CRYPTO 3D Jan K

Steven Miller

Likes crypto for the underlying math, very beautiful

Teach math about grad

about the IDEAS – not the techniques (you don't want to be the technician)

relation b/t queens & pawns

BTD, it was linguists at the table, not mathematicians

NB → notes are online

his list of themes including ① efficiency/speed ② redundancy

redund. is now a huge issue — how much can be info & how much is about reducing

Hardy thought his work (see Hardy in Mathematician's Apology) wouldn't help or hurt anyone.

Caesar cipher

how many ways? 26 letters

make a list. what's simple? frequency.

A	B	C	D	E	.....	I	.....	Z
J	K	L	M	N		Z	A	I

C	A	B
L	G	K

good for efficiency and speed, bad in terms of easy to break

Stephen suggests giving a message that is not going to be digested both encoded and unencoded

Add'l security
get rid of spacing
change code in media res (save for later he says)
add misspellings

Caesar: 26 possib.

general form of substitution ciphers:

A B C ...etc 26!
↓ ↓ ↓
26 25 24

If you rule out A→A B→B etc (26!−1)

can we quantify if we don't know?

there are 25! more possible ciphers than Caesar ciphers

NB as general rule when you look @ small sets you can easily see nongeneric behavior

But to keep ease of coding/decoding stick w/ Caesar and "clock math"

Clock 10+5 = 3 (??!)

$10+5 \equiv 3 \bmod 12$

$x \equiv y \bmod n$ means $x-y$ is divisible by n

Given x, go to $x \bmod 12$ $\{0,1,2,\ldots 11\}$

multiplication $10 \cdot 5 = 50 \equiv 4 \cdot 12 + 2 \equiv 2 \bmod 12$

use this to improve Caesar

Caesar cipher has just one parameter:

Caesar: given A → some letter

"there's another parameter lurking..."

A →(+1) B
↓ ↓
J →(+1) K

hidden second parameter?

New alphabet:

A → B C D E F

D → F B D F B

shift 2 doesn't work...

shift 3 → D A D A D A

shift 4 → will just be a subset of Z, no? will be bad

5 → D C B A F E

"If you are in a school that allows profanity this is a great a shit moment"

bad: 2, 3, 4, 6 (same as 3)

good: 1, 5 } 2^{n} parameter...

Student project: try this with other length alphabets

What's wrong w/ bads?

they have a nontrivial common factor (i.e. $GF \neq 1$)

now we can conjecture:.....

divisors of 26:
1, 2, 13, 26

Affine Caesar cipher

with euclidian algebra you can prove that you're safe as long as you don't use 1, 2, 13, 26 .. and mult:

ciphers now?

2 param A → unknown 26

step shift: 12

ciphers $26 \cdot 12 - 1$

a lot more!

1 ~~2~~ 3 ~~4~~ 5 6 7
~~8~~ 9 ~~10~~ 11 ~~12~~ ~~13~~
~~14~~ 15 ~~16~~ 17 ~~18~~ 19
~~20~~ 21 ~~22~~ 23 ~~24~~ 25 ~~26~~

but key sharing is still a problem - not always practical

next time - how can you "share a secret by yelling in public"

again - math is beautiful, but how practical?

NEW CODE:

used in Civil War: Vicksburg
coded message recently found
had been dumped by confed courier

Inverse power of Caesar cipher

use a word MATH
repeat
M A T H M A T H M A T H M A T

A 1
B 2
C 3
D 4

A + A = B A + B = C A + M = N B + Z = B
A + 1 = 2 1 + 2 = 3 1 + 13 = 14 2 + 26 = 2
C + Y = B

plaintext A C A B B Y
M A T H M A
N D U J O Z

Vigenere cipher

you can master this in an hour, no?

decode: C - B = A easy D - Y = C
2 - 25 = 23
↖ i 23 ≡ 3 mod 26

Parameter: a word of variable length

infinite # of codes

the ONLY secure method is a one-time pad with a word longer than the message

but if you use the same key it's vulnerable to attack
(NB Caesar is a key of L = 1)

How do you crack a standard cipher?

