MIDWAY:

- Pearl Harbor: Dec 7, 1941
- Japanese Naval Superiority: Around May 1942 it was:

Japan	10 carriers	11 battleships
US (Pacific)	3 carriers	0

- Concerns about attacking Midway; Doolittle's raid convinced some
- Midway plan: feint to Alaska, hit Midway with second fleet hiding west of Midway which attacks when US responds to Midway attack,
  Japanese: > 200 ships (8 carriers, 11 battleships)
- US intercepts/records volumes traffic, sense of plans
- Thought in Japanese dispatches that AF referred to Midway, but all not 100% convinced. No direct evidence for following story, but response was received:
  - ↳ Midway ordered by secret cable to radio water shortage. Later decrypted Japanese message says AF short on water...
- MacArthur: had planes flying back and forth in Coral Sea exchanging messages, gave impression US carriers there (Battlestar Galactica - original - episode like this).

MIDWAY

- Japanese change code, causing problems
- Japanese notice 72 of 180 messages from Pearl Harbor - marked urgent, fear carriers moving
- Nimitz gambles that decrypts right, date right...
- US only 73 ships : 3 carriers
  - did have numerical advantage at scene of battle.
- Japan lost four carriers, US none
- Shortly after battle (weekly month) newspaper article on "how did we know"? How should gov respond? Did this alert Japanese to code breaking?

RSA LECTURE

RSA algorithm

Bob: private: two large primes p, q

private: e, d (large) such that $(p-1)(q-1)$ divides $ed-1$

public: $N = pq$, e (encrypt)

Alice: Message $X \in \{0, 1, \ldots, N-1\}$

sends $X^e \bmod N$ to Bob (computes @ fast exponentiation)

Bob: Decrypts by computing $(X^e \bmod N)^d \bmod N$ with fast exponentiation

Goal is to explain why this works; saw last time can do steps reasonably efficiently, find primes fast, ...

Key inputs: Euclidean Algorithm, Group Theory

Group: set of elements with binary operation $*$ such that

(1) Closure: $g_1, g_2 \in G \to g_1 * g_2 \in G$

(2) Assoc: $g_1, g_2, g_3 \in G \to g_1 * (g_2 * g_3) = (g_1 * g_2) * g_3$

(3) Identity: Is an $e \in G$ st given any $g \in G$: $e * g = g * e = e$

(4) Inverse: Given any $g \in G$ is an h so that $g * h = h * g = e$

Examples: Integers under addition, Rationals under multiplication, Moves of a Rubic's cube...

RSA Lecture

Euclidean Algorithm: $\gcd(x,y)$ is largest integer dividing x and y. If $k \mid x$ and $k \mid y$ then $k \mid \gcd(x,y)$ (not trivial: must prove!). Given any x, y, there exist integers a, b s.t.

$$ax + by = \gcd(x,y)$$

Important Groups

$$(\mathbb{Z}/N\mathbb{Z})^* = \{n : 0 \le n < N \text{ and } \gcd(n,N) = 1\}$$

Ex: $(\mathbb{Z}/12\mathbb{Z})^* = \{1, 5, 7, 11\}$ DO THE MULTIPLICATION TABLE HERE

$(\mathbb{Z}/p\mathbb{Z})^* = \{1, 2, 3, \ldots, p-1\}$ if p prime AND $p \neq 5$

↳ Must prove: hard parts closure, inverses.

Inverse: say $x \in (\mathbb{Z}/N\mathbb{Z})^*$: need inverse

by Euclidean Alg: have a, b such that

$$ax + bN = \gcd(x,N) = 1$$

Thus $ax \equiv 1 \bmod N$, and a is the inverse!

Key fact: $(\mathbb{Z}/pq\mathbb{Z})^*$ has $(p-1)(q-1)$ elements

Consider $1, 2, 3, \ldots, pq$. Have p multiples of q, have q multiples of p, and double count one multiple of pq. Thus number of relatively prime elements is $pq - pq - qp + 1$ which is $(p-1)(q-1)$. Lots of structure: $\phi(N) = \#(\mathbb{Z}/N\mathbb{Z})^*$ is the Euler totient function.

