

# Intro to Modern Cryptography

- J. KATZ + Y. LINDELL

## POTS

FANTASTIC Q When is a problem Infosec one? [Ans] When the problem is impossible to solve logically / perfectly.

Will be shown with standard examples.

e.g.: Hashing password.

Theoretically impossible to be perfect if length is not infinite.

e.g.: Secure communication

$$\text{① } \text{to } \text{info}(R) = \text{info}(eve) \quad (S) \xrightarrow{\text{Enc}} (R)$$

$$\text{② } \text{to } \text{info-rec}(R) = \text{info-rec}(eve)$$

e.g.: Data integrity

If  $m$  was sent modified to  $m'$   $\rightarrow$  It is the same to receiver.  
and if  $m' \neq m$ ,  $L$  cannot thus identify.



OO Eg of non infosec  $\rightarrow$  Infosec

• problem in distributed computing  $\therefore$  now an infosec problem.

Solution: use signatures  $\Rightarrow$  implying signatures are impossible

FASCINATING Q. How to logically solve/circumvent a logical impossibility?

[Ans] Bring in another impossibility and make it destructively interfere with the original one.

We focus on 4-5 sources of impossibilities in the semester.

Course: See impossibilities

Introduce others

Solve them

1 per month approx.

### Sources of Impossibility.

① Computational Hardness [Resource Complexity]

Only happy  
cats are secure.

② Practical Uncertainties

Speed of light  
distance stuff

③ Natural Limits

④ Logical / Philosophical Impossibilities

### Random Words

- Hamming Distance

- Information security is God  
- all non-trivial works of  
science must include  
Info sec

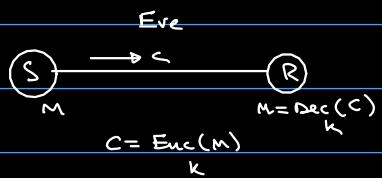
- logical norgo

Topics to cover

- Kerckhoff's Principle
- Designing/Breaking classical ciphers.

Starting off with secure communication networks.

- traditional ciphers, and how to break them.
- Shannon next class.
  - defined information
  - path breaking.

Caesar Cipher

$$c = (m + 3) \% n_c$$

$m$  = message  
 $c$  = coded message

$n_c$  = no. of characters in alphabet.

Big talk about his perspective of infosec as an 'art', and a bigger rant on what is art and what is science.

Exact words in book.

Kerckhoff's Principle

Security of a system must NOT depend on the OBSCURITY of the algorithm, rather must solely depend on the SECRECY of the KEY.

Kerckhoff's Reasons

1. Algorithms are reverse engineerable.

$$\text{eq: } h(x) = bx + c$$

Attacker can feed  $x_1, x_2, \dots, x_n$  and see that all outputs  $h(x_1), \dots, h(x_n)$  for  $g | h(x_i) - h(x_j)$ . And then solve for  $c$ .

2. Updation/ Recovery Complexity.

if passwd rarely in secure system: change pass.  
if algo " in obscurity " : // fixed .

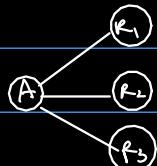
3. Secure Memory is costly.

ASK ACHIEV'A

Prob in modern times: UTM is algo and full input is key.

— bad information storage efficiency.

4. Scalable



Without: Diff algorithm for everyone.

With: only 'key' changes among people.

## Additional Reasoning

### 1. Ethical Hacking

hypothesis: no system is secure.

bug (algo) will be found because  $\square$

→ bug exists  
 → nonethical people exist  
 → only " " search for bug.  
 → " " will find "  
 → bug F, take that L

### 2. Standards

needed for efficiency.  
 if an algo is used by every system, it should obviously follow

Thus we can see why Caesar cipher fails.

Next iteration:

Shift Cipher:

$$c = (x+k) \bmod n_k$$

m = message

c = coded message

k = key

$n_c$  = no. of characters in alphabet.

