TAS: OUTLINE FOR DAY ONE

TIME	ACTIVITY
9:00 - 9:15	Introductions

- TAS Member introduces me
- Introduce Myself
  - Specialize Number Theory / Prob/Stats
    - sabermetrics: Padres
    - Benford: IRS
  - Riddles homepage
  - Personal: from Sharon, two kids, wife@BC
- Participants Introduce Themselves
  - What teach
  - Background
  - What want to get

9:25 - 10:30	Framing Lecture

- Describe big issues in cryptography: ASK
  - SECRECY
  - EFFICIENCY
  - SIMPLICITY
  - REDUNDANCY
- Lecture 1: Goals: see these, history, enough background to read book, class modules

TAS: OUTLINE FOR DAY ONE (CONT)

TIME	ACTIVITY
10:30 - 10:45	Coffee Break
10:45 - noon	Lecture 2 / DISCUSSION
1 - 3 pm	Lecture 3 / DISCUSSION

Interesting Riddles for TAS Course in Cryptography

Riddle 1: General Code

Consider our class of 11. One wants a security system such that any three of us can initiate the coffee break, but no two of us can. The password is a triple of three numbers, say (a,b,c). How do we assign information to the 11 people so that any three of us know (a,b,c) but no two of us know (a,b,c)?

Riddle 2: Pirates of the Cryptobean

A man on island 1 wants to send an engagement ring to his girlfriend on island 2. Each has a lock and the corresponding key. Some friendly pirates (who have a box) will freely transmit anything in the box back and forth as many times as desired; however, they will take and keep anything in an unlocked box. How can you get the ring from island 1 to island 2?

Riddle 3: Mathematicians in a Row

100 mathematicians are in a row; the last sees all 99 people in front of her, the second to last sees the first 98, and so on. Each person will have either a white or a black hat placed on their head. The hats are not independently placed – the choice depends on the strategy the mathematicians adopt. First the 100th person speaks, then five seconds later the 99th, then five seconds later the 98th, …. When it's your turn to speak you say either 'white' or 'black'; for each person who says the color of their hat correctly, the mathematicians gain another million dollars, while for each incorrect color the team loses one million dollars. Remember, whatever strategy is chosen is known to the person choosing the hats. What is the largest number of hats you can ensure are correctly identified?

Riddle 4: Three Hats and a Strange Probability

Three players enter a room and a red or blue hat is placed on each persons head. The color of each hat is determined by tossing a fair coin, with the outcome of one coin toss having no effect on the others. Each person can see the other players hats but not his own.

No communication of any sort is allowed, except for an initial strategy session before the game begins. Once they have had a chance to look at the other hats, the players must simultaneously guess the color of their own hats or pass. The group shares a $3 million prize if at least one player guesses correctly and no players guess incorrectly. If even one person speaks incorrectly, the team loses $3 million. If they play optimally, what percent of the time do they win?

Riddle 5: Safe Generals

You have 7 generals and a safe with many locks. You assign the generals keys in such a way that EVERY set of four generals has enough keys between them to open ALL the locks; however, NO set of three generals is able to open ALL the locks. How many locks do you need, and list how many keys does the first general get, the second,

TAS: LECTURE ONE: BASICS OF CRYPTOGRAPHY

QUESTION FOR THE CLASS

When you think of cryptography, what issues come to mind?

Some answers

(1) Secrecy: only INTENDED recipient can decode

(2) Efficiency: should be fast to encode/decode

(3) Simplicity: probability of miscoding small, easy to use

(4) Redundancy: Error correction/detection

Will discuss these issues and others

HISTORY

(1) Shaving head, writing message, waiting...

(2) Caesar cipher: when most can't even read, very vulnerable to attack.

(3) One time pad: must meet to exchange

(4) Enigma: WW II: Thought secure, not used to full potential
↳ starting with weather reports

(5) RSA, Elliptic Curves, Lattices/modular polynomials....

TAS: LECTURE ONE: BASICS OF CRYPTO

Spend a few minutes thinking about a riddle or two.

Riddle 1: Have 11 people. The password to start the coffee break is the 3-tuple (a, b, c). Give info to the 11 people in such a way that ANY 3 can get the password, but no two can.

Riddle 2: Man on island 1, woman on island 2. Each have a lock + corresponding key, man has engagement ring and wants to send to her. Pirate ship with box; pirates will transmit anything in box b/w the two islands, but being pirates will take anything in an unlocked box, but nothing in a locked one. Pirates can make multiple trips; how do you get the ring over?

