ENCRYPTION

\[ H \to Alice \xrightarrow{\text{SECRET KEY } k} Bob \xrightarrow{\text{RECOVER } M} \]

\[ \text{hello} \to \text{khoor} \]

DETERMINISTIC

Eve CAN DO EVERYTHING Bob CAN DO.

- ADD RANDOMNESS

\[ + t \mod 26 \quad \text{WHERE } t \text{ IS A RANDOM NUMBER} \]

\[ \text{hello} \to \text{o} \]

- INCREASE RANDOMNESS

1. PERMUTATE LETTERS RANDOMLY

Alice \to Bob

buy, sell, sell, buy, buy

tpa \quad tpa \quad tpa

FOR Eve TO ATTACK SHE HAS TO DO 26x AMOUNT OF WORK.
Random shift by block

hello world
+ tuphtuphtu...

1. Randomness is needed ← secret key
2. Not enough

Can we "hide" the message even if Eve has partial info?

\[ M \in \mathcal{G}_{90,13}^m \quad \kappa = 90,13^l \text{ random} \]

Assume \( u = \kappa \):

\[ C = M + \kappa \mod 2 \]

\[ \kappa = (M_1 + \kappa_1, \ldots, M_l + \kappa_l). \]

\[ C \rightarrow [\text{Bob}] \rightarrow C + \kappa = M. \]

\[ M + \kappa = C \]

\[ \text{Fixed Random Random} \]

\((\text{Enc}, \text{Dec})\) is perfectly ind-secure if \( \forall M, M' \)
\(\text{Enc}(\kappa, M)\) and \(\text{Enc}(\kappa, M')\) are identically distributed.
**SIM-SECURE**: Eve can sample $C$ without knowing $M$. $✓$ **UNIFORMLY RANDOM**.

**ISSUE?** $k=m$ | **UNREALISTIC IF $m$ IS LARGE**

**IS $k \leq m$ POSSIBLE? NO.**

1. $M \rightarrow C = \text{Enc}(k, M)$
2. $Eve$
3. $M' \rightarrow C' = \text{Enc}(k, M')$

**$M', M_1$ DISTINGUISHABLE** $\leftarrow$ **THERE EXISTS SOME OTHER** $M' \rightarrow X$ | **NO KEY**

**RELAXATION 1.** $\text{Enc}(k, M)$ and $\text{Enc}(k, M')$ not i.d. but merely "close".

$x, x'$ are $\varepsilon$-statistically close if for any possible test $D$ that outputs yes or no

$$|\Pr[D(x) = \text{yes}] - \Pr[D(x') = \text{yes}]| \leq \varepsilon$$

$\varepsilon = 0 \rightarrow$ **PERFECTLY INDISTINGUISHABLE**

$\varepsilon = 1 \rightarrow$ 99% of the time cannot tell apart.
Even ε = \( \frac{1}{2} \) impossible as long as 
\( k < m \). X but may be computationally expensive to do so.

**Ideal:** Perfect security

**Relaxed:** Statistical computational

**Cryptographic**

\[
\begin{align*}
k &= m - 1 & \varepsilon &= \frac{1}{2} \\
\ell &= m - 2 & \varepsilon &= \frac{3}{4}
\end{align*}
\]

\( k \ll m \rightarrow \varepsilon = 1 - 2^{-4n} \)

---

**Circuits:** Model of efficient computation

Circuit = directed acyclic graph

Sources: Inputs
Sinks: Outputs
Internal nodes: AND, OR, NOT gates

\[ f(x_1, x_2) = x_1 \text{ XOR } x_2 \]

Size = number of AND/or gates

Size = 3
Ex. Share(s): SAMPLE $X_1, X_2, X_3 \mid X_1 + X_2 + X_3 = s$

- Size = $2 \cdot \text{Size}(\text{XOR})$
- Measure of Efficiency

**Programs vs. Circuits**

<table>
<thead>
<tr>
<th>Size</th>
<th>Runtime</th>
</tr>
</thead>
<tbody>
<tr>
<td>$s$</td>
<td>$t$</td>
</tr>
<tr>
<td>$O(s)$</td>
<td>$O(s)$</td>
</tr>
</tbody>
</table>

- C that takes no real input, only randomness is a **sampler**
- C that takes no randomness is **deterministic**
X AND X' OVER SQRT(S) ARE (S, \varepsilon) - COMPUTATIONALLY INDISTINGUISHABLE IF FOR EVERY CIRCUIT
D: SQRT(S) \rightarrow 0, 1 \text{ OF SIZE AT MOST } S,
\left| \Pr[D(X) = 1] - \Pr[D(X') = 1] \right| \leq \varepsilon.