Attack

1. Can be broken by humans

2. Autobreaking:

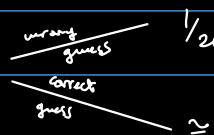
- frequency analysis

$$p_i = P(i^{\text{th}} \text{ char in m})$$

$$q_i = P(" " \rightarrow c)$$

Precompute  $\sum_{i=0}^{25} p_i^2 \approx 0.065$

Now compute  $\sum_{i=0}^{25} (p_i, q_{i+k})$



$$\approx 0.065$$

first principle learnt!

Principle of large key space

Next iteration:

Monoalphabetic Substitution Cipher

- Diff alphabets shift by different amounts.

- no repetitions allowed

- basically, permutation

applying first principle

for brute force:  $26!$  keys to search

Attack

$$\forall i \exists j : q_j \approx p_i$$

$\Rightarrow$  1. Sort  $q_i$ 's

2. Sort  $p_i$ 's

since distribution is same,

$$\text{eg: } P_a = Q_n, P_c = Q_t, P_t = Q_b$$

Issue: susceptible to frequency attacks.

Next iteration

### Vigenère Cipher

does not maintain frequency

e.g.:  $\begin{array}{c} \text{h e l l o} \\ \text{s e a s e} \\ \hline \text{z i l d} \end{array}$

#### FAILED ATTACKS

brute force: too many keys

freq anal: freq. not maintained

Can be broken if:

1. key length known

2.  $k$  " is findable.

#### Attack

##### PART 1:

if we know length of key,

e.g.: 3

$c_0 c_3 c_6 \dots$

partition ciphertext into  $((\text{length}))$  parts

$c_1 c_4 c_7 \dots$

then shift cipher attack on all  $((\text{length}))$  parts.

$c_2 c_5 c_8 \dots$

##### PART 2:

Guess an  $L$ .

take a string  $c_0 c_1 c_2 \dots$

$$\text{check if } \underbrace{\sum_{i=0}^{25} q_i^2}_{\text{easy}} = \underbrace{\sum_{i=0}^{25} p_i^2}_{\text{}}$$

easy

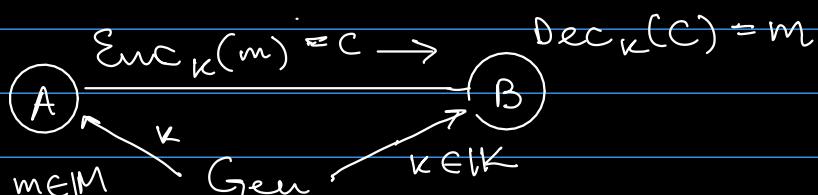
Topics for 10/01/2020

- Shannon's Perfect Secrecy
- Vernam Cipher is perfect (one-time pad)
- Limitations of Shannon's Approach

### \* Shannon's Perfect Secrecy

Definition of perfectly secure cipher.

An encryption scheme is a 4-tuple  
 $\langle \text{Gen}, \text{Enc}, \text{Dec}, \mathcal{M} \rangle$



$$\text{Dec}_K(\text{Enc}_K(m)) = m$$

Perfectly secret  
encryption  
scheme.

Schemes that meet this  
are largely impractical

An encryption scheme is said to be perfectly secret if for all probability distributions over  $\mathcal{M}$ , and for all  $m \in \mathcal{M}$ , for all  $c \in \mathcal{C}$  [where  $P(C = c) > 0$ ],

$$P[\text{Message} = m | \text{Ciphertext} = c] = P[\text{Message} = m]$$

We will prove one time pad is perfectly secret.

$$P[M = m | C = c] = P[M = m]$$

Random Variables

### Vernam Cipher

$$\mathcal{M} = \mathcal{K} = \mathcal{C} = \{0, 1\}^n \quad (\text{n-bit space})$$

$$\text{Gen : } K \xleftarrow{R} \{0, 1\}^n$$

$$\text{Enc : } C = m \oplus k$$

$$\text{Dec : } m = c \oplus k$$

- correctness is fairly obvious and not shown here.

$$\begin{aligned} a \oplus a &= 0 \\ m \oplus a \oplus a &= m \oplus 0 = m \\ \text{Dec}_k(\text{Enc}_k(m)) &= m \oplus k \oplus k = m \\ &\quad (\text{Proved}) \end{aligned}$$

### PROOF

First

Showing that definition of perfect security is equivalent to

$\forall p \in \mathcal{P}$  over  $\mathcal{M}$

$$\forall m \in \mathcal{M}, \forall c \in \mathcal{C}$$

$$P[C = c | M = m] = P[C = c]$$

have to do an iff.

