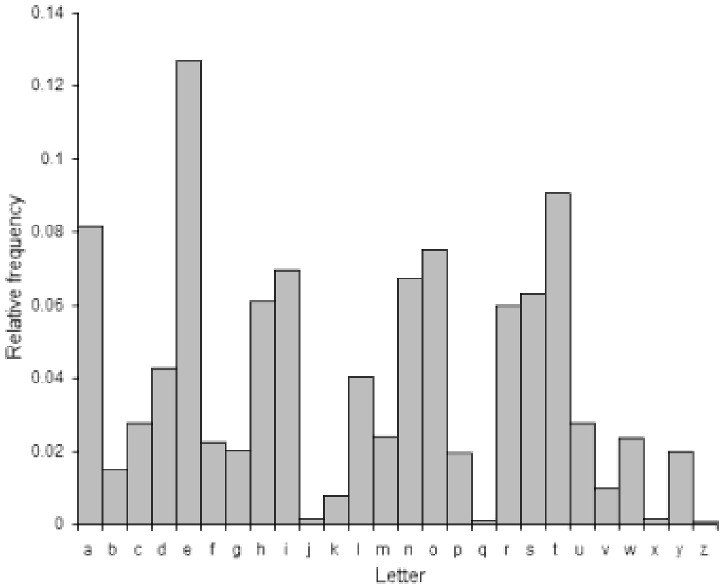
Column transposition

- Like rail fence, but with a password
  - Ciphertext: `EVLNE ACDTK ESEAQ ROFOJ DEECU WIREE`
  - Password: `ZEBRAS`
    - Length 6 = each row has 6 columns
    - Alphabetical order of letters: 6 3 2 4 1 5