Frequency analysis

next step... helping monkeys by giving them a new kbd based on what they just hit

→ custom cool project for programming students

KBD 1. is freq

2 is based on next (ie H is common after T)

use this to attack vigenere cipher

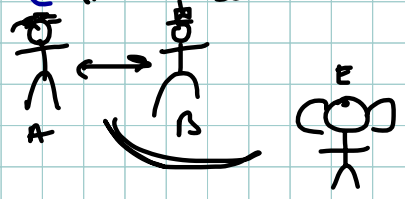
civil war message began with GENLBEAUREGARD

(crucial Stiller started all his emails w/ hello crypto class)

german messages started with weather

RSA - for a long time, the preferred way to encrypt

(Alice & Bob have met, Charlie or Eve is badguy)



how can they communicate securely w/o having met:

Method 1

choose two big primes

p, q ~ 10^{200} secret

public N = pq

passwd: p or q

↳ Security system only needs to know N & how to divide

Method 2

choose a 500 random digit number N ~ 10

private: N

passwd N

↳ security system knows answer

Factoring is thought to be hard, multiplication is "easy"

Steven tells story of Operation Fortitude as an example of crucial information b/c Germans convinced Patton not fired and so allies set up fake first Army under Patton to invade @ Calais

... and his point that what is known cannot be discussed...

Steven putting numbers in perspective

10^{18} sec/univ
10^{100} things — make universe a computer 10^{130}
10^{12} checks/sec

not going to break this by brute force!

In comparison enigma 10^{18} so Germans were confident

how many primes? in the limit, zero %

$\pi(x) = \#\{n \le x \text{ s/t } x \text{ prime}\} \sim \frac{x}{\ln(x)}$

you would be dumb: chose $p=q$ ...

"number theory has a role to play"

Riddle #1

password triple (a,b,c)

any 3 profs know enough to get paid

no two profs know enough

(assume 11 profs @ willing)

① since 1 person can't, nobody told a, b, c

② claim no ones told 2 of a/b/c

for communication to be subset of $\{a,b,c\}$ — shown not possible

③ claim no one is told one letter (no choice works for any 3)

④

Soln: prof $k \in \{1,2,3,\ldots 11\}$

gets $(k, f(k)) \subset (k, ak^2+bk+c)$

getting bigger:

world is (a, b, c, d ... n)

president has 10
provost 8
dean 6
tenured 2
junior 1
visitor 0

diff ppl have diff amt of info

you can take cliques into account by giving them pts in common

---

riddle #2

100 mathematicians in a line, each only sees ones in front
I am pure evil and want W or B hats to all
Math. hate strategy session — I hear all
Speak in order, each one says W or B; if correct get $1/million
if wrong lose $1/m

What is optimal strategy? about 2 things right?

① ~~everyone says color of~~ odd → 50%

② 3 says W if 1+2 are the same, B if diff → 60%

③ 100 says W if more W, B if more B. 50%

④ 100th says W if even # W, B if even # B → 99%

Related to streaming

transmit only changing pixels?

related to Taylor series? fourier? wavelets?
on other end computer only updates changes

riddle relates: 99 → 1 are smart computers & can update

How RSA works:

eve/charlie

Alice

Bob

chooses 2 big primes

computes $N = pq$

computes $\phi(N) = pq$

Choose e, d s/t

January 30, 2012 1:08 PM

Babylonians look 60

$$xy = \frac{(x+y)^2 - x^2 - y^2}{2}$$

Sort! all mult is squaring .. which you do w/ a lookup table

---

efficiency of comp'

ADD WRITTEN NOTES HERE

CRYPTO Session #2 Mon 6 feb

General Code:

7 generals; any 4 can "open"; no set of 3 can

choosen n locks; assign keys.

How?

Binomial Coeff $\binom{n}{k} = \frac{n!}{k!(n-k)!}$ # ways choose k from n order doesn't matter

$4 + 3 = 7$

$k \quad n-k \quad n$

ans $\binom{7}{4} = \frac{7!}{4!3!} = \frac{7 \cdot 6 \cdot 5 \cdot 4!}{4! \cdot 3 \cdot 2 \cdot 1} = 35$

35 choices of 4 generals

each choice a new lock

all gen's get N keys

"now that we've got full steam ..." let's talk about

BENFORD'S LAW (of digit bias)

(surprising #1 first)