E - STAT \leftrightarrow (\infty, \varepsilon) - COMP \leftrightarrow (2^k, \varepsilon) - COMP

A CUT OF SIZE 2^k CAN COMPUTE ANY FUNCTION ON 2^k BITS.

S \leq 2^{k/2} \rightarrow \text{ THERE EXIST FUNCTIONS THAT CANNOT BE COMPUTED BY CUTS OF SIZE } S.

(Enc, Dec) IS (S, \varepsilon) - MESSAGE INDISTINGUISHABLE IF \forall M, M', Enc(M, M') AND Enc(M, M') ARE (S, \varepsilon) - COMPUTATIONALLY IND.
WHAT ARE REASONABLE VALUES FOR $S$ AND $\varepsilon$?

$k$ = "SECURITY PARAMETER"

THEORY: Alice, Bob run in time polynomial in $k$ make Eve do "work" exponential in $k$.

Ex. $S = 2^{k/3}$ or $2^{\varepsilon k}$.

$S =$ AMOUNT OF WORK

$\varepsilon =$ LUCK $\in [0, 1]^k$

Eve can always randomly guess $k$.

Ggets lucky with prob $2^{-k}$.

Want $\varepsilon$ not much larger than this

Ex. $\varepsilon = 2^{-k/3}$ or $2^{-\varepsilon k}$.

RULE OF THUMB $\varepsilon \approx \frac{1}{S}$ can convert luck into work

Eve breaks $I$ Enc w/ $\varepsilon$

$t$ Enc w/ $P I - (1 - \varepsilon)^t \approx t \varepsilon$

PRACTICE $\varepsilon \approx \frac{1}{280}$, $S \approx 2^{80}$
SIMULATION-BASED DEFINITION

(Enc, Dec) is \((s, \varepsilon)\)-SIMULATABLE IN SIZE \(t\) IF THERE EXISTS A SAMPLER \(\text{Sim}\) OF SIZE \(\ell + s\) T. \(\forall M,\) OUTPUT OF \(\text{Sim}\) IS \((s, \varepsilon)\)-INDISTINGUISHABLE FROM \(\text{Enc}(k, M)\).

\[
\begin{align*}
\text{IND} & \quad \quad \text{SIM} \\
\left| \Pr\left[ \text{D(Enc}(k, M)) = 1 \right] - \Pr\left[ \text{D(Enc}(k, M') = 1 \right] \right| & \leq \varepsilon \\
\left| \Pr\left[ \text{D(Sim)} = 1 \right] - \Pr\left[ \text{D(Enc}(k, M)) = 1 \right] \right| & \leq \varepsilon \\
\forall D \text{ OF SIZE } \leq s
\end{align*}
\]

\((s, \frac{\varepsilon}{2})\)-NON-SIMILARITY \(\rightarrow\) \((s, \varepsilon)\)-INDISTINGUISHABILITY

\(\text{CONTRAPOSITIVE}\) COMES FROM PROOF

Proof IN CONTRAPOSITIVE

SUPPOSE Eve CAN \(\varepsilon\)-DISTINGUISH ENCRYPTIONS

\[
\Pr\left[ \text{D(Enc}(k, M)) = 1 \right] - \Pr\left[ \text{D(Enc}(k, M') = 1 \right] > \varepsilon.
\]

FOR SOME PAIR \(M\) AND \(M'\).

EITHER

\[
\Pr\left[ \text{D(Enc}(k, M)) = 1 \right] - \Pr\left[ \text{D(Sim)} = 1 \right] > \frac{\varepsilon}{2}
\]

OR

\[
\Pr\left[ \text{D(Sim)} = 1 \right] - \Pr\left[ \text{D(Enc}(k, M')) \right] > \frac{\varepsilon}{2}.
\]
\[ \text{Sim is dist from either } \text{Enc}(K,M) \text{ or } \text{Enc}(K,M') \text{ by sizes } S \text{ and adv. } \epsilon/2. \]

**Even if** \( \text{size}(\text{Sim}) = \infty \)

\((S,\epsilon)\) - INDIST'LIY \(\rightarrow\) \((S,\epsilon)\) - SIM'LIY

Sim outputs \( \text{Enc}(K, M_0) \) for some fixed \( M_0 \) (e.g. \( M_0 = \text{all zeros} \)) and random \( K \).

\( \text{size}(\text{Sim}) = \text{size}(\text{Enc}(\cdot, M_0)) \)

**Pseudorandom Generators**

\**OTP:**  \( \text{Enc}(Y, M) = M + Y \)  \( \text{Dec}(Y, C) = C + Y \)

\( \text{G} \)

\( K \) (\( k \) bits)

\( Y \) (\( m > k \) bits)

\( \text{G} \) is an \((S,\epsilon)\) - PSEUDORANDOM GENERATOR \n
If \( \text{G}(K) \) (\( K \) random) is \((S,\epsilon)\) - C.I.

