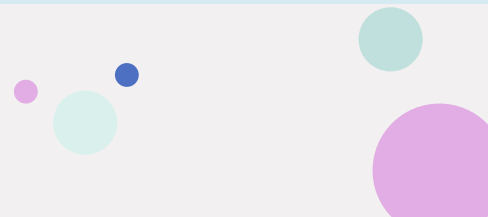




Lecture 13

One Way Functions, Hard-core Predicates, Goldreich-Levin

CS409: Introduction to Cryptography
Sruthi Sekar



WANTED

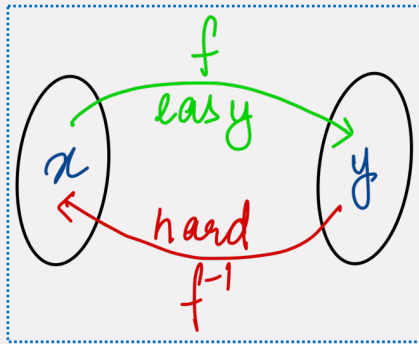
**Give me a simple construction of an EU-CMA secure MAC
just using a weak-PRF and nothing else!**
($\because$ GGM-based solution in solution sketch is an indirect way)

REWARD: Rs. 1000/- worth Zomato coupon!



Today

One-Way Functions (OWF) and Permutations (OWP)

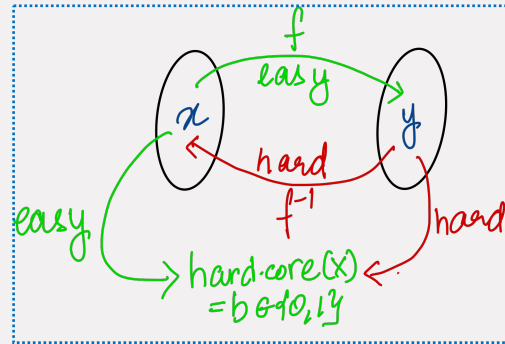


Define it



Build it

Hard-core Predicate (HCP)



Define it

Goldreich-Levin
Hard-Core Predicate

Build it

HCP for OWP

hardness



pseudorandomness

Pseudorandom
Generators

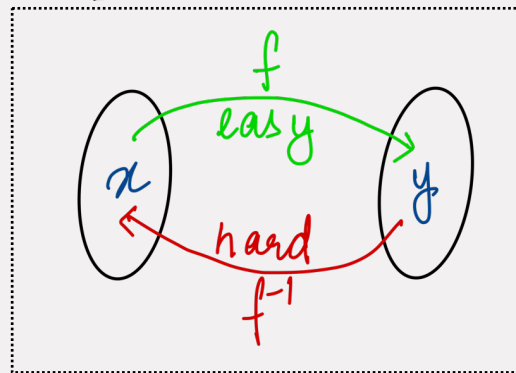
One-way Functions



INTUITIVELY

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

Sudoku solution



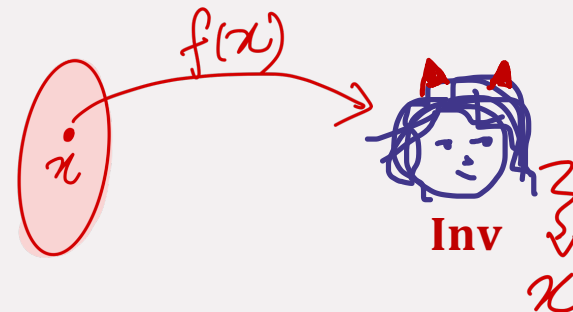
5	3			7				
6				1	9	5		
	9	8					6	
8				6				3
4			8		3			1
7				2				6
	6					2	8	
			4	1	9			5
				8			7	9

Sudoku puzzle

Attempt I at formally defining this:

$\forall$ PPT **Inv** and $\forall x, \exists \text{negl s.t.}$

$$\Pr[\mathbf{Inv}(f(x)) = x] \leq \text{negl}$$



Problem: Too much asking (*everywhere hardness*)