$X \longrightarrow M(x)\,10^{k}$

$M(x)$ mantissa/significant

$1 \le M(x) < 10$

$K(x)$ integer

Scientific notation eg avogadro 6.02×10^{23}

crypto 6 feb

guess 10% of the time

no, 1% as "new" start I/O

Typically ≈ 30%

("human beings are horrible random number generators")

IRPBS v. interested in estimating time from end in how many data points you need before first kicks in

Benford's law: Prob 1st digit is d is

$$\log_{10}\left(1+\frac{1}{d}\right) = \log_{10}\left(\frac{d+1}{d}\right)$$

Credit card company sees too many leading 4 second 8 or 9

48 * *

49 * *

what's threshold for investigation?

turns out it was $5000

(shows refs expense acct fraud too)

inside job!

Benford's law of digit bias

2^n	
1	1024
2	2048
4	4096
8	8192
16	16384
32	
64	
128	
512	

where are 9's & 7's?

1 Gig = 1000 Meg

1 Gb = 1024 Mb

$2^{10} \approx 10^3$

cycle through ... same #s ...

crypto 6 feb

February 6, 2012 9:30 AM

If we go high enough we will see 7 ; 9 @ properly.

Misleading data:

prime # thm:

$$\pi(x) = \#\{\text{primes } p \le x\}$$

$$\pi(x) \approx \frac{x}{\ln(x)} = \frac{1}{\ln x} x$$

$$\text{even}(x) \approx \frac{1}{2} x$$

claim 40% of integers prime

1, 2, 3, 4, 5, 6, 7, 8, 9, 10

11 12 13 14 15 16 17 18 19 20

yep!

Fibonacci #s as an appl to roulette

S: "method of divine inspiration"

Benford's law (1st digit bias) "is a result of looking at numbers the wrong way"

fundamental Equiv

$$X = M(X) \cdot 10^{K(X)}$$

$$y = \log_{10} X \bmod 1$$

throws away the integer part

clock arith: $10+5 \equiv 3 \bmod 12$

crypto

$$\log_{10} X = \log_{10}\left[M(x)10^{K(x)}\right]$$
$$= \log_{10} M(x) + \log_{10}(10^{K(x)})$$
$$= \log_{10} M(x) + K(x)\log_{10} 10$$
$$= \log_{10} M(x) + K(x) \quad \text{integer}$$

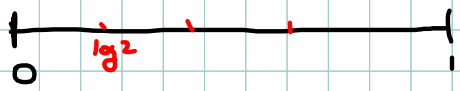
$$\Rightarrow y = \log_{10} X \equiv \log_{10} M(x) \mod 1$$

So... distrib of digits in X is same as distrib in y...
we don't care about order of magnitude

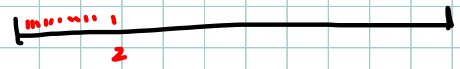
"these data down on 0-1 interval"

"even distrib" would be nice....

"y"



"X"

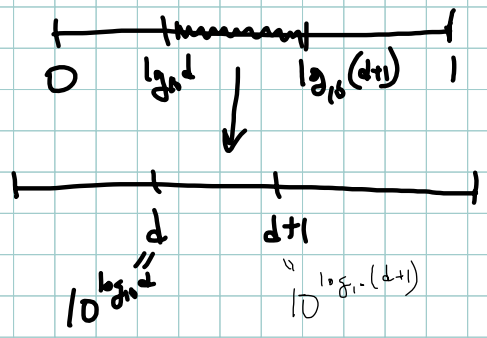


given $[a,b] \subset [0,1]$

$$\lim_{n\to\infty} \frac{\#\{n \le N : X_n \in [a,b]\}}{N} \longrightarrow b-a$$

$\log_{10} 2 \approx 0.3$

THIS is the transformation to make if you want to study digit frequency



February 6, 2012 9:54 AM

Benford's: roulette, crypto

Fundamental Result:

Kronecker's Thm:

if α is irrational, then the sequence $\alpha \bmod 1$, $2\alpha \bmod 1$, $3\alpha \bmod 1$, $4\alpha \bmod 1$ ...
fills evenly in $[0,1]$

Consider $\alpha = \frac{2}{3}$

$\frac{2}{3}, \frac{4}{3} \bmod 1 = \frac{1}{3}, 0, \frac{2}{3}, \frac{1}{3}, 0 \ldots$

if α is rational w/ denom q cycle w/ period at most q

Use this "to prove 2^n is Benford"

Thm: 2^n is Benford

Proof: $X_n = 2^n$

then X_n is Benf iff $y_n = \log_{10} X_n \bmod 1$ is evenly distrib

well $y_n = n \log_{10} 2 \bmod 1$

Show $\log_{10} 2$ is irrational & done!