Suppose this holds.

$$P[C = c | M = m] = P[C = c]$$

multiply both sides.

$$\frac{P[M = m]}{P[C = c]} \cdot P[C = c | M = m] = P[M = m]$$

$$\Rightarrow P[M = m | C = c] = P[M = m]$$

Workability  $\propto \frac{1}{\text{Intuitiveness}}$

### Second

Showing  $\forall c \in \mathcal{C}, \forall m_0, m_1 \in \mathcal{M}$  is eq to

$$P[C = c | M = m_1] = P[C = c | M = m_0]$$

2  $\rightarrow$  1 is trivial ( $P(C = c | M = m_1) = P(C = c), \text{LHS=RHS}$ )

$$P[C = c] = \sum_{m \in \mathcal{M}} P[C = c | M = m] P[M = m]$$

$$P$$

$$= P \sum_{m \in \mathcal{M}} P[M = m] = P$$

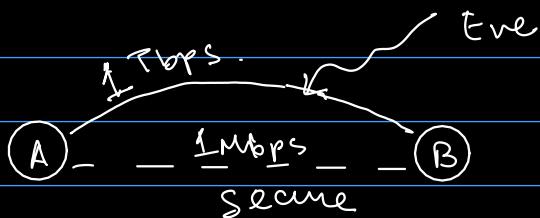
The above probability tells us that the encryption of  $m_0$  and  $m_1$  are indistinguishable.

For Vernam cipher:

$$\text{LHS} = P[C = c \mid M = m_0]$$

$$= P[C = m_0 \oplus k] = P[k = c \oplus m_0]$$

$$= \frac{1}{2^n} = \text{RHS} \quad (\text{P is not dependent on } m_0)$$

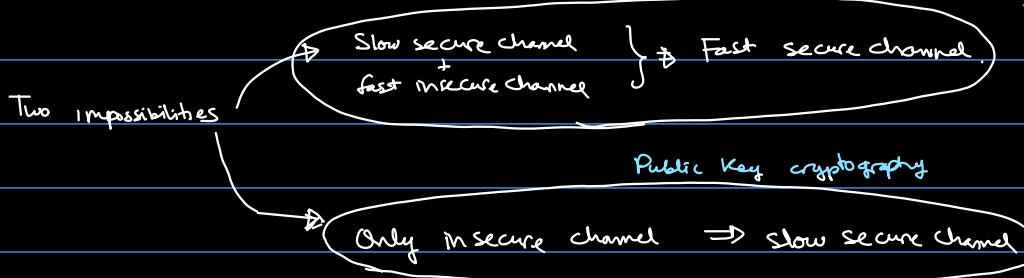


Uses of Vernam Cipher:

- i) To save your Shady business from the feds, encrypt the data and decrypt after raid.
- ii) Use secure channel on low load days to transfer keys and on high load days, use insecure channel by encrypting.

Now, bifurcation in the field.

Symmetric key cryptography.



Impossible if perfect security.

Both are impossible.

Now showing that limitations of Vernam cipher apply to any perfect cipher system as per Shannon's definition.

Universal  
Shannon theorem.

Thm: For any perfectly secret encryption scheme  $|K| \geq |M|$

Missing here:  
 $M$  is compressible.  
⇒ no. of bits required to store message is lower bound to no. of bits in key.

Shannon did:

$$H(|K|) \geq H(|M|)$$

We use a handy bypass to this.

ASK ATHREYA FOR INTUITION.

Proof :

Suppose not.

$$|\mathbb{K}| < |\mathbb{M}|$$

some ciphertext  $c$

$$\mathcal{D} = \{m \mid \exists k \in \mathbb{K} \text{ } \text{Dec}_k(c) = m\}$$

$$\text{now, } |\mathcal{D}| \leq |\mathbb{K}| \therefore < |\mathbb{M}|$$

$$\Rightarrow \exists m^* \in \mathbb{M} \text{ s.t. } m^* \notin \mathcal{D}$$

consider a dist where  $P(M=m^*) \neq 0$

$$\therefore P[M=m^* \mid C=c] = 0$$

but we said  $P(N=m^*) \neq 0$

$\Rightarrow$  Scheme is not perfectly secret

$\Rightarrow$  For perfectly secret scheme,  $|\mathbb{K}|$  must be at least  $|\mathbb{M}|$ .