RSA LECTURE: CONT

Key fact: Group G, $g \in G$, say n is the order of a if it is the smallest integer such that $g^n = e$. Have $n = \text{ord}_G(a)$ divides $\#G$, the number of elements in G.

Usually prove as a consequence of Lagrange's Thm, namely the size of a subgroup divides the size of the group. Let's try a proof of just our key fact.

Let $\#G$ be the size of G. For $a \neq e$, look at $a, a^2, \ldots, a^{\#G+1}$

By Dirichlet's Pidgeon Hole Principle at least two of these $\#G+1$ elements are equal: all in G and only $\#G$ things in G.

Wlog, say $a^{n_1} = a^{n_2}$, with $n_1 > n_2$. Using inverses find $a^n = e$ with $n = n_1 - n_2$. Know such an n exists now with $a^n = e$, assume have the smallest.

Assume now some element has $a^n = e$ and $n \nmid \#G$. Write $n = m_1 m_2$ with $m_1 \mid \#G$ and $(m_2, \#G) = 1$. Then $a^{m_1} \neq e$ by minimality of n and element a^{m_1} has $(a^{m_1})^{m_2} = e$. Thus may assume have some element $a \in G$ whose exponent is relatively prime to $\#G$.

If knew $a^{\#G} = e$ done: by above have $(n, \#G) = 1$ so there are integers α, β st $\alpha n + \beta \#G = 1$, so $a = a^{\alpha n + \beta \#G} = (a^n)^\alpha (a^{\#G})^\beta = e$

Know $a^{\#G} = e$ by Lagrange

DIFFIE-HELMAN-MERKLE KEY EXCHANGE

Idea: need to agree upon a secret in public & private meeting. Discovered (but classified) earlier by GCHQ (Britain)

Take some group G and a generator g. Standard: $(\mathbb{Z}/p\mathbb{Z})^*$ is cyclic and always has a generator.

PUBLIC: Group G, generator g

PRIVATE: Alice chooses a
Bob chooses b

PUBLIC: Alice posts g^a
Bob posts g^b

Shared Secret: Alice and Bob both know g^{ab}; Alice from $(g^b)^a$ and Bob from $(g^a)^b$

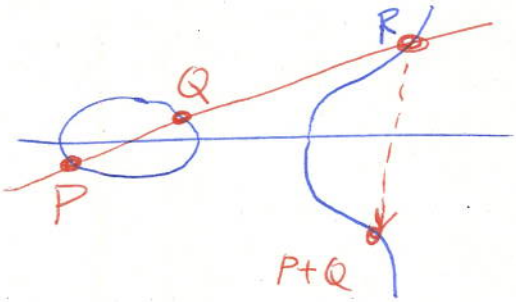
This is the discrete log problem: without knowing a and b, supposed to be hard to find g^{ab} given only g, g^a, g^b.

Elliptic Curve Cryptography

RSA based on $(\mathbb{Z}/pq\mathbb{Z})^*$

Can use more "complicated" groups.

Consider elliptic curve $y^2 = x^3 + ax + b$, a, b integers



$E(\mathbb{Q}) = \{(x,y) \in \mathbb{Q}^2 : y^2 = x^3 + ax + b\}$

↳ all solns with rational coords

↳ turns out to be a group!

Assume $P = (x_P, y_P)$ and $Q = (x_Q, y_Q)$ solve and have rational coords. Then line from P to Q, $mx + b$, has rational m, b. Find

$$(mx+b)^2 = x^3 + ax + b \Rightarrow x^3 - m^2x^2 + (a - 2mb)x + b - b^2 = 0$$

is a cubic with rational coeffs and know rationals x_P, x_Q are roots. Thus cubic equals $(x - x_P)(x - x_Q)(x - x_R)$ and see x_R must be rational. Define $P+Q$ as reflection about the line $y = 0$ of R. Turns out this is a group!

Group is more complicated than $(\mathbb{Z}/pq\mathbb{Z})^*$, hope that helps cryptography!