Fibonacci & Vegas:

Show 2^n is a recurrence relation/ difference equation
satisfies $a_{n+1} = 2a_n$ $a_0 = 1$ 1, 2, 4, 8, 16

Fib: $a_{n+2} = a_{n+1} + a_n$, $a_0 = 0$; $a_1 = 1$
how do we get to a_n FAST??

using divine inspiration method; then why don't play roulette

Divine Inspir:

Guess $a_n = r^n$

$r^{n+2} = r^{n+1} + r^n, \quad r \neq 0$

$r^2 = r + 1$

Solve $r^2 - r - 1 = 0$

$r = \frac{1 \pm \sqrt{5}}{2}$

this will solve fib(!?!)

($\pm, \sqrt{\ }, \frac{\ }{2}$ to get integers?)

Key fact:

If r_1^n is a soln and r_2^n is a soln (i.e. r_1, r_2 roots of $r^2 - r - 1 = 0$) then for any c_1, c_2 have $a_n = c_1 r_1^n + c_2 r_2^n$ is a solution.

("there is a prohibition against doing a/gebra in public; it's not supposed to be polite") :)

$n = 0$: $c_1 + c_2 = 0 \quad c_2 = -c_1$

$n = 1$: $c_1 \ldots$

Binet's Form!

$$a_n = \frac{1}{\sqrt{5}}\left(\frac{1+\sqrt{5}}{2}\right)^n - \frac{1}{\sqrt{5}}\left(\frac{1-\sqrt{5}}{2}\right)^n$$

storm says beautiful – would you guess this pdx integers ?!?! pick it out of a police lineup, eg?

golden mean $\frac{1+\sqrt{5}}{2}$

"the most irrational of all numbers"

February 6, 2012 10:12 AM crypto

ROULETTE

18 red
18 black
2 green] ← makes vegas happy!

bet "red" or "black"
bet $1 win $1 if right
lose $1 if wrong

If there are no greens...

Double plus one strategy:

Step 1: bet $1, win up $1

Step 2: if lost, bet $2 red, win, net $1

Step 3: if lost 3x; bet $4 red, win; up $1

else, rinse, repeat

Probs:

① Need a lot of $ for bets
- rich eccentric uncle hypothesis: he'll stake you

② Table limits: have min/ max bet/table

Imagine dead if 5 consec blacks. What's the prob?

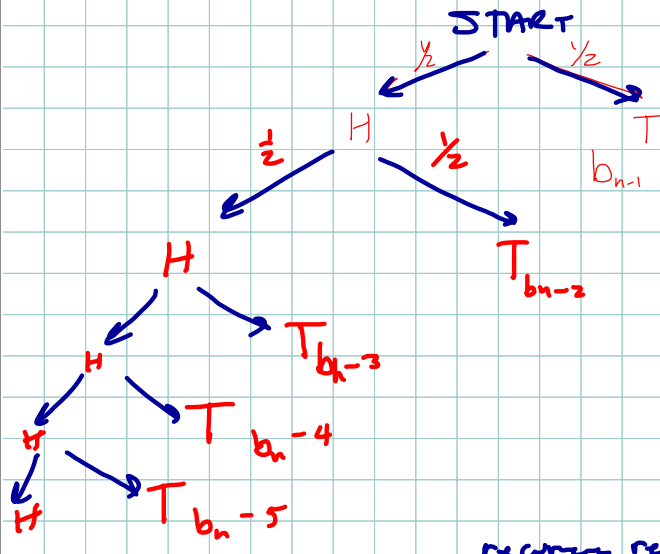
or: if you toss fair coin 100x; what is chance of at least 5 consec heads?

turns out it's ~50%!