$\therefore$  one-time pad not a one-off.

17.1.20

Oh no it's Chiranjeevi

Class on either 1. Finite Fields

2. Elliptic Curve.

Groups: (set, binary operation) satisfying axioms - closure      - Identity - associative    - Inverse	eg: $(\mathbb{Z}, +)$
--	-----------------------

for group  $G$ ,

if  $H \subset G$  and satisfies property,  $H$  is a subgroup of  $G$ .

Cyclic group if  $a \in G$ , and  $G = \{a^0, a^1, a^2, \dots\}$

eg. of  $(\mathbb{Z}_n, + n)$  groups

Next:

Ring, Integral Domain, Field.

Ring  $(R, +, \cdot)$  two binary operations on a set  $R$

a)  $(R, +)$  is a commutative group

b) Closure:  $a, b \in R \nmid a \cdot b \in R$

c) Associative:  $(a \cdot b) \cdot c = a \cdot (b \cdot c) \nmid a, b, c \in R$

d) Distributive laws:  $(a+b) \cdot c = a \cdot c + b \cdot c ; a \cdot (b+c) = a \cdot b + a \cdot c$

Ring need not be commutative with •

Commutative Ring is also " "

e.g. of ring:  $(\mathbb{Z}, +, \cdot)$  is a ring.

$(\mathbb{Q}, +, \cdot)$  " " "

Zero Divisors: For a ring  $R$ ,  $a, b$  s.t  $a(\neq 0) \in R$ ,  $\exists b \in R$ ,  $b \neq 0$ ,  $ab = 0$  or  $b.a = 0$

e.g.  $(\mathbb{Z}_n, +_n, \cdot_n)$

Integral Domain: A commutative ring with no zero divisors.

Division Ring: An integral domain s.t  $(R - \{0\}, \cdot)$  is a group.

Field:  $(F, +, \cdot)$

Finite field: Field where set  $F$  is finite.

a)  $(F, +)$  is commutative group

b)  $(F - \{0\}, \cdot)$  " " "

c) Distributive laws:  $(a+b).c = a.c + b.c$ ;  $a(b+c) = a.b + a.c$

Not a field:  $(\mathbb{Z}, +, \cdot)$ ,  $(\mathbb{Z}_n, +_n, \cdot_n)$  generally

field:  $(\mathbb{R}, +, \cdot)$ ,  $(\mathbb{Q}, +, \cdot)$ ,  $(\mathbb{Z}_n, +_n, \cdot_n)$  if  $n=p$ ,  $(\mathbb{Z}_n^*, +_n, \cdot_n)$

### Characteristic of Integral Domain (I)

least positive integer  $m$  s.t  $m.a = 0 \quad \forall a \in I$

If such  $m$  does not exist, characteristic of  $I$  is 0.

Lemma:

If  $(F, +, \cdot)$  is finite,  $\text{char } F = p$  (for some prime)

$\exists n \in \mathbb{N} \quad \nexists \text{ at least } 0, 1 \dots$  now  $1+1, 1+1+1, 1+1+1+\dots$

$$i \cdot 1 = j \cdot 1$$

$$(i-j) \cdot 1 = 0$$

$$n = i-j$$

Sums have to be repeated, as finite.

$n$  is prime • if  $n$  is not prime,  $n = ab$ . Now do we know  $a, b \in F$

$$(a \cdot b) \cdot 1 = 0$$

$$\Rightarrow (a \cdot 1)(b \cdot 1) = 0$$

$$\Rightarrow a \cdot b = 0$$

$(a, b, \text{ nonzero})$

$\Rightarrow$  one of  $a, b$  zero divisor

contradicting to definition

$\Rightarrow n$  is prime.