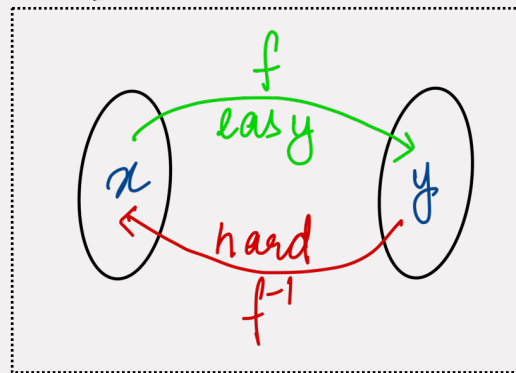
One-way Functions



INTUITIVELY

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

Sudoku solution



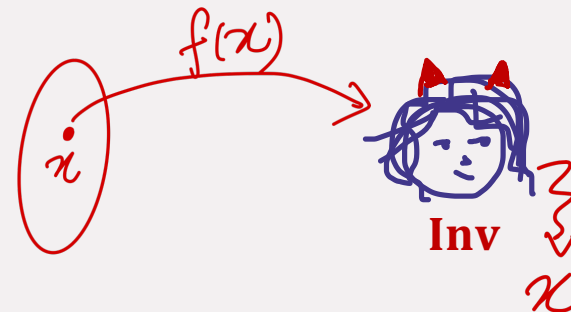
5	3			7				
6				1	9	5		
	9	8					6	
8				6				3
4			8		3			1
7				2				6
	6					2	8	
			4	1	9			5
				8			7	9

Sudoku puzzle

Attempt II at formally defining this:

$\forall$ PPT **Inv**, $\exists x, \exists \text{negl}$ s.t.

$\Pr[\mathbf{Inv}(f(x)) = x] \leq \text{negl}$



Problem: Too little asking (*worst-case hardness*)

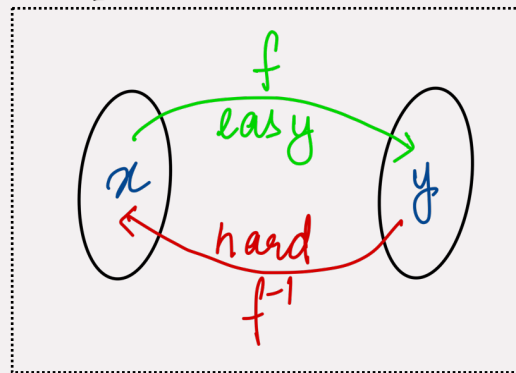
One-way Functions



INTUITIVELY

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

Sudoku solution



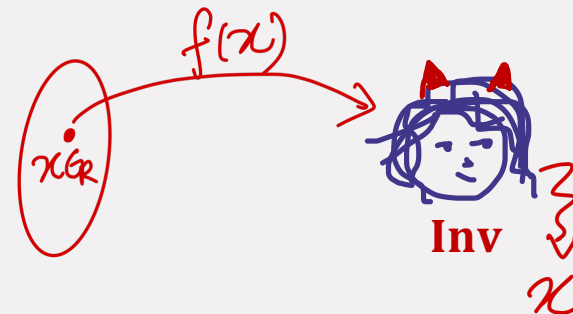
5	3		7			
6			1	9	5	
	9	8				6
8			6			3
4			8	3		1
7			2			6
	6				2	8
			4	1	9	5
			8		7	9

Sudoku puzzle

Attempt III at formally defining this:

$\forall$ PPT **Inv**, $\exists$ negl s.t.

$$\Pr_{x \in_R \{0,1\}^n} [\mathbf{Inv}(f(x)) = x] \leq \text{negl}(n)$$



Problem: Consider $f(x) = 0^{|x|}$ (what is the problem?)

