




Lecture 25

Modular Arithmetic, Groups and Cryptography

CS105: Discrete Structures

Instructor: S. Akshay, Guest Lecturer: Sruthi Sekar

Recap: Defining Groups

- Group $(\mathbb{G},*)$ consists of set $\mathbb{G}$ and operation $* : \mathbb{G}\times\mathbb{G} \longrightarrow \mathbb{G}$ that satisfies:
  1. **Closure Property**: For all $a, b \in \mathbb{G}$, $a * b \in \mathbb{G}$ (denote $*(a, b)$ as $a * b$)
  2. **Associativity**: For all $a, b, c \in \mathbb{G}$, $a * (b * c) = (a * b) * c$
  3. **Identity**: There exists an $e \in \mathbb{G}$ such that $a * e = a = e * a, \forall\, a \in \mathbb{G}$
  4. **Inverse**: For every $a \in \mathbb{G}$, there exists $a^{-1} \in \mathbb{G}$ such that $a * a^{-1} = e = a^{-1} * a$
  5. **Commutativity (additional property)**: For all $a, b \in \mathbb{G}$, $a * b = b * a$
- **Order** of a group $|\mathbb{G}|$: number of elements in $\mathbb{G}$.

Abelian groups

IS THIS A GROUP? WHAT IS THE ORDER?

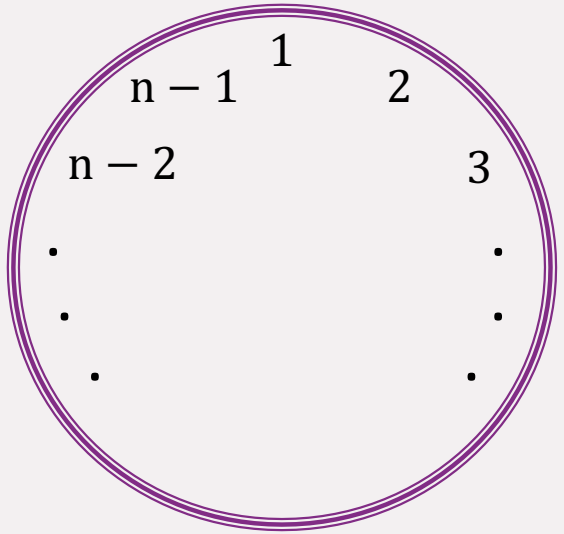
✓ $\mathbb{Z}$ =(Integers, +)

✗ $\mathbb{R}$ =(Real Numbers, ×)

Recap: Additive Group $(\mathbb{Z}_n, +\bmod n)$

$\mathbb{Z}_n = \{0,1, \dots, n-1\}$ (all integers modulo n)
For integers a, b: $(a \pmod n + b \pmod n) \pmod n = (a+b) \pmod n$

- **Closure**: easy to see and prove!
- **Associativity**: easy to see and prove!
- **Identity**: 0
- **Inverse**: For any $a \in \mathbb{Z}_n$, $(-a) \pmod n = (n-a) \pmod n$
- **Commutativity** : $(a+b) \pmod n = (b+a) \pmod n$
- **Order of the group (denoted by $|\mathbb{Z}_n|$)** : n



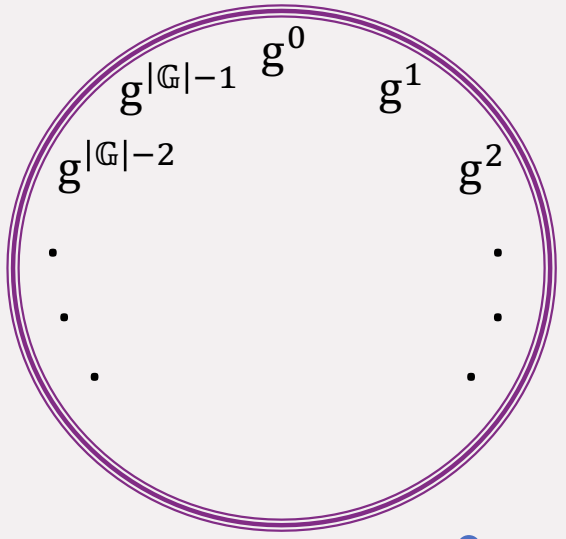
Recap: Properties of Groups

Lagrange's Theorem For any $g \in \mathbb{G}, g^{|\mathbb{G}|} = g * g * \cdots * g$ ($|\mathbb{G}|$ times) = identity, i.e., $|g|$ divides $|\mathbb{G}|$