Why these riddles?

Riddle 1: "basic" math useful, "intelligent" agents

Riddle 2: key exchange without meeting: share a secret in public!

TAS: LECTURE ONE: BASICS OF CRYPTO (CONT)

Let's start discussing some of the issues raised for cryptography.

CAESAR CIPHER

Clock arithmetic: $10 + 5 = 3$

Use clock with 26 hours

Standard Shift to all.

↳ Question for class: how to break caesar cipher?

↳ soln: trial and error.

GENERALIZING CAESAR

See notes for affine cipher

Choose a, b st. a and 26 rel prime

Send letter ξ to $a\xi + b \bmod 26$; explain why need $(a,b) = 1$

How many choices for a? 1 ~~2~~ 3 ~~4~~ 5 ~~6~~ $7 \ldots$

Not many possibilities, still susceptible

TAS: LECTURE ONE: INTRO TO CRYPTO (CONT)

OTHER METHODS

(1) Perfect Code: See Chapter 3: graphs

(2) RSA: involves number theory

Consider two systems:

public: $N = pq$

private: 200 digit primes p, q

password: p or q

private: $X \sim 5000$ digits

password: X

Question: {Which method is better/more secure?
Why is the second method less secure?

↳ Soln: Method 1: only need to know how to divide
will know password when hear it

Method 2: need to know password
can "torture" computer

TRAPDOOR MATHEMATICS

Want something hard one way, easy another (if know a little bit).

↳ Given p, q easy to find pq; given pq currently hard to find p, q (some methods: see factorization chapter).

TAS: INTRO TO CRYPTO: LECTURE ONE: CONT

IDEA BEHIND RSA

PRIVATE: $p, q \longmapsto$ PUBLIC N

$$\underbrace{\text{PRIVATE: } e, d \text{ s.t. } \underset{\varphi(N)=(p-1)(q-1)}{\varphi(N) \text{ divides } ed-1} \longmapsto \text{Public } e}_{\text{BOB}}$$

Alice: message X, number at most $N-1$

Alice sends message $X^e \bmod N$ to Bob: Deposit $\$1000$ in Acct ___

Bob computes $(X^e \bmod N)^d \bmod N = X$!

QUESTIONS / CONCERNS ABOUT METHOD:
What are your thoughts about this?

↳ (1) Does $(X^e \bmod N)^d \bmod N = X$?

(2) Is it hard to find p, q? To find e, d?

(3) How hard is it to compute $(X^e \bmod N)^d \bmod N$?

(4) Is the message really from Alice?

Finding p, q not bad; given e find d with Euclidean Alg (fast), Computing $X^e \bmod N$ fast with fast exponentiation.

TAS: LECTURE ONE: INTRO TO CRYPTO (CONT)

(3) Horner's Algorithm

Question: how many operations to compute a polynomial at a point?

↳ex: $14x^8 + 12x^7 - 11x^6 + 2x^5 - 3x^4 + 2x^3 - 8x^2 + 5x + 2$?

Soln: Could do fast exponentiation for each x^{power} and then combine, on the order of $n \log_2 n$. This is better than order n^2, but can we do better?

Yes! can do order n!

$$(((((((14x + 12)x - 11)x + 2)x - 3)x + 2)x - 8)x + 5)x + 2$$

Question: Always ask: Who gives a damn? Thoughts?

Applications to chaos/fractals.

Mandelbrot set: $z_{n+1} = z_n^2 + c$ for a fixed c

(or consider more general maps). On my old computer took too long without implementing this

TAS: LECTURE ONE: INTRO TO CRYPTO (CONT)

(4) Euclidean Algorithm: Finds not just $\gcd(x,y)$ but also a, b st $ax + by = \gcd(x,y)$

Question: anyone teach in classes?

Say we have Euclidean Algorithm

Given $N = pq$ must find e, d st $ed \equiv 1 \pmod{\varphi(N)}$

↳ say e and $\varphi(N)$ are <u>not</u> relatively prime

↳ This can happen, but "rare"

↳ find a, b st $ae + b\varphi(N) = \gcd(e, \varphi(N)) = 1$

↳ take $d = a$.