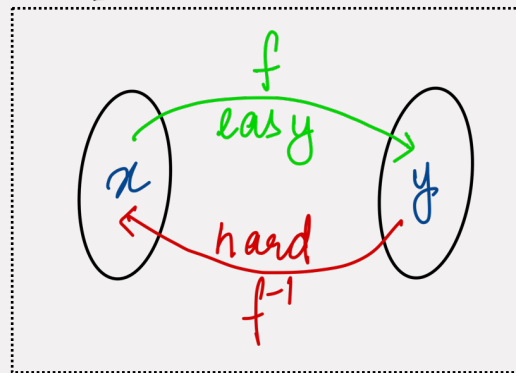
One-way Functions



INTUITIVELY

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

Sudoku solution



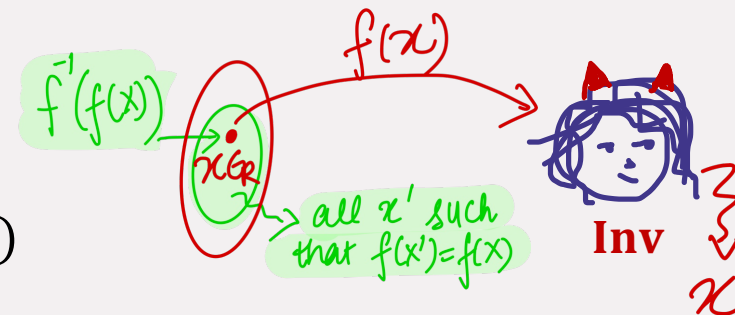
5	3			7				
6				1	9	5		
	9	8					6	
8				6				3
4			8		3			1
7				2				6
	6					2	8	
			4	1	9			5
				8			7	9

Sudoku puzzle

Attempt IV at formally defining this:

$\forall$ PPT **Inv**, $\exists$ negl s.t.

$$\Pr_{x \in_R \{0,1\}^n} [\mathbf{Inv}(f(x)) \in f^{-1}(f(x))] \leq \text{negl}(n)$$



Single function vs family of functions: Easier to build parametrized family of OWFs!

One-way Functions

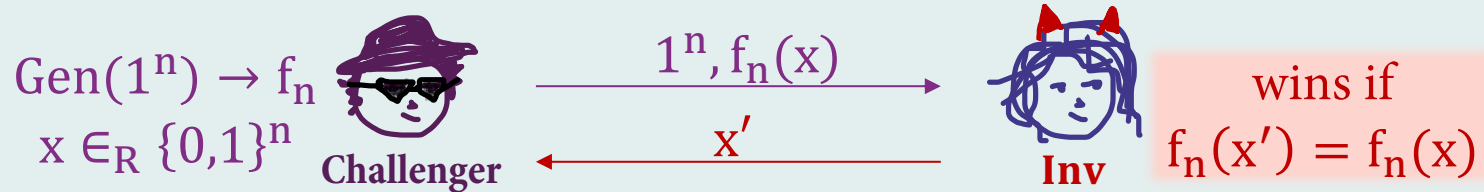
Definition 1 (One-way Function Family)

$$\{f_n: \{0,1\}^n \rightarrow \{0,1\}^{m(n)}\}_{n \in \mathbb{N}}$$

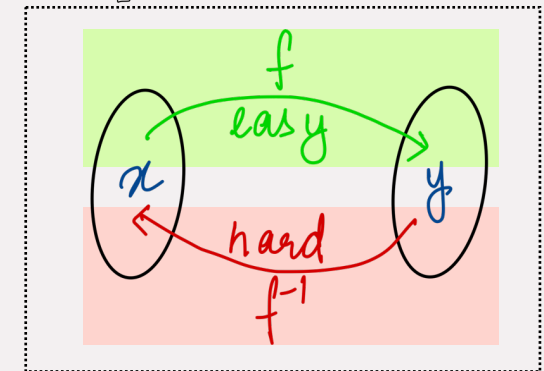
$$\text{Gen}(1^n) \rightarrow f_n$$

- $\exists$ an efficient deterministic algorithm f such that $\forall x, f(n, x) = f_n(x)$
- $\forall$ PPT **Inv**, $\exists$ negl s.t. $\forall n$

$$\Pr_{x \in_R \{0,1\}^n} [\text{Inv}(1^n, f_n(x)) \in f_n^{-1}(f_n(x))] \leq \text{negl}(n)$$



INTUITIVELY



- **Length-preserving OWF**: $m(n) = n$
- **One-way permutation Family**: for each $f_n \leftarrow \text{Gen}(1^n)$, f_n is length-preserving and bijective.

Quiz Time

OWF or not?