Notation: g^i is used to denote $g * g * \cdots * g$ (i times), $|g|$, the order of $g \in \mathbb{G}$ is $\min_i(g^i = \text{identity})$

Finite Cyclic Group $\exists\, g \in \mathbb{G}$ such that $\mathbb{G} = \{g^0, g^1, \ldots, g^{|\mathbb{G}|-1}\}$. g is called generator of the cyclic group.

EXAMPLE: $(\mathbb{Z}_n, +\bmod n)$: a generator is 1. Find all generators?



Theorem: Prime order groups are cyclic

Every group $\mathbb{G}$ with $|\mathbb{G}| = p$, where p is a prime, is cyclic.
Every element other than the identity is a generator of $\mathbb{G}$.

DID YOU THINK OF ANY GROUP YOU SAW IN THIS COURSE BEFORE?

Multiplicative Group $(\mathbb{Z}_n^*, \times \bmod n)$

Is $(\mathbb{Z}_n = \{0,1,\dots,n-1\},\ \times \bmod n)$ a group? **NO (0 has no inverse!)**

Is $(\{1,\dots,n-1\},\ \times \bmod n)$ a group? **NO (E.g. closure doesn't hold in $(\{1,2,3\}, \times \bmod 4)$)**

Let's start with trying to accommodate inverses. $x \in \mathbb{Z}_n$ has a multiplicative inverse, if $\exists\ y \in \mathbb{Z}_n$ s.t.:

$$xy = 1 \bmod n \Leftrightarrow xy = nq + 1 \text{ for some integer } q \Leftrightarrow xy - nq = 1$$

This means that $\gcd(x, n) = 1$!

$\therefore$ for an integer x, there exists an integer y such that $xy = 1 \bmod n$ if and only if $\gcd(x, n) = 1$

Greatest common divisor	$\gcd(x, n)$: largest positive integer d that divides both x and n

Bezout's Identity	Let $d = \gcd(x, n)$. There exists integers a, b such that $ax + bn = d$

HW: Try to prove this!

Multiplicative Group $(\mathbb{Z}_n^*, \times \bmod n)$

Multiplicative group of integers mod n

$(\mathbb{Z}_n^*, \times \bmod n)$: set consists of integers $1 \le a < n$ such that $\gcd(a, n) = 1$

EXAMPLE: Take $(\mathbb{Z}_{10}^* = \{1,3,7,9\}, \times \bmod 10)$. $(7 \times 9) \bmod 10 = ?$, $(3 \times 9) \bmod 10 = ?$

Why is $(\mathbb{Z}_n^*, \times$ mod n) a group?

- **Closure**: For $x, y \in \mathbb{Z}_n^*$, $\gcd(x, n) = \gcd(y, n) = 1 \Rightarrow \gcd((x \times y) \bmod n, n) = 1$ (**HW: Prove it**)
- **Associativity**: easy to see and prove!
- **Identity**: 1 ($x \times 1 = x = 1 \times x \bmod n$)
- **Inverse**: For any $x \in \mathbb{Z}_n^*$, Bezout's $\Rightarrow ax + bn = 1$ for some integers a, b $\Rightarrow$ **a**$x = 1 \bmod n$.
- **Commutativity** : $(x \times y) (\bmod n) = (y \times x) (\bmod n)$
- **Order of the group (denoted by $|\mathbb{Z}_n^*|$)** : ?

