Recap: 2PC: Alice has x, Bob has y
Want to learn f(x,y) & nothing more

Intuitive idea of security:
"it is impossible to gain unauthorized information"

impossible to realize
Settle for something weaker
"it is INFEASIBLE to gain unauthorized information"

In CS: feasible = can be solved in poly time
efficient = algo. that runs in poly time

"impossible to realize, too!"
Dumb adversary: guesses secret key

"it is INFEASIBLE to gain unauthorized information, except w/ very small probability"

How small is small enough?
Adversary guesses at n-bit key ⇒ succeed w/p $\frac{1}{2^n}$
Adversary that makes 2 guesses ⇒ $2\frac{1}{2^n}$
$n^y$ guesses ⇒ $n^{y\frac{1}{2^n}}$
**Def:** \( f : \mathbb{N} \to \mathbb{R} \) is negligible if for all polynomials \( p(n) \),
\[
\lim_{n \to \infty} p(n) f(n) \to 0
\]

**Idea:** Attack runs in poly time, succeeds w/p \( f(n) \)
repeat attack \( p(n) \), might succeed w/p \( p(n) \cdot f(n) \)

**Alt Def:** \( f \) is negligible if for all polynomials \( p \)
\[
f(n) < \frac{1}{p(n)} \quad \text{for sufficiently large } n
\]

**Note:** Asymptotic property!

How do we say "Adversary doesn't gain unauthorized info"?

Example of secret-key encryption

\[
\text{KeyGen}(n) : \text{sample an } n\text{-bit key}
\]

\[
\begin{align*}
\text{Enc}(k, m) & \to c \\
\text{Dec}(k, c) & \to m
\end{align*}
\]

"Seeing c leaks no info about m"

Adversary sees a sample from some distribution

\[
\begin{align*}
k & \leftarrow \text{KeyGen}(n) \\
c & \leftarrow \text{Enc}(k, m) \\
\text{output } c
\end{align*}
\]

Call the output distribution of this process \( \mathcal{D}_n \).
for each \( m \), \( P^m_n \) is a prob. distribution different values of \( m \) induce diff \( P^m_n \) (assign diff probabilities to some ciphertexts) 

What if differences in these distributions are "hard to notice" in poly time?

**Def:** \( P^m_n \) & \( P^{m'}_n \) are (computationally) indistinguishable if, for all poly-time \( A \):

\[
\left| \Pr \left[ x \leftarrow P^m_n : A(x) = 1 \right] - \Pr \left[ x \leftarrow P^{m'}_n : A(x) = 1 \right] \right| \text{ is negligible in } n.
\]

**Security of Enc:**

for all \( m, m' \), \( P^m_n \) & \( P^{m'}_n \) are indisting...

(no poly time \( A \) can tell difference between enforcements of \( m \) vs \( m' \))

**Note:** only applicable when someone sees \( c \) but not \( k \) only considers seeing 1 \( m \) encrypted under \( k \)

**Real Def:** make the security definition into an interactive game