# Lecture 03 (More on Definitions and Observations)

- $x \leftarrow S \implies x$ is uniformly chosen from $S$
- $|C| \geq |M|$ since inverse (partial) function exists
- $K$ is sampled uniformly

## 1 Relation Between $|K|$ and $|M|$

1. To ensure that the definition of perfect indistinguishability holds, $|\{k_i | enc(m, k_i) = c\}|$ should be independent of $m$ for each $c$
2. Therefore, we should have at least cardinality of the above set times the number of keys as the message space
3. In general, we can say that $|K| \geq |M|$
4. This is terrible news :(

## 2 Shannon's OTP's Limitations

1. Each key can only be used only once
2. Russians used OTP for encryption and this was cracked
3. Malleability attacks (why is sir good at remembering names?)
   - can find out $\tilde{m}$

## 3 Practical Encryption Schemes - $|K| < |M|$

1. Use a deterministic function such that if input is random, then output "looks" random
2. Allow for $\epsilon$ error in probability

Above two won't work. Instead, we try to provide security against polynomial time adversaries.

### 3.1 Security Game

Given two messages $m_0, m_1$ by adversary, challenger picks a random bit $b$ and a random key $k$. Challenger gives $enc(m_b, k)$ and the adversary has to identify $b$ 'efficiently' (polynomial time) correctly with probability $\leq \frac{1}{2}$ (only equality will hold otherwise, we can have an adversary which can guess the opposite of an adversary that has $< 1/2$ leading to contradiction).

# 4 Questions

1. Relation Between $|K|$ and $|C|$ (my thoughts: can't say anything)
2. Come up with a definition for two time security