Checksum

Lots of good articles on check-sum schemes, UPC codes...

Last time mentioned simple one:

$$a_n \; a_{n-1} \; \cdots \; a_2 \; a_1$$

Choose a_1 (check digit) so that $a_n + \cdots + a_1 \equiv 0 \bmod 10$

↳ unique choice of a_1: catches single digit errors

↳ Can we do better?

Consider say $a_6 \; a_5 \; a_4 \; a_3 \; a_2 \; a_1$, a_1 check digit.

Choose a_1 st $3(a_6 + a_4 + a_2) + 1\cdot(a_5 + a_3 + a_1) \equiv 0 \bmod 10$

↳ Can solve, unique a_1

Claim 1: Catches any single error

↳ because 3 and 1 relatively prime to 10

Claim 2: Catches any transposition? Not quite.

↳ say flip a_4 a_3. Instead of $3a_4 + a_3$ now have $3a_3 + a_4$. Difference is $2(-a_3 + a_4)$

↳ no error if $a_3 = a_4$

↳ catches unless $a_4 - a_3 \equiv 0 \bmod 5$

↳ catches "most" transpositions

SIGNATURES

Very important to be able to verify sender.

Main way hash functions, here's a rough idea.

	ALICE	BOB
private:	p_a, q_a e_a, d_a with $e_a d_a \equiv 1 \bmod (p_a-1)(q_a-1)$	p_b, q_b e_b, d_b with $e_b d_b \equiv 1 \bmod (p_b-1)(q_b-1)$
Public:	$N_a = p_a q_a$ e_a (encrypt)	$N_b = p_b q_b$ e_b (encrypt).

Idea: Alice encrypts her name/message using her key and tacks that on to message to Bob, encrypting all using his key.

S = signature = Hi - I'm Alice: Trust me!

$S^{d_a} \bmod N_a$. Bob can decrypt as e_a is public!

Rest of message is M, take on $S^{d_a} \bmod N_a$ at end, raise all to e_b. When Bob raises to d_b not all becomes text; takes rest to $e_a \bmod N_a$.

Combinatorics and Enigma

Riddle 5: Have locks and keys. Distribute keys to 7 generals so that any 4 can open all the locks but no 3 can. How many locks needed, how are keys distributed?

Answer: $\binom{7}{4} = 35$ locks, give one key to four generals for each lock. Then any set of four always can. Must make sure no set of three can. Easiest: There are $\binom{7}{4} = 35$ subgroups of four generals. For each subgroup add a new lock, give a key to each of four. Clearly missing three generals can't open this lock!

Basic Combinatorics

$n!$ # ways order n people (estimating size)

$n(n-1)\cdots(n-(k-1))$ # ways to pick k from n, order matters

$$= \frac{n!}{(n-k)!} = {}_nP_k$$

$\frac{n(n-1)\cdots(n-(k-1))}{k!}$ # ways pick k from n, order doesn't matter

$$= \frac{n!}{k!(n-k)!} = {}_nC_k = \binom{n}{k}$$

Enigma + Combinatorics

Lots of combinatorics in studying Enigma.

Key Problem: how many ways to pair 26 letters?

↳ answer: $\binom{26}{2}\binom{24}{2}\cdots\binom{2}{2} / 13!$

↳ algebra $\Rightarrow$ $25 \cdot 23 \cdot 21 \cdots 3 \cdot 1 = 25!!$

↳ Better: Induction: Assume true for $2n-1$

If have $2n+2$ then 1 paired with something: $2n+1$ choices. Now pair remaining $2n$; know $(2n-1)!!$ ways; get $(2n+1)\cdot(2n-1)!! = (2n+1)!!$

Other fun problems

(1) How many ways divide C cookies among P people? $\binom{C+P-1}{P-1}$

↳ related to Stat Mech, Num Theory

(2) Lottery: Choose 6 of 40, order doesn't matter: $\binom{40}{6} \approx 3,838,380$

↳ if order matters: $\binom{40}{6}\cdot 6! = \binom{40}{6} \approx 8,145,060$ versus $40^6 \approx 5,688,889$