Assignment 1 is due on Tuesday! (2017-01-31) (Last day for help is tomorrow!!)
Recall: Perfect secrecy

- Ciphertext reveals absolutely nothing about plaintext, no matter how powerful the attacker: \( \forall m_0, m_1 \in M, \Pr[c \leftarrow Enc_k(m_0) \mid k \leftarrow \text{Gen}(1^n)] = \Pr[c \leftarrow Enc_k(m_1) \mid k \leftarrow \text{Gen}(1^n)] \)

- Shannon’s “Bad News” Lemma: perfect secrecy \( \Rightarrow |m| \leq |k| \)

- “Bad News” Corollary: can only encrypt one plaintext per key

Idea: Let’s make a compromise: insist only that \( Enc_k(m) \) reveals “practically nothing” to any “conceivable-yet-realistic attacker”
Defining “realistic attackers”

- **Idea 1**: Attacker can run fastest known algorithm on **1,000 Amazon EC2 instances** for **100 years**
  - Some IU student's PhD thesis contains a faster algorithm

- **Idea 2**: Attacker can **invest 10 million USD** on hardware
  - Attacker invests **1 billion USD**
  - Intel releases a newer, faster CPU

- **Idea 3**: Attacker controls a botnet with **1 million PCs**
  - Botnet grows to **10 million PCs and 100 million IoT devices**
Defining “realistic attackers”

The “right” idea: Attacker embodied by an efficient algorithm; succeeds with insignificant probability negligible

Defⁿ (concrete security): An encryption scheme (Gen, Enc, Dec) is (t, ε)-secure if, for every probabilistic algorithm A that runs in time t,

\[ |\Pr[A(Enc_k(m_0)) = 1] - \Pr[A(Enc_k(m_1)) = 1]| \leq \varepsilon. \]

A must be the “best possible” algorithm!
Efficient attackers

• An “attacker” is called efficient if its strategy is described by a PPT algorithm

Q: Why equate “efficient” with “PPT”?

A: Experience tells us “doable in polynomial time” ≈ “eventually doable in practice”

Also, nice closure properties: \( f, g \in \text{poly}(n) \) implies

\[ f(n) + g(n) \in \text{poly}(n) \]
\[ f(n) \times g(n) \in \text{poly}(n) \]
\[ f(g(n)) \in \text{poly}(n) \]
\[ \forall c > \mathbb{R}, f(n)^c \in \text{poly}(n) \]
Security parameters

- Goal: work around requirement to consider the “best possible” algorithm
  - Need to consider an infinite sequence of encryption schemes, indexed by a security parameter

**Defn**: An encryption scheme is a triple of PPT algorithms \((\text{Gen}, \text{Enc}, \text{Dec})\), where

- \(\text{Gen}: \mathbb{1}^n \rightarrow K\) is a (randomized) key generation algorithm
- \(\text{Enc}: K \times M \rightarrow C\) is a (randomized) encryption algorithm
- \(\text{Dec}: K \times C \rightarrow M\) is a (deterministic) decryption algorithm

security parameter
Stream ciphers

Idea: Replace truly random one-time pad with a "pseudorandom" one-time pad!

Consider efficient (and deterministic) function $G: \{0,1\}^n \rightarrow \{0,1\}^{\ell(n)}$

- Plaintexts and ciphertexts $\ell(n)$-bits long; keys just $n$-bits long
  - $\text{Gen}(1^n)$ outputs a uniform random pad $k \in \{0,1\}^{\ell(n)}$
  - $\text{Enc}_k(m)$ exclusive-ORs the message and $G(k)$; that is, $c := m \oplus G(k)$
  - $\text{Dec}_k(c)$ exclusive-ORs the ciphertext and $G(k)$; that is, $m := c \oplus G(k)$

$G(k)$ is called a key stream
Stream ciphers

- The function $G: \{0,1\}^n \rightarrow \{0,1\}^{\ell(n)}$ “stretches” the $n$-bit seed/key into an $\ell(n)$-bit stream/pad.
Indistinguishability against eavesdroppers

Onetime indistinguishability game

\[ \text{Adv}_{\text{onetime}}(A) := \left| \Pr[b = b'] - \frac{1}{2} \right| \]
Indistinguishability against eavesdroppers

**Defn**: An encryption scheme \((\text{Gen, Enc, Dec})\) has indistinguishable encryptions in the presence of an eavesdropper if, for every PPT algorithm \(\mathcal{A}\), there exists a negligible function \(\epsilon: \mathbb{N} \to \mathbb{R}^+\) such that

\[
\text{Adv}_{\text{onetime}}(\mathcal{A}) \leq \epsilon(n)
\]
That’s all for today, folks!