Multiplicative Group $(\mathbb{Z}_n^*, \times \bmod n)$

Multiplicative group of integers mod n

$(\mathbb{Z}_n^*, \times \bmod n)$: set consists of integers $1 \le a < n$ such that $\gcd(a, n) = 1$

EXAMPLES:

- Take $(\mathbb{Z}_8^* = \{1,3,5,7\}, \times \bmod 8)$. **Order: 4** **Cyclic? NO**
- Take $(\mathbb{Z}_{10}^* = \{1,3,7,9\}, \times \bmod 10)$. **Order: 4** **Cyclic? YES (3 is a generator)**
- Take prime p $(\mathbb{Z}_p^* = \{1,2,\cdots,p-1\}, \times \bmod p)$.

  Order: p − 1 **Cyclic? YES (Why? How many generators?)**

Order of $\mathbb{Z}_n^*$

called **Euler totient function of** $n = \prod_i p_i^{\alpha_i}$ **(the prime factorization of n)**: $\varphi(n) = \prod_i (p_i^{\alpha_i} - p_i^{\alpha_i - 1})$

Is $\mathbb{Z}_n^*$ cyclic? Yes, when $n = p$, for some prime p. Otherwise, need not be cyclic!

Chinese Remainder Theorem

Motivating Example (A simple magic trick): Find your birth-date with two simple questions.

Q1: What is your birth-date modulo 5? **Q2: What is your birth-date modulo 7?**

0	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	27
28	29	30	31	32	33	34

$(x \pmod 5, x \pmod 7) \longleftrightarrow x \pmod{35}$

Chinese Remainder Theorem

Group Isomorphism denoted by $\mathbb{G} \equiv \mathbb{H}$

There exists a bijective map $\phi: \mathbb{G} \longrightarrow \mathbb{H}$ such that $\forall a, b \in \mathbb{G}, \phi(a *_{\mathbb{G}} b) = \phi(a) *_{\mathbb{H}} \phi(b)$

Example of a Group Isomorphism:

For any cyclic group $\mathbb{G}$ with generator g and order n $\phi_g: (\mathbb{Z}_n, + \bmod n) \longrightarrow \mathbb{G}: \ \phi_g(x) = g^x$

Every finite cyclic group of order n is isomorphic to $(\mathbb{Z}_n, +\bmod n)$

Chinese Remainder Theorem

Group Isomorphism denoted by $\mathbb{G} \equiv \mathbb{H}$

There exists a bijective map $\phi: \mathbb{G} \longrightarrow \mathbb{H}$ such that $\forall a, b \in \mathbb{G}, \phi(a *_{\mathbb{G}} b) = \phi(a) *_{\mathbb{H}} \phi(b)$

Chinese Remainder Theorem (CRT):

Let $N = pq$ where $p, q > 1$ are relatively prime (i.e., $\gcd(p, q) = 1$), then

(additive group) $\mathbb{Z}_N \equiv \mathbb{Z}_p \times \mathbb{Z}_q$ and $\mathbb{Z}_N^* \equiv \mathbb{Z}_p^* \times \mathbb{Z}_q^*$ **(multiplicative group)**

With the same bijection map

$$\phi(x) := ([x \bmod p], [x \bmod q])$$

In the birthday demo we started with: we needed to "*efficiently*" find the inverse of this map.

$$\phi^{-1}((x_1, x_2)) := (c_1 x_1 + c_2 x_2) \bmod N, \text{ where } c_1 = q \cdot (q^{-1} \bmod p),\ c_2 = p \cdot (p^{-1} \bmod q)$$

****ϕ^{-1} or ϕ usually need not be "*efficiently*" computable, CRT is an example where both are!**

$\mathbb{G} \times \mathbb{H}$ consists of all ordered pairs $(g, h), g \in \mathbb{G},\ h \in \mathbb{H}$ with the operation: $(g, h) * (g', h') := (g *_{\mathbb{G}} g', h *_{\mathbb{H}} h')$

Chinese Remainder Theorem

Where does isomorphism help?

Given $\mathbb{G} \equiv \mathbb{H}$ with , one can choose to do group computations in the group where it is more efficient!

EXAMPLES $N = pq$ for distinct primes p and q

CRT tells you that addition, multiplication and group exponentiation mod N can be **transformed to analogous operations** mod p and mod q.