Why double strategy is "dumb"

q_n = prob (5 consec heads in n tosses)

b_n = Prob (no 5 consec heads ....) $= 1 - q_n$



$$b_n = \frac{1}{2} b_{n-1} + \frac{1}{4} b_{n-2} + \frac{1}{8} b_{n-3} + \frac{1}{16} b_{n-4} + \frac{1}{32} b_{n-5}$$

recurrence relation solve like fibonnacci

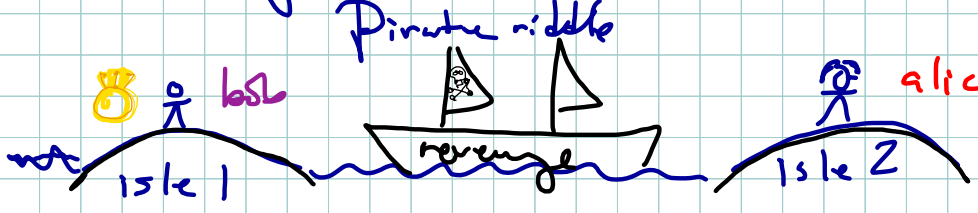
$$b_0 = b_1 = b_2 = b_3 = b_4 = \underline{1}$$

If you don't solve the system exactly you can work it out w/ excel

When you lose you lose Big!

---

return to crypto:



pirates have a box with two locks

bob has 1 key Alice the other

Alice accepts proposal w/ ring

February 6, 2012 10:40 AM

pirates will transport and not open box, but will take from unlocked box

[RELATED TO eCOMMERCE – how to have a secret in public]

Step 1: bob puts in ring & locks
2: send to alice; who locks
3: send to Bob; who unlocks
4: send to Alice; who unlocks

Not efficient. If we only have to do it once, that's OK but not great for multiple runs.

 = code word for Vigenere cipher

(Secret method for making passwords → Σ back door)

Math version?

Diffie–Hellman (Merkle) Public Key Exchange

S.I.M.: talks about power of using simple private story to make powerful applications & opposes it to the old idea of math. machines (eg trains) & "I was right - it was trivial" style of math proofs & papers

Rubik's cube – can be "solved" but have centers rotated

"brings us to equivalence classes"

February 6, 2012 10:59 AM

crypto

Group Theory: (or "abstract algebra")

A group is a set G with a binary operation $\oplus$

$b: G \times G \to G \quad b(g_1, g_2) = g_3$

① Closed: $\forall$ ("for all") $x, y \in G, \; x \oplus y \in G$

② Assoc: $\forall x, y, z \in G; \; (x \oplus y) \oplus z = x \oplus (y \oplus z)$

③ Identity: $\exists$ ("there exists") $x \in G \;\; \exists y$ in G s.t. $x \oplus y = y \oplus x = 0$

So is there an example?

Ex ⇨ integers ($all, \mathbb{Z}$) under addition

but not under multiplication

Ex ⇨ all rationals under mult:

appears so, but not for zero...

so not $\forall$ ... NO. Zero has no inverse

Ex ⇨ $\mathbb{Q}^* = \{p/q \neq 0, p, q, \text{ints}\}$

all nonzero rationals

↳ Group

Rubik's cube: need group elements: all possible configs

binary operations: moves - single twist

show $\exists$ a group structure

other groups: Clock groups

crypto

clock groups under addition: $\mathbb{Z}/n\mathbb{Z} = \{0, 1, 2, \ldots n-2, n-1\}$

$\mathbb{Z} = \{\ldots -1, 0, 1, \ldots\}$ = integers under clock addition mod n

associativity inherited

identity 0

group: inverse of k is $n-k$

(if $k=0$, inverse is 0)

Clock groups under mult: $\mathbb{Z}/12\mathbb{Z}$

no. $(0, 2, 4, 6, 8, 3, 6, 9, 0)$ bad

"Life is too short to deal w/ terrible numbers"

Modified clock groups under multiplication

$(\mathbb{Z}/n\mathbb{Z})^* = \{1, 5, 7, 11\}$ with 12 clock hours

exs:

③ Identity: 1 is unit

④ assoc: inherits

S.M.: "if I had to give mathematicians a one-adjective description it would be LAZY. which leads to jokes about the lengths mathematicians will go to to reduce a problem to a previously solved problem"

Euclidian Alg: way to find gcd

given x and y, returns greatest common divisor

Ex: $\gcd(15, 42) = 3$

$15 = 3 \cdot 5$

$42 = 2 \cdot 3 \cdot 7$

$\gcd(15, 120) = 15$

$15 = 3 \cdot 5$

$120 = 2^3 \cdot 3 \cdot 5$

$\gcd(15, 17) = 1$

say relatively prime

February 6, 2012 11:44 AM

(...) goes through naive algorithms...