Now,  $(\mathbb{Z}_p, +_p, \cdot_p)$  is a field  $\text{char } = p$

if for any given  $F$ ,  $\text{char } F = p$ ,  $\mathbb{Z}_p (= \mathbb{Z}_{p, \mathbb{Z}}) \subset F$

- if  $(F, +, \cdot)$  is finite,  $\text{char } F = p$  (for some prime  $p$ )

Let  $(F, +, \cdot)$  be a finite field  $|F| = q$ , let  $F \subset K$  where  $K$  is also a finite field

then  $K$  has  $q^n$  elements where  $n$  is denoted  $K$  over  $F$

$\{v_1, v_2, \dots, v_n\}$  is a basis of  $K$  over  $F$

$a \in K, a = a_1v_1 + a_2v_2 + \dots + a_nv_n, a_i \in F$

$$|K| = q^n$$

$$(K, +, \cdot), \text{char } K = p$$

e.g.:  $(\mathbb{C}, +, \cdot)$  is a vector space over  $(\mathbb{R}, +, \cdot)$

$$|K| = p^n$$

given a prime, field with exactly those many elements

Read Herstein

## Elliptic Curves

Can be defined over finite fields  
 gives an abelian group.  
 multiple curves can be taken.

should not have multiple roots.

$$y^2 = x^3 + ax + b \quad \text{defined over } F$$

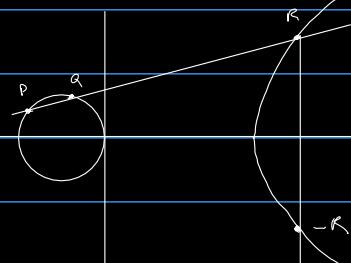
$p, a \quad l = \overline{pq}$

$l$  intersects this curve exactly at one more point

$$P+Q = -R$$

$$P+O = O+P$$

$$R-R=O$$



How this helps in crypto:

2 parties agree on:

1. Field  $F$

2. Eq. of elliptic curve

3. Random  $B$

Alice

Bob

$F, a, b, B$

private  
 $mB$

private  
 $nB$

$m(nB)$

$n(mB)$

published

shared key

## Review

1940s

→ Shannon's Perfect Secrecy  
and Pessimistic Result  
 $[P.S. \Rightarrow |K| \geq |M|]$

1970s- early 80s

- Two famous Relaxations

One Universal  
Assumption

Class focuses on Mid 70s - early 80s.

They noted that due to pessimistic result, they had to relax some fundamental assumptions, and hopefully they would be sufficient.

Current situation: The two necessary relaxations are almost sufficient, assuming "some yet undiscovered object exists"

In Perfect Secrecy

Adversary was unbound.

However, we know [adversary is computationally bounded] → First Relaxation.

Zero error

with finite passwords, one must necessarily work.

[Instead of zero error, "small negligible value of error"] → Second Relaxation

turns out, these 2 are almost sufficient: Security against

- computationally bounded adversary
- negligible error

Definition of efficiency / practicality: bounded by polynomial time

↳ helps model adversary as Probabilistic Polynomial Turing Machines (PPTM)

What is a  
"computationally bounded  
adversary"?

Security Parameter  $k$ 

Practical Adversaries: PPTM in Security Parameter

Note:

define  
"negligible error"

Negligible Function: A function  $\mu(n)$  is said to be negligible  $\xrightarrow{n \rightarrow \infty}$  if it is smaller than the universe of any polynomial for a sufficiently large  $n$ .

$$\left\{ \forall p() \quad \exists n_0 \text{ s.t. } \forall n \geq n_0, \mu(n) \leq \frac{1}{p(n)} \right\}$$

∴ Secrecy (Relaxed):  $\nexists$  PPTM Adversary;  $P[A \text{ can break } h] \leq \text{negl}()$

What exactly do we need to reasonable negligibility - and very few functions do not work.

Adversary trying to crack system will try multiple times. } probability grows polynomially.  
 ↳ will try polynomial no. of times. }  
 now,  $\frac{1}{\text{fixed no.}}$  will be surpassed in time.  
 We need  $\frac{1}{\text{polynomial limit + 1}}$  negligibility.

negligible means "smaller than the inverse of any polynomial".