1. **Want to compute:** $14 \times 13 \bmod 15$ (in $\mathbb{Z}_{15}^*$)

$$\phi_{CRT}(14) = (14 \bmod 5, 14 \bmod 3) = (4,2)$$
$$\phi_{CRT}(13) = (13 \bmod 5, 13 \bmod 3) = (3,1)$$

$$(4,2) * (3,1) = ((4 \times 3 \bmod 5), (2 \times 1 \bmod 3)) = (2,2)$$

$$\phi_{CRT}^{-1}((2,2)) = 2 = 14 \times 13 \bmod 15$$

2. **Want to compute:** $29^{100} \bmod 35$

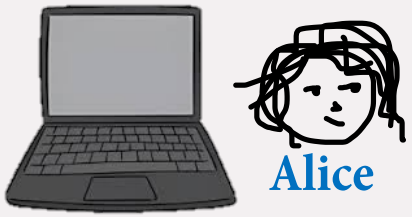
$$\phi_{CRT}(29) = (29 \bmod 5, 29 \bmod 7) = (-1 \bmod 5, 1)$$

$$(-1 \bmod 5, 1)^{100} = ((-1)^{100} \bmod 5, 1) = (1,1)$$

$$\phi_{CRT}^{-1}((1,1)) = 1 = 29^{100} \bmod 35$$

MULTIPLICATIVE GROUPS ARE VERY USEFUL FOR CRYPTOGRAPHY

Problem of Secure Communication



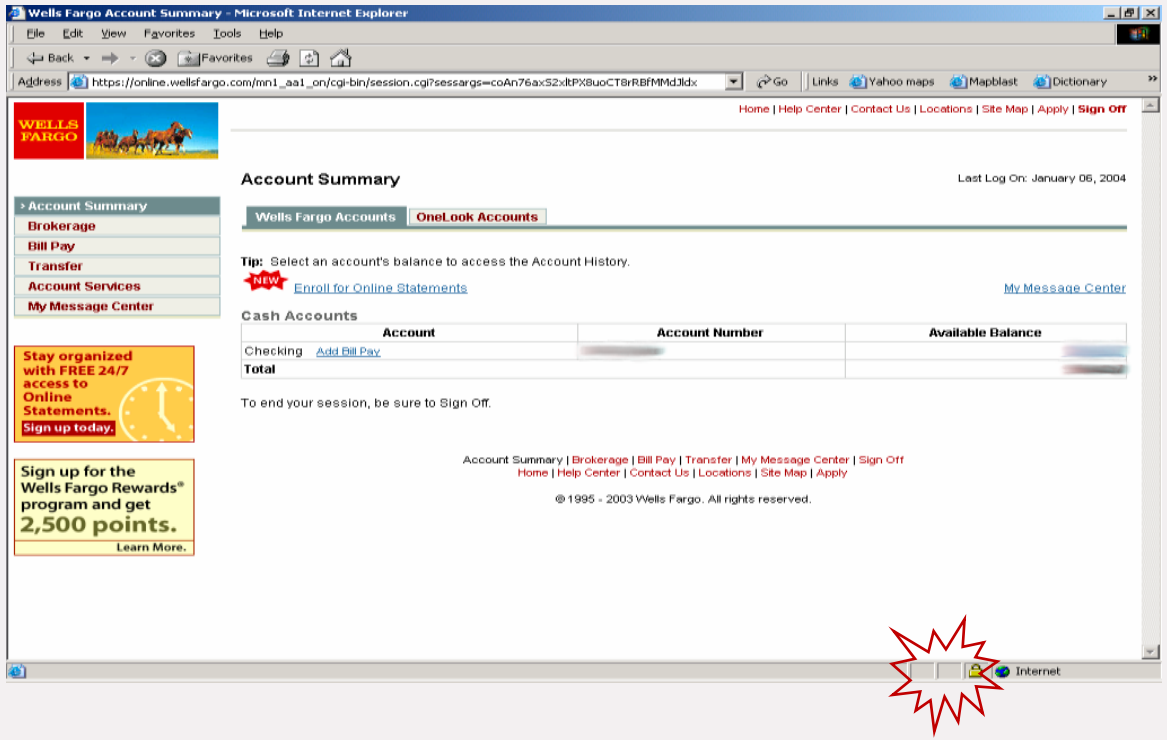
Alice

HTTPS

SSL/TLS



Bob





Eve

Protect against eavesdropping

Problem of Secure Communication



Two main parts of SSL/TLS:

1. Establish a ***shared secret key*** using a ***"public channel".***
2. Using the ***shared secret key***, send the data securely, while ensuring confidentiality and integrity.

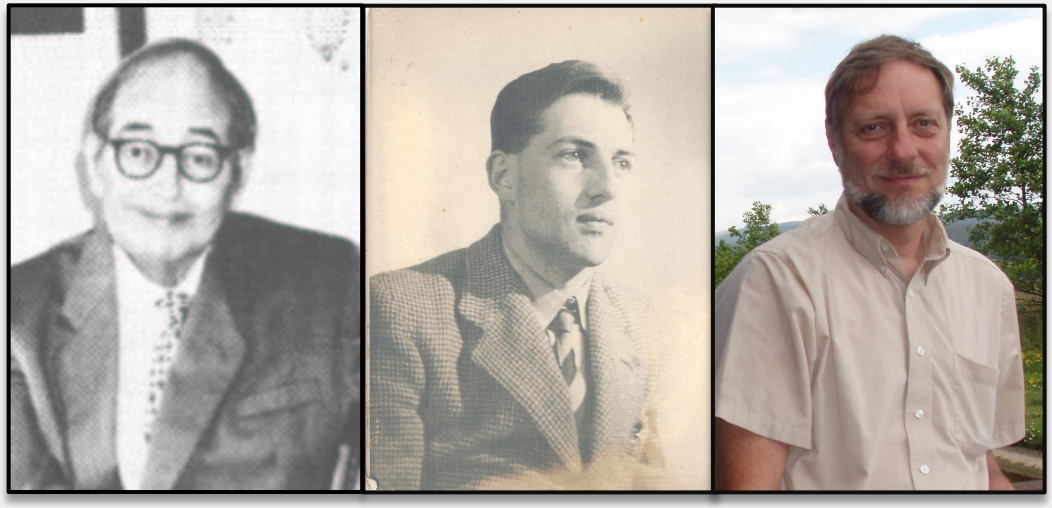


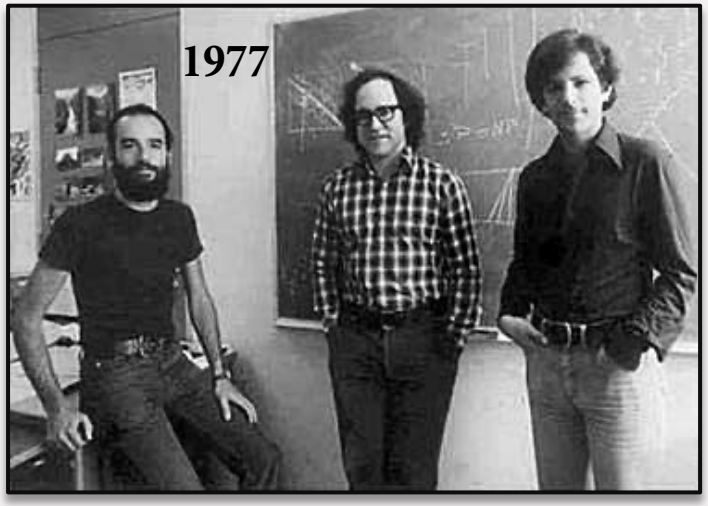
Protect against eavesdropping

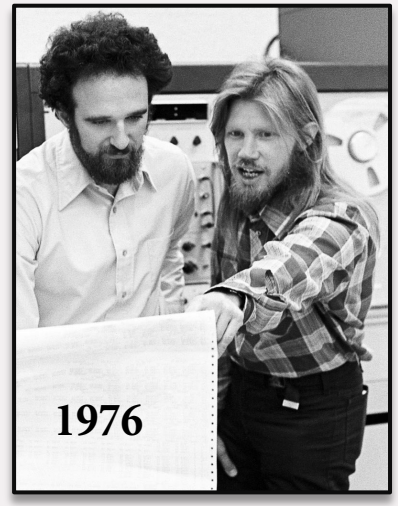
Key Exchange: Magical invention! Let's see how to do this using multiplicative groups!