6	3	2	4	1	5
W	E	A	R	E	D
I	S	C	O	V	E
R	E	D	F	L	E
E	A	T	O	N	C
E	Q	K	J	E	U

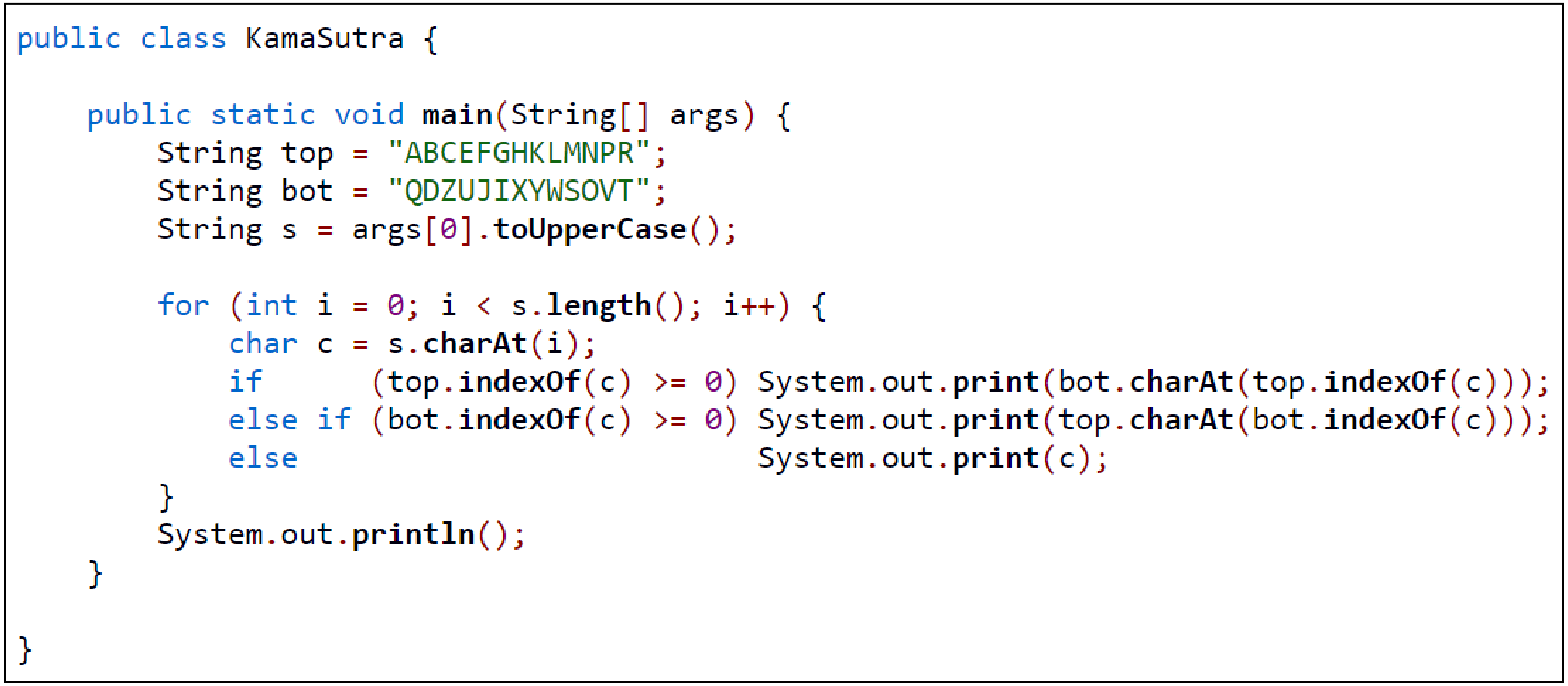
Transposition cipher summary

- Transposition: rearrange letters in some way
  - But: no changes to overall distribution of letters!
  - Cryptanalysis:
    - Usage is easy to detect
      - Compare with frequency of letters in the language
    - Partial decryption yields some sensible text
    - Subject to optimization techniques:
      - e.g. simulated annealing
      - e.g. genetic algorithms



Substitution

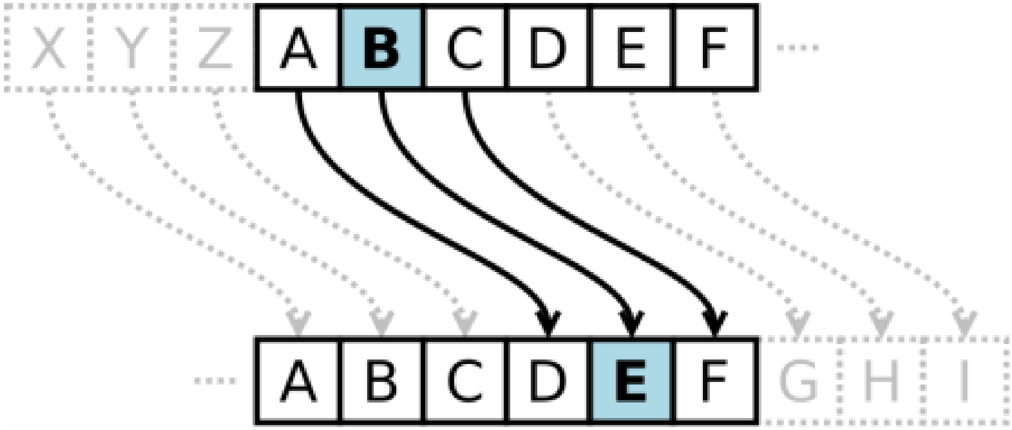
- Substitution ciphers
  - Replace one letter with another and vice-versa
    - e.g. A→D, D→A
  - Kama Sutra #45: Art of Secret Writing
    - Conceal details of secret liaisons, pair letters at random



```java
public class KamaSutra {

    public static void main(String[] args) {
        String top = "ABCEFGHKLMNPR";
        String bot = "QDZUJIXYWSOVT";
        String s = args[0].toUpperCase();

        for (int i = 0; i < s.length(); i++) {
            char c = s.charAt(i);
            if      (top.indexOf(c) >= 0) System.out.print(bot.charAt(top.indexOf(c)));
            else if (bot.indexOf(c) >= 0) System.out.print(top.charAt(bot.indexOf(c)));
            else                          System.out.print(c);
        }
        System.out.println();
    }

}
```

Caesar cipher

- Caesar's cipher
  - a.k.a. Shift cipher, Caesar's code, Caesar shift
  - Shift three to protect military communication

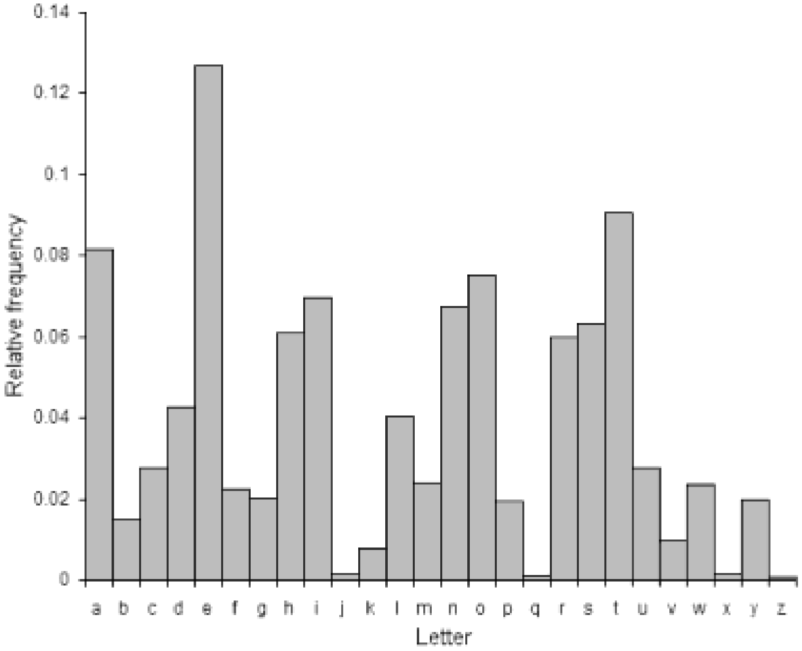


"If he had anything confidential to say, he wrote it in cipher, that is, by so changing the order of the letters of the alphabet, that not a word could be made out. If anyone wishes to decipher these, and get at their meaning, he must substitute the fourth letter of the alphabet, namely D, for A, and so with the others." -Suetonius, Life of Julius Caesar