$\varphi(N) = (p-1)(q-1)$ is # integers at most N that are rel prime to N

Must we keep $\varphi(N)$ private? If we know N and $\varphi(N)$ can we find p and q?

$$N = pq$$

$$\varphi(N) = (p-1)(q-1) = N - (p+q) + 1$$

$\Rightarrow$ know pq and $p+q$

↳ leads to a quadratic eq

↳ $pq = x$, $p+q = y$

↳ $q = \frac{x}{p}$, $p + \frac{x}{p} = y \rightarrow p^2 - yp + x = 0$

so $p = \dfrac{y \pm \sqrt{y^2 - 4x}}{2}$

So must keep $\varphi(N)$ private (of course, if public d is easily found)

TAS: LECTURE ONE: INTRO TO CRYPTO: CONT

What is The Euclidean Algorithm?

↳ See interest in details

```
↳ wlog: $y > x$
    write $y = a_1 x + r_1$   with $0 \le r_1 < x$
    if $r_1 = 0$ done else
        ~~$r_2$~~ $x = a_2 r_1 + r_2$   with $0 \le r_2 < r_1$
        if $r_2 = 0$ done else
            $r_1 = a_3 r_2 + r_3$   with $0 \le r_3 < r_2$
```

Continue

↳ Show get linear combination

↳ Show $r_{n+2} / r_n \le 1/2$ so decays fast

RSA REVISITED

- Fast exponentiation helps: need to use a lot
- Euclidean algorithm helps, but less important as only generate (e, d) once
- Problem encrypting a big message. RSA "mixes" so could do a "simpler" encryption but use RSA to send The key.
  - ↳ Simplicity is important!

TAS: ~~OUTLIN~~ LECTURE ONE: INTRO TO CRYPTO: CONT

<u>Riddle 3</u>: 100 people in a row; nth sees $n-1$ in front. Strategize. Last speaks first, one second later next to last, then ... Can only say "white" or "black." Everyone who is right adds $1 million to team's coffers; anyone wrong costs team $1 million. I'm listening to your strategy and put hats on you as diabolically as possible. How many people can you ensure speak correctly?

<u>Riddle 4</u>: 3 people, each sees other two. White or black hat randomly placed on each person; each hat choice is independent of others and white with prob 1/2. Open eyes, wait 5 seconds, and then either say "white", "black" or stay silent. If all who speak are correct team gets $1 million; if even one speaker is wrong team loses $1 million. How often do you win with best strategy?

<u>Riddle 5</u>: Have Seven generals. Assign keys to locks so that any four can open but no set of 3 can. How many locks needed, and how accomplish?

Riddle 3 related to "intelligent" assistant doing computations on end (video: send changes), Riddle 4 related to error correction, Riddle 5 related to binomial coeffs.

TAS: LECTURE ONE: INTRO TO CRYPTO: CONT

ERROR DETECTION AND CORRECTION

- Hamming stories: only run on weekends, computer halts when find error: if know something is wrong, why can't it fix it?

- Assume probability of an error is low (<u>very</u> low)

  ↳ Popular error detection: CHECK SUM (add to book)

  Message string $a_1 a_2 a_3 \cdots a_{n-1} a_n$ and a_n chosen so that $a_1 + a_2 + \cdots + a_n \equiv 0 \bmod 10$.

  ↳ note given $a_1, a_2, \dots, a_{n-1}$ that unique choice for a_n

  ↳ Can easily detect one error, but don't know where

  ↳ see on ISBN numbers, ...

  ↳ more clever choice can detect other errors such as transpositions...

  ↳ Nice, but want to know <u>where</u> error is.

  ↳ "Most" of message is info: $\frac{n-1}{n}$

TAS: LECTURE ONE: INTRO TO CRYPTO - CONT

Error Correction and Detection!

(1) Tell me three times: Majority Rules

- Unlikely to get same wrong answer twice
- Often used by military (target solns)
  - ↳ Pre-cogs in Minority Report

- Message 1011011, send 111 000 111 111 000 111 111

- Can detect and correct one error in every 3 blocks
  - ↳ Problem: only 1/3 of message is information!

(2) Hamming Codes

- Based on the 3 hat riddle
- 16 code words in Hamming (7,4) code (see Section 1.5)

  1111111, 0010110, 1010101, 0111100, 0110011,
  1011010, 0011001, 1110000, 0001111, 1100110,
  0100101, 1001100, 1000011, 0101010, 1101001, 0000000

  - ↳ given any of the $2^7 - 16 = 128 - 16 = 112$ non-code words, must be a transmission error as sending one of these 16.

  - ↳ Measure distance b/w two 7-tuples by number of places differ. Call this the Hamming Distance

  - ↳ note distance b/w elements in code at least 3.
  - ↳ change each code word in only one place: exhausts all!