Lecture 2

Encryption
- Correctness
- Security [Shannon]
- OTP
- Impossibility
- Towards relaxing the definition

A cryptosystem consists of three algorithms:
1. Key generation alg. \( G() \rightarrow \text{key } s \)
2. Encryption \( E(m,s) \rightarrow \text{ciphertext } c \)
3. Decryption \( D(c,s) \rightarrow \text{message } m \)

**Correctness:** \( \forall m \in M, \forall s \in G(), D(E(m,s), s) = m \)

**Security:** \( E(m_0) \neq E(m_1) \neq m_0, m_1 \)

Ciphertext does not convey any info (to Eve) about plaintext.

Shannon: \( \forall m \in M, \forall c \quad Pr_M[m] = Pr_{M,G,E}[m|c] \)

Experiment LHS: \( Pr_M[m] = Pr_{M'}[m' \in M: m'=m] \)

Experiment RHS: \( Pr_{M'}[m' \in M; s \in G; c = Enc(m',s): m'=m \land c=c'] \) they denote the same thing

One-time pad cryptosystem (aka Vernam Cipher) for message space \( M = \mathbb{Z}_2^n \)

- \( G(n) \) output \( S \in \{0,1\}^n \)
- \( E(m,s) = m \oplus S \)
- \( D(c,s) = c \oplus S \)

**Correctness:** \( D(E(m,s), s) = D(m \oplus S, s) = (m \oplus s \oplus s) = m \)

**Security:** \( Pr[m] = Pr[m \oplus c] \)

\[ Pr[m \oplus c] = Pr[M \oplus c] \quad \mid \quad Pr[M \oplus c] = Pr[M] Pr[c] \]

\[ Pr[c|m] = Pr[S = c \oplus m | m] = 2^{-n} \]
\[ \Pr[c] = \sum_{m \in M} \Pr[m \land c|m] = \sum_{m \in M} \Pr[m] \Pr[c|m] = 2^{-n} \sum_{m \in M} \Pr[m] = 2^{-n} \]

So, \[ \Pr[m|c] = \frac{\Pr[m \land c]}{\Pr[c]} = \frac{\Pr[m]}{2^{-n}} \]

**Theorem 1**
Let \((G, E, D)\) be a correct cryptosystem for \(M\).
Let \(S\) denote the space of all possible keys.
If \(|M| > |S|\), then \(\exists m, c\) s.t. \(\Pr[m] \neq \Pr[m|c]\)

**Proof**
Let \(c\) be given. Let \(M(c) = \{m : \exists s \in S\) s.t. \(D(cs) = m\}\)
Claim: \(|M(c)| \leq |S| < |M|\)
Let \(m \in M(c)\). Then \(\Pr[M|m] > 0\), but \(\Pr[m|c] = 0\)

**Theorem 2**
Let \((G, E, D)\) be a correct public-key cryptosystem for \(\{0, 1\}^n\).
Then it is not Shannon-secure.
\((G\) outputs \((pk, sk)\), \(E(m, pk)\) outputs \(c\), \(D(c, sk)\) outputs \(m)\)
\((s.t.\ \#(pk, sk) \in G, D(E(m, pk), sk) = m)\)

**Proof**
Given \(PK, C\):
Run \(G\) repeatedly with all possible random inputs, until it outputs \((PK', SK')\) s.t. 
enumerate \(all\) \(SK\), find one that corresponds to \(PK\)
\(PK' = PK\).

Consider \(\Pr[m] < 1\)
But \(\Pr[m|PK, C] = 1\)

Towards relaxing Shannon's definition:
Whatever Eve learns about \(m\) given \(c\), she already knew based on \(M\).
\(\text{computationally bounded}\)

\(PRG: \{0, 1\}^n \rightarrow \{0, 1\}^{2n}\)
Indist. from random string of length \(n\):
\[ R \approx PRG(r) \]
random string of length \(2n\)
random string of length \(n\)
Formalize that: $R \approx PRO(r)$ or $E(0) \approx E(1)$

- Distinguishers $\mathcal{D}$, they cannot win in this game; with prob. $\frac{1}{2} + \text{negligible}(k)$

1) Challenger picks challenge type (i.e., $R$ or $PRO$), sample $S$ from the corresponding distribution

2) $\mathcal{D}(S)$ tries to determine challenge type, wins if correct

$\Rightarrow$ **Security Parameter** $k$: good guys are small $\text{poly}(k)$

bad guys are large $\text{poly}(k)$, still cannot win

$\Rightarrow$ A function $\mathcal{A}: \mathbb{N} \rightarrow [0,1]$ is negligible if for all $k_0$, exists $k > k_0$, $\mathcal{A}(k) < \frac{1}{k^n}$