http://www.counton.org/explorer/codebreaking/caesar-cipher.php

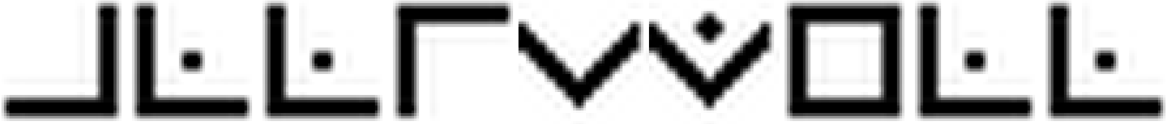
Breaking Caesar's cipher

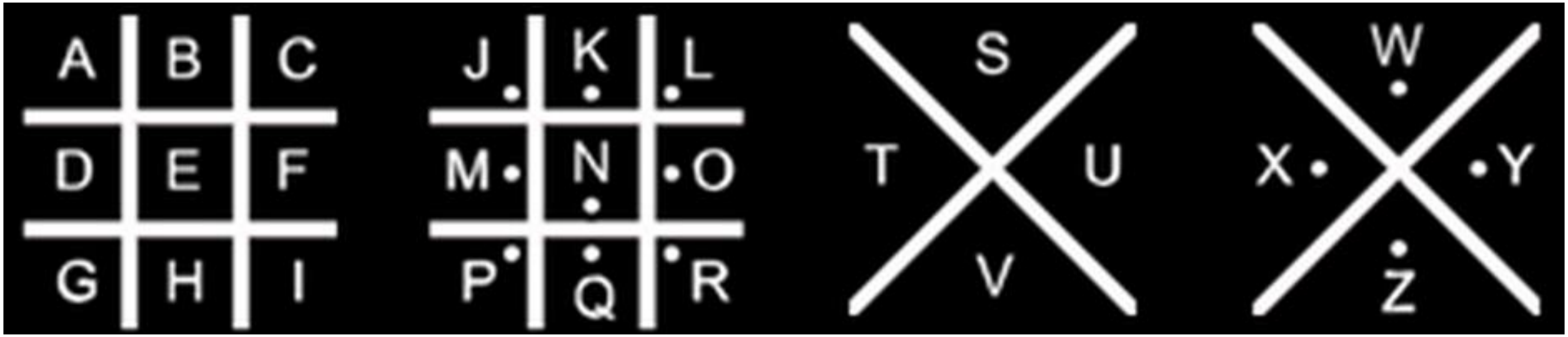
- If you know cipher is a Caesar shift:
  - – Try all 25 possible shifts
    - Only one is probably non-gibberish
  - – Look at frequency distribution of letters
    - Compare with letter distribution of language
    - Find shift that makes ciphertext distribution match



Pigpen cipher

- Freemasons, 18th century
  - Keep records private

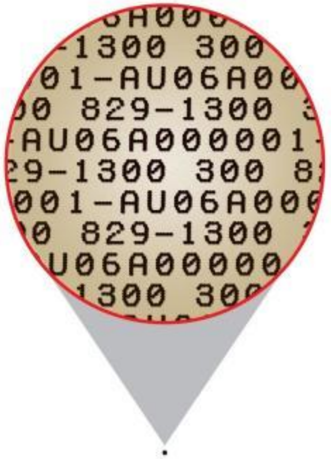


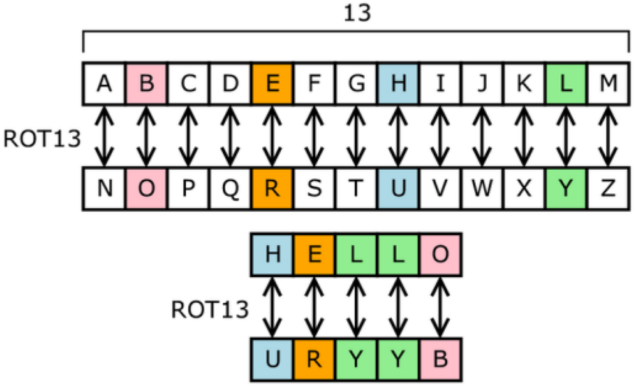


all is well

Summary

- Secret writing
  - Steganography: hiding the message
    - Analog forms of hiding or making invisible
    - Digital forms of hiding in data, events, etc
  - Cryptography: scrambling the message
    - Transposition ciphers
    - Substitution ciphers
      - Caesar's shift




13
A B C D E F G H I J K L M
ROT13
N O P Q R S T U V W X Y Z
H E L L O
ROT13
U R Y Y B