Advent of Public Key Cryptography [1970s]

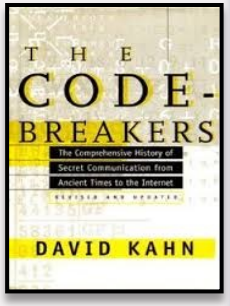
Non-secret encryption **RSA** **Diffie-Hellman**







James Ellis **Clifford Cocks** **Malcolm Williamson** **Adi Shamir** **Ronald Rivest** **Leonard Adleman** **Martin E. Hellman** **Whitfield Diffie**



"The collaborative work of **Clifford Cocks, James Ellis, and Malcolm Williamson** at **GCHQ** resulted in the discovery of **public key cryptography (PKC)** in the early 1970s. Even though outside researchers subsequently made similar discoveries, the UK's **GCHQ** did not make it public until 1997." *–National Security Agency (NSA)*

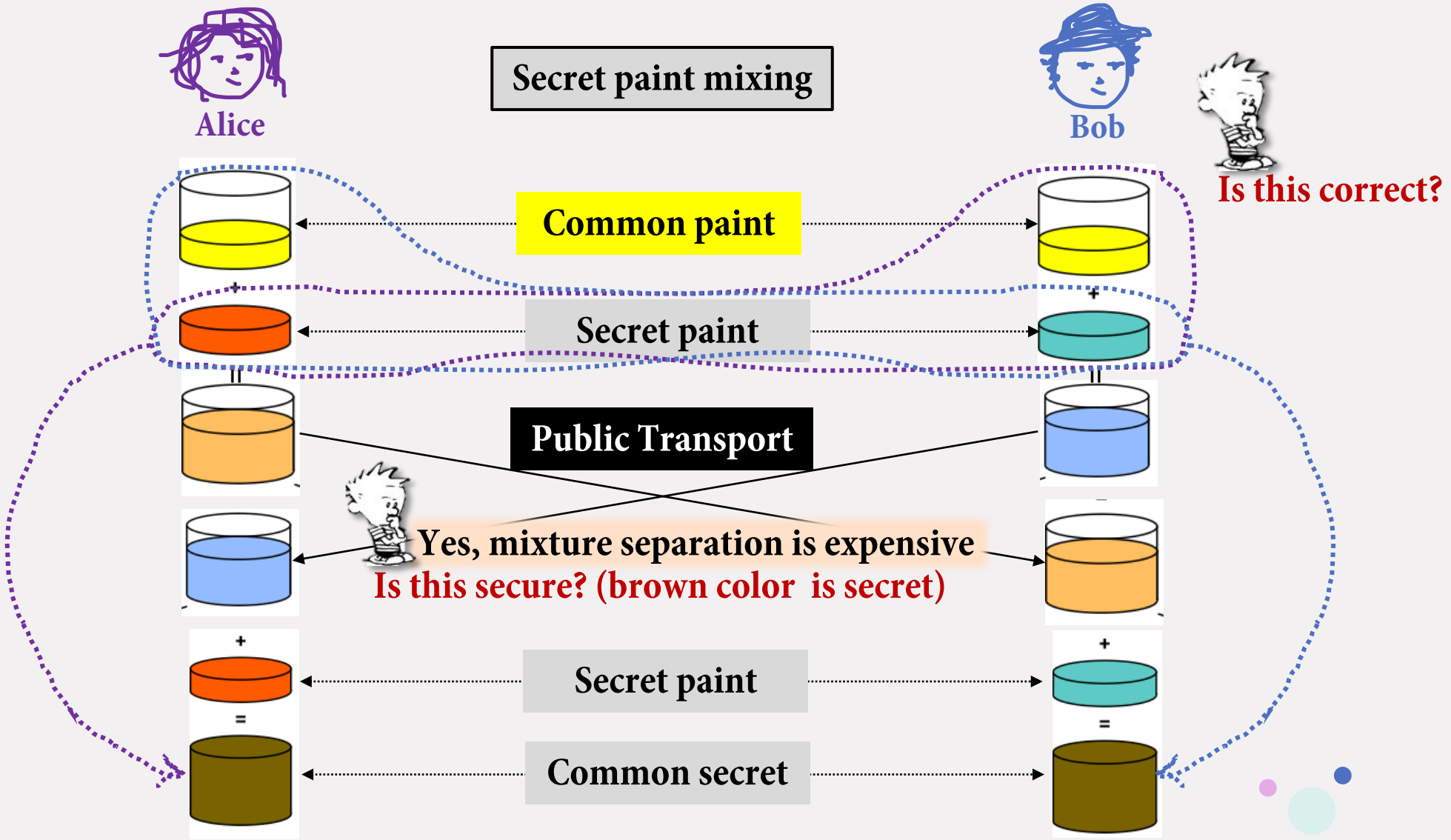
1974 Undergrad student project

"The human mind treats a new idea the same way the body treats a strange problem, it rejects it."

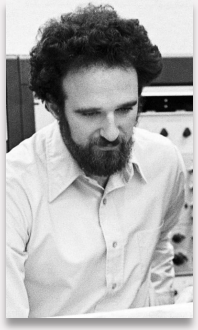


Ralph Merkle

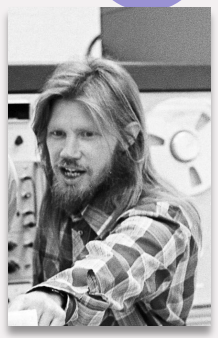
An Analogy for a Key Exchange Protocol