Euclidean Alg takes at most $1+2\log_2 X$ steps $(X<Y)$

- Euclidean Alg gives $a, b < t$ $ax + by = \gcd(X, Y)$

(eg: StM: shows that there is an optimal movie schedule but it may not be findable in < 2 hrs)

for the moment it's a black box
can look it up in many places

"There's so much info now on Wikipedia, what do you need a professor for? My job is to tell you the order in which to click on the pages."

---

want closure and inverses

	1	5	7	11
1	1	5	7	11
5	5	1	11	7
7	7	11	1	5
11	11	7	5	1

not practical for big sets

NB: $1^2 = 5^2 = 7^2 = 11^2$

each # its own inverse!

proof of inverses: let $X \in (\mathbb{Z}/12\mathbb{Z})^\times = \{1, 5, 7, 11\}$

by check, $\gcd(X, 12) = 1$

by Euclidean Alg, have $\gcd$ st $ax + b12 = 1$

February 6, 2012 11:55 AM

... or $ax = 1 + b12$

So $ax = 1 \bmod 12$

So a is invertible if x is a mod 12 and a relatively prime
but is it in the set?

So inverse is a mod 12 which is in $(\mathbb{Z}/12\mathbb{Z})^*$

... and leave Closure as an exercise!

can replace 12 with n
for RSA, $n = pq$

after lunch, authentication
and error correction

(Stu: returns to the story of Voyager & the story of design constraints on that proj!)

February 6, 2012 1:03 PM

[back from lunch...]

Sidenote: proving irrationality

x is irrational if $x \neq p/q$ for p, q integers

Proof by contradiction:

assume $\sqrt{2}$ is rational

Thus $\sqrt{2} = p/q$, wlog, assume $\gcd(p,q) = 1$

$\Rightarrow 2 = p^2/q^2$ or $2q^2 = p^2$; if p is odd, $p = 2m+1$

2012-02-07 08:26:52 23/31

If p is odd, $p = 2m+1$ so $p^2 = 4m^2 + 4m + 1$ odd

$\Rightarrow p$ is even, $p = 2m$

$\Rightarrow 2q^2 = p^2 = (2m)^2 = 4m^2 \rightarrow q^2 = 2m^2$

$\Rightarrow q$ is even, $q = 2n$

$\Rightarrow \gcd(p,q) \geq 2$ → contradiction

February 6, 2012 1:08 PM

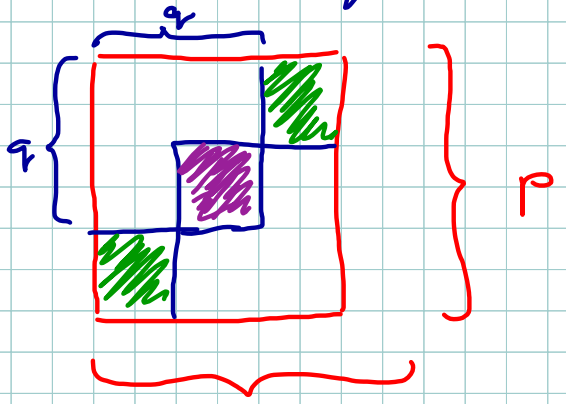
Stanley Tennenbaum (1950s)

(John Conway pub, 9th ST)

Geometric proof...

assume $\sqrt{2} = p/q$ and q smallest possible

Same as $2 = \frac{p^2}{q^2}$ or $2q^2 = p^2$



Smaller $\tilde{p}, \tilde{q}$ st

$\tilde{p}/\tilde{q} = \sqrt{2}$

2 =

↓ contdtn

QQ if StMi doesn't bring it up, ask abt the pythag proof based on known ans to n^2

February 6, 2012 1:18 PM

back to PUBLIC KEY EXCHANGE:

