DTTF/NB479: Dszquphsbqiz Day 8

- Announcements:
  - Knuth quotes, part 1
- Questions?
- Today:
  - Congruences
  - Chinese Remainder Theorem
  - Modular Exponents

Hill Cipher implementation

- Encryption
  - Easy to do in Matlab.
  - Or find/write a matrix library for language X.
- Decryption
  - Uses matrix inverse.
  - How do we determine if a matrix is invertible mod 26?

How to break via known plaintext?

- Good work on last session's quiz.

Idea:

Assume you know the matrix size, n.

Then grab n sets of n plaintext chars ←→ ciphertext

This gives n^2 equations and n^2 unknowns.

Then solve using basic linear algebra, but mod n.

Caveat: sometimes it doesn't give a unique solution, so you need to choose a different set of plaintext.

Hmm. This could make a nice exam problem…

Substitution ciphers

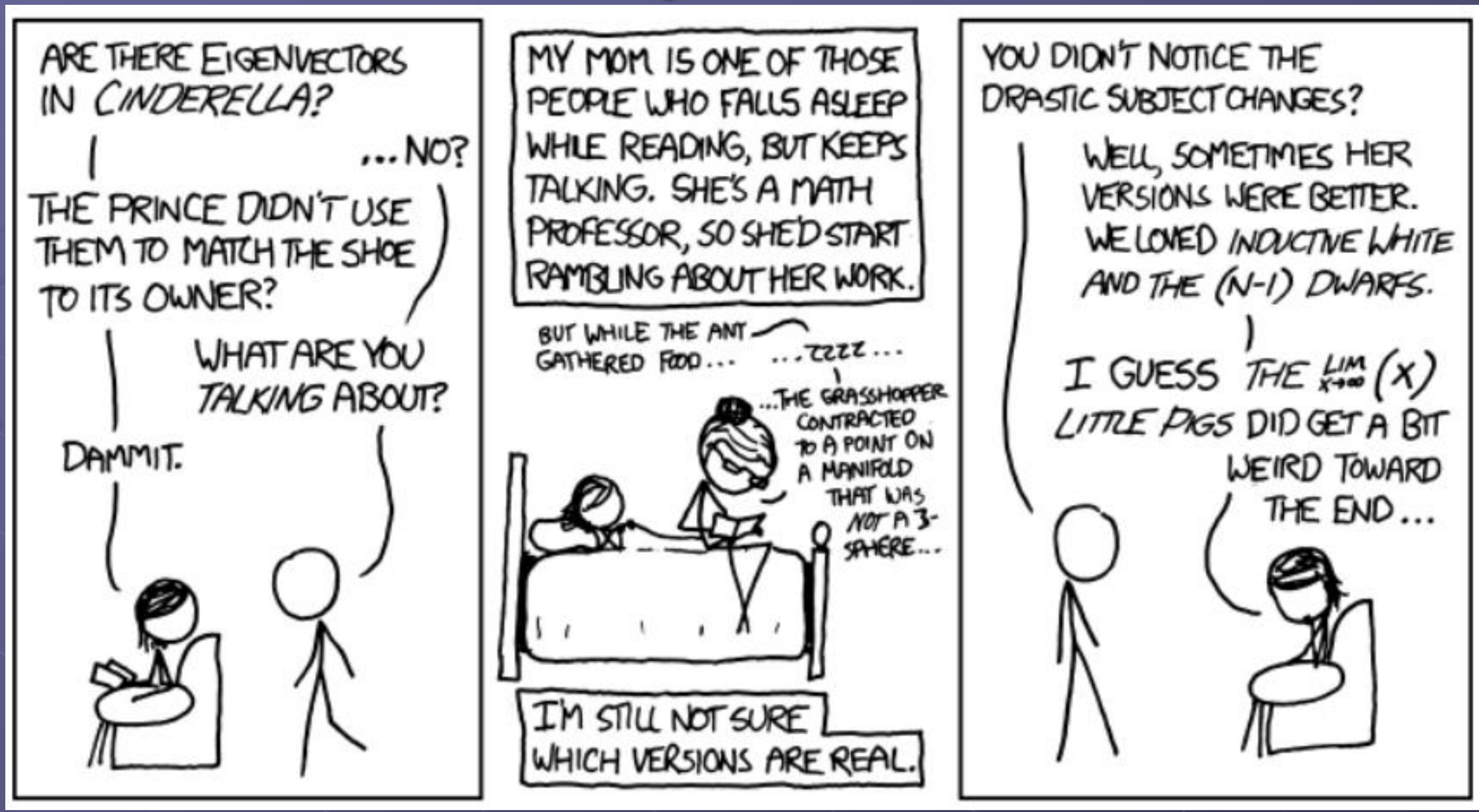
- Each letter in the alphabet is always replaced by another one.
  - Which ciphers have we seen are substitution ciphers?

  - Which aren't and why?

- Breaking ciphertext only uses linguistic structure. Frequencies of:
  - Single letters
  - Digrams (2-letter combinations)
  - Trigrams
  - Where do T&W get their rules like "80% of letters preceding *n* are vowels"? (p. 26)
    - See http://keithbriggs.info/documents/english_latin.pdf

- Lots of trial and error when done by hand.
- Could automate with a dictionary.

Fairy Tales



HTTP://XKCD.COM/872/

Goldilocks' discovery of Newton's method of approximation required surprisingly few changes.