**[Codebook, Simon Singh]



Diffie-Hellman Key-exchange [1976]



Cyclic Group ($\mathbb{G}$, q, g)

Group Order Generator



Alice



How do you use this group to agree on a secret key?

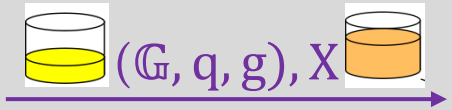


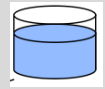
Bob

Pick a cyclic group $(\mathbb{G}, q, g)$ 

Pick random $x \in \mathbb{Z}_q$ 

$X = g^x$ 





Pick random $y \in \mathbb{Z}_q$ 

$Y = g^y$ 



$Key_{Alice} = Y^x$ 



Is this correct?

$Key_{Bob} = X^y$ 

What is the assumption needed to prove security against eavesdroppers?

"Discrete log separation is hard"

Given $(\mathbb{G}, q, g), g^x, g^y$ the key looks random to **Eve** (and she cannot find it!)

****This is believed to be hard in certain multiplicative groups!**

Cryptography is based on “hard-problems”

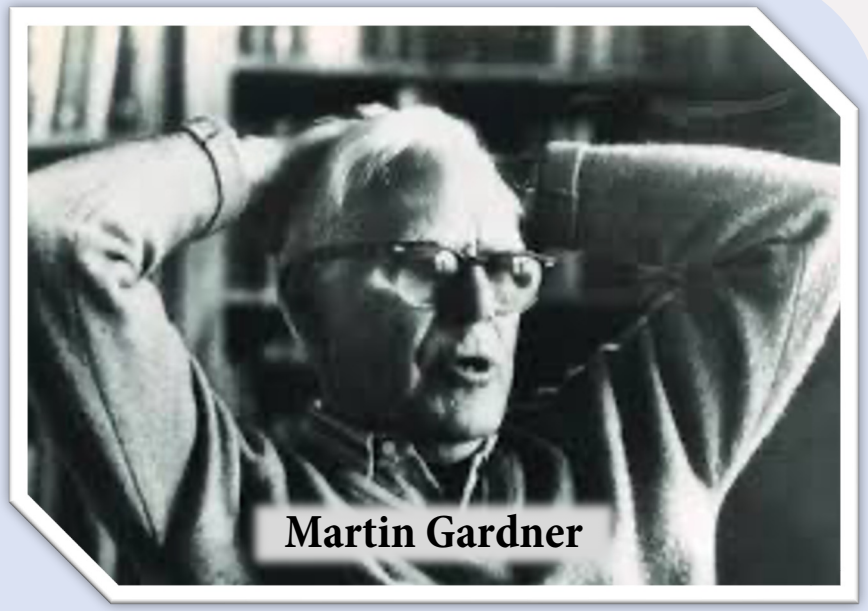
Hard Problem (example): It is believed that factoring N generated as product of two large primes is hard!