✓ $f_1(x) := f(x) || 0^{|x|}$, where f is a OWF

✓ $f_3(x) := G(x)$, where G is a PRG

? $f_2(x_1 || x_2) := x_1 || f(x_1 || x_2)$, where f is a OWF

HW 2: Prove security of f_1
and f_3 via a reduction!

HW 1:
Come up with an example of f such that
1. f_2 is one-way and 2. f_2 is invertible.

Quiz Time

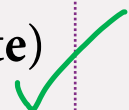
OWF Family or not?

$f_{a,p}(x) := ax \bmod p$, where $a, x \in \mathbb{Z}_p^*$ and p is a prime. (Multiplication mod prime) 

$f_p(x) := x^2 \bmod p$, where $x \in \mathbb{Z}_p^*$ and p is a prime. (Squaring mod prime) 

$f_{p,g}(x) := g^x \bmod p$, where $x \in \mathbb{Z}_{p-1}$, $\mathbb{Z}_p^* = \langle g \rangle$, p is a prime. (Exponentiation mod prime) 

(If Dlog Assumption holds (in $\mathbb{Z}_p^*$ it is believed to hold) then $\{f_{p,g}\}$ is a OWF family)

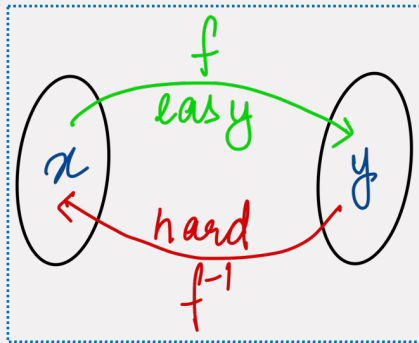
$f_N(x) := x^2 \bmod N$, where $x \in \mathbb{Z}_N^*$ and $N = pq$ (large primes p and q). (Squaring mod composite) 

(If factoring N is hard (factoring assumption), then $\{f_N\}$ is a OWF family)

HW 3: Show that taking square root mod N
is equivalent to factoring N
(Hint: $x^2 - y^2 = (x + y)(x - y) \bmod N$)

Today

One-Way Functions (OWF) and Permutations (OWP)

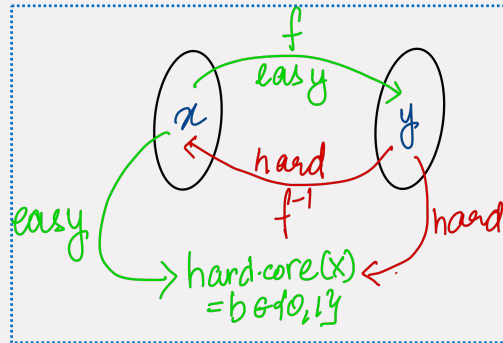


Define it



Build it

Hard-core Predicate (HCP)



Define it

Goldreich-Levin
Hard-Core Predicate

Build it

HCP for OWP

hardness



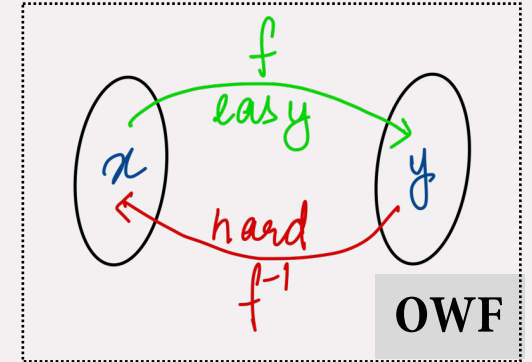
pseudorandomness

Pseudorandom
Generators

Hard-Core Bit

One-way function/permutation

Alternate view: x cannot be computed **in its entirety** by any efficient algorithm (except with negligible probability)



Is it possible that f leaks a lot of information about x , even if it is one way?

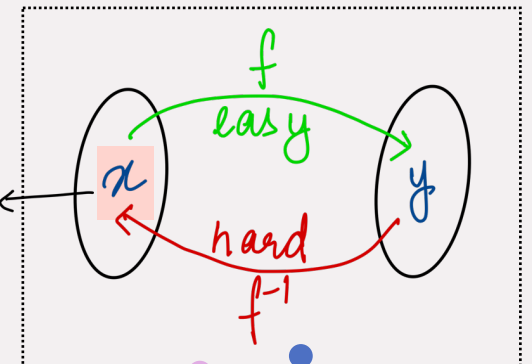
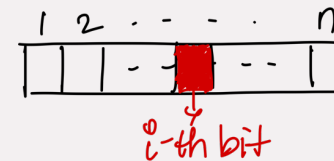
Yes! (f is a OWF (prove it) but reveals half its input!)

