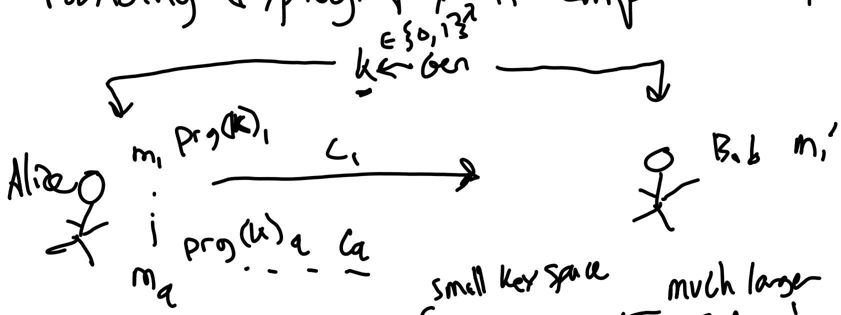
Pseudorandomness

Monday, August 30, 2021 3:58 PM

Founding Cryptography on Computational assumptions



small key space

much larger codomain.

pseudorandomness $prg : K \to K^q$

"Considered to be random, as long as you don't know the seed."

$PRG : K \to C$

"without the seed, output of PRG indistinguishable from truly random samples"

$$\forall \mathcal{A}. \left\| \Pr\begin{bmatrix} \text{real} \\ k \xleftarrow{\$} K \\ x \leftarrow prg(k) \\ b \leftarrow \mathcal{A}(x) \\ \hline b=0 \end{bmatrix} - \Pr\begin{bmatrix} \text{random} \\ x \xleftarrow{\$} C \\ b \leftarrow \mathcal{A}(x) \\ \hline b=0 \end{bmatrix} \right\| \le negl(\lambda)$$

any adversary

any PPT

Problems thought to be hard

- Prime factorization

think $\nexists$ an algorithm $prog(n)$ that outputs prime factorization for any n and takes #steps $\le p(|n|)$ for some polynomial p.

- Satisfiability for circuits, circuit w/ #n inputs

- hamiltonian - knapsack. - tsp.

- distinguishing PRGs

- one way functions

given $f: D \to C$

$$\forall \mathcal{A}. \Pr\left[\begin{array}{c} x \xleftarrow{\$} D \\ y \leftarrow f(x) \\ x' \leftarrow \mathcal{A}(y) \\ \hline f(x') = y \end{array}\right] \leq negl(\lambda)$$

PPT: $\underbrace{\text{polynomial time}}_{\lambda \text{ security}}$ probabilistic TM.

$M(1^\lambda, \ldots; z)$ terminates in $poly(\lambda)$ steps.

- Negligible

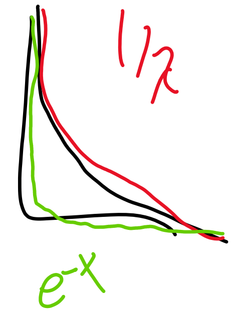
"function that gets smaller faster than any polynomial $\left(\frac{1}{p(x)} \text{ for any poly } p(x)\right)$"

- $f(\lambda)$ is $negl(\lambda)$ if

$$\forall \text{ poly } p(\lambda), \quad \lim_{\lambda \to \infty} p(\lambda) f(\lambda) = 0$$

ex. $f(\lambda) = 0$ ✓ $f(\lambda) = 1$ ✗

$f(\lambda) = \frac{1}{\lambda^2}$ m, $p(\lambda) = \lambda^{?}$ $p(\lambda) \cdot f(\lambda) = \lambda$ ✓



$$f(\lambda) = \frac{1}{2^{\sqrt{\lambda}}}$$

For next time $f(\lambda) = e^{-\lambda}$

"let c be the degree of $p(\lambda)$"