This is the basis for the widely used RSA encryption!

“A new kind of cipher that would take millions of years to break.”
-Scientific American about RSA, Aug 1977

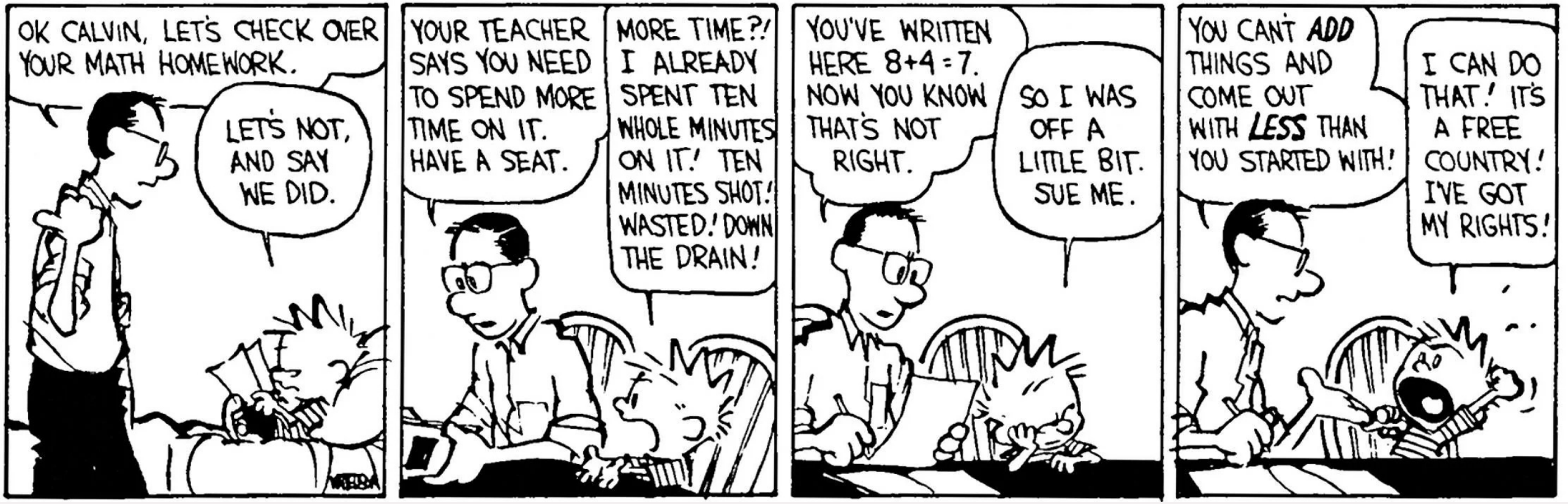
Gardner’s Challenge(1977): 129-digit number (prize: 100 $)

- N = 1 1438 1625 7578 8886 7669 2357 7997 6146 6120 1021 8296 7212 4236 2562 5618 4293 5706 9352 4573 3897 8305 9712 3563 9587 0505 8989 0751 4759 9290 0268 7954 3541


Martin Gardner

How many years did it take to get this 100$?

Took 17 years and 600 volunteers to factor this (26th April 1994) to get the deciphered message:
“the magic words are squeamish ossifrage”



THANK YOU

Video recommendations: numberphile (by Ron Rivest)