$f(x_1 || x_2) := x_1 || g(x_2)$, where g is a OWF and $|x_1| = |x_2|$

In general, can we identify what about x is hidden by a OWF f ?

ATTEMPT I

i -th bit is hardcore if
 x_i is hard to predict, given $f(x)$

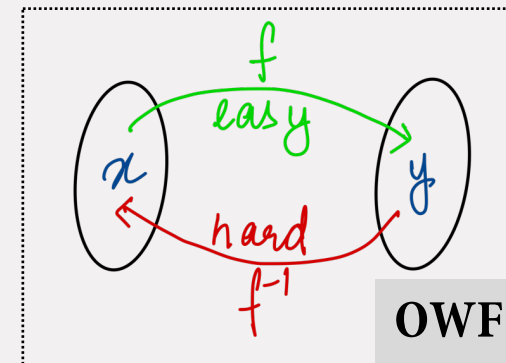


(HW 4) Problem: $\exists$ OWFs for which every input bit is “easy” to predict!

Hard-Core Predicates (HCP)

One-way function/permutation

Alternate view: x cannot be computed **in its entirety** by any efficient algorithm (except with negligible probability)



Is it possible that f leaks a lot of information about x , even if it is one way? **Yes!**

In general, can we identify what about x is hidden by a OWF f ?

Hard-core predicate

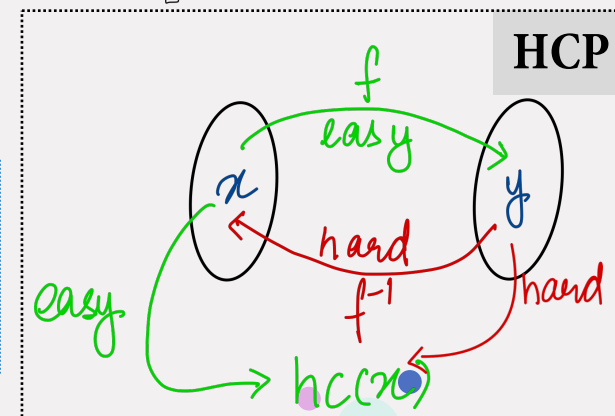
$hc: \{0,1\}^* \rightarrow \{0,1\}$ of a function f is such that:

$hc(x)$ easy to compute given x

$hc(x)$ is hard to compute given $f(x)$



INTUITIVELY



Hard-Core Predicates (HCP)

Definition 2 (Hard-core predicate of a function family)

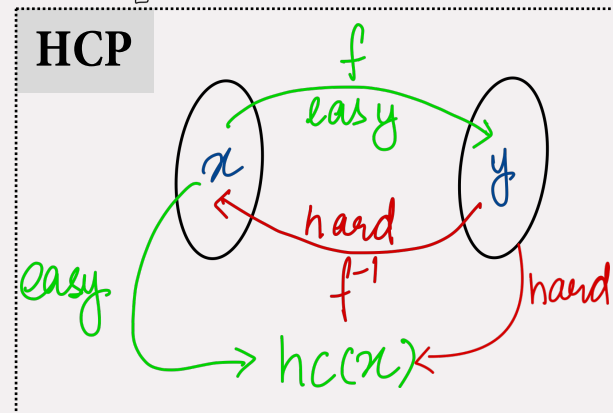
$$\{f_n: \{0,1\}^n \rightarrow \{0,1\}^{m(n)}\}_{n \in \mathbb{N}}$$

A predicate $hc: \{0,1\}^n \rightarrow \{0,1\}$ is a **hard-core predicate** for the above function family if for every **PPT** predictor **Pred**, $\exists \text{negl}$ such that $\forall n$

$$\Pr_{x \in_R \{0,1\}^n} [\mathbf{Pred}(1^n, f_n(x)) = hc(x)] \leq \frac{1}{2} + \text{negl}(n)$$



INTUITIVELY



SOME IDEAS FOR HCP:

$hc(x) \stackrel{\text{def}}{=} \bigoplus_{i=1}^n x_i$ Is it hard-core for every one-way function?