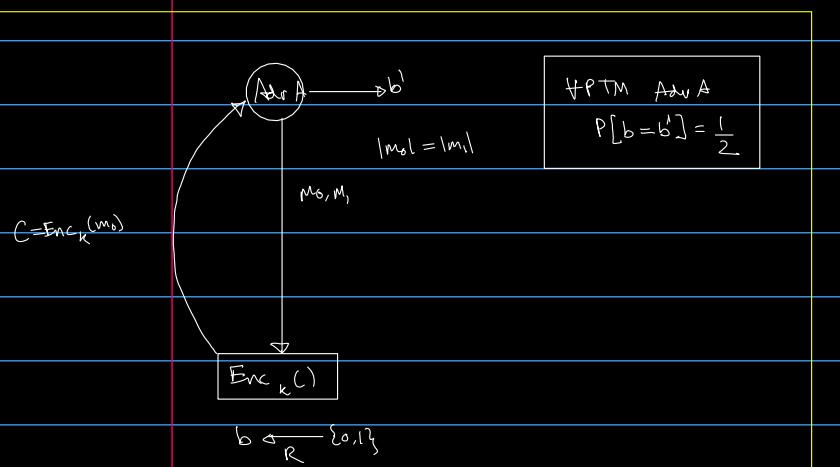
for example exponential growth

$\nexists p()$ ,  $\exists n_0$  s.t.  $\forall n \geq n_0$

$$\frac{1}{2^n} \leq \frac{1}{p(n)}$$

} future proofs, in the sense:

- with increased computation (polynomial bound), we keep the algorithm, increase security parameter  $n$  only.



Bottleneck: no known encryption scheme is known to meet this definition.

↗

Apart from these 2 relaxations, if

exists, it is possible.

- pseudorandom generator
- collision resistant hashing
- one way hash functions exist

All are the same mathematical objects. One way functions.

Does this exist? No fun due there is a faster.

Field, at this point, trifurcated.

① Heuristic Security.

(Secure because we have assumed it is)

e.g.: 1960s - mid 1990s was DES

late 1990s - current is AES

} focusing least attention to this.

because

- heuristics are prone to obsolescence
- no answer for security

③ Proven Security  $\rightarrow \emptyset$  | taught when it exists

② Provable Security

We will give a conditional proof.

Definition of One-Way Function

A function  $f: \{0,1\}^* \rightarrow \{0,1\}^*$  is said to be one way if : (easy to compute, hard to invert)

a) Easy to compute,  $x \rightarrow f(x)$ , polynomial time.

b) Hard to invert :  $\nexists \text{ PPTM } A$

$$P[A(f(x)) = y \mid f(x) = f(y)] \leq \text{negl}(|x|)$$

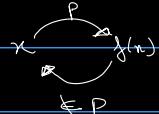
$P(\text{successfully inverting function})$  is negligible in previously defined terms.

Trio of impossibility results: Two famous relations + one way functions exist.

Not too sure  
on topic heading.  
Ask someone.

Now, demonstrating that proving that one way functions exist is at least NP-hard.

One Way functions:



NP, complexity theory

proving that reverse process has to be NP,

$L \in NP$  if- L has an efficient verifier

decider: given  $x, x \in L$ ?

Verifier: given proof, we can verify it.

if  $x \in L$ ,  $\exists$  at least 1  $v$  which works

A verifier  $V$  is said to verify  $L$  if

$$L = \{x \mid \exists v, V(x, v) = \text{accepts}\}$$

Now,

if  $\exists$  p(t) NDTM,  $\exists$  efficient verifier ??? ASK ATREUS

Reverse process has efficient verifier

as it must be NP

TODAY

- Pseudo-randomness
- An encryption scheme
- Discrete Log Problem

24.01.2020

### Discrete Logarithm Problem (DLP)

Given the group  $\mathbb{Z}_p^*$  and its generator  $g$ , and  $y = g^x$ . Find  $x$ .

There are no known algorithms that can solve this in polynomial time.

conjecture: this is a one-way function

Concept of one-time pads using computational entropy.

