Reminder

• Problem set 1 reminder due this Wed

• Need to solve problem 2.6 part b (from Katz-Lindell) book, as well.
Last time

• Defining encryption formally
• Information theoretic (perfect) vs. computational secrecy
• Limitation of perfect secrecy (and even its relaxations)

Today

• Secrecy based on (unproven) computational assumptions
• Pseudorandom generators (and functions)
Computational Privacy/Security

A scheme is \((t, \varepsilon)-secure\) if every adversary running for time \(t\) succeeds in breaking the scheme with probability at most \(\varepsilon\).

- What it means to “break” depends on the exact security def.

- Ideal: \(t > \text{“feasible computation”}\) and \(\varepsilon < \text{“negligible probability”}\)

  \[ t(n) \leq n^c \quad \text{for some constant } c \]

  \[ \varepsilon(n) \leq \frac{1}{n^c}, \text{ if } n \text{ is large enough.} \]

- Example: \(t = 2^{100}\) \(\varepsilon = 2^{-100}\) (age of universe \(\approx 2^{80}\) seconds)
Examples

- NP-Complete / hard:
  - Boolean SAT problem.

TSP:
- Input: weighted graph
- Run-time: $2^n$
- Easy.

Conjecture: There is no poly-time alg for TSP.

Some constant:
- $O(1)$
- $100$

Find a tour that goes to all nodes using minimal distance total.

Quick run-time: $O(n \log n)$

Feasible

Poly-time.

Input size

Conjecture: There is no poly-time alg for TSP.

Large prime numbers (into prime factors)
Computational Indistinguishability Secrecy

- Eve (eavesdropping) security: Even if Eve knows \( m \in \{m_0, m_1\} \) she cannot guess \( m \) in time \( t(n) \) with probability greater than \( \frac{1 + \varepsilon(n)}{2} \).}

\( t(n) \), \( \varepsilon(n) \) are functions of “security parameter” \( n \) (e.g. key length \( n = 1000 \))
“Efficient” time and “Negligible” probability...

• Efficient: polynomial time over input length

\[ t(n) \leq \text{poly}(n) \]

\[ \exists c, \forall n, t(n) \leq n^c \]

• Negligible: smaller than any inverse polynomial (over input length)

\[ \forall c, \exists n_0, e(n) \leq \frac{1}{n^c} \text{ if } n \text{ is large enough.} \]
Formal definitions of security

The adversarial indistinguishability experiment $\text{PrivK}^{\text{eav}}_{A,\Pi}(n)$:

1. The adversary $A$ is given input $1^n$, and outputs a pair of messages $m_0, m_1$ of the same length.
2. A random key $k$ is generated by running $\text{Gen}(1^n)$, and a random bit $b \leftarrow \{0,1\}$ is chosen. The ciphertext $c \leftarrow \text{Enc}_k(m_b)$ is computed and given to $A$.
3. $A$ outputs a bit $b'$.
4. The output of the experiment is defined to be 1 if $b' = b$, and 0 otherwise. If $\text{PrivK}^{\text{eav}}_{A,\Pi}(n) = 1$, we say that $A$ succeeded.

**DEFINITION 3.9** A private key encryption scheme $\Pi = (\text{Gen}, \text{Enc}, \text{Dec})$ has indistinguishable encryptions in the presence of an eavesdropper if for all probabilistic polynomial-time adversaries $A$ there exists a negligible function $\text{negl}$ such that

$$\Pr[\text{PrivK}^{\text{eav}}_{A,\Pi}(n) = 1] \leq \frac{1}{2} + \text{negl}(n).$$

where the probability is taken over the random coins used by $A$, as well as the random coins used in the experiment (for choosing the key, the random bit $b$, and any random coins used in the encryption process).
Two main issues:

• How to realize this definition?