From a uniform \( m \)-bit string \( Y \) for \( m > k \).
WHERE DO WE GET A PRG?
DO THEY EVEN EXIST? NOT SURE.

$p \neq \text{NP}$

$m = k + 1 : 2^k \text{ keys} \rightarrow 2^{k+1} \text{ outputs}$

$\Pr [\exists k \text{ s.t. } G(k) = Y] \leq \frac{1}{2}$

IF CAN ANSWER EFFICIENTLY
→ CAN DISTINGUISH $G(k)$ FROM $Y$

ONE-WAY FUNCTION

EASY

THEOREM CAN BUILD

A PRG FROM ANY OWF.

CANDIDATE EXAMPLES OF PRG IN LECTURE 4

LARGER $m$ SHOULD BE HARDER TO GET... ACTUALLY $m = k + 1$
WILL BE ENOUGH.
\((s, \varepsilon)\)-PRG \(\rightarrow (s, \varepsilon)\)-SIM ENCRYPTION

\[
\text{Enc}(k, M) = G(k) + M \\
\text{Dec}(k, C) = G(k) + C
\]

\text{Sim: OUTPUT UNIFORMLY RANDOM Y.}

\text{PROOF BY CONTRAPOSITIVE: SUPPOSE \exists D OF SIZES}

\[
\left| \Pr[D(G(k) + M) = 1] - \Pr[D(Y) = 1] \right| \geq \varepsilon
\]

\text{LET } D'(x) = D(x + M)

\[
\Pr[D'(G(k)) = 1] = \Pr[D(G(k) + M) = 1] \\
\Pr[D'(Y) = 1] = \Pr[D(Y + M) = 1] = \Pr[D(Y) = 1]
\]

\text{size}(D') = \text{size}(D) = s. \quad (M \text{ IS FIXED, ONLY ADDS SOME NOT GATES TO D})

\[
G : 90,13^s \rightarrow 50,13^m \\
\text{EX: } k = 500, \ m = 2000
\]

\text{STRETCH OF } G = m - k
Theorem. If $G$ is an $(s, \varepsilon)$-PRG of stretch $m - \ell$, then $G'$ is a $(s', \varepsilon')$-PRG of stretch $2(m - \ell)$.

<table>
<thead>
<tr>
<th>A</th>
<th>B</th>
<th>C</th>
</tr>
</thead>
<tbody>
<tr>
<td>$X_L$, $G(X_L)$</td>
<td>$Z$, $G(Z)$</td>
<td>$Y_L$, $Y_R$</td>
</tr>
</tbody>
</table>

$\frac{Y_L}{m - \ell}$, $\frac{Y_R}{m}$

HYBRID

TRULY RANDOM

$(X_L, G(X_L))$ is c.i. from $(Y_L, Y_R)$.

Proof. Suppose

$\left| \Pr[\text{D}(X_L, G(X_L)) = 1] - \Pr[\text{D}(X_L, X_L) = 1] \right| > \varepsilon'$

for some D of size $s'$. Then

$\Pr[\text{D}(A) = 1] - \Pr[\text{D}(B) = 1] > \frac{\varepsilon'}{2}$ or $\Pr[\text{D}(B) = 1] - \Pr[\text{D}(C) = 1] > \frac{\varepsilon'}{2}$

CASE 2: $D'(y) = D(Y_L, y)$ distinguishes $G(Z)$ from $Y_R$ for random $Y_L \rightarrow G$ is not $(s', \varepsilon'/2)$-P'random

CASE 1: Next time
\[
|P[D(A) = 1] - P[D(B) = 1]| \geq \frac{\varepsilon'}{2}
\]

\[\text{size } s' + t \quad \text{size } s' \quad \text{size } t\]

Let \(D'(x) = \begin{cases} D(x_1 \ldots x_{m-k}, G(x_{m-k+1} \ldots x_m)) & \text{if } m-k \text{ is odd} \\
D(A) & \text{if } m-k \text{ is even}
\end{cases}\)

\[D'(G(k)) = D(A) \quad D'(R) = D(B)\]

\[
|P[D'(G(k)) = 1] - P[D'(R) = 1]| \geq \frac{\varepsilon'}{2}
\]

So \(G\) is not \((s' + t, \varepsilon/2)\)-PRANDOM in either (1) or (2), \(G\) is not \((s' + t, \varepsilon/2)\)-PRANDOM.

Set \(s' = s - t, \ \varepsilon' = 2\varepsilon\).