Alice
a secret

Bob
b secret

choose a g in $(\mathbb{Z}/n\mathbb{Z})^*$ and yell it out (PUBLIC)

computes g^a → share with world → computes g^b

(PUBLIC) ←

computes $(g^b)^a$

computes $(g^a)^b$

secret is $g^{ab} = (g^a)^b = (g^b)^a$

use this as code word for Vigenère cipher

Problem:
Eve knows g, g^a, g^b

Eve doesn't know a, b, g^{ab}

Eve wants to find a, b
↳ knows g, can find the g^{ab}

$$\frac{\log(g^a)}{\log(g)} = \frac{a\log(g)}{\log(g)} = a$$

log prob

these aren't ordinary numbers anymore....

$$\frac{\log(g^a \bmod n)}{\log(g \bmod n)}$$

} discrete log problem thought to be hard

"and this is thought to be a hard prob b/c I know ppl who have worked on it for a while and when ppl = experts and while = decades it's convincing..."

BUT

February 6, 2012 1:31 PM

crypto pm dg²

digression: D-dg, allied cipher, how long does it need to be secure? Months? Days? Hours? In some settings (battlefield) encryption/decryption need to be fast... Navajo transmissions in open air is rapid, but has implementation problems

StMi mentions public key exchange as a way to use elementary matrix in a novel way — wants to develop HS module on this as a motivator

AUTHENTICATION

(eg: how can you convince the bank that the message is from you?)

Review RSA:

Alice

choose: P_a, q_a primes

computes/publishes: $N_a = P_a q_a$

computes the secret: $(P_a-1)(q_a-1) = \emptyset(N_a)$

finds e_a, d_a st $e_a d_a \equiv 1 \bmod \emptyset(N_a)$
$\equiv 1 \bmod (P_a-1)(q_a-1)$

publishes e_a encrypt d_a decrypt

X message mod N_a

Sends X^{e_a} and N_a to Alice...

Bob

P_b, q_b primes

public $N_b = P_b q_b$

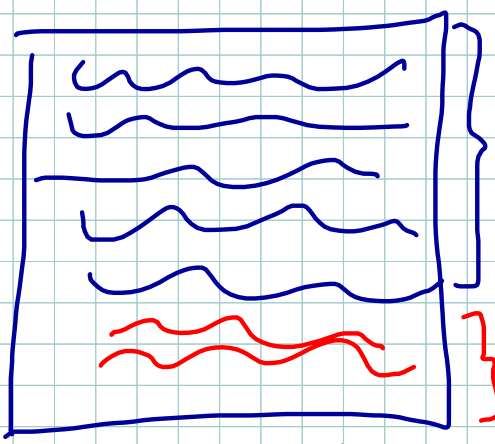
secret $\emptyset(N_b)$

e_b (public) d_b (private)

⋮

February 6, 2012 1:53 PM

Bob's message:



"it is a huge industry to be able to verify identity."
SYMMETRY

Can encrypt with e_a or d_a OR e_b or d_b and decrypt with the other.

$X^{d_b} \bmod N_b$ → gets to message

$X_{message}$ → send to Alice

$X_{message}^{e_a} \bmod N_a$

$(X_{msg}^{e_a} \bmod N_a)^{d_a}$ ← alice decrypts

food + gobbledygook

↳ alice uses e^b and N^b to decode right...
and Eve can't pretend to be Bob b/c she doesn't know d_b

February 6, 2012 2:05 PM

Finding e_a, d_a, and d

way to find e and d

step 1: choose ANY number mod N, call it e

2: apply Euclid alg. to e and (p-1)(q-1)
get a, b st ...

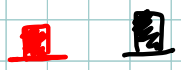
February 6, 2012 2:12 PM

crypto

Hamming codes

efficient ways to detect and fix errors

Hat Riddle



red/blue hat placed randomly on each.

close eyes, get hat

open eyes; say your color all simultaneously.

if all speakers correct, each gets $1/m.
if even 1 wrong, each lose $1/m

Strategy 1: do not play.