No! Consider $f(x) \stackrel{\text{def}}{=} (g(x), \bigoplus_{i=1}^n x_i)$, where g is a OWF



In fact, for any fixed hc , $\exists$ OWF f for which hc is not an HCP of f

Trivial HCP: Consider $f(x) = 0^n$ then x_i is hard-core $\forall i$
But, f is not a OWF!

This kind of HCP from “information loss” is useless for us

Goldreich-Levin HCP

Given any one-way function, can we find a deterministic hard-core predicate for it?

We don't know, it remains open!

Something
weaker

Goldreich-Levin Theorem

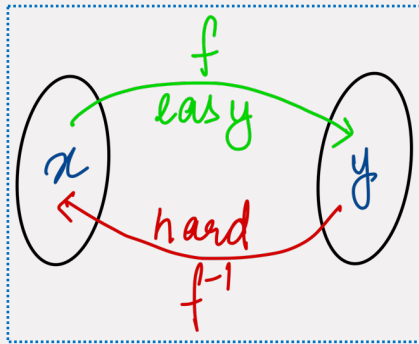
For every one-way function f , $\exists$ a related one-way function $g(x, r) \stackrel{\text{def}}{=} (f(x), r)$ for $|x| = |r| = n$ with a deterministic hard-core predicate $hc: \{0,1\}^{2n} \rightarrow \{0,1\}$ defined as

$$hc(x, r) = \bigoplus_{i=1}^n x_i \cdot r_i$$

****If interested in proof, refer to Katz and Lindell! We will skip it in this course!**

Today

One-Way Functions (OWF) and Permutations (OWP)

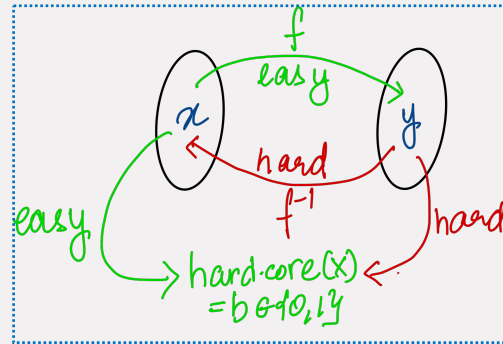


Define it



Build it

Hard-core Predicate (HCP)



Define it

Goldreich-Levin
Hard-Core Predicate

Build it

HCP for OWP

hardness



pseudorandomness

Pseudorandom
Generators

OWP $\Rightarrow$ PRG

Theorem: OWP with HCP gives a PRG

Let $f: \{0,1\}^n \rightarrow \{0,1\}^n$ be a one-way permutation, and let hc be a hard-core predicate of f .
Then, $G(s) \stackrel{\text{def}}{=} f(s) || hc(s)$ is a pseudorandom generator with expansion factor $n + 1$

Proof Sketch: $\exists \text{Pred}^G$ against $G \Rightarrow \exists \text{Pred}^{hc}$ against the hard-core predicate hc of f

$s \in_R \{0,1\}^n$

$f(s) = y_1 || y_2 || \dots || y_n$

?