Basics 4: Congruence

- Def: a≡b (mod n) iff (a-b) = nk for some int k
- Properties

$$\begin{aligned}
&Consider\ a,b,c,d \in Z, n \neq 0\\
&a \equiv b \pmod{n}\ if\ \exists k \in Z\ s.t.\ a = b + nk\\
&a \equiv 0 \pmod{n}\ iff\ n \mid a\\
&a \equiv a \pmod{n}\\
&a \equiv b \pmod{n}\ iff\ b \equiv a \pmod{n}\\
&a \equiv b, b \equiv c \pmod{n} \Rightarrow a \equiv c \pmod{n}
\end{aligned}$$

$$\begin{aligned}
&If\ a \equiv b, c \equiv d \pmod{n}, then\\
&(a+c) \equiv (b+d) \pmod{n}\\
&(a-c) \equiv (b-d) \pmod{n}\\
&ac \equiv bd \pmod{n}\\
&If\ \gcd(a,n) = 1\ and\ ab \equiv ac \pmod{n}, then\\
&b \equiv c \pmod{n}
\end{aligned}$$

- You can easily solve congruences ax≡b (mod n) if gcd(a,n) = 1.
  - For small numbers, do by hand
  - For larger numbers, compute a^{-1} using Euclid

Solving $ax \equiv b \pmod{n}$ when $\gcd(a,n) \neq 1$

- Let $\gcd(a,n)=d$
- If d doesn't divide b then no solution
- Else divide everything by d and solve $(a/d)x=(b/d)(\mathrm{mod}\ (n/d))$
- Get solution x_0
- Multiple solutions: $x_0, x_0+n/d, x_0+2n/d, \ldots x_0+(d-1)n/d$
- Always write solution with the **original** modulus
- This is an easy program to code once you have Euclid…

←Example: $2x \equiv 7 \pmod{10}$

Example:

$3x \equiv 3 \pmod{6}$

- How could we write $x \equiv 16 \pmod{35}$ as a *system* of congruences with smaller moduli?

Chinese Remainder Theorem

- Equivalence between a single congruence mod a composite number and a system of congruences mod its factors

- Two-factor form
  - Given gcd(m,n)=1. For integers a and b, there exists *exactly 1* solution (mod mn) to the system:

$$x \equiv a \pmod{m}$$
$$x \equiv b \pmod{n}$$

Q3,Q4

CRT Equivalences let us use systems of congruences to solve problems

- Solve the system:

$$x \equiv 3 \pmod{7}$$
$$x \equiv 5 \pmod{15}$$

- How many solutions?
  - Find them.

$$x^2 \equiv 1 \pmod{35}$$

Chinese Remainder Theorem

- n-factor form
  - Let m_1, m_2,… m_k be integers such that gcd(m_i, m_j)=1 when i ~= j. For integers a_1, … a_k, there exists *exactly 1* solution (mod $m_1 m_2 \ldots m_k$) to the system:

$$
\begin{aligned}
x &\equiv a_1 \pmod{m_1} \\
x &\equiv a_2 \pmod{m_2} \\
&\ldots \\
x &\equiv a_k \pmod{m_k}
\end{aligned}
$$

Modular Exponentiation

- Compute last digit of 3^2000
- Compute 3^2000 (mod 19)
  Idea:
  - Get the powers of 3 by repeatedly squaring 3, BUT taking mod at each step.

Modular Exponentiation

(All congruences are mod 19)

- Compute 3^2000 (mod 19)
- Technique:
  - Repeatedly square 3, but take mod ***at each step***.
  - Then multiply the terms you need to get the desired power.
- Book's powermod()

$$3^2 \equiv 9$$
$$3^4 = 9^2 \equiv 81 \equiv 5$$
$$3^8 = 5^2 \equiv 25 \equiv 6$$
$$3^{16} = 6^2 \equiv 36 \equiv 17 (or - 2)$$
$$3^{32} = 17^2 \equiv 289 \equiv 4$$
$$3^{64} = 4^2 \equiv 16$$
$$3^{128} \equiv 16^2 \equiv 256 \equiv 9$$
$$3^{256} \equiv 5$$
$$3^{512} \equiv 6$$
$$3^{1024} \equiv 17$$

$$3^{2000} \equiv (3^{1024})(3^{512})(3^{256})(3^{128})(3^{64})(3^{16})$$
$$3^{2000} \equiv (17)(6)(5)(9)(16)(17)$$
$$3^{2000} \equiv (1248480)$$
$$3^{2000} \equiv 9 (\mathrm{mod} 19)$$

Modular Exponentiation

- Compute 3^2000 (mod 152)

$$3^2 \equiv 9$$
$$3^4 = 9^2 \equiv 81$$
$$3^8 = 81^2 \equiv 6561 \equiv 25$$
$$3^{16} = 25^2 \equiv 625 \equiv 17$$
$$3^{32} = 17^2 \equiv 289 \equiv 137$$
$$3^{64} = 137^2 \equiv 18769 \equiv 73$$
$$3^{128} \equiv 9$$
$$3^{256} \equiv 81$$
$$3^{512} \equiv 25$$
$$3^{1024} \equiv 17$$

$$3^{2000} \equiv (3^{1024})(3^{512})(3^{256})(3^{128})(3^{64})(3^{16})$$
$$3^{2000} \equiv (17)(25)(81)(9)(73)(17)$$
$$3^{2000} \equiv (384492875)$$
$$3^{2000} \equiv 9$$