### Pseudo-Random number generator

An efficient deterministic code  $G$ , that inputs  $n$ -bit string and outputs  $\lambda(n)$ -bit string is a PRG if

a) Expansion:  $\lambda(n) > n$

b) Pseudo-randomness:  $\forall \text{ PPTM distinguisher } D$  (that try to distinguish pseudo-randomness from randomness)

$$P[D(G(u_n)) = 1] - P[D(u_n) = 1] \leq \text{negl}(n)$$

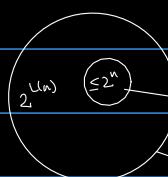
exist if one-way functions exist.

$G$  is a PRG if no efficient distinguisher can distinguish between a uniformly distributed random no. of length  $\lambda(n)$  and a expanded number from a smaller key of length  $n$



Use case: send key k over slow secure channel.

Have  $G$  on both sides to get key of sufficient length to allow practical usage of one-time pad.



Even if every seed is expanded to be unique, hard cap.

world of pseudorandom seed  
world of full length key.

ratio is tiny

to make the claim of indistinguishability is a tall ask.

e.g.: a distinguisher can ask for  $2^n + 1$  samples  $P(\text{collision}) = 1$

Distinguishers definitely exist, but polynomial time unknown.

this is not polynomial time.

(Idea: Any test created by any polynomial time distinguisher will be passed by both.)

Proof:  $\text{PRGs} \Rightarrow \text{one way function}$ .

$$G(s) = y \quad (\text{intuitive implication})$$

Proof: One way function  $\Rightarrow \text{PRG}$ .

$$p = \text{prime}$$

$$\{1, 2, \dots, p-1\} \quad g \text{ is generator of } \mathbb{Z}_p^* \text{ if } \\ \xrightarrow{\text{iff}} \{g^0, g^1, g^2, \dots, g^{p-1}\}$$

Discrete log problem

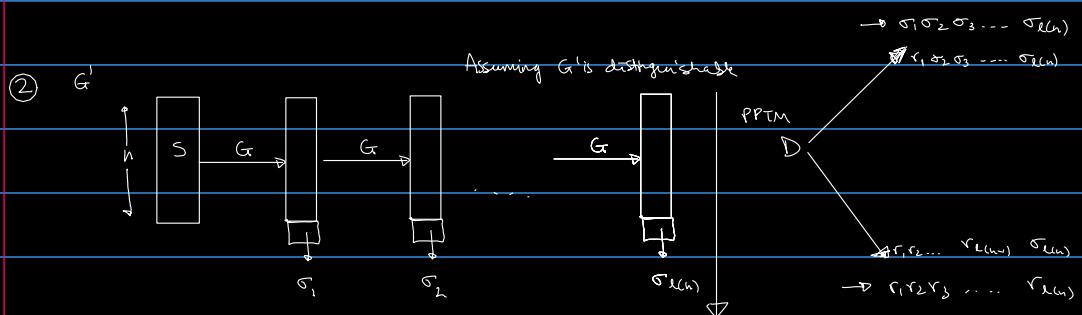
Given the group  $\mathbb{Z}_p^*$  and generator  $g$ ,  $y = g^n \bmod p$ , find  $n$ .

No efficient algorithm.

$$\begin{array}{c}
 f: \{0,1\}^n \longrightarrow \{0,1\}^n \\
 \xrightarrow{\text{PRG } G} \\
 \hline
 \text{①} \quad G: \{0,1\}^n \xrightarrow{\text{n-bit seed as input}} \{0,1\}^{n+1} \\
 \qquad \qquad \qquad \xrightarrow{\text{(n+1)-bit seed as output}}
 \end{array}$$

$\text{DLP} \Rightarrow G$

- Proof that
1. If I have length-preserving one-way function, I can make a PRG  $G$  that can expand its seed by 1 bit.
  2. If I have PRG  $G$  that can expand its seed by 1 bit, I can have PRG  $G'$  that can expand its seed by an arbitrary length.



PROOF THAT  $G'$  IS PRG

If  $G$  is PRG.

If  $D$  can distinguish 1st from last,

$\exists i$  st  $i^{\text{th}}$  row and  $(i+1)^{\text{th}}$  row is distinguished.