Pred^{hc}

Pred^G

i

$y_1 y_2 \dots y_i$

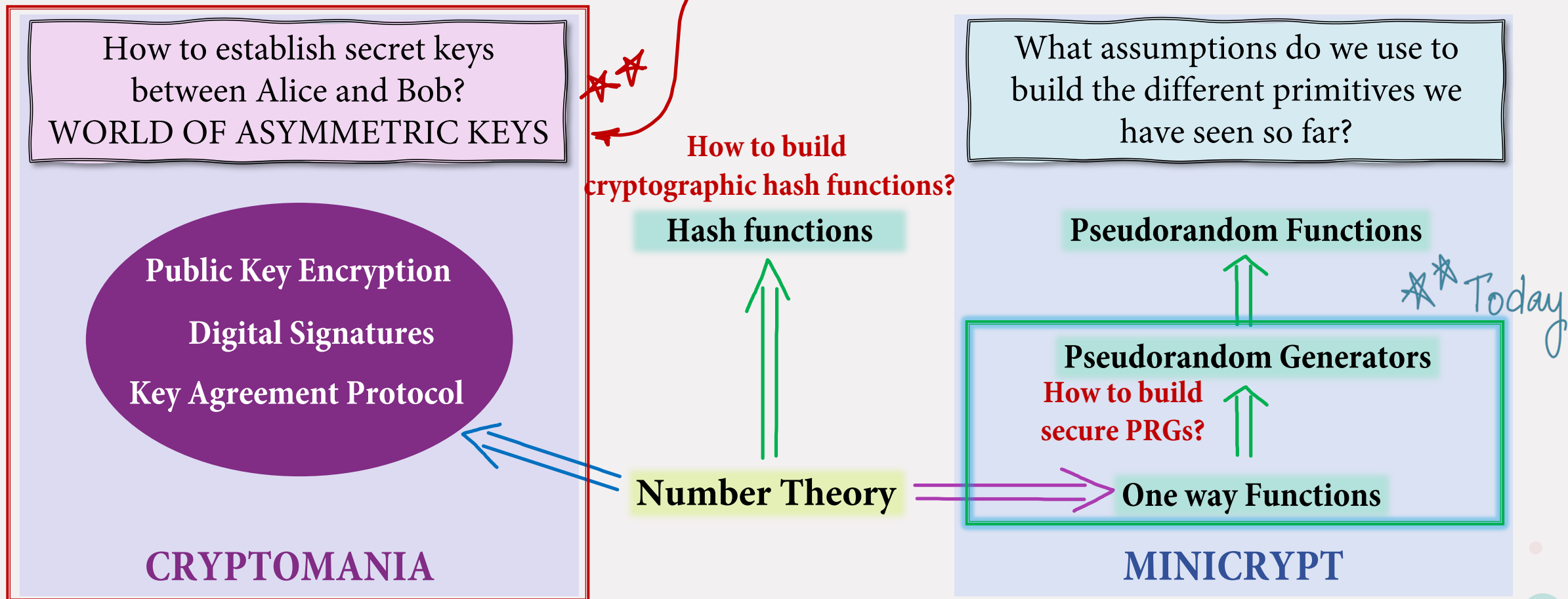
b

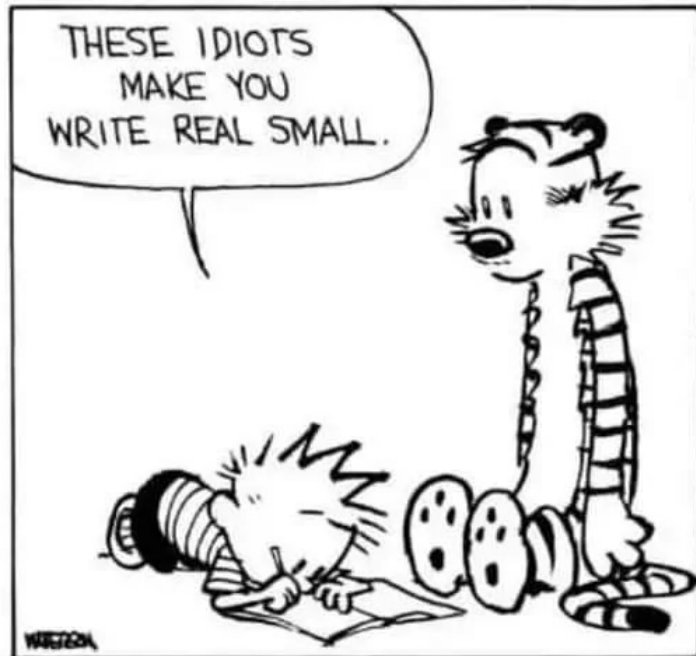
Predicts y_{i+1} w.p.
 $> 1/2 + \text{non-negl}$

1. Pred^G is useful only if $i = n$.
2. Pred^G has no advantage in predicting $y_1 || y_2 || \dots || y_n$ (f permutation $\Rightarrow$ output random)

****OWF $\Rightarrow$ PRG, but the proof is harder!**

Next Week





THANK
YOU