• Is this the best definition addressing all issues? (No, it is still weak, but we will get back to this)
**Pseudo-randomness**
(random in eyes of computationally bounded)

\[ \underbrace{0 \mid 0 \mid 0 \mid 0 \mid 0 \mid 0 \mid 0 \mid 0 \mid 0 \mid 0} \text{ \( \times 100 \) times.} \]

\[ \frac{1}{2^{100}} \]

\( \text{Word 1} \)

\[ X = X_1 \mid \ldots \mid X_n \text{ \( \subseteq \) } 2^{100} \]

\( \text{truly randomly generated} \)

\[ Y = Y_1 \mid \ldots \mid Y_n \text{ \( \subseteq \) } 2^{100} \]

\( \text{more likely to be random.} \)

\( \text{generated \( \& \) differently.} \)
Pseudo-random generator (PRG)

• A magical tool that let us still do “one-time-pad” using short keys!
Formal definition of PRGs

For all poly-time adv A, there is a negligible function \( \varepsilon(n) \) such that

\[
P_0 \left[ \text{Win} \left[ \text{Adv} \right] \right] \leq \frac{1}{2} + \varepsilon(n)
\]

for all possible \( y \in \mathbb{U}_n \).
Using PRGs \( \rightarrow \) encrypting one long message

\[
\text{assume the existence of a PRG } g : x \rightarrow x, \ |x| = \frac{n}{2} \text{-bit}
\]

\[
\text{Goal:}
\]

Construct an ind. secure private-key encryption scheme \( (\text{Enc}, \text{Dec}, k(\cdot)) \)

Work on messages of length \( n \).

\[
\text{Thm: if } g \text{ is a secure PRG } \rightarrow B \text{ is a secure SKE.}
\]

\[
\begin{align*}
\text{Enc}(k, m) : g(k) \oplus m \quad &\text{Compared with } k \text{-bitwise} \\
\text{Dec}(k, s) : g(k) \oplus m \quad &\text{key } k \text{ at random} \\
\end{align*}
\]

\[
\text{Dec}(k, \text{Enc}(k, m)) = m
\]
Equivalent definition of PRG (applies to any ind. Security game – see PS1)

Guessing game

\[ b \sim \{0, 1\} \]
- if \( b = 0 \)
  - \( c \sim X_0 \)
- else
  - \( c \sim X_1 \)

\[ \Pr \left[ \text{Win} \right] \leq \frac{1 + \epsilon}{2} \]

\[ \Pr_{\text{World}_1} \left[ \text{ADV}(c) = 1 \right] - \Pr_{\text{World}_2} \left[ \text{ADV}(c) = 1 \right] \leq \epsilon \]
Proof of security for PRG \( \rightarrow \) ind-secure encryption

Assuming \( g : secure \) \( (t, \epsilon) \)-PRG

Goal: \( B = (\text{Enc}, \text{Dec}) \) is a secure Enc.

\( (\frac{1}{2}, 10\epsilon) \)-secure

World 0

Hybo

Hyb 1

World 1

\[ P_0 \{ \text{ADV} \rightarrow 1 \} = P_0 \]

\[ P_0' \]

\[ P_1' \]

\[ \Delta P_1 \{ \text{ADV} \rightarrow 1 \} = P_1 \]

View of ADV is the same!

\[ \text{Goal } P_1 - P_0 < \epsilon \]
Proof: Suppose this is **NOT** the case!

Suppose $A_1$ is poly time $t$ such that $P'_o - P_o > \varepsilon$

We construct Adversary $A_2$ that runs in poly time and breaks security of PRG by $\varepsilon$!

A$_2$ is given $y$, $y \oplus m_0 \rightarrow y'$ calls $A(y')$ and outputs $A(y')$. 

\[ \text{easy: } \Pr[A_2^{\text{output 1}} \text{ on } u_n] = P'_o \]
\[ \Pr[A_2^{\text{output 1}} \text{ on } g(u_n)] = P_o \]

\[ m_{0'} \rightarrow m_{0', A^D} \]
\[ m_{0'} \rightarrow m_{0', A^D} \]

\[ m_0 \oplus g(u_{n/2}) \]

\[ m_0 \oplus U_n \]

\[ P_o \{ \text{out} = 1 \} = P_o \]

\[ P'_o \{ \text{out} = 1 \} = P'_o \]

Claim: $P'_o - P_o < \varepsilon$