$\Rightarrow D$  has power to distinguish  $\sigma_i, r_i$

$\Rightarrow D$  ... one of the  $G$ s.

but None can be , contradiction.

$\therefore$  if  $G$  is PRG,  $G'$  is also PRG.

PROOF that if one-way functions exist, single bit expanding PRGs exist.

$$\textcircled{1} \quad G(s) = f(s) \parallel h(s)$$

length-preserving  
PRG  
trivial enough with  
one-way function

looking at first  $n$ -bits, no polynomial function should be able to predict next  $n+1$  bits with  $\leq \frac{1}{2} + \text{negl}(n)$  probability.

given  $s$ , easy to compute  $h(s)$

$$h(s) \quad \text{given } f(s), P[A(f(s)) = h(s)] \leq \frac{1}{2} + \text{negl}(n)$$

$$h: \{0,1\}^n \rightarrow \{0,1\}$$

hard-core predicates of  $f(\cdot)$

now, looking directly at DLP:

$$f(x) = g^x \bmod p$$

$$\text{then } h(x) = \text{MSB}(x)$$

DLP: given  $g^x \bmod p$

what is  $x$

DLP(MSB): given  $g^x \bmod p$

what is MSB( $x$ )

$$[x \geq \frac{p-1}{2}]$$

polynomial

Now, we will show that if there is polynomial time algorithm for DLP(MSB) will also lead to a " " " DLP, which is already discounted.

\textcircled{1} DLP<sub>L</sub>: Given  $g^x \bmod p$ , what is the LSB( $x$ )?

DPL<sub>L</sub>  $\in P$

\textcircled{2} DPL<sub>L</sub> + DLP<sub>M</sub>  $\Rightarrow$  DLP.

$$\text{Let } y = g^x \bmod p$$

Fermat's Little Theorem implies that

$$y^{p-1} \equiv 1 \pmod{p}$$

F.L.T

$a^{p-1} \equiv 1 \pmod{p}$   
 if  $\text{GCD}(a,p) = 1$

$$\therefore (g^x)^{p-1} \pmod{p} \geq 1$$

$$\text{Find } y^{\frac{p-1}{2}} \pmod{p} = g^{x \cdot \frac{(p-1)}{2}} \pmod{p}$$

$$\begin{cases} x \text{ is even} \\ x \text{ is odd} \end{cases}$$

$$g^{\frac{p-1}{2}} \pmod{p} \equiv 1 \quad \text{if } x \text{ is even}$$

$$\text{we know that } g^{\frac{p-1}{2}} \pmod{p} \equiv 1$$

$$\text{But } g^{\frac{p-1}{2}} \pmod{p} \equiv +1 \text{ or } -1$$

now we know it cannot be 1, it has to be -1.

$$g^x \bmod p$$

$x \text{ is even} \quad \swarrow \quad \searrow \quad x \text{ is odd}$

$\pm g^{\frac{x}{2}} \bmod p \quad g^{\frac{x+1}{2}} \bmod p.$

This won't tell me which was the original  $x$  unless I know

(SQR)  $\rightarrow g^{\frac{x}{2}} \bmod p, g^{\frac{x+1}{2}} \bmod p.$  }  $\boxed{\text{if } x > p^{-1}/2}$   
 which was our problem for DLP.

$p \equiv 3 \pmod{4}$

Given  $x$  find  $\sum \text{st } z^2 \pmod{p} = x.$

$$z^2 = x^{\frac{p+1}{2}} \bmod p$$

$$z^2 = x^{\frac{p-1}{2}} \bmod p$$

$$\Rightarrow x^{\frac{p-1+2}{2}} \bmod p$$

$$= \cancel{x^{\frac{p-1}{2}} \cdot x} \bmod p$$

because  $x \in \mathbb{Q} \setminus \mathbb{Z}$   $x^2 = x \Rightarrow$

$$\Rightarrow x^{\frac{p-1}{2}} \bmod p \\ = x^{\frac{p-1}{2}} \bmod p \\ = 1 \pmod{p}$$

So if  $p = 7$

$$\sqrt{2} = 2^{\frac{7+1}{4}} = 4$$