Strategy 2: only one person designated speaker; says some color; win 50%

Strategy 3: speak only if see 2 of same color, say OPPOSITE

A	B	C	
R	R	R	lose
R	R	B	win
R	B	R	w
R	B	B	w
B	R	R	w
B	R	B	w
B	B	R	w
B	B	B	lose

each person is right 2x wrong 2x, silent 4x

right 50% of time

BUT wrong answers clump and right answers spread

and in this game it matters

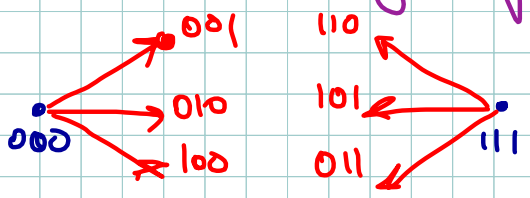
(someone brings up the Monty Hall riddle)

and this (somehow?!) leads to error detection and correction

February 6, 2012 2:28 PM

"Tell me 3 things"

send 0 or 1
transmit 000 or 111
receive 010
↳ message is probably 000



can find and correct one error
but the cost is that only 33% of transmission is info

Hamming (7,4) code

16 codewords

1	1	1	1	1	1	1
0	0	1	0	1	1	0
1	0	1	0	1	0	1
0	1	1	1	1	0	0
0	1	1	0	0	1	1
1	0	1	1	0	1	0
0	0	1	1	0	0	1
1	1	1	0	0	0	0
0	0	0	1	1	1	1

etc...

7 digits: 2^7 messages
16 messages: 2^4
4 of 7 bits info
3 are detect/correct

Can measure diff b/t any two strings: 7 strings are one flip away of each word
4/7 is info ≈ 57% info

but only finds/corrects 1 in 7
(other one is 1 in 3)

EtMi asks what is special about 7?
he answers that it's 2^3-1 that is at work here but doesn't explain

---

coda:

Classroom applications:
- Benford (what data set you use is important)
- riddles
- gambling (mb card counting and the tradeoff b/t efficiency and ease of use)

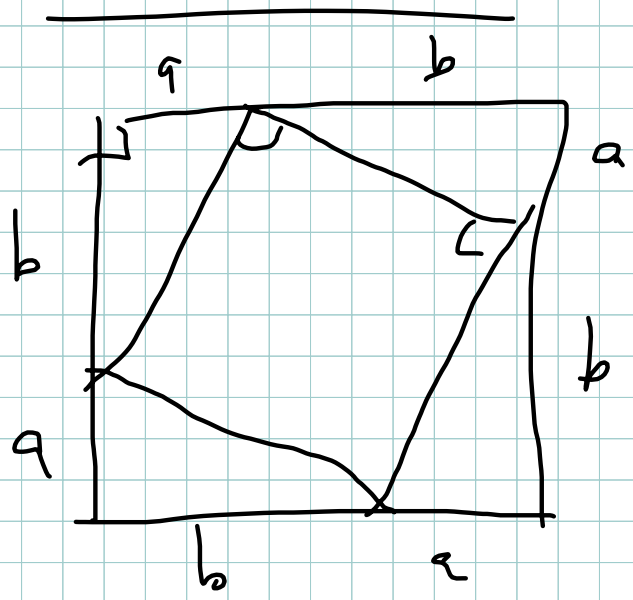
CODA^2:

5 queens on 5×5 bd
at 3 queens are safe.

STM: says 2 steps in saving:

① Solve dual problem (3 queens at 5 pairs safe)
Q ↔ P

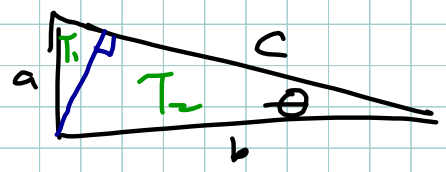
② only 6 [illegible] moves



[illegible] of shortest
[illegible] is $\frac{bh}{2}$

Dimensional Analysis

There is a fn. $f(\phi)$ s.t. area of right Δ w/ angle ϕ at hyp h is $f(\phi)h^2$



area big tri is $c^2 f(\theta)$

$\text{area}(T_1) + \text{area}(T_2) = \text{area}(\text{big } \Delta)$

$a^2 f(\theta) + b^2 f(\beta) = c^2 f(\beta)$

could get $f(\theta)$ from Heron

as $f(\theta) \neq 0$, $a^2 + b^2 = c^2$

WHY does this work? b/c you have three similar triangles!

where $\theta_A = \theta_B = \theta_C \ldots$