alternate view of

\[ \text{Let } M_0, M_1 \in M \]

perfect security \(\equiv\) Dist \[ E_k[M_0] \]

\[ E_k[M_i] \]

are the same for \( k \leftarrow^k \mathcal{K} \)

and any two \( M_0, M_1 \),

Any perfectly secure symmetric encryption requires \(|M| \leq |K|\)

Proof: Fix any \( M \). There are at most \(|K|\) different

encryptions of \( E_k(M) \) possible of different choices of \( k \) in

script \( k \)
By equivalent def. above

\[ S = \bigcup_{k \in K^3} E_k(M_0) \cap K^3 = \bigcup_{k \in K^3} E_k(M_i) | k \in K^3 \]

Set of possible ciphertexts

\[ \therefore \text{ only } |K| \text{ ciphertexts possible} \]

Unique decoding requires at least \( |M| \) possible ciphertexts
MAC security

\[ M \quad \text{message space} \]

\[ \mathcal{Z} \quad \text{tag space} \]

\[ K \quad \text{key space} \]

Desirable properties

\[ \forall M, t \quad \Pr_K [ T_K (M) = t ] \text{ is small} \]

ideally \[ \frac{1}{|\mathcal{Z}|} \]

tags uniformly distributed

Tag generation function

\[ T_K (M) \quad T : M \times K \rightarrow \mathcal{Z} \]

\[ \forall A : \mathcal{M} \times \mathcal{Z} \rightarrow \mathcal{M} \times \mathcal{Z} \quad \text{adversary function} \]

receiver check

\[ T_K (m') = t' \quad \Pr_K [ A (M, T_K (M)) = (m', t') \text{ such that} ] \]

\[ M' \neq M \text{ and } T_K (M') = t' \text{ is small} \quad \text{ideally} \quad \frac{1}{|\mathcal{Z}|} \]
Easily achievable:

Pairwise independent (Universal Hash Functions) Families

ex. \( h_{a,b}(m) = am + b \mod p \) where \( p \) is prime

\[ M = \mathbb{Z}_p = \mathbb{Z} \]

\[ K = \mathbb{Z}_p \times \mathbb{Z}_p \]

\[ M = \mathbb{Z}_{13}^n, \quad K = \mathbb{Z}_{13}^n \times \mathbb{Z}_{13}^n \]

\[ k = \{ \mathbb{Z}_{13} \times \mathbb{Z}_{13} \mid a, b \in \mathbb{Z}_{13}^{n+1} \} \]

\[ h_{a,b}(m) = \text{middle } k \text{ bits of } am + b \]

\[
\begin{array}{c}
\begin{array}{c}
\text{h+1}
\end{array}
\end{array} + \begin{array}{c}
\begin{array}{c}
a \hspace{2cm} m
\end{array}
\end{array} = \begin{array}{c}
\begin{array}{c}
h \hspace{2cm} \mathbb{Z}_{13}^n \hspace{2cm} l \hspace{2cm} n \hspace{2cm} b
\end{array}
\end{array} + \begin{array}{c}
\begin{array}{c}
h(a,b)
\end{array}
\end{array} \]
\[ am + b = t \quad \text{and} \quad m \neq m' \]

\[ a m' + b = t' \]

\[
\begin{bmatrix} m & 1 \\ m' & 1 \end{bmatrix} \begin{bmatrix} a \\ b \end{bmatrix} = \begin{bmatrix} t \\ t' \end{bmatrix}
\]

\[
\Pr_{a,b} \left[ h_{a,b}(m) = t \right] = \frac{1}{p}, \quad \Pr_{a,b} \left[ h_{a,b}(m) = t, h_{a,b}(m') = t' \right] = \frac{1}{p^2}
\]

For \( m \neq m' \) \[
\begin{bmatrix} m & 1 \\ m' & 1 \end{bmatrix}
\]

is invertible

\[ \Rightarrow \text{exactly one choice of } a, b \text{ that works} \]

\[
\Pr_{a,b} \left[ h_{a,b}(m') = t' \mid h_{a,b}(m) = t \right] = \frac{1}{p}
\]

For \( m' = m \)
Cryptanalysis cycle
Keep trying to improve cryptosystems based on attack methods
"Provable security under specific assumptions"
Reducions between primitives

One-way functions
Pseudorandom functions
f is easy
but f^{-1} is hard

Symmetric encryption
ex. \( f(a, b) = a \times b \) multiplication

f^{-1} factoring

Trapdoor functions
look hard, but with a short secret, you get an easy path.
Security:

assumptions: parties are probabilistic

polyomial time

definition: A function $V: \mathbb{N} \rightarrow \mathbb{R}^+ \geq 0$

is negligible iff

$V(n)$ is $\frac{1}{n^c}$

$V(n)$ goes to 0 faster than any polynomial function of $n$

eventually $V(n) \leq \frac{1}{n^c}$ for any $c$
**Defn:** A sequence of probability distributions

\[ D = \{ D_n \}_{n \in \mathbb{N}} \] where \( D_n \) is a distribution on \( [0,1]^n \) is called an ensemble.

**Defn:** Given two distributions \( D_N \) and \( \xi_N \) on \( [0,1]^n \), the statistical distance between \( D_N \) and \( \xi_N \) is defined as

\[
\text{dist}(D_N, \xi_N) = \frac{1}{2} \sum_{x \in [0,1]^n} |\Pr_{D_N}[x] - \Pr_{\xi_N}[x]| \]

\[
= \max_{S \subseteq [0,1]^n} \left( \Pr_{D_N}(S) - \Pr_{\xi_N}(S) \right)
\]
Defn: Two ensembles are statistically indistinguishable iff there is a negligible function such that

\[ \forall n, \quad \text{dist}(\mathcal{D}_N, \mathcal{E}_N) \leq \varepsilon(n) \]

\[ \varepsilon(n) = \frac{1}{2^{\frac{n}{3}}} \]
Security parameter $k$

Key distribution algorithm gets $1^k$

$E_k(M, 1^k)$

$D_k(C, 1^k)$

Key Generation ($1^k$) produces $K$

Previously,

$E_k(m_0)$ and $E_k(m_1)$ have identical distributions

Slightly weaker:

$E_k(m_0)$ and $E_k(m_1)$ are statistically close

Statistical distance $E(k)$ where $E$ is negligible

Similar problems to Shannon's lower bound.
Defn: Two ensembles $D$ and $E$ are computationally indistinguishable iff for all probabilistic polynomial time algorithms $A$

$$\varepsilon(n) = \left| \Pr_{x \in D} \left[ A(x) = 1 \right] - \Pr_{x \in E} \left[ A(x) = 1 \right] \right|$$

is a negligible function of $n$. \[ [Yao]\]

For example, compare $D$ to $U$

$D$ looks random when negligible distance from $D$ to $U$ in polynomial time.
Next time → systems people use in practice

block ciphers

stream ciphers